Cyberint

Continuous Intelligence-led Cybersecurity Tests

Solution Brief

Banking Regulation Ready

Global Banking Regulations Require Next-Generation Cybersecurity Testing

Supervisory authorities say traditional Penetration Testing falls short of providing adequate indication of the bank's resilience to emerging Cyber Threats:

Hong-Kong Monetary Authority (HKMA) -- Cyber Resilience Assessment Framework (2016)

HKMA defines requirements for Intelligence-led Cyber Attack Simulation Testing (iCAST) designed to replicate current real life cyber attacks based on specific and up-to-date threat intelligence.

Swiss Financial Market Supervisory Authority (FINMA) -- Operational Risks at Banks (REV 2016).

According to FINMA, financial institutions should perform regular cybersecurity tests on their resilience to the increasingly complex cyber-attack scenarios.

Bank of England -- CBEST Vulnerability Testing Framework (2016)

CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests.

CybeReadiness **Argos**

Continuous Intelligence-Led Cyber Security Testing

CyberInt observes your Cyber defense from the attackers' perspective -- so that your readiness always precedes your adversaries' attempts.

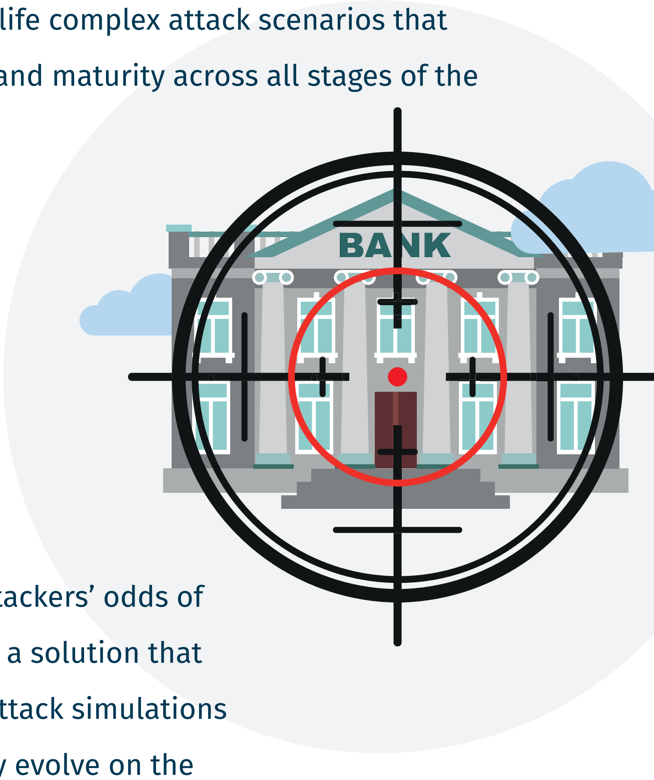
CyberInt's ‘Paul’ solution for financial institutions presents a unique combination of our Argos Threat Intelligence Platform and our CybeReadiness Suite. The solution provides a new approach towards intelligence-led cybersecurity testing: a vehicle for continuous assessment of an organization’s Cybersecurity posture and for comprehensive threat mitigation.

Our team of cyber experts work together with cutting-edge technologies to provide Automated Red Team activities.

We simulate attacks against your organization, effectively testing your organization's cybersecurity posture (People, Processes, and Technology) end-to-end, providing metrics and KPIs to measure your cybersecurity readiness.

Automate Cyber Attack Simulation to Take Control of your Defences

Our CybeReadiness suite is a uniquely developed set of modules which automate various types of attack scenarios against your business. These simulate real-life complex attack scenarios that collectively validate your organization's awareness, efficiency, and maturity across all stages of the attack 'Kill Chain'.



Intelligence-led Attack Simulation: What is it good for?

While penetration testing is essential for understanding the attackers' odds of penetrating a specific business asset, these tests don't provide a solution that caters to a changing threat landscape. Paul's intelligence-led attack simulations recreate attacks that precisely mimic real-life scenarios as they evolve on the threat landscape.

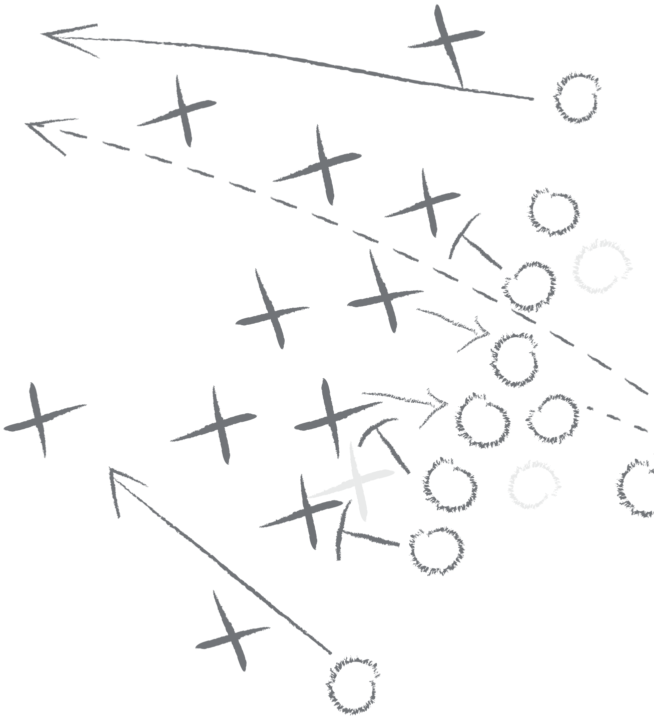
Intelligence-led Attack Simulation: How Do We Do It?

Discovering and Analyzing your Digital Footprint

As an initial step, our Discovery and Reconnaissance practices utilize your internal inputs to map your digital footprint and identify your crown jewels (i.e. Critical Services and Systems).

Argos™ Threat Intelligence platform correlates your intelligence profile with multiple sources it gathers on the Darknet, Deep Web, and Open Web -- and produces real-time, targeted intelligence of your business' unique vulnerability points and threat scenarios.
Our team of analysts then identify and analyze your real, personalized threat scenarios, which embody the risk elements that have the potential to materialize and endanger your business' security posture.

Building Test Scenarios and Running Attack Simulations



Our simulation frameworks are continuously updated according to emerging threats; APT (multiple types), Phishing, Spear Phishing, DLP testing, SIEM simulation, Social Engineering, Data Theft Attack, Account Takeover, DDoS Attack, among others.

Armed and defined with the intelligence insights, we help you build and define your resilience and testing plan against all potential attack scenarios.

