

DORA Threat-Led Penetration Tests

How TLPT operations differ from classical Red Teams
and how to ensure readiness for 2025

Wavestone Insight Day | 2024-04-23

Round table



Jean MARSUALT
Manager



Younes LAABOUDI
Senior Consultant



*900 consultants
worldwide*



*100 auditors
in France*



*20 operators
in France*

**Cybersecurity and
Operational
Resilience**

**Audit & Incident
Response**

**Adversary
Simulation Offer**

Today's agenda

1. **DORA & TLPT: REGULATORY CONTEXT & TIMELINE**
2. **TLPT EXERCISES: OPERATION OVERVIEW AND KEY DIFFERENCES WITH RED TEAM**
3. **2025 READINESS: HOW TO PREPARE IN 2024 WITH WAVESTONE**
4. **Q&A**

A person in a dark suit is seated at a wooden desk, holding a wooden gavel with a brass head. The gavel is positioned over a circular wooden block. The background is slightly blurred, showing a white wall and a stack of papers on the desk. The overall lighting is soft and professional.

DORA & TLPT

Regulatory context

and

timeline

The DORA regulation & Threat-Led Penetration Tests



DORA

Digital Operational Resilience Act

European Union **regulation** aiming to **strengthen** the **financial sector's resilience** to ICT-related major incidents.

Requires



TLPT

Threat-Led Penetration Testing

Engagement which **simulates a realistic global attack** based on the **current threat landscape**, **without** exposing the systems to **malicious impacts**.



Who is concerned?

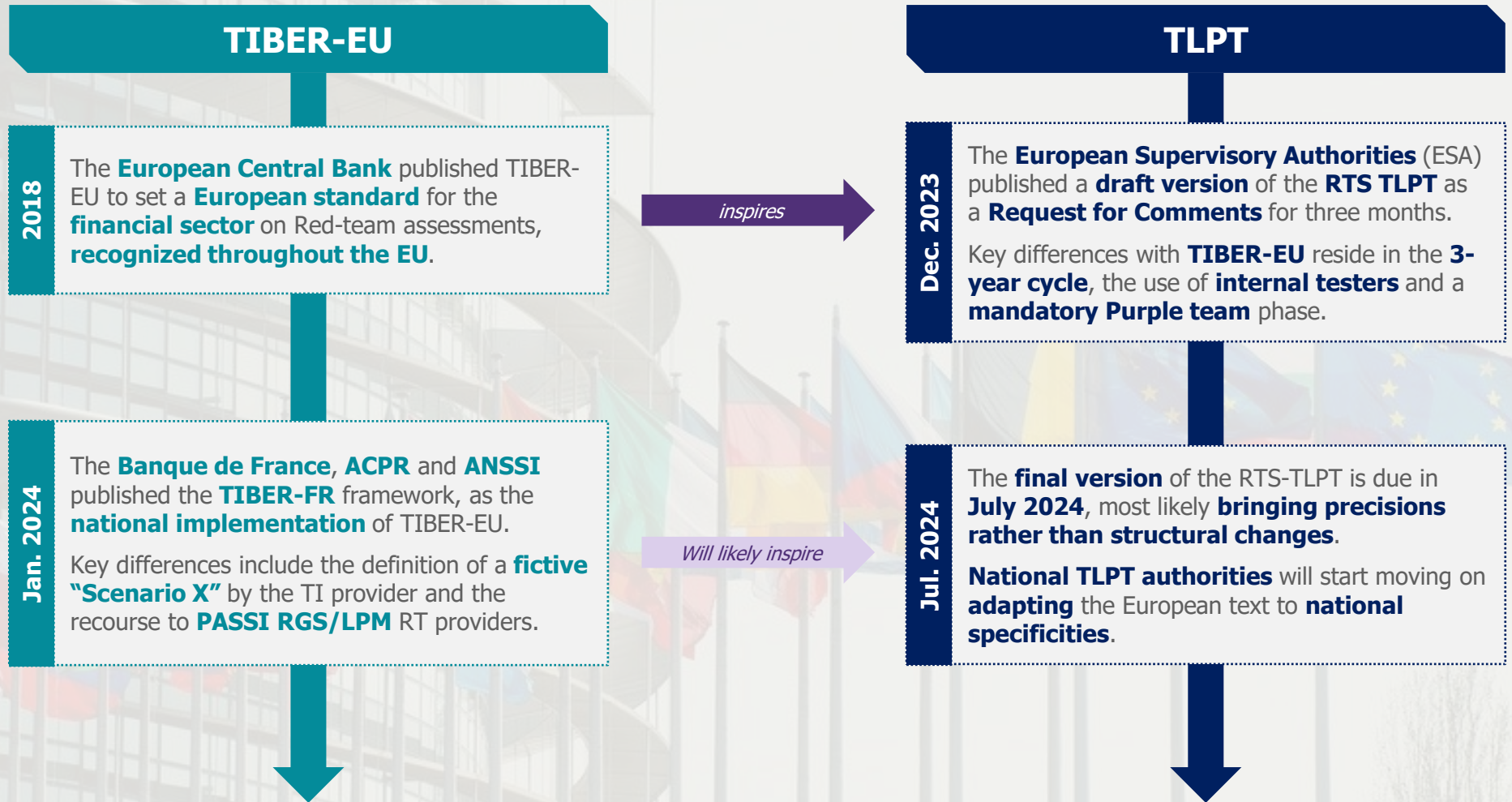
DORA mainly targets the **financial sector** (bank, insurances, etc.), but **TLPT operations** focus on financial entities with:

- / **A notable impact on the financial sector**
- / **Potential financial stability concerns**
- / **A specific ICT risk profile**

These are **guidelines** with ad-hoc **opt-in/opt-out** cases. If you have a doubt whether you are concerned or not, ask the regulators:

tiber-fr@banque-france.fr

TIBER-EU as inspiration for TLPT operations



TLPT exercises

A vintage telescope on a tripod is positioned in the center of the frame, pointing towards the right. The background is a blurred cityscape at dusk or dawn, with a purple and blue color palette. The text is overlaid on the image in white.

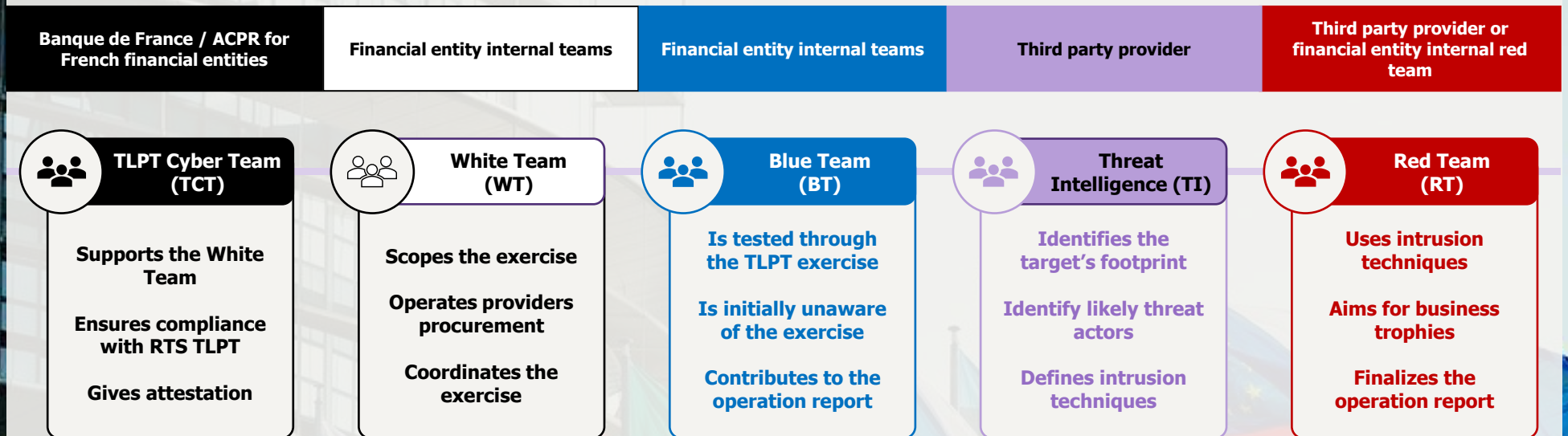
Operation overview

and

Key differences

with Red team

Actors involved in TLPT engagements



Requirements for TI testers

- / Must be **external** to the company
- / Can be the **same provider** as the **RT** given team **independence**
- / Requires **at least 2 people**

Requirements for RT testers

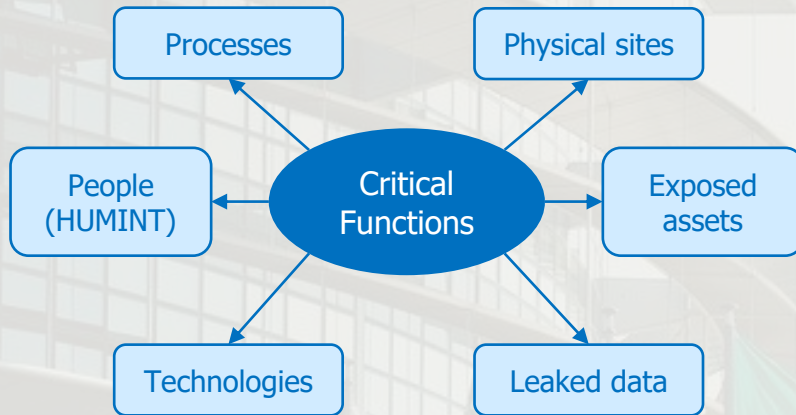
- / Can be **internal** if **hierarchically independent** from Information System Direction & **different from Blue Team**
- / Must be **external every 3 exercises**
- / Requires **at least 3 people**

Overview of a TLPT operation



Intelligence gathering to improve Red Team scenarios

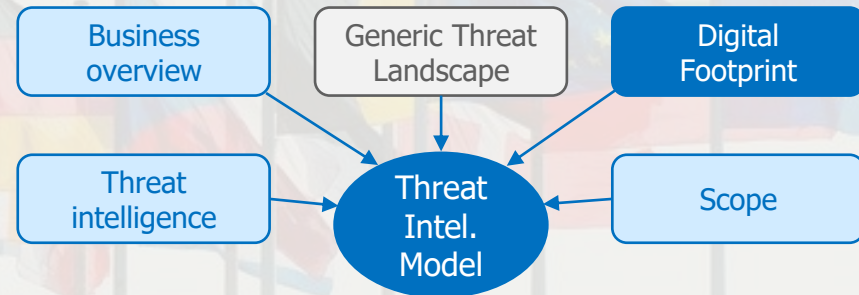
1. Digital Footprint



Identify useful & attractive data on clear web, dark web, with open & closed information sources

2. Threat modeling

Use the financial Generic Threat Landscape and client inputs on business to identify plausible Threat Actors



Techniques, Tactics & Procedures

3. Red Team intrusion scenarios



Significant evolutions from the classical Red Teaming philosophy

Improvable Red Team aspects

Red Team has **too many interpretations**, most often observed as **orthogonal evaluation** of **detection capabilities** as well as **cybersecurity maturity**

Outside of rare Assume Breach cases, there may be **no assessment** of the **internal** security level when **no intrusion vector** is found. Also, **AD is often targeted first**, failing to provide a **clear vision** on the **security level of business processes**

Operations are often **stopped upon detection**, giving **false impressions of security** and the providers goal becomes **stealthiness** rather than evaluation, making it **harder** to define the **Blue team action plan**

Operations are often **constrained** by **low budgets** or **short deadlines**, **increasing** the **risk of detection** or **decreasing** the **depth** of the security **assessment**



With TIBER-EU / TLPT

Operations are **standardized**, offer an **improved approach** to Red Teaming and follow a **clear structure** described in **TIBER-EU framework**

End-to-end testing with advanced **business scenarios** is the main goal, using **leg-ups** to **aid providers** should the target environment be **mature enough**

Detection is an **objective for the Blue team** rather than a **failure** for the Red team, to provide a **clearer picture** of the its **intrinsic capabilities**

Operations are **forced** to happen on a **longer timeframe**, better simulating real-world threat actors with **opportunistic approach** or **advanced tooling**

A woman with dark hair, wearing a red dress, is shown in profile, looking thoughtfully to the left. The background is a soft-focus sunset or sunrise over a body of water, with warm orange and yellow light. The entire image has a semi-transparent purple overlay.

2025 Readiness:

How to prepare

in 2024

with Wavestone

The challenges of Threat-Led Penetration Testing

International presence

- / Segmentation of activities in **multiple countries** and **subsidiaries**
- / Selection of **leading TLPT authority** and compliance with **foreign laws**
- / Relying on **joint TLPT** operations to **limit overload** on internal support teams

Business lines partitioning

- / **Segment** and **scope Critical Functions** to optimize **costs & workload**
- / Identify **global support teams** and **providers** solicited for **each TLPT**
- / **Validate** the testing **strategy** with **regulators** to forecast organization

Continuous testing

- / TLPT as the **final evaluation** and **attestation** of **continuous** efforts
- / **Stable maturity level** requires continuation of **audit & testing activities**
- / **Pentests** on global **infrastructure** & standard **Red Team** also contribute

Working with Wavestone in 2024 to prepare for 2025



DORA & TLPT organization

- / TLPT **Target operating model** & governance definition
- / **Gap analysis** of existing vs TLPT regulatory requirements
- / **TCT emulation** and **WT support**: scoping, trophies, logistics and gap analysis

CONSULTING TEAMS



Service Provider for TLPT operations

- / **Threat Intelligence** provider for TLPT operations aided by **external providers** on aspects tied to **operational CTI**
- / **Red Team** provider for TLPT operations: **TI scenario implementation, technical testing** on external & internal

ADVERSARY SIMULATION



Support to continuous testing

- / **Audit campaigns steering** and/or **technical testing**
- / Penetration testing performed on **business applications**, global **infrastructure** and external **cartography**
- / Standard **Red & Purple Team** operations

AUDIT TEAMS



Questions?

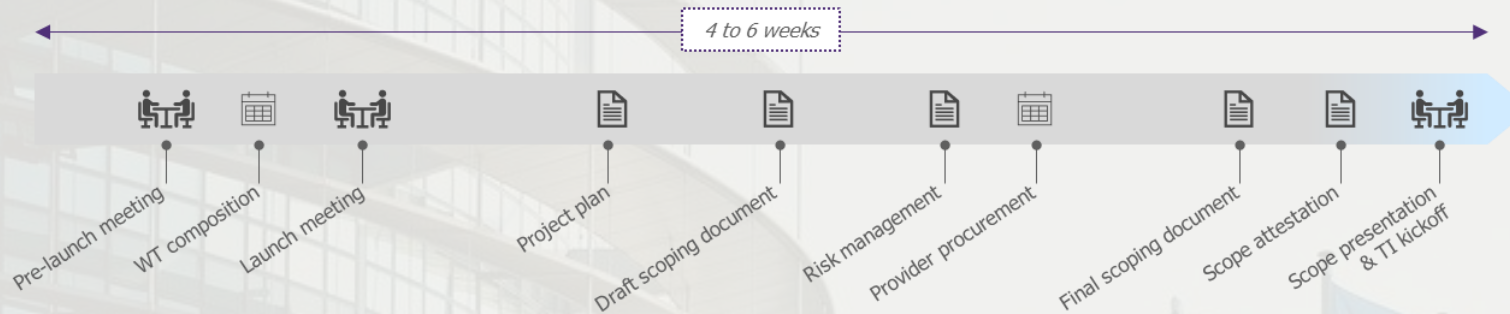


The Positive Way
WAVESTONE

<https://www.wavestone.com>
<https://riskinsight-wavestone.com>

FOCUS: Preparation phase

The goal of the preparation phase is to **prepare** the global operation in terms of **critical functions scoping**, preliminary **risk assessment** and provider **procurement**.



The role of the **White Team** is to:


- / **Organize** the operation
- / **Propose** the operation **scoping** in terms of
 - > Critical function selection
 - > Initial trophies (flag) definition
 - > Optional handling of international components
- / Identify **risks** and **mitigations** inherent to the operation
- / **Draft the procurement** papers (RFP)
- / Issue its **pre-selection of providers**
 - > External provider for the Threat Intelligence
 - > External or internal for the Red Team

The role of the **TLPT Cyber Team** is to:

- / **Support** the **WT** in its scoping definition of the operation
- / **Support** the **WT** in its procurement process
- / **Validate** the final choice of scope and trophies
- / **Validate** the selection of **providers** (in regard to TLPT requirements) and the **optional** recourse to **internal** Red Team testing teams

FOCUS: Threat intelligence testing

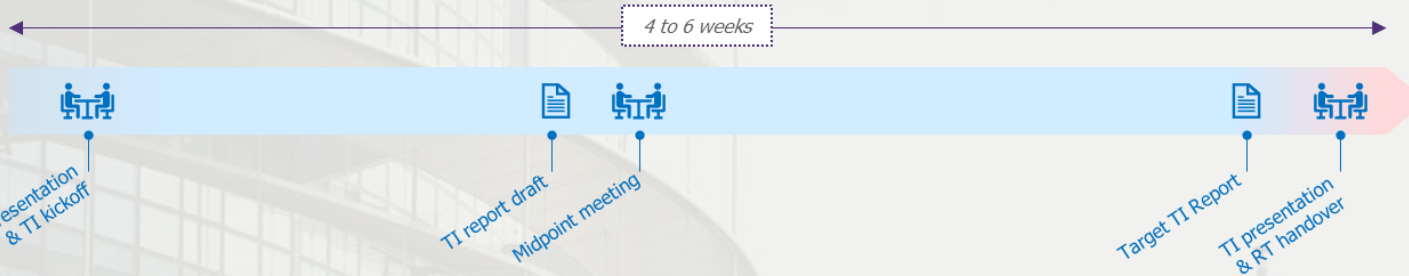
This phase aims to identify the **publicly available information** tied to the target scope, what **Threat Actors** would use them for trophies completion and what their **techniques** are.

 **TLPT Cyber Team (TCT)**

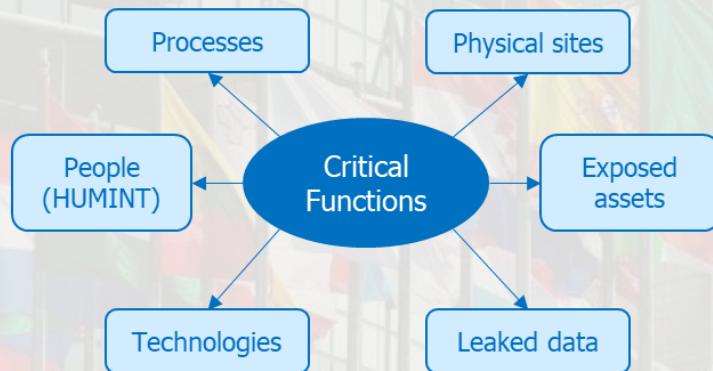
 **White Team (WT)**

 **Blue Team (BT)**

 **Threat Intelligence (TI)**



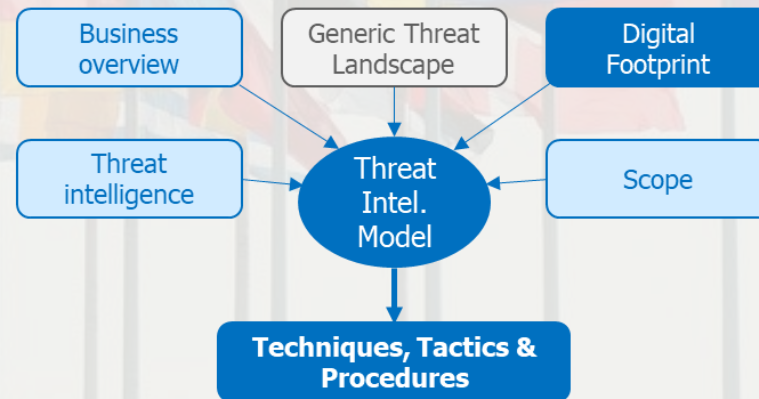
1. Digital Footprint



Identify useful & attractive data on clear web, dark web, with open & closed information sources

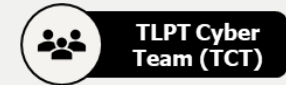
2. Threat modeling

Use the financial Generic Threat Landscape and client inputs on business to identify plausible Threat Actors



FOCUS: Red Team testing

The goal of this phase is to **implement the technical scenarios** defined in the TI phase to **fulfill business trophies** within the **limits** of the Threat Actors' *modus operandi*.



Classical Red Teaming

- > Approach based on **cross-evaluation** of detection capabilities and security level
- > Possibility of being "**stuck**" on the outside if **no intrusion vector** is found
- > Business scenarios are often unlocked after **Active Directory compromise**
- > Operations are often **stopped upon detection** gives **false impressions** of security and the provider aims to **fully evade detection**
- > The **success** of the operation almost **fully relies on the service provider**

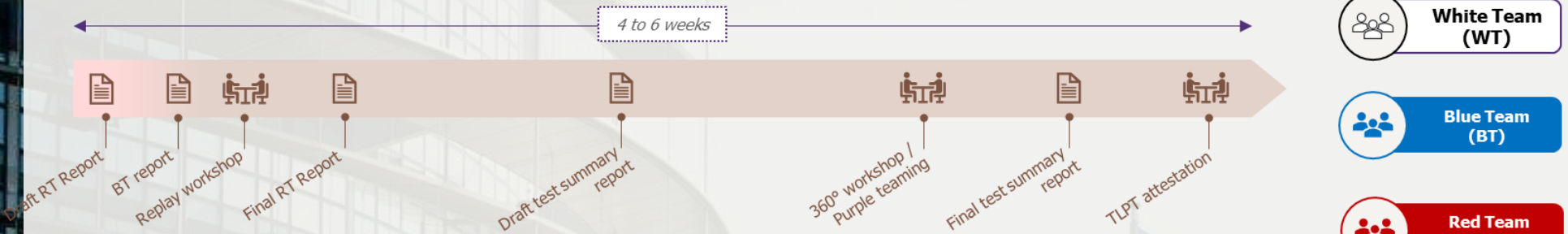







TIBER-EU and TLPT

- > Operations are **standardized**, offer an **improved approach** to Red Teaming and follow a **clear structure** described in **TIBER-EU framework**
- > **End-to-end testing** with advanced **business scenario** is the main goal, using **leg-ups** to aid providers should the client be **mature enough**
- > **Detection** is an **objective** for the **Blue team** rather than a **failure** for the Red team, to provide a clearer picture of the its intrinsic **capabilities**
- > Operations are **forced** to happen on a **longer timeframe**, better simulating real-world threat actors with **opportunistic approach**

FOCUS: Closure phase

This phase aims at **sharing** the operation's results and maximizes their **understanding** and **usefulness** through dedicated **workshops** and **purple team** activities to pave the next steps



-  **TLPT Cyber Team (TCT)**
-  **White Team (WT)**
-  **Blue Team (BT)**
-  **Red Team (RT)**
-  **Threat Intelligence (TI)**

The RTS TLPT offers **4 possibilities** for **Purple Team** activities:

