RegCORE Client Alert

TIBER-EU – Purple Teaming Best Practices: Can the "truth" be found in the middle between red and blue teams?

August 2022

ECB publishes its TIBER-EU – Purple Teaming Best Practices

Can the "truth" be found in the middle between red and blue teams?

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

QuickTake

On 8 August 2022 the European Central Bank (**ECB**) published its "Purple Teaming Best Practices" (**Best Practices Publication**),[1] outlining how purple teaming (**PT**) can be set up and managed within the European framework for the ECB's threat intelligence-based ethical red teaming (**TIBER-EU**) process.

The PT Best Practices Publication complements the TIBER-EU framework, originally released in May 2018.[2]The TIBER-EU framework sets out a controlled and tailored testing approach to increase the resilience of digital networks of financial service firms and the entire financial services sector across the EU. The TIBER-EU framework is based on the following three phases (a) preparation, (b) testing and (c) closure.

This Client Alert and its coverage of the PT Best Practices Publication should be read in conjunction with the following EU RegCORE Client Alerts:

- Revisiting the ECB's 2018 framework on testing cyber-resilience and combatting digital financial crime (published September 2021);
- Revisiting the ECB's rules for selecting service providers for cyber-resilience testing (published September 2021); and

[1] Available here

[2] Available here.

- Revisiting the European Central Bank's cyber-resilience oversight expectations (CROE) (published December 2021) which provides a further framework of supervisory expectations that co-exists with the TIBER-EU testing framework and which will continue to apply, possibly with amendments when the EU's Regulation on digital operational resilience (DORA) comes into force.

In August 2020, the following documents were published by the ECB:

- the TIBER-EU Attestation Template;
- the TIBER-EU Guidance for Targeted Threat Intelligence;
- the TIBER-EU Guidance for the Red Team Test Plan; and
- the TIBER-EU Scoping Specification Template.

In September 2020, the ECB further published the following two documents that are relevant for use during a TIBER-EU closure phase:

- the TIBER-EU Guidance for Red Team Test Report; and
- the TIBER-EU Guidance for Test Summary Report.

Each of these ECB publications have in some (but not all) EU jurisdictions, been supplemented by further guidance from national competent authorities (**NCA**s). Consequently, certain national specifics may also apply to how TIBER-EU testing is run in those jurisdictions and how NCA's supervisory expectations are applied. A number of jurisdictions outside of the EU have also built or are building similar frameworks to that of TIBER-EU. One such example is the Bank of England's CBEST Intelligence-Led Testing framework, which while sharing conceptual similarities to the aims of TIBER-EU, also has its own specifics in what is required. A number of financial services firms that are expected to comply with TIBER-EU may have to comply with similar testing regimes in other jurisdictions and comparisons of testing experience and findings from differing tests can be useful in their own right for the tested entity but also the regulatory authorities.

Recap: How does TIBER-EU work?

TIBER-EU testing activities enable European-level and national authorities to work with financial infrastructures and institutions to put in place a program for controlled, bespoke tests that are based on realistic and genuine cyber-attacks.

The testing involves both a "red team" (**RT**), functioning as the offensive attacker team, and a "blue team" (**BT**), acting as the defensive operator team, as well as a "white team" (**WT**), which monitors the test and carries out a risk assessment. An in-depth analysis of the structure and functioning of TIBER-EU tests are provided in a separate EU RegCORE Client Alert that can be found here.

Importantly the ECB's TIBER-EU framework publications and the PT Best Practices emphasise that:

> "Conducting tests on live production systems underpinning critical functions contains an inherent element of risk of disruption, such as denial-of-service, unexpected system crash, damage to critical live production systems, or the loss, modification or disclosure of sensitive data. Every effort is therefore made to minimise these risks and to ensure that these tests are conducted in a controlled manner."

Given these risks, the TIBER-EU framework, the WT conducts a risk assessment prior to the test and maintains active and robust risk management controls, that it monitors and adjusts during the testing process.

Choosing the right RT, BT and WT members is crucial to the success of a test as well as to minimise adverse risk and disruption. Since the introduction of the TIBER-EU framework, the ECB has further specified certain parts of and steps in the testing process, e.g., through the publication of the "TIBER-EU Framework Services Procurement Guidelines" (the **Procurement Guidelines**). This publication sets out rules on selecting and commissioning of service providers. We have discussed the requirements of the Procurement Guidelines and the ECB's expectations in our Client Alert available here.

With more than 75 TIBER-EU tests having been performed across different EU sectors and jurisdictions, stakeholders have pointed out the need for further instructions on how PT as an activity should be incorporated into the TIBER-EU process.[3] The ECB complied with this request and suggested specific PT Best Practices, which are discussed in this Client Alert.[4] Further publications may also be made available by the ECB (including from its TIBER-EU Knowledge Center) and from the NCAs.

[3] Find corresponding press release here.

[4] Note that these Best Practices serve as guidance only and can be used on a voluntary basis.

Purple Teaming – in between attacker and defender

- **What is Purple Teaming?**

In the context of TIBER-EU tests, PT refers to the collaborative activity between the RT simulating a cyberattack and the BT defending the entity being tested. A PT is not designed to replace the red-teaming nature of the TIBER-EU test but aims to enhance the collaboration between the RT and BT in certain circumstances and to increase the learning experience derived from that test.

- **Why incorporate Purple Teaming?**

The PT Best Practices answer the question of why PT should be used by stating that such PT activity supports the adoption of an exploratory mindset, which allows the BT to gain a better understanding of the strengths and weaknesses of its protection and detection capabilities. The overall aim of PT is to maximise the value of learning experience for the entity undergoing the TIBER-EU test and thereby improving the tested entitiy's capabilities to deal with potential cyber risks.

Furthermore, the PT contributes to increasing a tested entity's understanding of threat actors' tactics, techniques and procedures (**TTP**s). It supports the tested entity in identifying remediation actions and implementing appropriate mitigation measures.[5]

- **When to implement Purple Teaming?**

The ECB's PT Best Practices can be used by participants and teams involved in a TIBER-EU test to gain more expertise on how PT may be used in different phases[6] of the TIBER-EU process. Stakeholders involved in PT are the TIBER Cyber Team (**TCT**), the Threat Intelligence (**TI**) provider along with each of the WT, RT and BT. Definitions and further explanations regarding the roles of the different teams can be found under section 2.5 of the PT Best Practices Publication.

Specifically, PT activity may be implemented during the following phases of the TIBER-EU process:

(1) in the testing phase (however, recommended to only used as a last resort, when circumstances arise leading to a situation in which the TIBER-EU test would otherwise end prematurely); and

(2) in the closure phase (used to enhance the "mandatory replay workshop" – a stage that is highly recommended by ECB).

(1) Purple Teaming in the testing phase

Rationale

It takes a considerable amount of effort to perform a TIBER-EU test. Therefore, invalidation of a test should be avoided unless the test fails to meet the requirements and outcomes of the TIBER-EU framework. However, unexpected circumstances may arise that force stakeholders to act in a certain way to keep the balance between the goal of maximising the learning experience and the interpretation of the framework.

In such situations, it may be prudent to include a PT during the testing phase so that the test can be continued, and the ultimate goal of learning experience can be achieved. In doing so, the attack scenario should also be re-evaluated so that it fits the PT while reflecting the TTPs. Since a PT does not come into play for all unexpected circumstances, each situation must be assessed individually prior to implementing PT as a practice.[7]

The following graphic is Figure 1 as set out in the ECB's PT Best Practices publication.

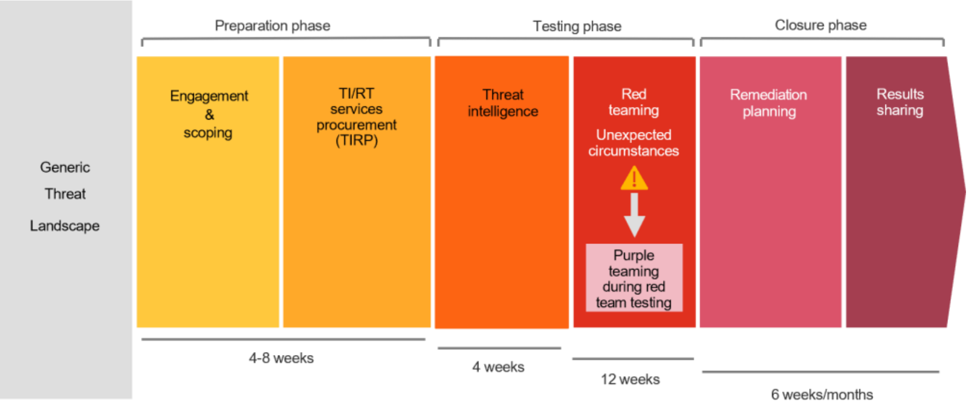
[5] Find corresponding press release here.

[6] Further information on the phases of the TIBER-EU process is laid out in section 4 of the TIBER-EU Framework.

[7] Section 3.1 of the PT Best Practices Publication.

Indicative PT timeline in the testing phase

Process: circumstances leading to purple teaming during testing phase



Circumstances leading to a PT's involvement

It is up to the TCT to evaluate each case, in close dialogue with the WT, RT and TI providers, and then to decide whether PT is an option or if there is another option like for example pausing the test.

However, some circumstances might indeed inevitably lead to PT arising, notably:

- if the BT has discovered RT actions, so that the test has been exposed. In such cases, a PT does not have to be introduced in every situation; if it is possible, a cover story can be used, for example.
- situations where it is likely that significant disruption could occur from the emulated attack;
- if there is a real cyberattack occurring at the same time that needs to be prevented;
- if there is a high probability that the uninformed BT will overreact, which could have a bad effect on the systems. This reaction may not be appropriate in the context of the TIBER-EU test but would be in the case of a real attack. However, the BT in this situation has no way of knowing whether its reaction is appropriate;
- to avoid situations where the BT does not react as it normally would because it suspects the attack is not real; and
- if, due to the perceived seriousness of the incident, the BT involves external parties, such as the police, government agencies or financial institutions.[8]

Minimum requirements of PTs during the testing phase

The main reason why a PT should be included in the testing phase is if there are or potential or actual circumstances leading to a situation that is beyond the control of the WT, RT and TCT. In every case it needs to be discussed, if PT should be included and when. The Best Practices Publication suggests the following points should be considered as part of that discussion, namely whether:

- the WT is proposing a PT and specifying the exact objectives and its scope;
- the TCT agrees to the PT and all other points as well;
- the test continues to be administered in accordance with the spirit of the TIBER-EU's overall framework (i.e., the PT should be considered an option of last resort and not as a relaxation of TIBER-EU requirements) and the focus on maximising the learning experience and outcome for the tested entity;
- the WT liaises with TI and RT providers (as necessary) to adapt existing scenarios or implement alternative scenarios to maximise the value of the test for the tested entity;
- to agree to expectations regarding the outcome, communication channels, response and recovery activities, confidentiality boundaries, start and end dates, escalation paths, allocated resources (including budget), and reporting formats to be introduced; and
- the PT outcomes will be clearly documented and form an integral part of the recovery plan.[9]

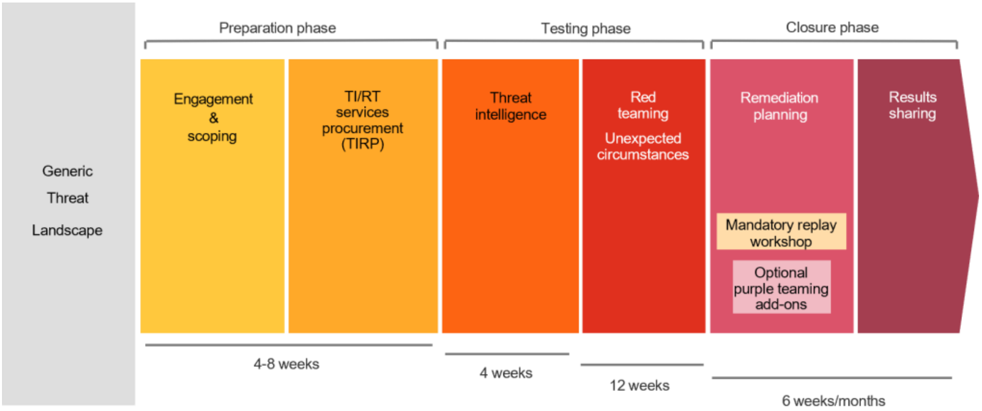
[8] Section 3.2 of the PT Best Practices Publication.

[9] Section 3.3 of the PT Best Practices Publication.

The following graphic is Figure 2 as set out in the ECB's PT Best Practices Publication.