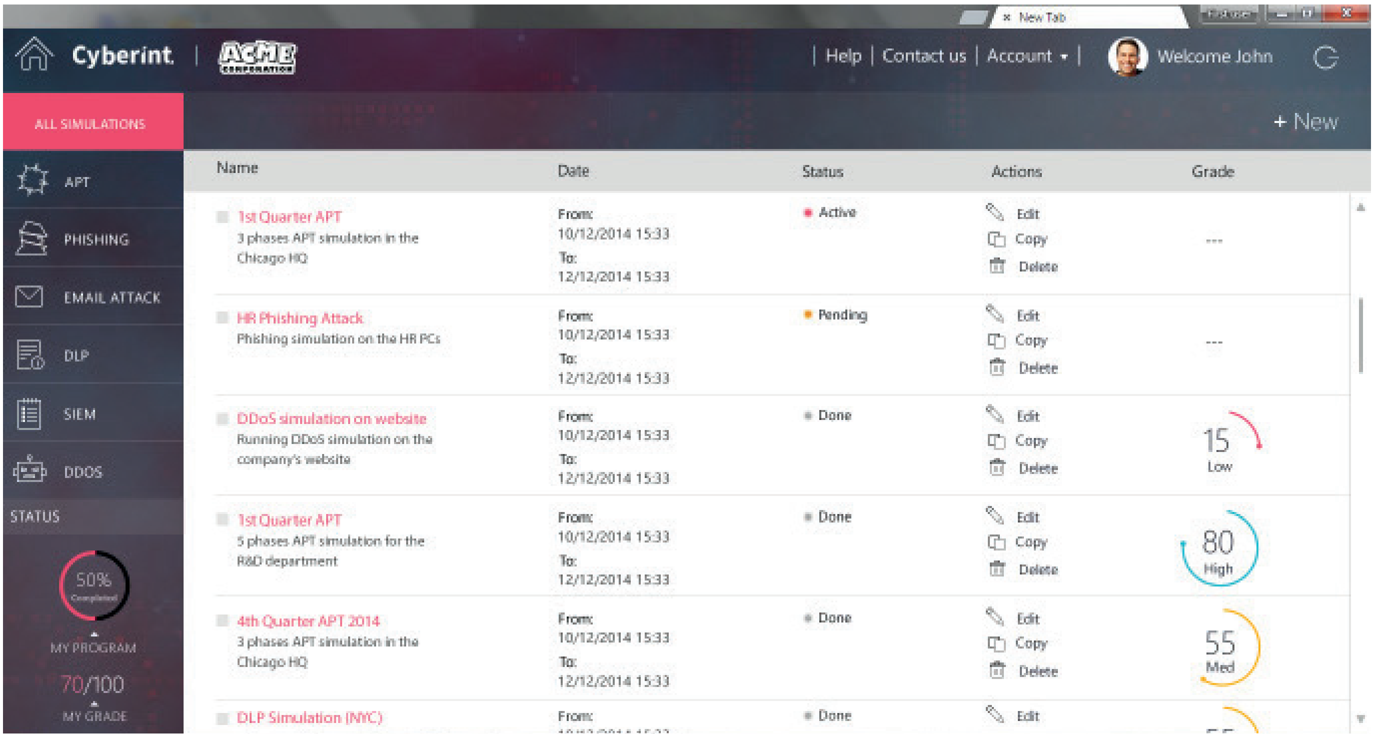
Our CyberReadiness™ Suite allows you to schedule the attack simulations according to your individual business needs and

Simulation Results

Based on the summative testing, we provide you with updated insights and continuous feedback on your cyber posture's progress and general stamina in an ongoing manner.

This includes:

- Testing your organization’s controls
- Employees’ awareness
- Internal process for detection, prevention and response, detailed KPIs.



Name	Date	Status	Actions	Grade
1st Quarter APT 3 phases APT simulation in the Chicago HQ	From: 10/12/2014 15:33 To: 12/12/2014 15:33	Active	Edit Copy Delete	---
HR Phishing Attack Phishing simulation on the HR PCs	From: 10/12/2014 15:33 To: 12/12/2014 15:33	Pending	Edit Copy Delete	---
DDoS simulation on website Running DDoS simulation on the company's website	From: 10/12/2014 15:33 To: 12/12/2014 15:33	Done	Edit Copy Delete	15 Low
1st Quarter APT 5 phases APT simulation for the R&D department	From: 10/12/2014 15:33 To: 12/12/2014 15:33	Done	Edit Copy Delete	80 High
4th Quarter APT 2014 3 phases APT simulation in the Chicago HQ	From: 10/12/2014 15:33 To: 12/12/2014 15:33	Done	Edit Copy Delete	55 Med
DLP Simulation (NYC)	From:	Done	Edit	

About CyberInt

By looking beyond the perimeter and providing constant vigilance of cyber activities, CyberInt eliminates potential threats before they become crises. Our expertise in cyber intelligence and protection of online activities defends companies of all sizes and industries. Our personalized services arm your company with the tools to protect itself from targeted threats.

We look at your business from an attacker’s perspective. We think like hackers and understand how they behave. Enabling a comprehensive understanding of what needs to be monitored and safeguarded, setting us up to provide safety beyond the perimeter.

Israel: Tel: +972-3-7286777 | Ha-Mefalsim 17 St | 4951447 | Kiriat Arie | Petah Tikva | Israel

United Kingdom: Tel: +44203514151525 | Old Broad Street | EC2N 1HN | London | United Kingdom

LATAM: Tel: +507 395-1588 | Edificio Mapfre | Costa del Este | Avenida La Rotonda | Panamá

APAC: Tel: +65-316-357-6010 | Anson Road | #33-04A | International Plaza | Singapore