Cyber Operational Resilience Intelligence-led Exercises (CORIE)® Framework

Appendix B: Provider Guide

for threat intelligence and red teaming service providers

Version 2.0

July 2022

Council of
Financial Regulators

Contents

Glossary

Term	Explanation
Adversary Attack Simulation	An exercise that uses Threat Intelligence to model and execute an adversary attack simulation. Also known as a Red Team Exercise.
APRA	Australian Prudential Regulation Authority.
ASIC	Australian Securities and Investments Commission.
Blue Team	The FI's team tasked to defend against adversaries attacking their organisation.
CFR	Council of Financial Regulators.
Control Group (formerly White Team)	The FI's team tasked to oversee an Exercise.
CORIE	Cyber Operational Resilience Intelligence-led Exercises.
CTC	CORIE Team Coordinators – tasked with the day-to-day management of the program in accordance with this guide. The CTC includes representative members from the CFR.
Exercise	A cyber operational resilience intelligence-led exercise, likely to consist of an adversary attack simulation, e.g., Red Team Exercise.
FI	A financial institution (including an entity responsible for financial market infrastructure) that participates in the program.
Gold Team Exercise	A Table Top exercise that involves the Provider performing crisis simulations. The exercise involves the FI's senior executives (Gold Team) or crisis management team. The exercise is also known as a Table Top Crisis Simulation.
Modus Operandi	A manner or mode of operating or working.
OSINT	Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources.
Participant	A financial institution (including an entity responsible for financial market infrastructure) that participates in the program.
Provider	A third-party that an FI engages to perform an Exercise. Recognised Providers are identified by having met minimum requirements.
PID	Project Initiation Document.
PIM	Project Initiation Meeting.
Purple Exercise	An exercise that involves the Red Team replaying attacks to help the Blue Team identify gaps to remediate. Also known as a Replay Adversary Attack Simulation.
RBA	Reserve Bank of Australia.
Red Team	The Provider team tasked to simulate an adversary attacking the FI.
Red Team Exercise	An exercise that uses Threat Intelligence to model and execute an adversary attack simulation. Also known as an Adversary Attack Simulation.
Regulator	One or more of APRA, ASIC, and the RBA.

Replay Adversary Attack Simulation	An exercise that involves the Red Team replaying attacks to help the Blue Team identify gaps to remediate. Also known as a Purple Exercise.
Table Top Crisis Simulation	A Table Top exercise involving the Provider performing crisis simulations. The exercise involves the FI’s senior executives (Gold Team) or crisis management team. The exercise is also known as a Gold Team Exercise.
Threat Intelligence	Threat intelligence[1] is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

[1] https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

1. Introduction

The Cyber Operational Resilience Intelligence-led Exercises (CORIE) scheme has been developed by the CFR to aid in preparation and execution of industry-wide cyber resilience exercises2. CORIE's 'red team' exercises mimic the tactics, techniques and procedures (TTP's) of real-life adversaries, employing creativity and utilising tools and techniques that may not have been anticipated and planned for. These exercises measure the ability of an organisation to detect, respond, withstand, repel and recover from the operations of a real adversary based on such TTPs, so as to maintain critical business processes and protect sensitive data.

Real-life adversaries such as state-sponsored attackers are neither constrained by scope nor time. CORIE mimics adversaries through fewer traditional testing restrictions and longer time duration to fully exploit opportunities. As a result, CORIE complements traditional security testing programs, such as vulnerability assessments, penetration testing and continuous red teaming – financial institutions should continue to maintain their existing security testing regimes.

Consistent with the objective of testing the cyber resilience of all sizes of institutions and levels of maturity across the Australian financial industry, CORIE has been designed to be scalable based on a tiering assessment that considers the cyber maturity of a financial institution (FI), organisational size, and market share amongst other factors. The frequency of exercises depends on the FI's Cyber Risk Assessment (CRA) tier.

Exercise types include:

- Adversary Attack Simulation – Red Team exercise
- Replay Adversary Attack Simulation – Purple exercise
- Table Top Crisis Simulation – Gold Team exercise

Exercises are intended to be conducted by independent providers, bringing a fresh perspective and as close to an unbiased view as possible coupled with advanced adversary simulation capabilities. Australian based providers are preferred due to accessibility when co-ordinating effort. However, providers may use resources, including people and technology, which are based outside Australia. Multiple providers can be used across the exercises for gathering threat intelligence on participating financial institutions and conducting the red-team attacks for the simulated cyber scenario.

This guide details the standards required to execute exercises detailed in the CORIE framework.

This guide is useful for FIs to ensure Providers meet the necessary experience and certifications.

Providers should use the information to ensure they have the necessary experience and certifications to meet the standard. Consider the training courses listed here to help achieve the skill required to deliver CORIE.

These certification and experience requirements can be used as a guide for financial institutions to further develop their own cyber security staff to grow internal red team capabilities.

As industry certifications and recommended training evolves, so too will this guide.

[2] The role of the CFR is to contribute to the efficiency and effectiveness of financial regulation and to promote the stability of the Australian financial system. Membership of the CFR consists of the Australian Prudential Regulation Authority (APRA), the Australian Securities and Investments Commission (ASIC), the Reserve Bank of Australia (RBA), and the Department of Treasury. https://www.cfr.gov.au/financial-stability/cyber-security.html

2. Providers

Providers that wish to participate in the program should meet specified minimum standards.

Providers with a significant presence in Australia are preferred due to ease of use when co-ordinating effort.

A Provider may participate in the program as a Threat Intelligence Provider and/or a Red Team Provider.

2.1 Threat Intelligence Provider

A Threat Intelligence Provider gathers threat Intelligence on adversaries targeting FIs in Australia.

Other sources of intelligence used in the program may include:

- Government
- Internal FI sources
- Proprietary feeds
- Intelligence sharing platforms
- Generic public threat intelligence.

A Threat Intelligence Provider engaged by an FI must satisfy the FI that it has a mechanism to gather information and develop threat intelligence from the dark web and that all threat intelligence will be gathered in a legal and ethical manner.

FIs should satisfy themselves that the Threat Intelligence Provider they engage has certified resources to threat model and perform analysis on real-world threats that appear, or are known, to be targeting the FI.

FIs should satisfy themselves that the Threat Intelligence Provider they engage has appropriately certified resources and demonstrable experience to provide both a Threat Intelligence Report and Targeting Report to both the FI and CFR.

2.1.1 Threat Intelligence Team Member Requirements

FIs should satisfy themselves that the personnel of the Threat Intelligence Provider they engage meet the requirements set out in section 2.1.1.3.

A Threat Intelligence team should have qualified and experienced consultants capable of performing analysis, threat modelling and reporting at the time of the engagement.

The team should consist of at least one Threat Intelligence Lead and one Threat Intelligence Analyst.

2.1.1.1 Threat Intelligence Lead

A Threat Intelligence Lead is expected to have knowledge and expertise in leading a team specialising in producing threat intelligence. They should have the ability to gather threat intelligence in a realistic, legal and safe manner with the ability to document appropriate supporting evidence.

2.1.1.2 Threat Intelligence Analyst

Threat Intelligence Analysts are expected to have knowledge and expertise to gather threat intelligence in a realistic, legal and safe manner, collecting appropriate supporting evidence.

2.1.1.3 Threat Intelligence Skills Matrix

Certifications indicating the necessary experience and skills include[3]:

Role	Certification/Experience
Threat Intelligence Lead	**Required certification:** • CREST Certified Threat Intelligence Manager (CCTIM), or • GIAC Gold Cyber Threat Intelligence (GCTI) **Required experience:** • 3 years of related intelligence experience *Optional training courses:* • *SANS FOR 578: Cyber Threat Intelligence* • *SANS SEC 487: Open-Source Intelligence Gathering and Analysis*
Threat Intelligence Analyst	**Required certification:** • CREST Registered Threat Intelligence Analyst (CRTIA), or • GIAC Cyber Threat Intelligence (GCTI) **Required experience:** • 1 year of related intelligence experience *Optional training courses:* • *SANS FOR 578: Cyber Threat Intelligence* • *SANS SEC 487: Open-Source Intelligence Gathering and Analysis*

[3] During the pilot program an exemption can be granted to Providers where team members are working towards attaining required certifications. Exemptions will be determined by the CTC.

2.2 Red Team Exercise Provider (Adversary Attack Simulation)

FIs should satisfy themselves that the personnel of the Red Team Provider they engage meet the requirements set out in section 2.2.1.5.

Red Team Providers should have qualified and experienced team members capable of performing management, OSINT, reconnaissance, surveillance, cyber-attack simulation, social engineering, physical breach, and reporting at the time of the engagement.

A Red Team should consist of at least a Red Team Lead, a Red Team Specialist, and an Exploit Development Specialist.

2.2.1 Red Team Member Requirements

2.2.1.1 Red Team Lead

Red Team Leads are expected to have strong practical and theoretical knowledge and expertise in simulating sophisticated adversaries targeting organisations within the financial industry, along with expertise in leading a Red Team. The Red Team Lead should have skills to create schedules, test plans, action summaries, and run meetings and workshops with the FI. Red Team Leads should be proficient in identifying, managing and communicating exercise risks to the FI's Control Group. They should also provide practical advice and solutions to resolve challenges that typically arise during engagements.

2.2.1.2 Red Team Specialist

Red Team Specialists are expected to have practical knowledge and expertise in simulating sophisticated adversaries targeting organisations within the financial industry. They should have skills encompassing exploitation of vulnerabilities, social engineering phishing campaigns, implant development, evasion skills and lateral movement within a compromised network.

2.2.1.3 Exploit Development Specialist

Exploit Development Specialists are expected to have experience developing software exploits and improving public exploits for use in production environments. The Exploit Development Specialist should have skills around exploit development, reverse engineering, assembly and disassembly, along with a comprehensive knowledge of different operating systems and their defences.

Exploit Development Specialists are not expected to be engaged in the exercise on a full time basis, but should be available to create, modify, and improve exploits for the exercise when required.

2.2.1.4 Red Team Member

Red Team Members are expected to have knowledge and expertise in simulating adversaries targeting organisations in the financial sector. They should have skills to support the Red Team Specialist and execute specific tasks assigned to them. Due to the increased scope of larger exercises, Red Team Members provide support for tasks requiring less complexity. Red Team Members should not work on the exercise without a Red Team Specialist. Actions on targets are the responsibility of the Red Team Lead and Red Team Specialist, including those of the Red Team Member.

2.2.1.5 Red Team Skills Matrix

Certifications indicating the necessary experience and skills include[4]:

Role	Certification/Experience
Red Team Lead	**Required certification:** One of: • CREST Certified Simulated Attack Manager (CCSAM), or • SANS SEC564 or SANS SEC565 and one of: • CREST Certified Simulated Attack Specialist (CCSAS) • CREST Certified Infrastructure Tester (CCT Inf) • Offensive Security Certified Expert (OSCE) / (OSCE3) • GIAC Advanced Penetration Tester (GXPN) **Required experience:** • 7 years of red teaming or penetration testing experience *Optional training courses:* • *SANS SEC564: Red Team Ops and Threat Emulation* • *SANS SEC565: Red Team Operations Adversary Emulation* • *SANS SEC699: Purple Team Tactics Adversary Emulation* • *SPECTEROPS Adversary Tactics: Red Team Operations* • *GIAC Penetration Tester (GPEN)* • *Silent Break: Dark Side Ops 1* • *CORELAN: Corelan "Bootcamp" exploit*

[4] During the pilot program an exemption can be granted to Providers where team members are working towards attaining required certifications. Exemptions will be determined by the CTC.

Red Team Specialist	***Recommended certification:*** One of: • CREST Certified Simulated Attack Specialist (CCSAS), or • GIAC Advanced Penetration Tester (GXPN) and one of: • Zeropoint Certified Red Team Operator (CRTO) • Pen tester academy Certified Red Team Expert (CRTE) • INE/eLearn Security Penetration Tester Extreme (eCPTX) and one of: • CREST Certified Infrastructure Tester (CCT Inf), or • Offensive Security Certified Expert (OSCE) / (OSCE3), or • Offensive Security Experienced Professional (OSEP) **Required experience:** • 5 years of red teaming or penetration testing experience *Recommended training courses:* • *ZEROPOINT Certified Red Team Operator (CRTO)* • *PENTESTER ACADEMY Certified Red Team Expert (CRTE)* • *Offensive Security Experienced Professional (OSEP)* • *SPECTEROPS Adversary Tactics: Red Team Operations* • *SANS SEC 564 Red Team Ops and Threat Emulation* • *SANS SEC 660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking* • *SANS SEC699: Purple Team Tactics Adversary Emulation* • *NETSPI Silent Break: Dark Side Ops 1 and 2* • *CORELAN: Corelan “Bootcamp” exploit* • *GIAC Penetration Tester (GPEN)*
Exploit Development Specialist	**Recommended Certifications and Training** • *Offensive Security Certified Expert (OSCE)/(OSCE3)* • *Offensive Security Exploitation Expert (OSEE)* • *Offensive Security Experienced Professional (OSEP)* • *GIAC Advanced Penetration Tester (GXPN)* • *CORELAN: Corelan “Advanced” exploit* • *SANS SEC 760 Advanced Exploit Development for Penetration Testers* • *NETSPI Dark Side Ops -1 and 2* • *Dark Vortex MOS and OTD* **Required experience:** • 3 years of exploit development experience • Public attributed CVEs

Red Team Member	**Recommended certification:** One of: • CREST Certified Infrastructure Tester (CCT Inf), or • GIAC Advanced Penetration Tester (GXPN) And one of: • Offensive Security Certified Professional (OSCP), or • Offensive Security Certified Expert (OSCE)/(OSCE3) **Required experience:** • 3 years of penetration testing experience *Optional training courses:* • *SANS SE 560: Network Penetration Testing and Ethical Hacking* • *SANS SEC760 Advanced Exploit Development for Penetration Testers* • *SANS SEC699: Purple Team Tactics Adversary Emulation* • *Offensive Security Certified Professional (OSCP)* • *Offensive Security Certified Expert (OSCE)/(OSCE3)* • *Offensive Security Exploitation Expert (OSEE)* • *Offensive Security Experienced Professional (OSEP)* • *Silent Break: Dark Side Ops 1* • *CORELAN: Corelan “Bootcamp” exploit*

2.3 Provider for Replay Adversary Attack Simulation – Purple Exercise

A Purple Exercise should be completed by Tier 1, 2 and 3 FIs annually.

Purple Exercises originate from the concept of the Red Team and Blue Team intermixing. The Red Team, who simulate attacks, collaborates with the Blue Team, which is the team responsible for detecting and responding to cyber-attacks in an organisation.

Where an FI has an internal testing capability that meets the requirements of this section, the internal team can be used to conduct this exercise rather than using an external Red Team Provider. The internal team then becomes known as the Provider for all intents and purposes.

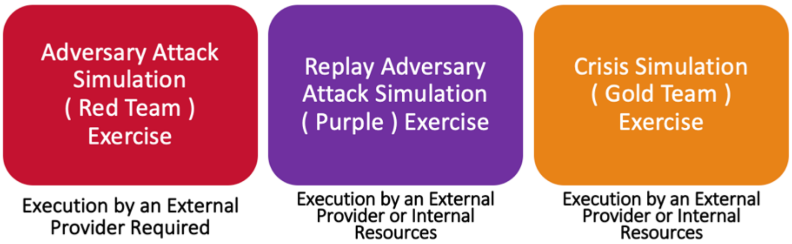
Adversary Attack Simulation (Red Team) Exercise
Execution by an External Provider Required
Replay Adversary Attack Simulation (Purple) Exercise
Execution by an External Provider or Internal Resources
Crisis Simulation (Gold Team) Exercise
Execution by an External Provider or Internal Resources

Figure 1 - External and internal resources

Providers must have qualified team members to mimic the tactics, techniques, and procedures of known advanced persistent threats.

The Provider’s Red Team will work closely with the FI’s Blue Team.

2.3.1 Purple Exercise Member Requirements

Purple Exercises can be conducted by the following Red Team Provider members:

- Red Team Specialist
- Red Team Member

2.4 Provider for Crisis Simulation Table Top – Gold Team Exercise

A Gold Team Exercise should be completed by Tier 1, 2 and 3 FIs annually.

Providers must have qualified team members that can clearly communicate, and have knowledge concerning details of scenarios involved adversary attack simulation. Team members must have knowledge of the appropriate defensive counter measures and risk management used within FIs.

As the skills required match many of those required by the Red Team Provider to lead an adversary attack simulation, a Red Team Provider can be used for a Gold Team Exercise.

Consistent with approach to Purple Exercises, where an FI has an internal testing capability that meets the requirements of this section, the internal team can be used to conduct this exercise rather than using an external Red Team Provider.

That team then becomes known as the Provider for all intents and purposes.

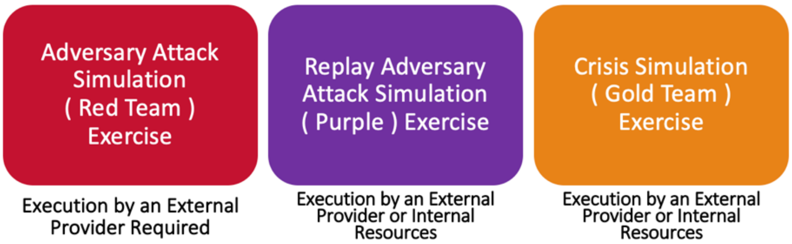
Adversary Attack Simulation (Red Team) Exercise
Execution by an External Provider Required
Replay Adversary Attack Simulation (Purple) Exercise
Execution by an External Provider or Internal Resources
Crisis Simulation (Gold Team) Exercise
Execution by an External Provider or Internal Resources

Figure 2 - External and internal resources

2.4.1 Gold Team Member Requirements

2.4.1.1 Gold Team Lead

Executives may have little prior awareness or exposure to the concepts, terms or details of adversary attack simulation, therefore Gold Team Leads should have strong communication and facilitation skills to lead in role playing activities simulating diverse crisis events.

Gold Team Leads should understand risk management, along with possessing strong practical and theoretical knowledge in simulating sophisticated adversaries, and defensive capabilities used to prevent, detect and respond accordingly. Further, Gold Team Leads must be able to convey risks in terms of business impact and likelihood, so that executive management understand appropriate actions to undertake.

Provider staff with skills necessary to lead a Gold Team can be assigned the role of Gold Team Lead. However, either a Red Team Lead or Red Team Specialist should also be a member of the Provider's team.

3. Annex A: CTC Contact Details

The CTC can be contacted by emailing: corie@rba.gov.au