Privasec GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

Cyber Resilience Testing under the CORIE Framework

Fact Sheet v1.1

Background

The Council of Financial Regulators (CFR) released a framework in December 2020 that can be used to build Red Team scenarios to assess the level of Australian financial services industry's cyber resilience. A proactive stance to cyber security is required to maintain information security capabilities that commensurate with the size and extent of the threats the organization's information assets face.

The Cyber Operational Resilience Intelligence-led Exercises (CORIE) framework is a pilot programme of exercises that will mimic the Tactics, Techniques and Procedures (TTPs) of real-life adversaries, creating and utilising tools, and using techniques that may not have been anticipated or planned for.

Also known as Red Team exercises, these assessments help Financial Institutions (FI) stay competitive and secure by leveraging an unbiased view, and by third-party providers mimicking real-world Advanced Persistent Threats (APT).

The pilot program will focus on the following objectives:

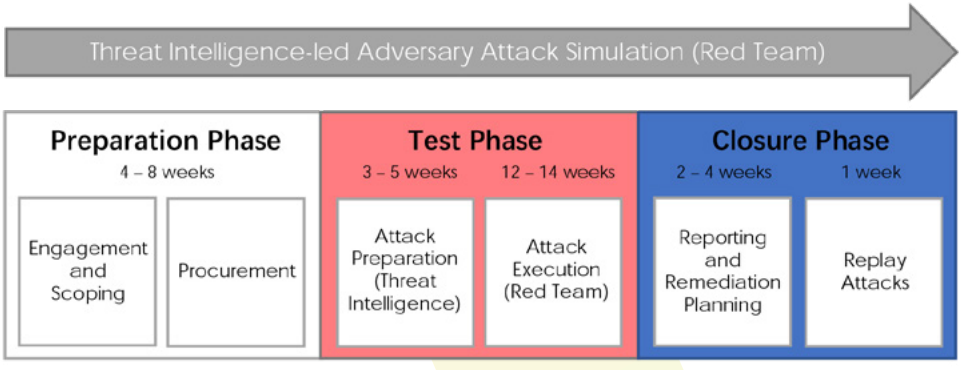
- Provide data and information to inform relevant Australian Regulators of systemic weaknesses that may present a risk to the integrity of the Australian financial markets and financial system.
- Assess FI's resilience to known adversaries targeting the FI (based on Threat Intelligence).
- Provide the relevant Regulator and FI with a plan of remediation to address any identified weaknesses.

What is Red Teaming?

In Red Team exercises, the adage "The best defense is a good offense" applies.

Highly skilled security consultants will enact a series of real-life adversary simulations to test the ability of the organisation's people, processes and technology to prevent, detect, recover and respond to potential real-world attacks.

The Red Team pilot exercise consists of six stages performed across three phases:



Privasec, as an independent cyber security firm, can act as a third-party Red Team provider of these exercises during the Test and Closure Phase. The Test Phase comprises the Attack Preparation and Attack Execution stages. Attack Preparation entails acquisition of Threat Intelligence to shape scenarios in the Attack Execution stage.

In the Closure Phase, the Red Team will share the Attack Execution activity and finalise the Attack Execution Report. A Remediation Plan Report is then given to summarise key risks identified within the Red Team report after Replay Attacks have completed – with all findings included with a risk-management-based overlay.

Privasec – the Preferred Red Team Partner

1. Threat Intelligence is gathered, including Internal FI Threat Intelligence which is shared to help define realistic threat scenarios against approved business services.
2. Threat Intelligence to Red Team handover.
3. The Red Team will work with the White Team to develop scenarios and document them in a test plan.
4. Test plans will detail threat scenarios converted by the Red Team into realistic and effective Red Team scenarios, which are shared with the FI and CTC.
5. A Communication Plan between the White and Red Team should be agreed on, prior to the start of the Attack Execution.
6. Attack Execution phase begins and the Red Team Provider will execute the simulation as per the agreed test plan.
7. All actions will be captured in an Attack Execution Log, including any deviation from defined attack plans.
8. Regular update meetings are held with the White Team to keep them informed throughout the exercise.
9. Red Team will calibrate the "noise" in their actions in coordination with the White Team to determine a detection and response threshold.
10. CORIE's Closure Phase comprises the Red Team sharing Attack Execution (log) activity, finalising the Attack Execution report, and conducting debrief meetings with the FI and CTC to create a remediation plan.

CORIE Red Team Provider Requirements

To ensure that third-party providers are certified and capable of performing Red Team exercises, CORIE Team Coordinators (CTC) will assess if they meet the specified minimum standards.

Threat Intelligence

FIs should ensure that the Threat Intelligence Provider they engage has appropriate resources and demonstrable experience to provide a Threat Intelligence Report and Targeting Report to both the FI and CFR.

Red Team

FIs should ensure that the Red Team Provider has qualified and experienced team members capable of performing management, open-source intelligence (OSINT) gathering, reconnaissance, surveillance, cyber-attack simulation, social engineering, physical breach, and reporting aligned with the CORIE standard.

How we can help you

The CORIE framework is designed to be a continuous loop, in addition to existing vulnerability assessments, penetration testing and continuous Red Team exercises.

Leveraging our extensive experience in the field of technical security, we create test plans that mimic real-world APTs that FIs must be capable of withstanding.

We regularly upskill our team and stay updated on industry certifications. Beyond that, we ensure that our clients receive regular updates and provide them with the best services to fit their specific needs.

Click here for more detailed information on the CORIE Framework.

Ask our consultants about our certifications and how we can support you in your Red Team exercises today.

About Privasec

Privasec is an independent security, governance, risk, and compliance consulting firm. We are driven by business outcomes bridging the gap between the technical and business worlds to create meaningful business cases and enhance decision making.

Over the last decade, our consultants have delivered a broad range of engagements across various industry sectors. Privasec consultants have worked with leading consultancies in senior roles. Our consultants apply industry knowledge and relationships to help their clients navigate the governance, security and compliance landscape and achieve the required outcome.

At Privasec we believe in partnering with our clients by building long-lasting relationships based on trust, integrity and care. We are vendor technology agnostic and will always disclose to our customers, any interest we may have when advising on technical solutions. We uphold high standards in Honesty, Rigour, Flexibility and Service. Our success is our people and that's why we take the time to find not only the right skill-sets, but also the right culture-fit.

To learn more about Privasec and our services, please visit our website:

https://www.privasec.com/

GET THE BALL ROLLING

Talk to your consultant or ring us today to understand your needs and provide a proposal to get started on your Privacy journey.

You can call us at **1800 996 001** or email us at **info@privasec.com**

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

DRONE SEC UAS HACKING, HARDENING & DEFENCE

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+603 2788 3709 (MY)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 2, 64 Clarence Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
138 Robinson Road
Oxley Tower #10-01
Singapore 068906

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia