I-CRT
Intelligence-led Cyber Resilience Testing

The Office of the Superintendent of Financial Institutions (OSFI) is now asking Canada's systemically important (SIBs) and internationally active insurance groups (IAIGs) to perform controlled assessments of their cyber resilience.

I-CRT is a supervisory tool that supplements Guideline B-13, allowing Federally Regulated Financial Institutions (FRFI's) to meet regulatory expectations to have measures in place that create resilience against cyber-attacks and disruptions. This ensures the stability and security of the financial sector in Canada.

OSFI has created the Intelligence-led Cyber Resilience Testing (I-CRT) framework, which aims to simulate relevant real-world threats to assess cyber resilience, using independent suppliers, to help SIBs and IAIGs identify areas where they could be vulnerable to sophisticated cyber-attacks.

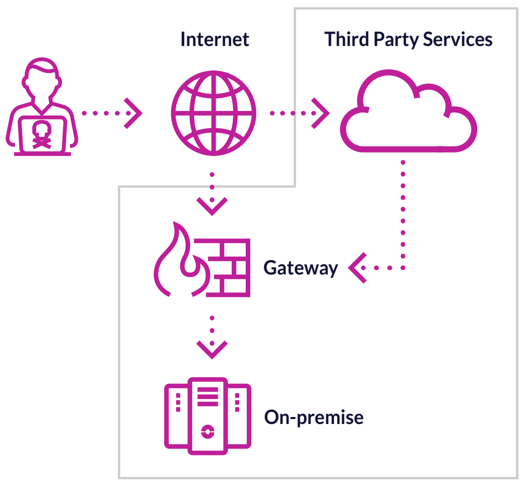
How does I-CRT differ from traditional testing?

In traditional penetration testing, the goal is to uncover vulnerabilities within a specific scope. I-CRT, on the other hand, requires an evaluation to obtain focused threat intelligence for the CBFs to create threat scenarios.

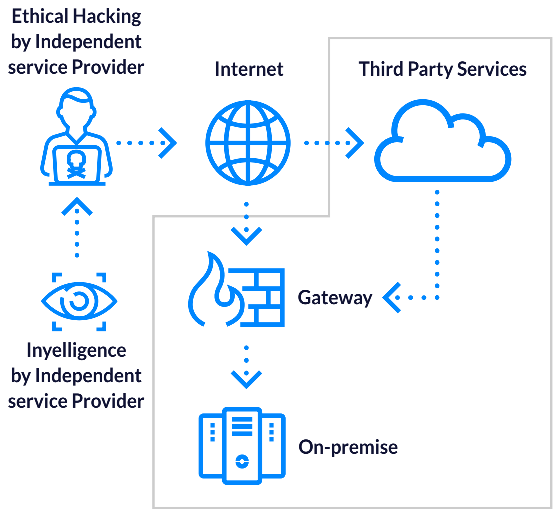
Red Teaming does not follow automated patterns and is not an emulation of a threat actor's TTPs. Instead, it is a bespoke and tailored simulation of threat actor's sophistication levels and capabilities, enabling the testing team to make decisions similar to the threat actor, based on new intelligence as the attack unfolds.

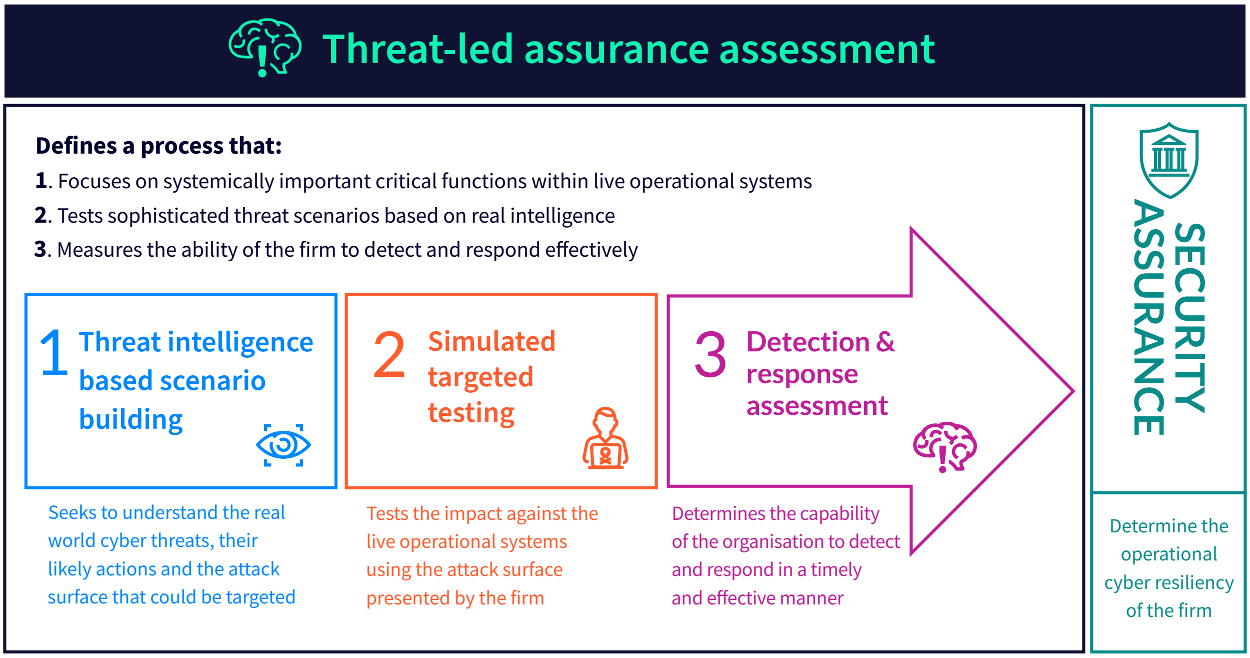
It is a practical approach to test and assess an FRFI's ability to detect and respond to a cyber-attack.

Traditional Penetration Testing & Red Teaming



Intelligence Led Cyber Resiliency Testing


Ethical Hacking by Independent service Provider
Internet
Third Party Services
Gateway
Inyelligence by Independent service Provider
On-premise



Threat-led assurance assessment

Defines a process that:

1. Focuses on systemically important critical functions within live operational systems

2. Tests sophisticated threat scenarios based on real intelligence

3. Measures the ability of the firm to detect and respond effectively

1 Threat intelligence based scenario building

Seeks to understand the real world cyber threats, their likely actions and the attack surface that could be targeted

2 Simulated targeted testing

Tests the impact against the live operational systems using the attack surface presented by the firm

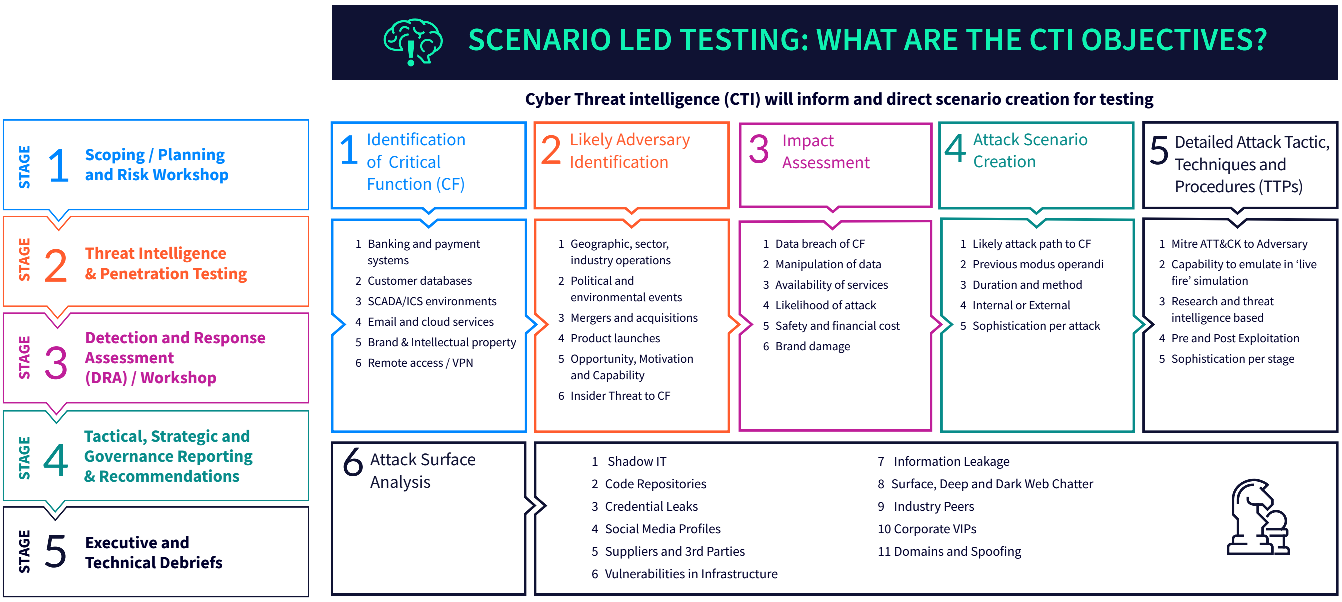
3 Detection & response assessment

Determines the capability of the organisation to detect and respond in a timely and effective manner

SECURITY ASSURANCE

Determine the operational cyber resiliency of the firm

An I-CRT exercise will be delivered in the following five high-level stages:



STAGE 1 **Scoping / Planning and Risk Workshop**

STAGE 2 **Threat Intelligence & Penetration Testing**

STAGE 3 **Detection and Response Assessment (DRA) / Workshop**

STAGE 4 **Tactical, Strategic and Governance Reporting & Recommendations**

STAGE 5 **Executive and Technical Debriefs**

SCENARIO LED TESTING: WHAT ARE THE CTI OBJECTIVES?

Cyber Threat intelligence (CTI) will inform and direct scenario creation for testing

1 Identification of Critical Function (CF)

1 Banking and payment systems
2 Customer databases
3 SCADA/ICS environments
4 Email and cloud services
5 Brand & Intellectual property
6 Remote access / VPN

2 Likely Adversary Identification

1 Geographic, sector, industry operations
2 Political and environmental events
3 Mergers and acquisitions
4 Product launches
5 Opportunity, Motivation and Capability
6 Insider Threat to CF

3 Impact Assessment

1 Data breach of CF
2 Manipulation of data
3 Availability of services
4 Likelihood of attack
5 Safety and financial cost
6 Brand damage

4 Attack Scenario Creation

1 Likely attack path to CF
2 Previous modus operandi
3 Duration and method
4 Internal or External
5 Sophistication per attack

5 Detailed Attack Tactic, Techniques and Procedures (TTPs)

1 Mitre ATT&CK to Adversary
2 Capability to emulate in 'live fire' simulation
3 Research and threat intelligence based
4 Pre and Post Exploitation
5 Sophistication per stage

6 Attack Surface Analysis

1 Shadow IT
2 Code Repositories
3 Credential Leaks
4 Social Media Profiles
5 Suppliers and 3rd Parties
6 Vulnerabilities in Infrastructure
7 Information Leakage
8 Surface, Deep and Dark Web Chatter
9 Industry Peers
10 Corporate VIPs
11 Domains and Spoofing

Threat intelligence against Critical Business Functions (CBF's)

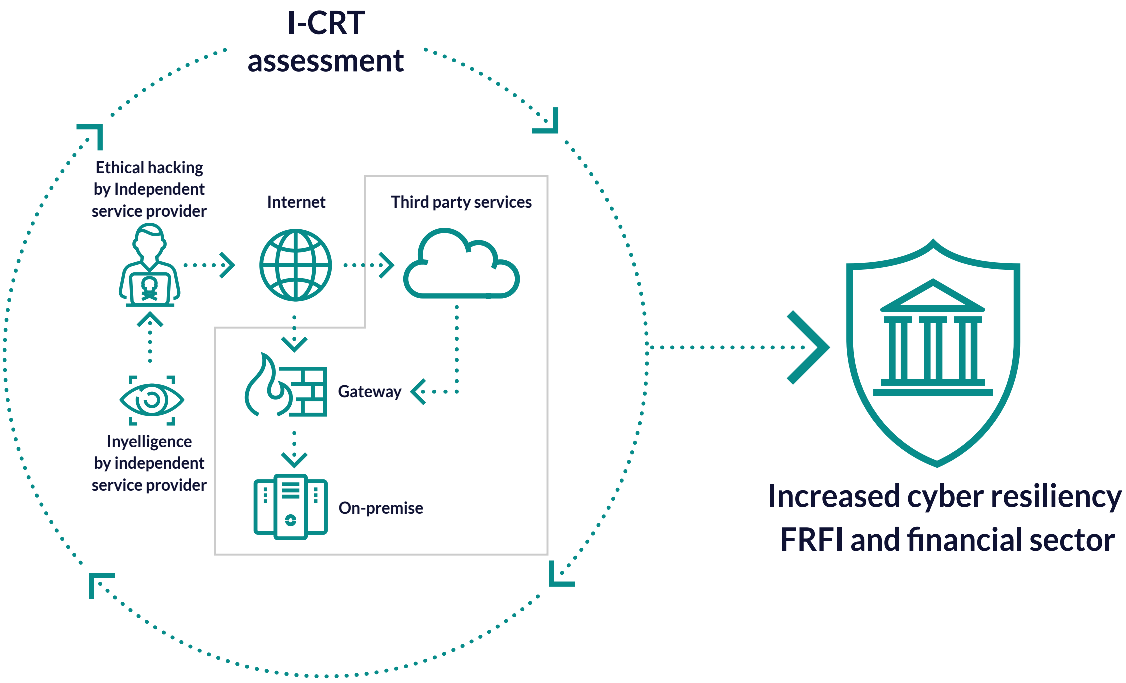
I-CRT requires organizations to commission a TIP, Threat Intelligence Service Provider, to conduct a threat intelligence gathering exercise. LRQA Nettitude is an approved Threat Intelligence provider across regulatory frameworks (CBEST, GBEST, iCAST, TIBER) and can deliver the following:

- Intelligence on geo-political threats known to be operating in the sector and sub-sector
- TTP and Modus Operandi of threat actors known to be targeting similar types of organizations including MITRE references
- Open Source Intelligence (OSINT) relating to the organization and the industry they operate within
- Gather and review closed source intelligence relevant to the organization 02 GBEST Threat Intelligence Requirements
- Creation of a series of scenarios that reflect real-world 'likely' threats
- Inclusion of TTP's to be simulated, goals to be executed and targets to be pursued
- All Threat Intelligence is reviewed and ratified by OSFI prior to Red Team execution

LRQA Nettitude has comprehensive methodologies for Threat Intelligence, and is continually adapting its information sources and collection techniques, providing you with relevant and timely actionable intelligence and advice.

How LRQA Nettitude can help you

LRQA Nettitude's I-CRT service has been developed to provide insight and assurance through the simulation of real-world threat actors using known tactics, techniques, and procedures (TTPs) to assess and enhance your organization's security posture. With our team of consultants, we partner with your organization and OSFI to ensure risk management is at the forefront of all I-CRT engagements.


I-CRT assessment
Ethical hacking by Independent service provider
Internet
Third party services
Gateway
On-premise
Inyelligence by independent service provider
Increased cyber resiliency FRFI and financial sector

What makes LRQA Nettitude unique?

LRQA Nettitude has been delivering compliance-driven technical assurance assessments for over a decade. As a multi-accredited company, we have a team of in-house, highly skilled, and certified individuals, supported by a team of consultants that have been active contributors to the Simulated Target Attack & Response (STAR), CBEST, TIBER, iCAST and GBEST.

I-CRT requirements have been designed for Canadian FRFI's while maintaining alignment with global threat-led frameworks.

LRQA Nettitude has developed its own state-of-the-art custom tooling, PoshC2, that allows the simulation of a wide range of threat actors from commodity threat actors to advanced persistent threats (Nation State) that are known to be prevalent.

- Reflection of the types of TTPs that threat groups are known to be leveraging.
- This toolset is unique within the industry and is one of the reasons why LRQA Nettitude's team has been highly successful in supporting the organization's intelligence-led assurance strategies.
- LRQA Nettitude has also developed open-source tooling that allows for a wider range of threat actors to be accurately simulated which is backed by subject matter experts in Red Teaming, with high levels of skill and experience in mature and complex environments

Get in touch

Visit **www.nettitude.com** for more information
or email enquiries to **solutions@nettitude.com**

UK Head Office
1 Trinity Park
Bickenhill Ln
Birmingham
B37 7ES

Americas
810 Seventh Avenue
Suite 1110
New York
NY, 10019

Asia Pacific
18 Cross Street
#02-101
Suite S2039
Singapore 048423

Europe
Fidiou 9
Athina
106 78
Greece