SUOMEN PANKKI
EUROJÄRJESTELMÄ
FINLANDS BANK
EUROSYSTEMET

DORA and TLPT testing

Lecture for Haaga-Helia on 31 March 2026

Marko Buuri
Payment Systems Department, Bank of Finland

TIBER-FI

Learning objectives

By the end of this lecture, you should be able to understand at high level

- what is DORA,
- what are the TLPT tests and how are they organized,
- what is TIBER-EU (or TIBER-FI) and how does it relate to this, and
- principles of how the threat intelligence and red team testing activities are delivered in these projects.

Disclaimer

- This presentation is an introduction and due to format constraints focuses on select key aspects of DORA TLPT projects and testing.
- Always check the detailed requirements and full explanations from the regulation in effect before making decisions.

What is DORA?

What is DORA?

- Digital Operations Resilience Act (DORA) is an EU-wide regulation for financial sector resilience. It came applicable in January 2025.
- DORA affects over 20 000 financial sector entities and their ICT third-party partners.
- There are five pillars of activities in DORA that the financial sector entities must follow. Most pillars are further detailed in technical standards (so called RTS and ITS) which also are regulation as they are.
- Every member country needs to appoint a competent authority for DORA and in Finland, this authority is the Financial Supervisory Authority (the FIN-FSA, *Finanssivalvonta*).

What about resilience testing?

DORA includes requirements for two types of testing:

1. Basic digital operational resilience testing, that include for example vulnerability assessments, network security reviews, gap analyses, source code reviews, narrow-scoped penetration tests etc. These activities are required for all the financial entities under DORA.
2. Threat-led penetration testing (TLPT), which are required for significant entities identified by competent authorities (i.e. the FIN-FSA).

There is a specific regulation technical standard (RTS) detailing the requirements for the TLPT projects.

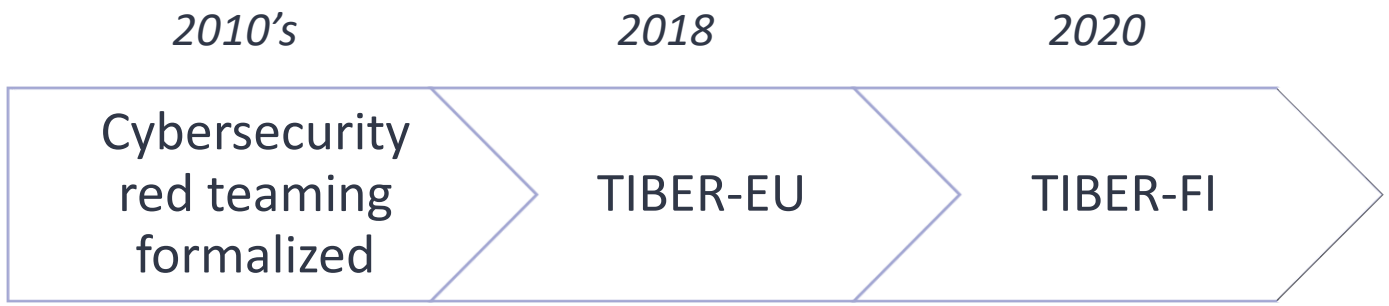
Positioning testing types

Adversary	Testing activity
Nation states **Exceptional**	Adversary simulations, including TLPTs
Organized crime **Highly skilled**	Basic testing activities
Opportunists & Hacktivists **Skilled**	Security scanning
Automations	

What is TIBER-EU?

Background to TIBER-EU

- In 2010's, cybersecurity red teaming started to become formalized and gain popularity in critical sectors like the financial sector.
- In 2018, European Central Bank (ECB) released the TIBER-EU framework to provide a common reference for red team-based testing. Many countries adopted it as their own TIBER implementations. TIBER stands for "Threat Intelligence-Based Ethical Red Teaming".



Situation under DORA

- By following TIBER-EU and local TIBER guidance, a financial entity can best ensure their project is well-controlled, produces good results, and fulfils the RTS's requirements of how a test must be organized.
- Bank of Finland remains the owner of TIBER-FI. The framework is now updated to align with DORA and the recent updates to TIBER-EU.
- Under agreement with the FIN-FSA, the Bank of Finland also continues to operate the TIBER-FI Cyber Team (TCT-FI), which provides test managers to all the TIBER-FI tests.

Available guidance relevant in Finland

Main document

“TIBER-FI procedures and guidelines” is available in English as a PDF at www.suomenpankki.fi/tiberfi

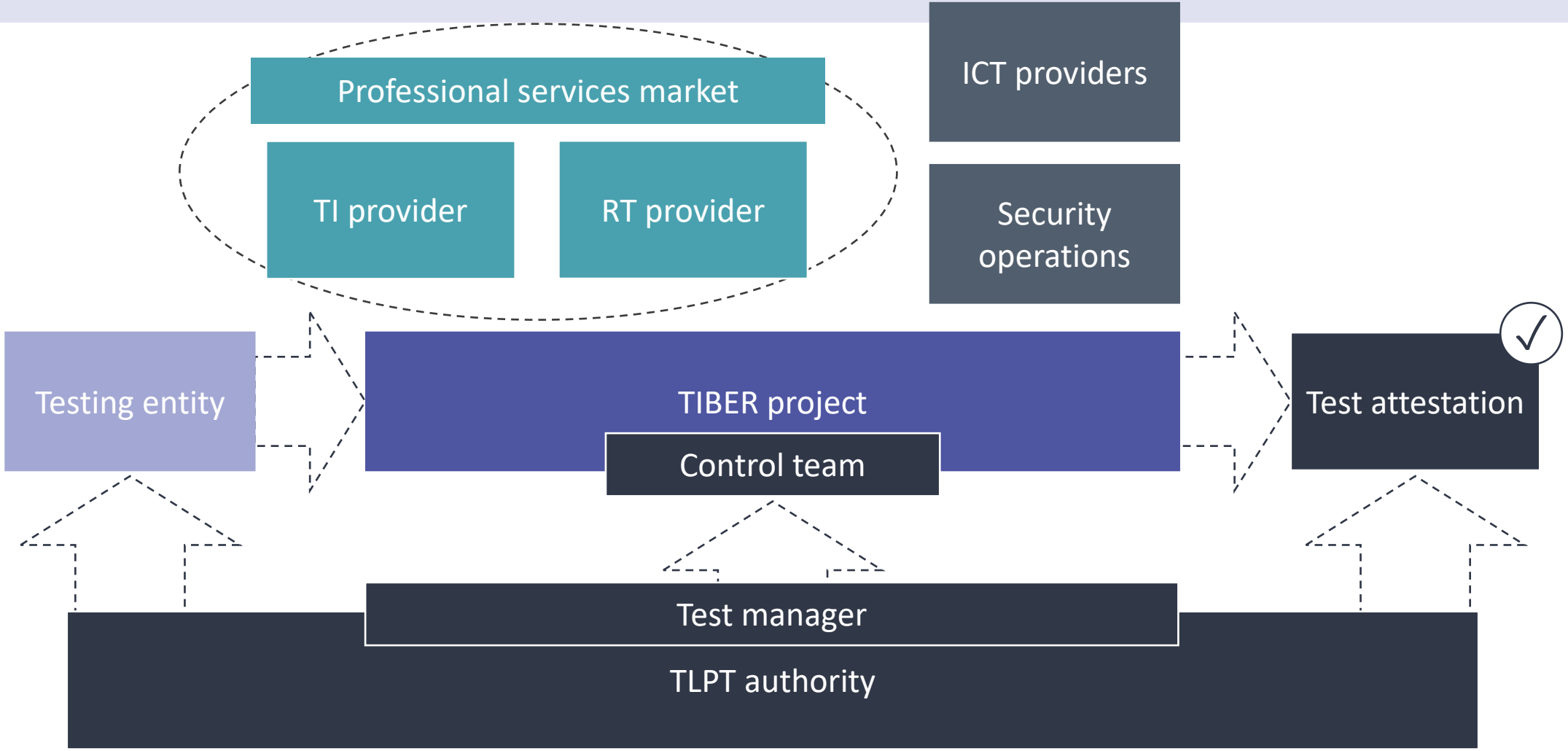
Guidance documents

Available from ECB’s TIBER-EU web site

- TIBER-EU Control Team Guidance
- TIBER-EU Initiation Documents Guidance
- TIBER-EU Guidance for Service Provider Procurement
- TIBER-EU Scope Specification Document Guidance
- TIBER-EU Targeted Threat Intelligence Report Guidance
- TIBER-EU Red Team Test Plan Guidance
- TIBER-EU Red Team Test Report Guidance
- TIBER-EU Blue Team Test Report Guidance
- TIBER-EU Purple Teaming Guidance
- TIBER-EU Remediation Plan Guidance
- TIBER-EU Test Summary Report Guidance
- TIBER-EU Attestation Guidance

Overview of the testing process

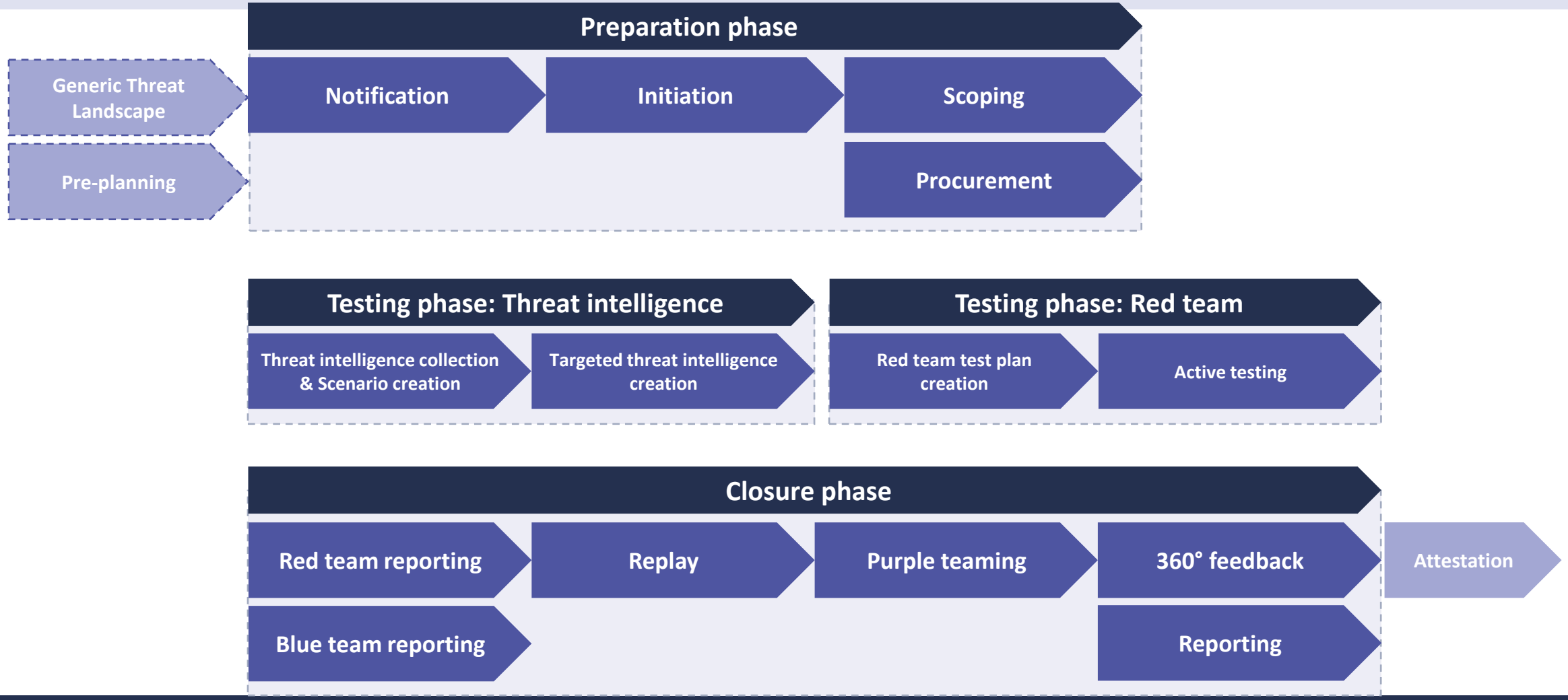
Stakeholders in mandated TIBER projects



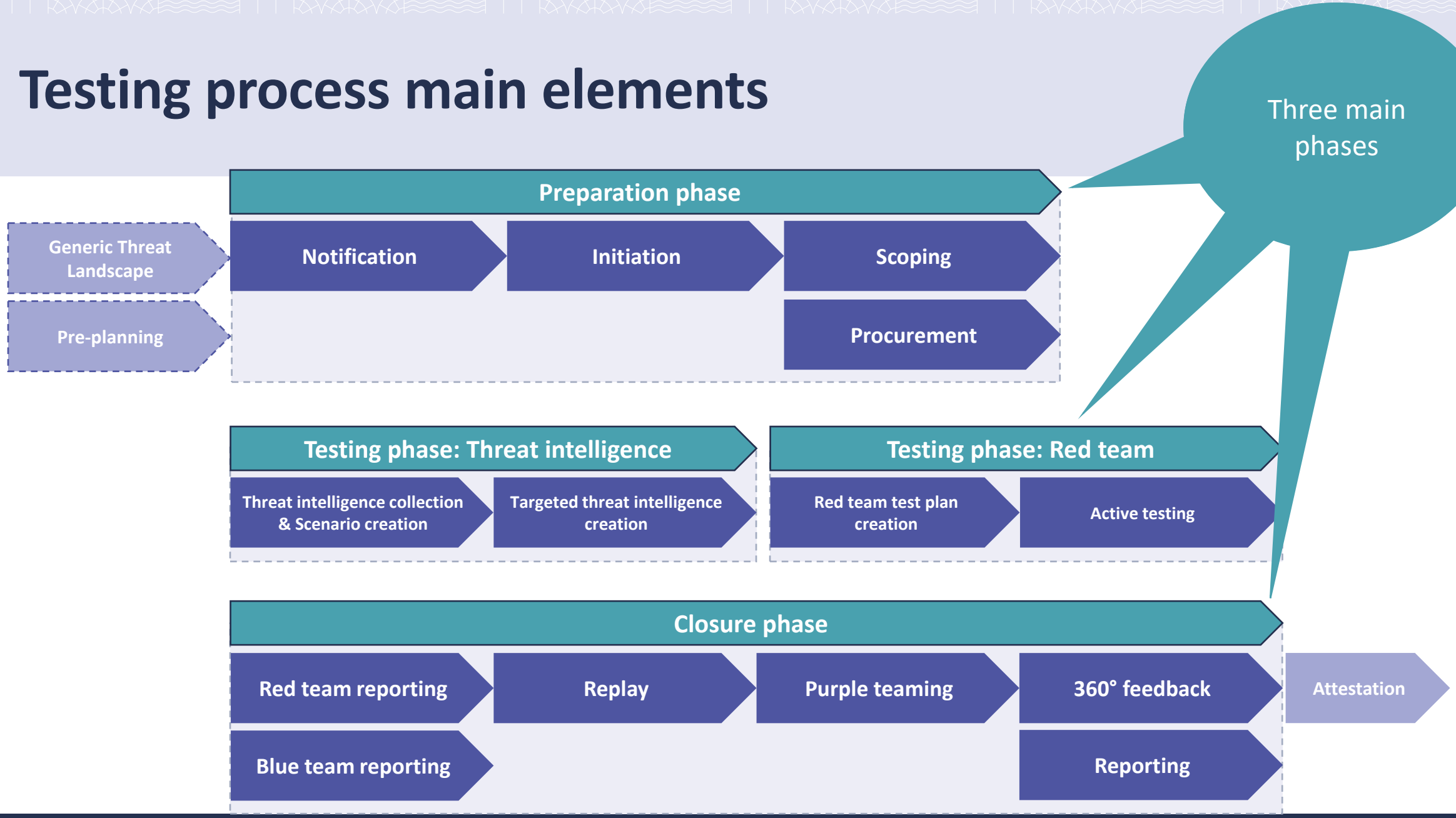
Key roles

- Control team (CT) and control team lead (CTL)
  - The CT holds key responsibilities pertaining to executing the test compliance with the requirements of TIBER-FI.
  - The CTL coordinates project management, test activities, information flow between the necessary stakeholders, and alignment with TIBER-FI requirements. The CTL should be a senior/manager level person with excellent understanding of the business and operations.
- Service providers: Threat intelligence provider (TIP) and red team testers (RTT) need to be staffed separately and can be two providers or one firm delivering both.
- Blue team (BT)
  - The BT are the employees and stakeholders defending the financial entity's use of ICT systems and services.
  - It is critical that the BT be completely excluded from the preparation and conduct of the TIBER-FI test.

Testing process main elements

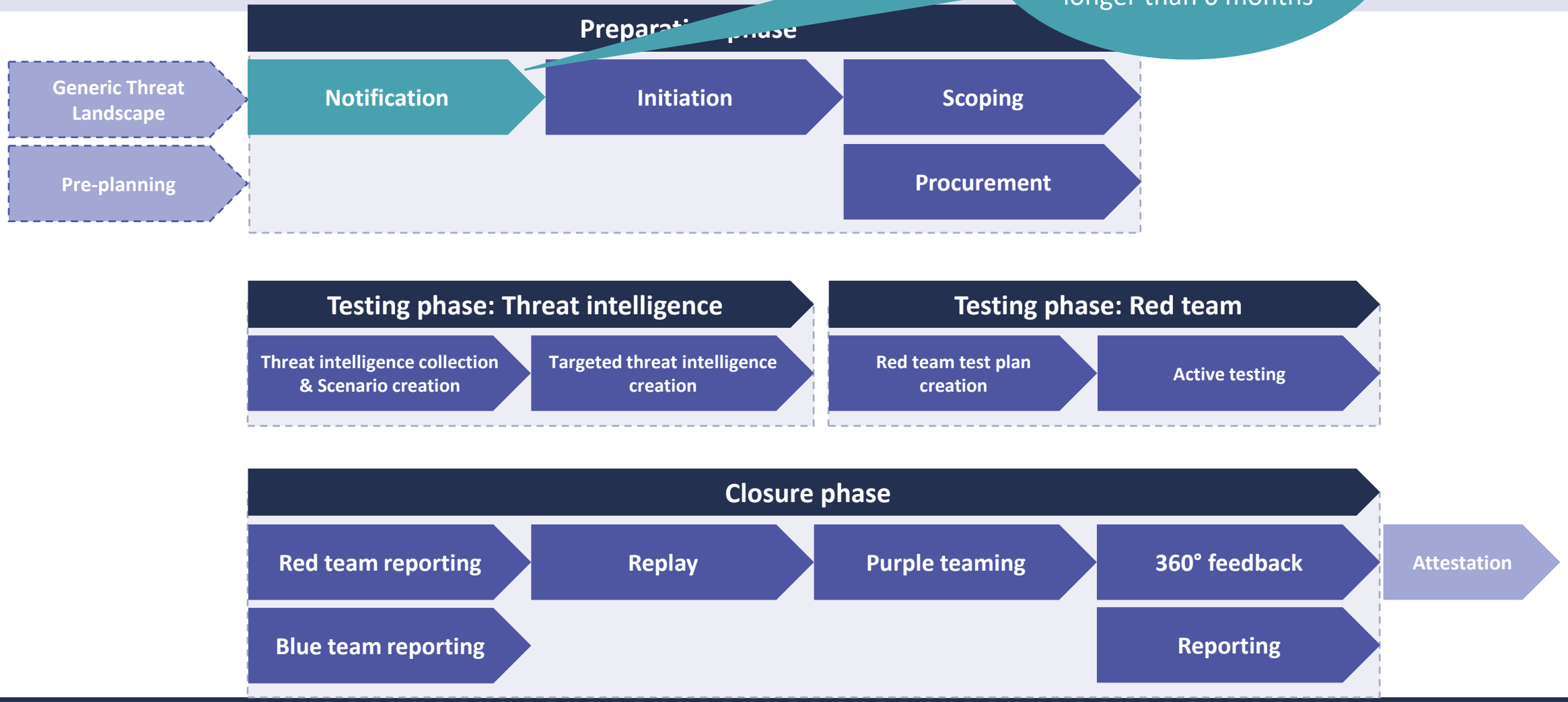


Testing process main elements

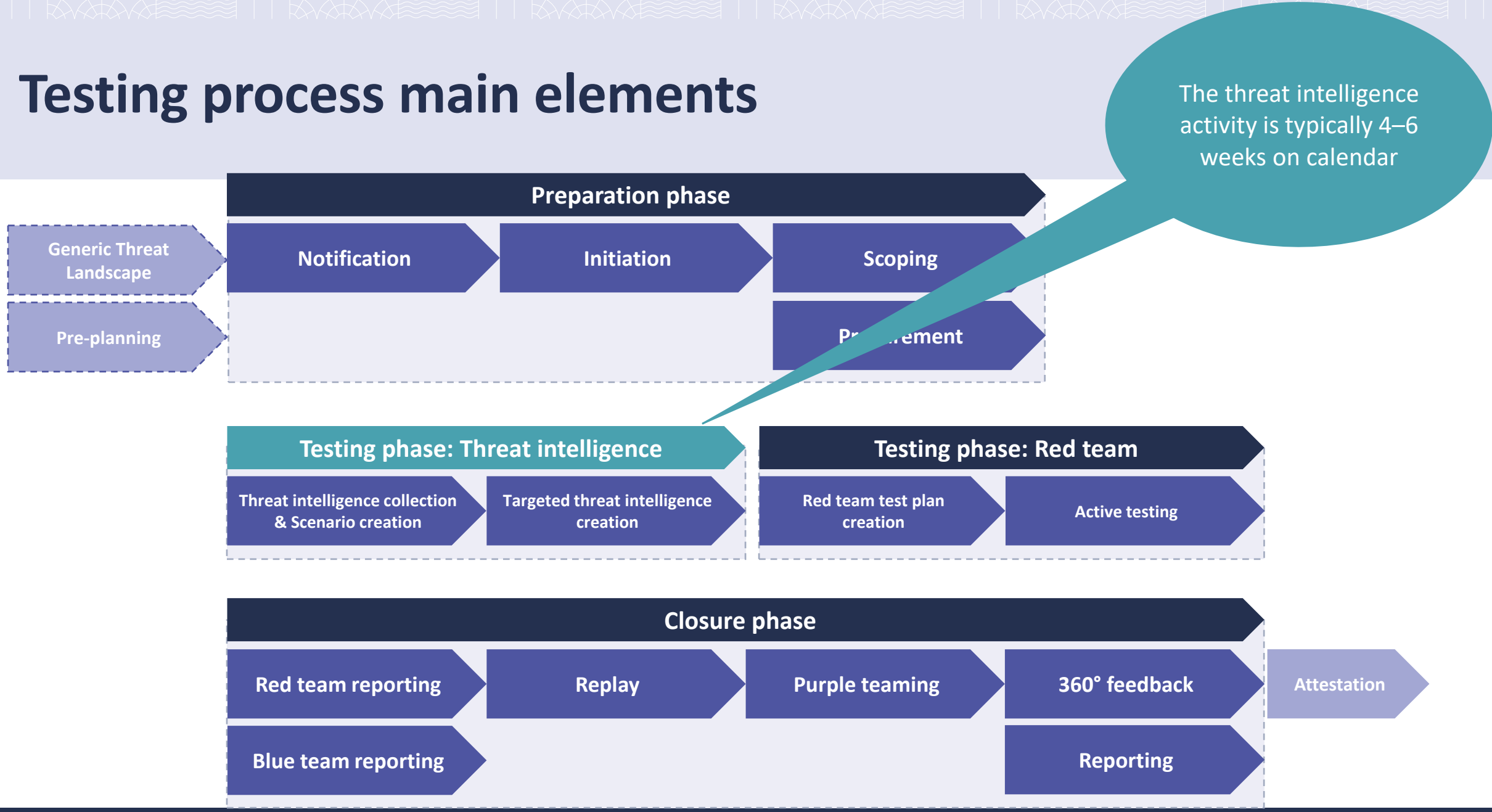


Testing process main elements

A notification letter from the TCT initiates the preparation phase which may last no longer than 6 months

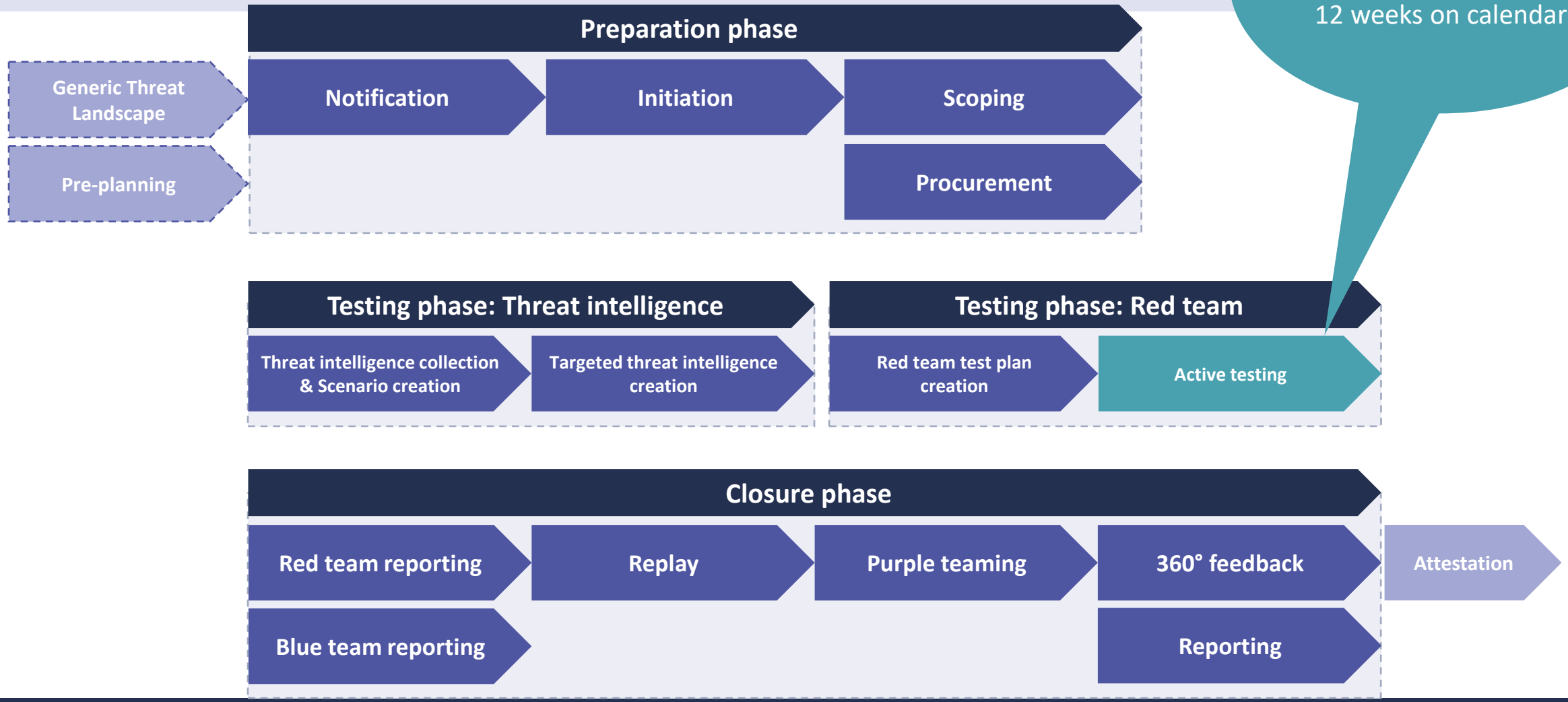


Testing process main elements

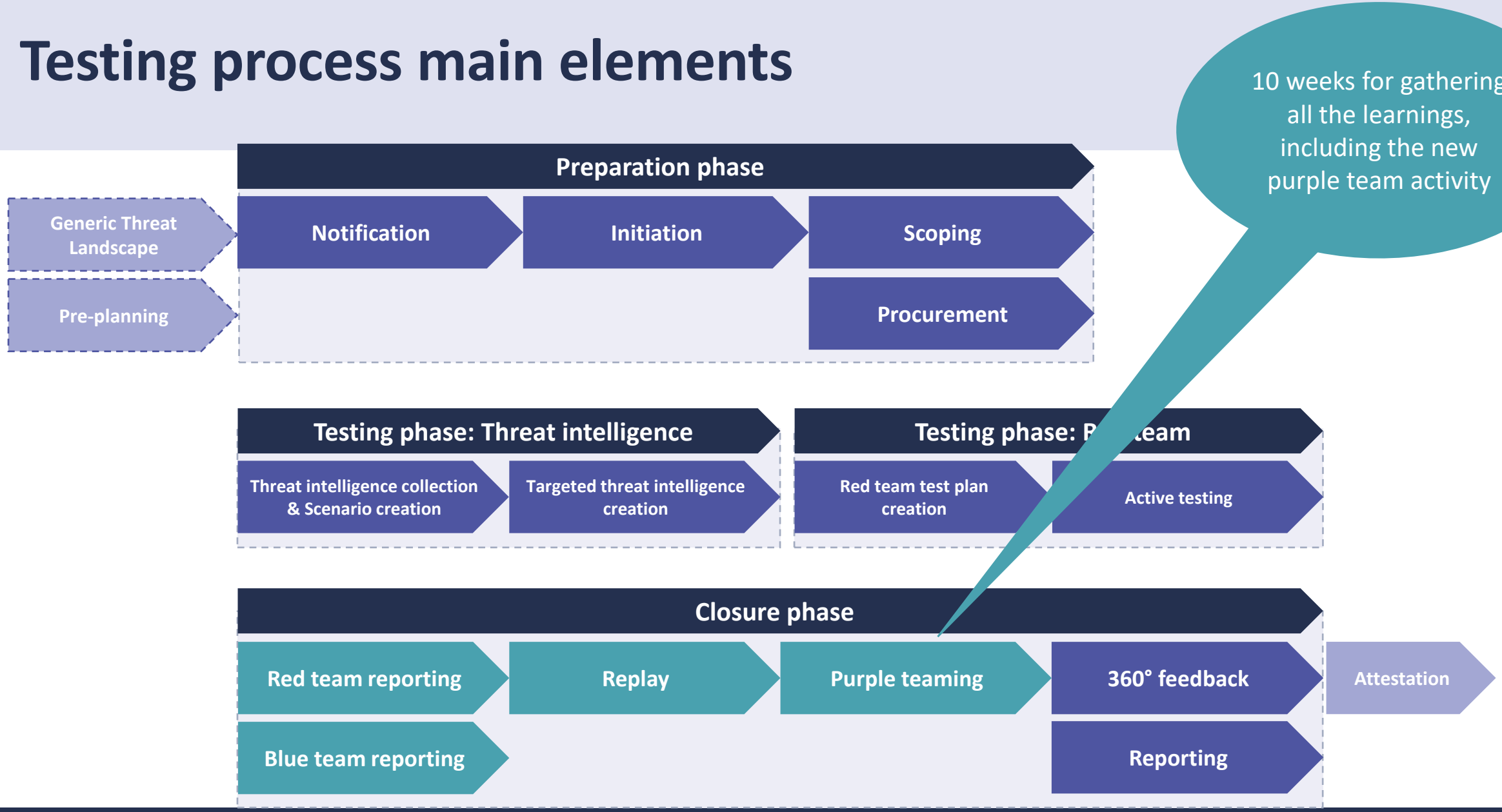


Testing process main elements

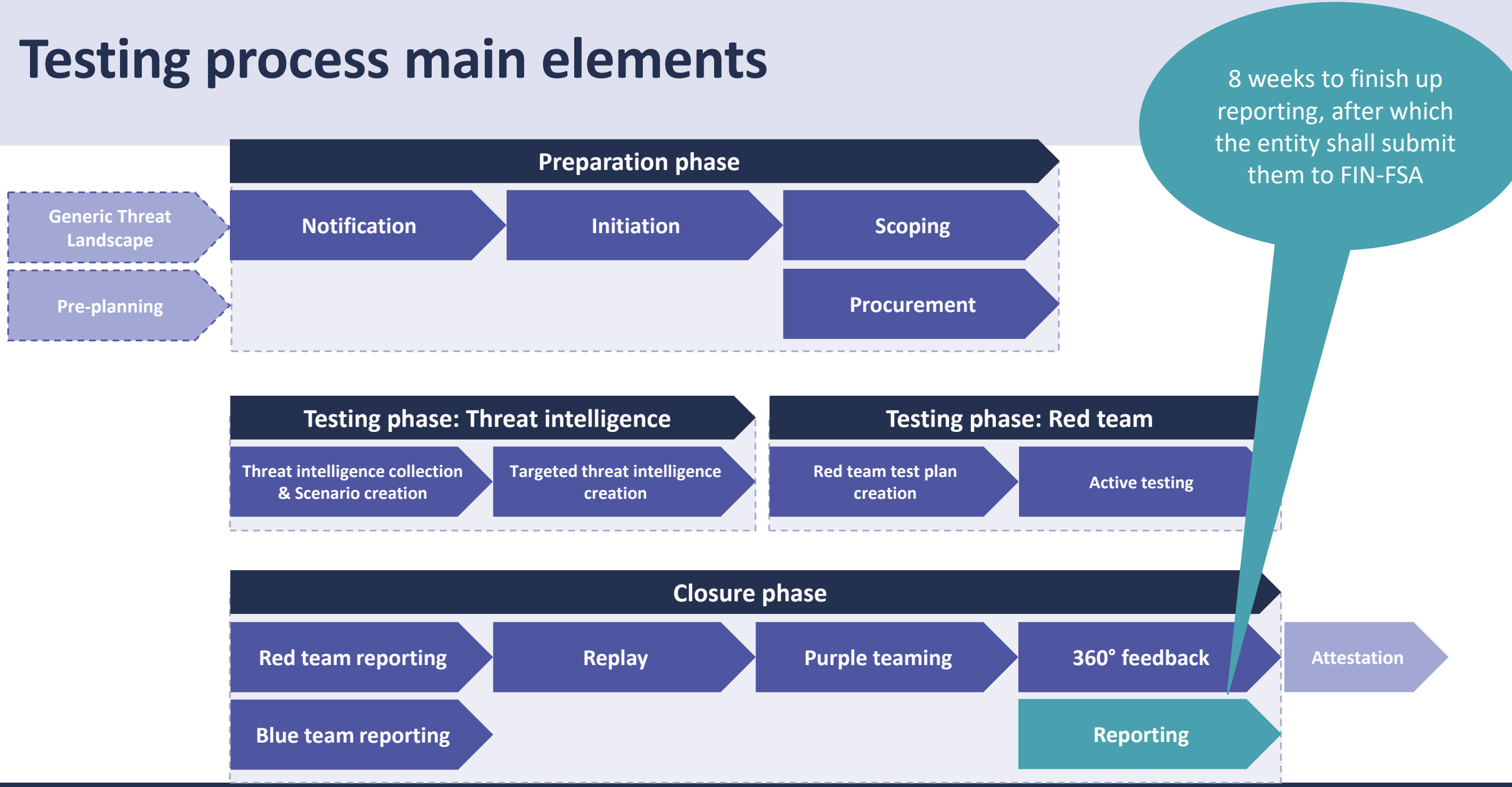
The red team testing activity is at minimum 12 weeks on calendar



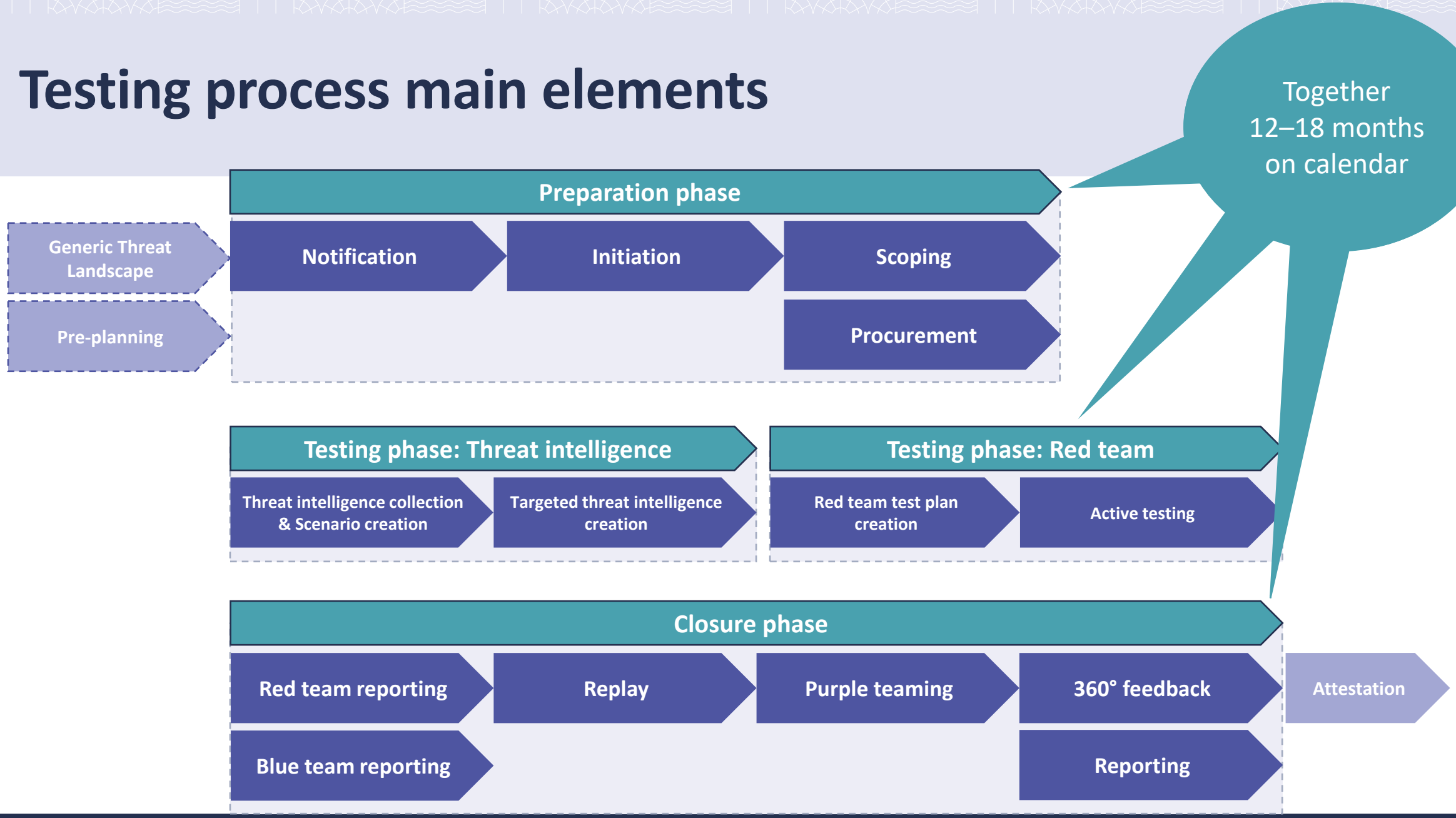
Testing process main elements



Testing process main elements



Testing process main elements



Threat intelligence activity

Defining meaningful scenarios

Providers

Technologies

Integrations

Internet footprint

Vulnerability history

Business context

Users

Contents

Locations

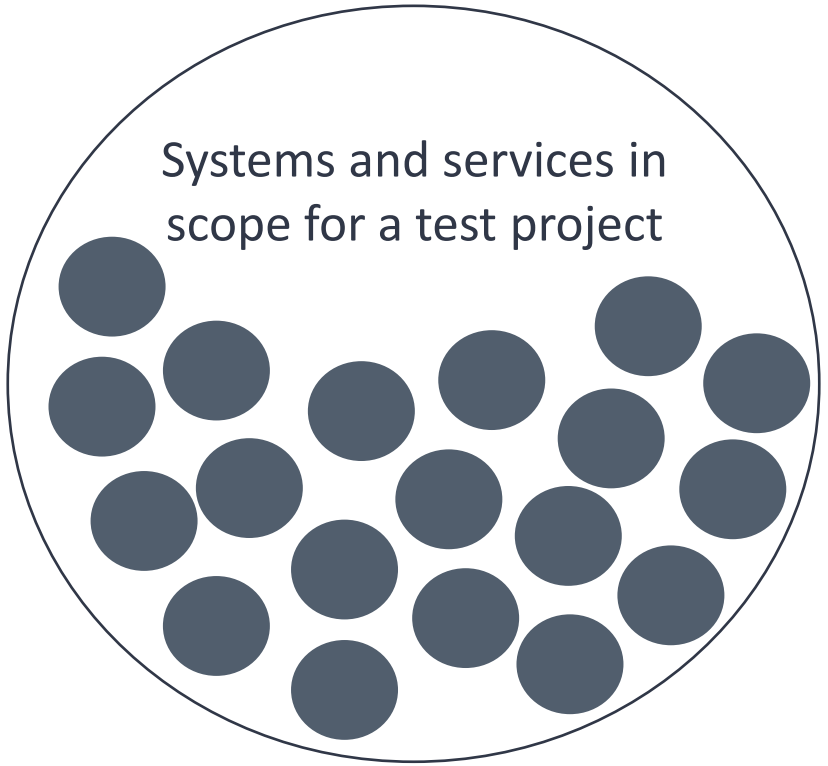
Value for criminals

Defining meaningful scenarios

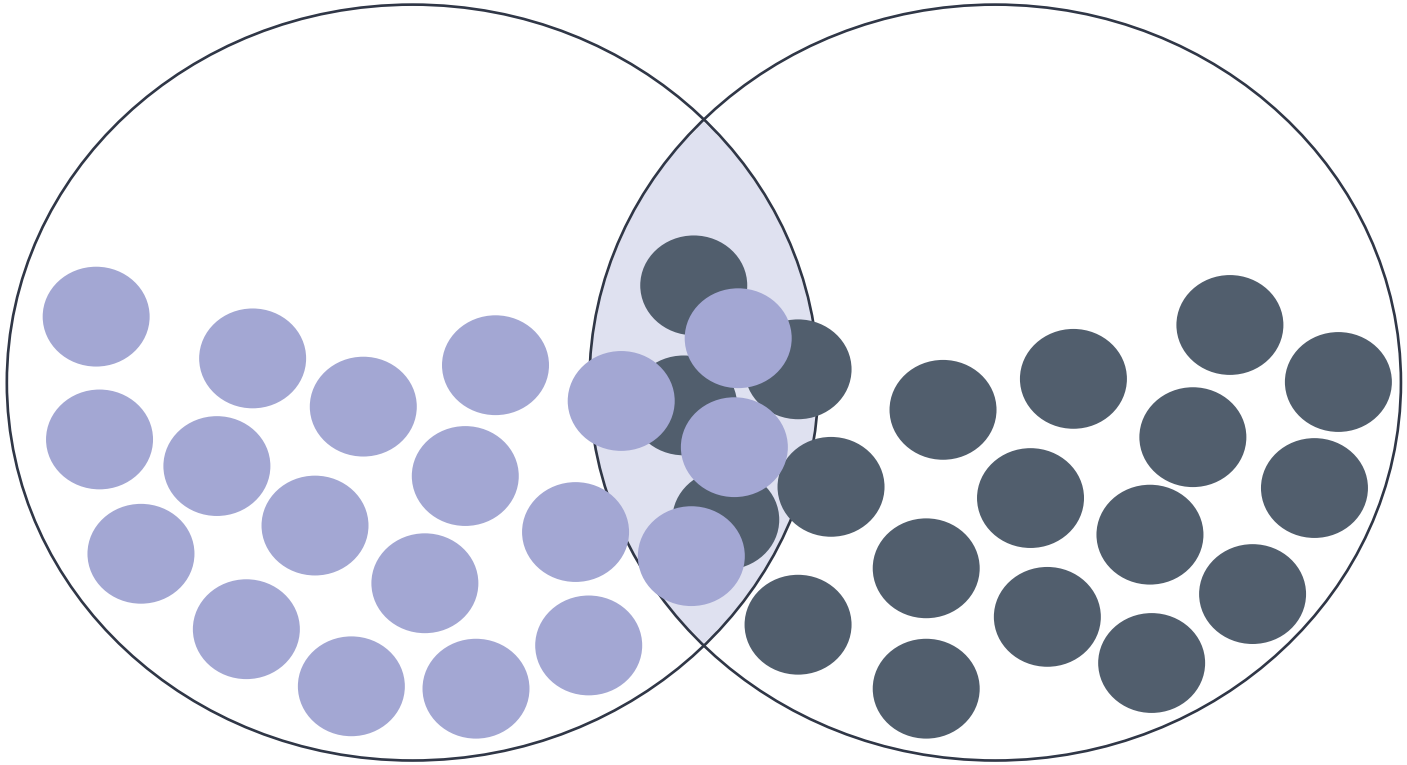
Cyber threat landscape in the financial sector

Systems and services in scope for a test project

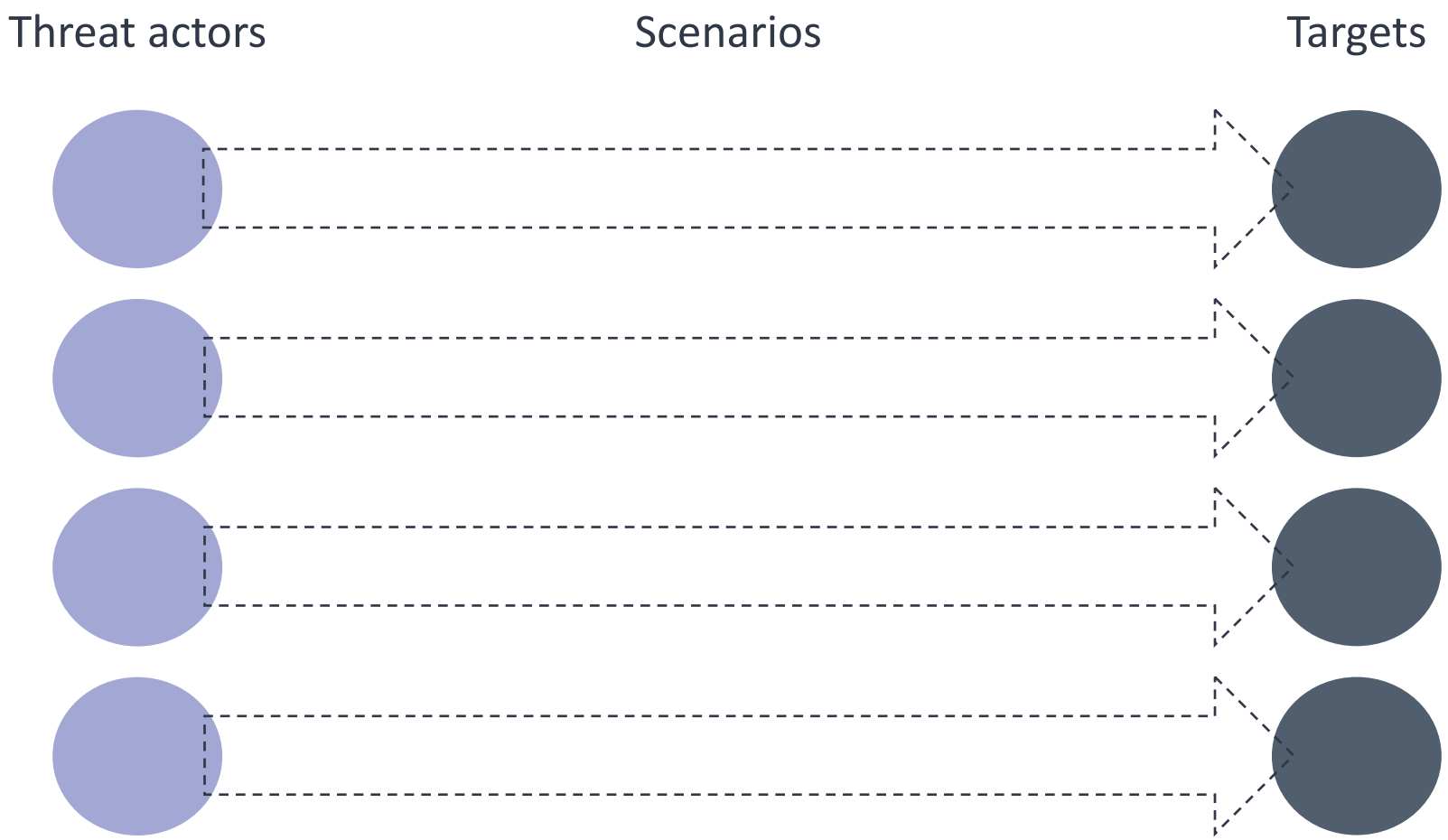
Defining meaningful scenarios



Defining meaningful scenarios



Defining meaningful scenarios

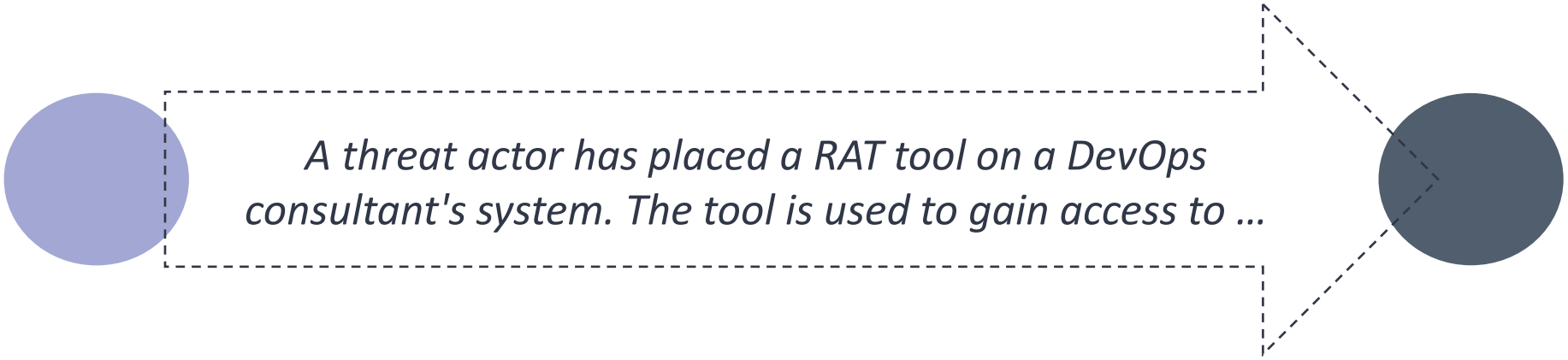


Defining meaningful scenarios

Threat actor description

Scenario description

Flag description



Defining meaningful scenarios

Threat actor description

Attack path TTPs

Flag description

Threat actor descriptions include intent, capabilities, and relevant context.

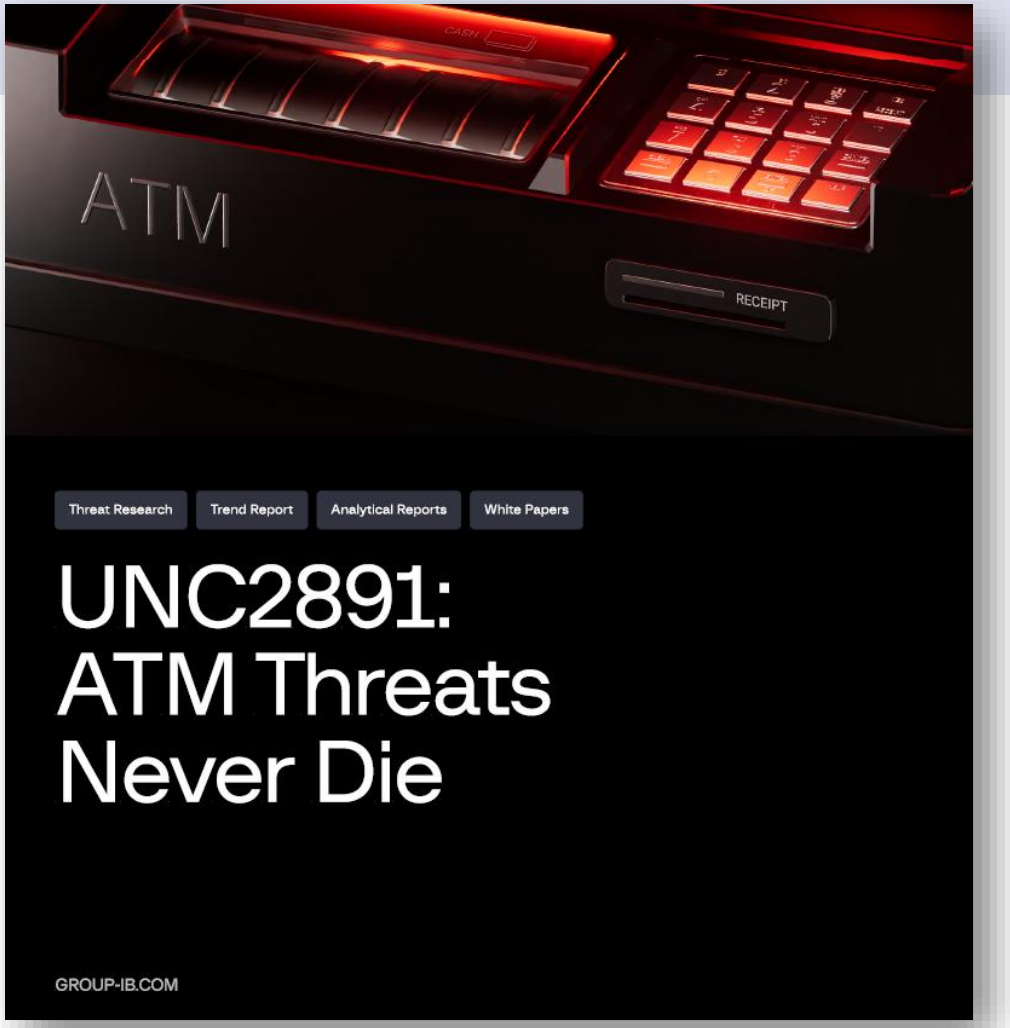
In–Through–Out as in ”The Unified Kill Chain” framework

Flags impact confidentiality, integrity or availability of systems or data.

ATM attacks by UNC2891

ATM attacks as reported by Group-IB in July 2025 and November 2025 reports:

- At least two banks breached in Indonesia.
- At least in one case gained initial access to an ATM network through a device implant.
- Using Linux bind mounts to hide backdoor processes from process listings
- Attempting to deploy a kernel-module to manipulate HSM responses and spoof ATM authorization messages.
- The ultimate goal was enabling fraudulent cash withdrawals from ATMs.



Case: ATM attack by UNC2891

In	Through	Out
Deploy a Raspberry Pi with a 4G modem behind an ATM. Install a rootkit and a backdoor on a compromised server. Use Linux bind mounts to hide backdoor processes from process listings. Set up a persistent C2 foothold from a mail server with internet access. Use DDNS services for C2.	Move laterally towards ATM network servers, install a rootkit and a backdoor on compromised systems.	*Transact fraudulent cash withdrawals.*

The attack was detected and countered before the assumed goal.

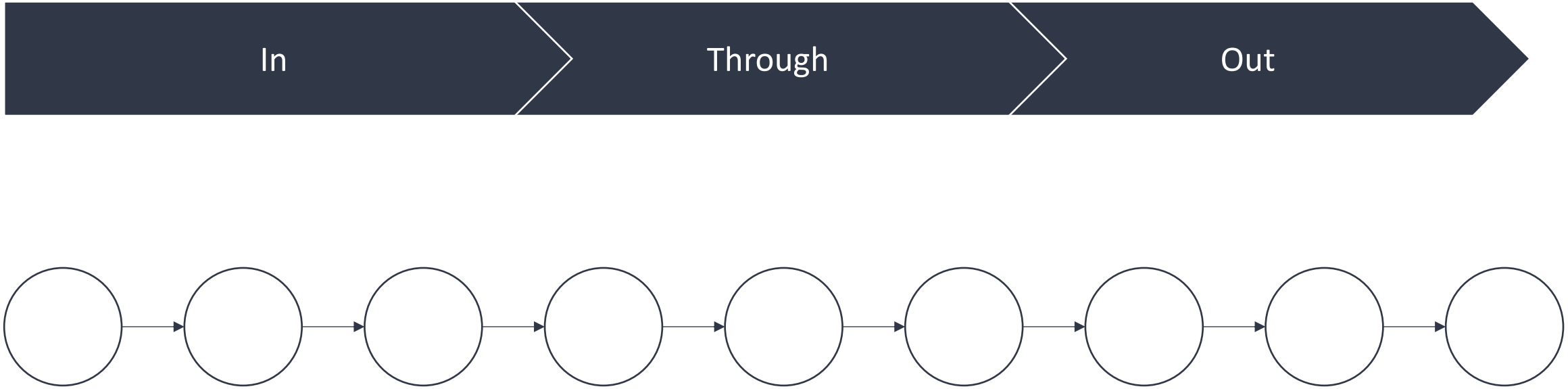
Examples of topical elements in scenarios

- Initial access through a services partner, e.g., an IT consultant.
- Initial access through poisoned open-source software.
- Initial access through a VPN zero-day.
- Initial access through a physical break-in.

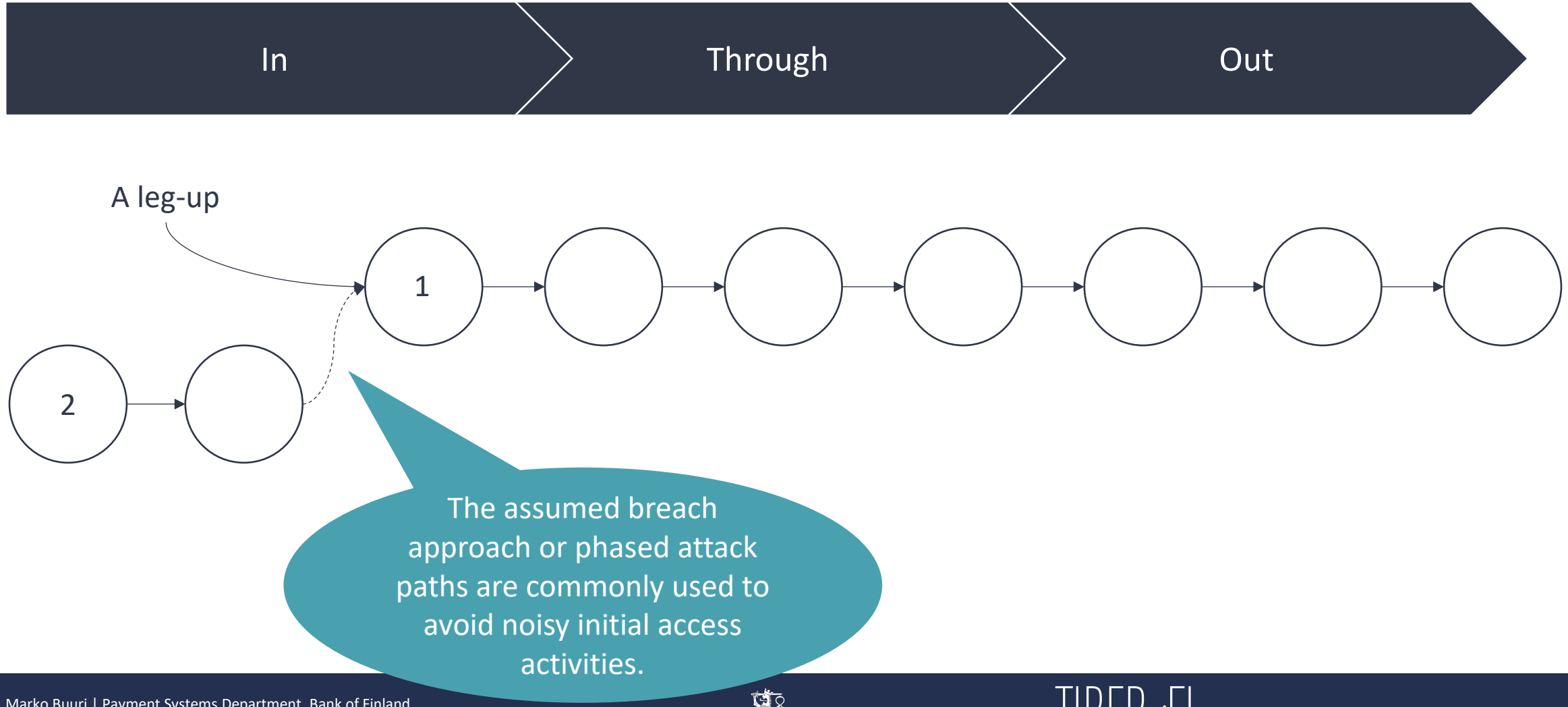
- Targeting systems that deal with payment material and payment messages.
- Targeting opportunities for double-extortion (data exfiltrated and encrypted).
- Targeting on-premises solutions rather than in-cloud.

Red team testing activity

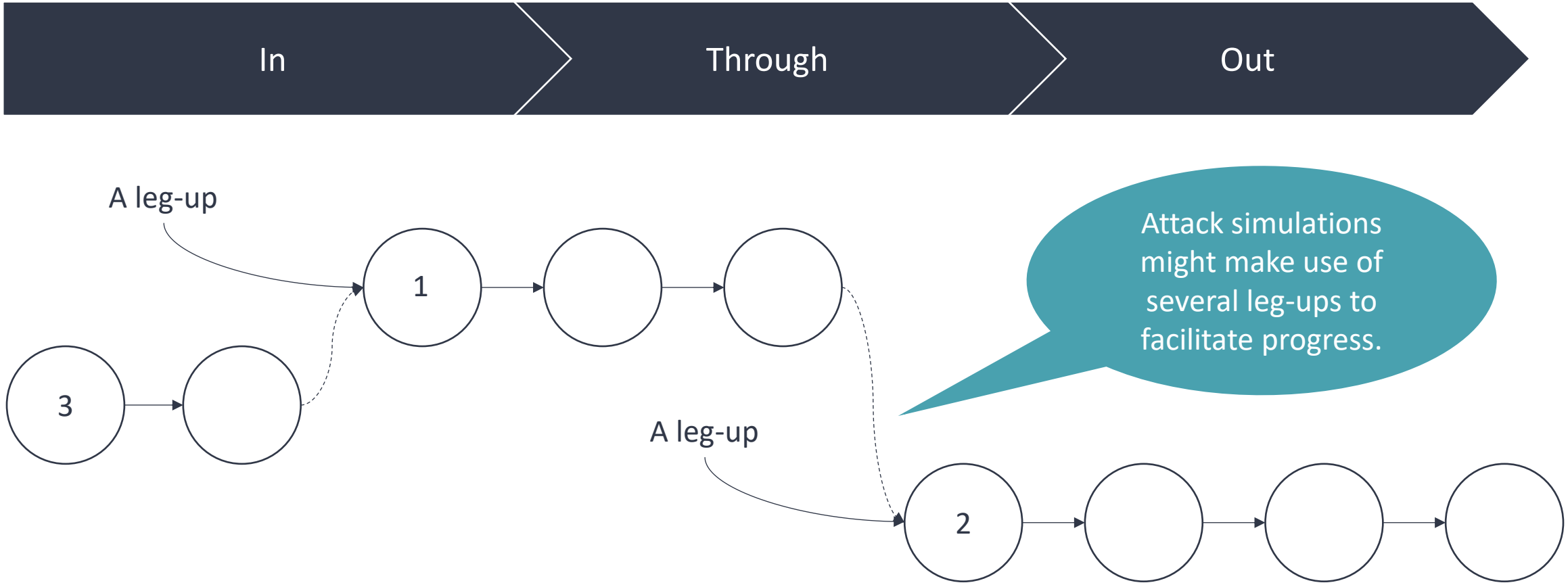
Executing the attack paths



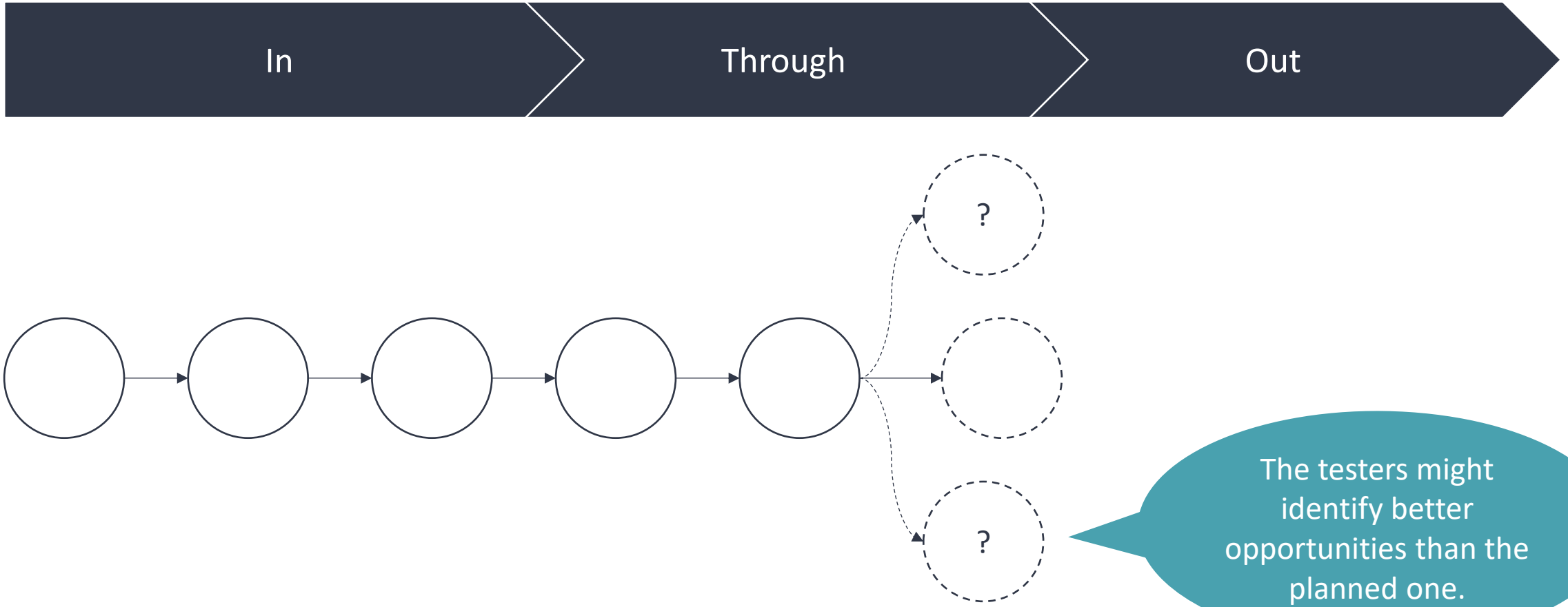
Executing the attack paths



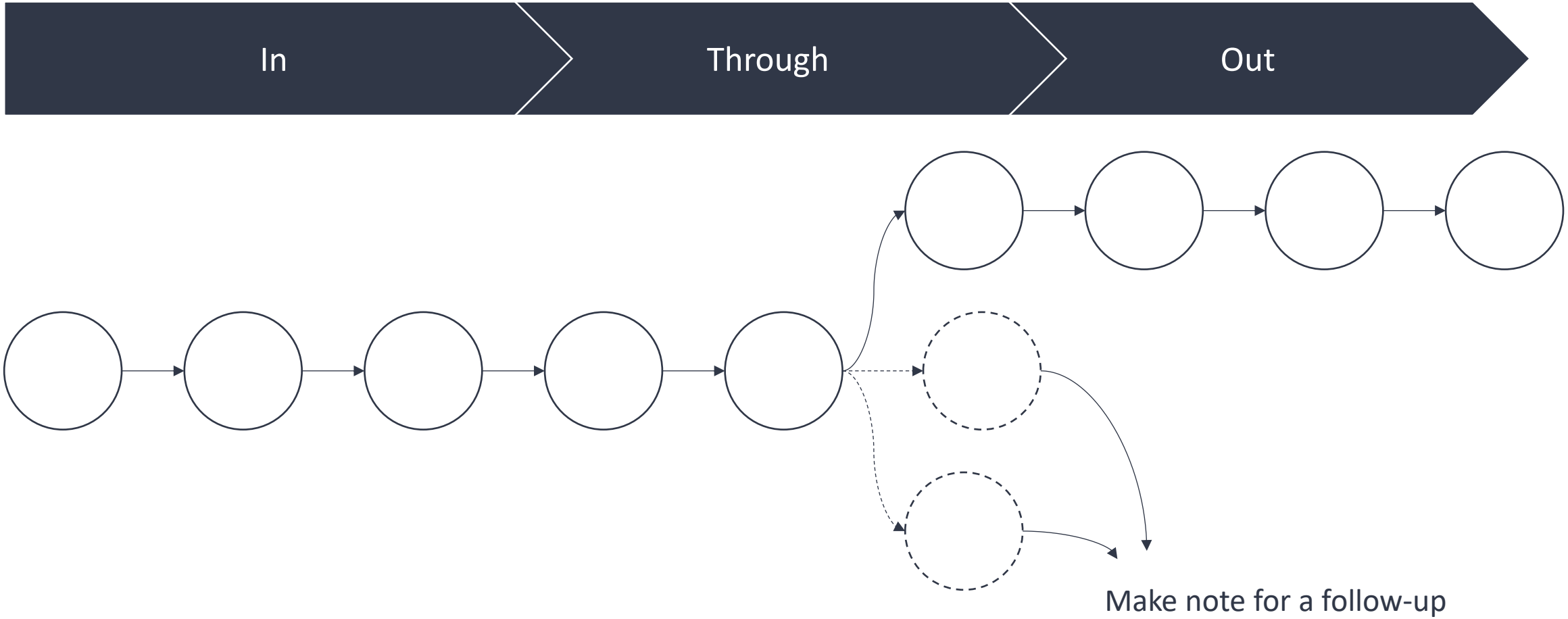
Executing the attack paths



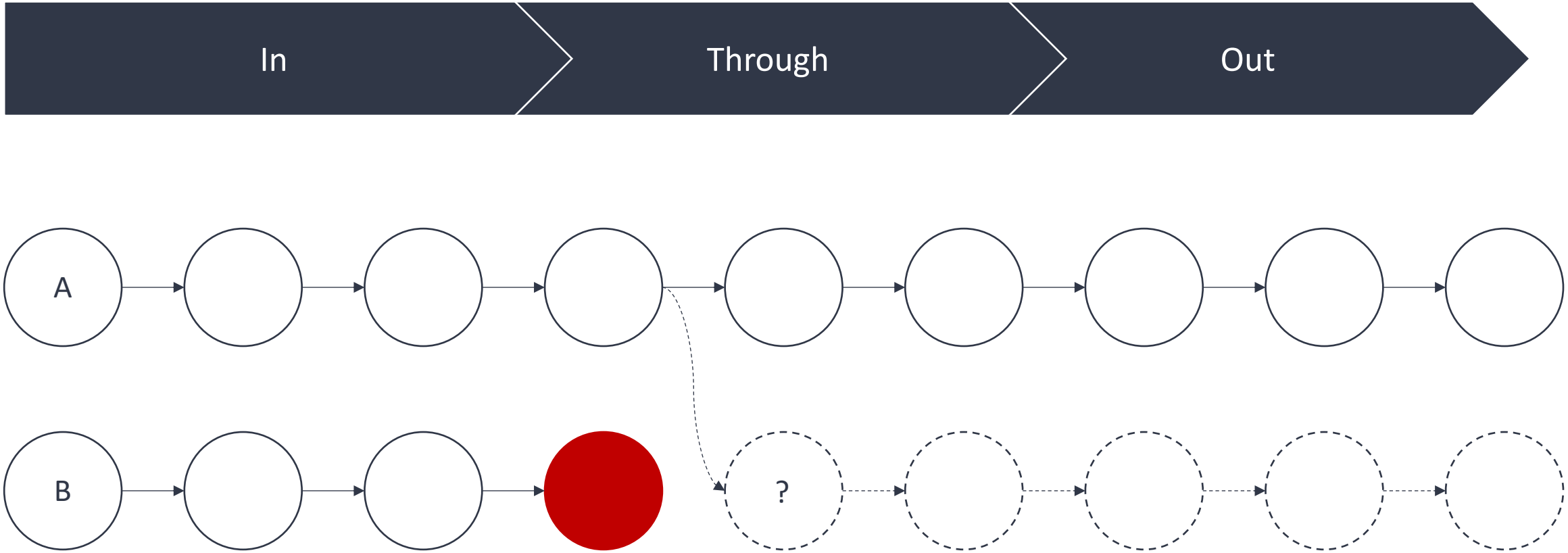
Executing the attack paths



Executing the attack paths



Executing the attack paths



A possible opportunity to resume a prevented scenario.

Common red team blunders – *"It worked in our lab!"*

- Treating the project as a test of your skills and not acknowledging soon enough when it is the time to use a leg-up and move forward.
- Overconfidence in using basic off the shelf tooling with little tailoring, risking detection.
- Underestimating the general level of controls maturity at the financial sector.
- Not communicating clearly enough with the control team about the state of each scenario, the next planned actions, and any support expected.

What happens if the red team gets caught?

- Scenarios must be planned and their execution conducted so that assets in each scenario will provide no investigative leads to the others.

- The control team will need to manage the situation so that the project can remain undisclosed for the other parts, when possible.

- When a project can't resume red teaming, it is possible to pivot to a purple teaming mode to continue testing. Often this is executed so, that the testers continue their planned actions and the security team is asked to only make notes of their detections.

About leg-ups

Why are leg-ups used?

- In projects we are operating with time constrains – actual threat actors would have more time to learn the target environment and plan their next steps.
- The test project is supposed to provide learnings along the attack paths about the protection, detection and response controls – justifies enabling the testers to make progress.
- Some activities are more likely detected in security monitoring than others and might lead to the project being exposed – test first with initial access provided.

Leg-up types

Information leg-ups

- Target clarification
- Technical hints
- Timing information
- Process insights

Access leg-ups

- Network positioning
- Privilege escalation
- Service accounts
- Physical access
- Bypass mechanisms

Difficulties in providing leg-ups

- IT change management processes are nowadays well controlled, which might limit delivery of access leg-ups, when they require configuration changes or new equipment deployments.

- IAM processes tend to be strict in the financial sector entities, making it often difficult to create accounts and to assign them roles with relevant permissions.

What next?

What next?

- Looking to get to this profession?
  - Evaluate the best options for you to develop your skills and get opportunities to join projects that will enable your progression.
  - Seeking professional certifications is probably most beneficial for one's development during early to mid-career.
  - Consider joining a professional red team that you know can help your progression to the next level.
- As a red team tester, you can't skip being an expert in IT technology before being an expert in testing.
  - You will have to be familiar with common enterprise IT, legacy on-prem technologies and modern cloud stacks.
  - Working in an enterprise IT department especially early in the career is valuable experience.
- A lead DORA TLPT red team tester must have 5 years of professional experience minimum per regulation.

Thank you!

marko.buuri@bof.fi
tiberfi@bof.fi

www.suomenpankki.fi/tiberfi

TIBER-FI

SUOMEN PANKKI
EUROJÄRJESTELMÄ
FINLANDS BANK
EUROSYSTEMET