Indicative PT timeline in the closure phase

Process: Normal TIBER-EU flow with optional purple teaming during replay



(2) Purple Teaming during the closure phase

Rationale

In the closure phase of a TIBER-EU test, a PT should be conducted in addition to the "mandatory replay workshop". Applying a PT at this stage may help improve RT and BT collaboration, as well as improve learning opportunities, defensive capabilities, and the return on investment of the test.[10]

Planning

The ECB states that a PT should best occur between the delivery of RT and BT reports and the replay workshop, which ensures that the information obtained is still fresh. The duration and scope of PT should be customised for each test. However, care should be taken in selecting the appropriate PT type to strengthen BT and RT cooperation as well as the effectiveness of defensive controls put in place to protect against offensive actions.[11]

Results

Limitations such as detection by BT are not supposed to not exist for a PT in the closure phase. In addition, PT's expert knowledge should be used directly, leading to a deeper understanding of the events. PT results should also be used to improve processes and planning and strengthen the organisation's cyber resilience overall.[12]

Types of Purple Teaming

Not only can a PT be implemented during different phases of the TIBER-EU process, but there are also different types of PT that vary in their purpose, form, level of BT involvement and specificities and thus intended learning experience.

Due to the individuality of each TIBER-EU test the implementation of a certain type of PT depends on the specific needs and conditions of the TIBER-EU test overall and careful consideration should be taken when setting what PT approach to apply when and how. The following table lists potential types of PT which might be used alone or in combination.[13]

[10] Section 4.1 of the PT Best Practices Publication.

[11] Section 4.1 of the PT Best Practices Publication.

[12] Section 4.3 of the PT Best Practices Publication.

[13] Section 5 of the PT Best Practices Publication.

Types of Purple Teaming approaches	
(1**) Testing Phase**[14]	**(2) Closure Phase**[15]
1.1 *Catch-and-release* • Useful for testing an entity’s defensive capabilities when there have been repeated detections by the BT during the final stage • Initiated by revealing to the BT that a test is being performed and installing a communication channel between the RT, BT and WT • The BT uses this channel to report the detected Indicators of Compromise (**IoC**) to the RT • If the identified IoCs are confirmed to be part of the TIBER-EU test, the BT will then perform the agreed measures to allow the test to continue	2.1 *Alternative scenario: tabletop discussion* • Allows a less technical audience (e.g. management) to be included in the discussion • Enables an investigation of alternative attack vectors and a discussion or simulation of the “what ifs” without a strict focus on technical systems • Facilitate an 360° view of the wider aspects of an entity’s security • Possible ways of carrying out a tabletop discussion include: a) a role play to simulate alternative offensive and defensive measures and their consequences b) the theoretical evaluation of scenarios that are closely related to the TIBER-EU test c) the simulation of potential consequences reaching far beyond the test d) the inclusion of senior management
1.2 *Collaborative proof-of-concept* • Useful to provide evidence of a weakness discovered during TIBER-EU tests in situations where practical testing on the production systems by the RT alone is not feasible • Collecting all the evidence required to illustrate the feasibility of a certain attack vector without actually fully performing the attack • This might include a theoretical discussion of the expected outcome as well as a practical test of partial aspects of the attack • Close cooperation between RT and BT is required to consider all offensive and defensive aspects of an attack	2.2 *Re-exploration of planned scenarios on live systems* • Enables a combination of the expertise of the RT and the BT to practically show the offensive and defensive potential of an attack step or attack chain • While being quite resource-intensive, it can deliver highly comprehensive learning experience for the BT • Particularly helpful in cases, where the BT struggled to detect RT activities during a test • Running through a chosen attack step by step can include: a) walking through an RT activity that was not visible in the BT logs during testing phase b) walking through an RT activity that was not visible in log entries, but the malicious activity was not detected by the BT during testing phase c) walking through an RT activity that triggered an alert during testing but was not triaged properly d) walking through an RT activity that triggered a defensive response that effectively closed the attack but was unable to prevent the attackers from meeting their objectives
1.3. *War game* • Might be suitable when the TIBER-EU test is known to the BT at a very early stage	2.3 *Alternative scenario: exploration on live systems* • Various tested attack scenarios can often not be comprehensively evaluated during the testing phase due to time and other constraints

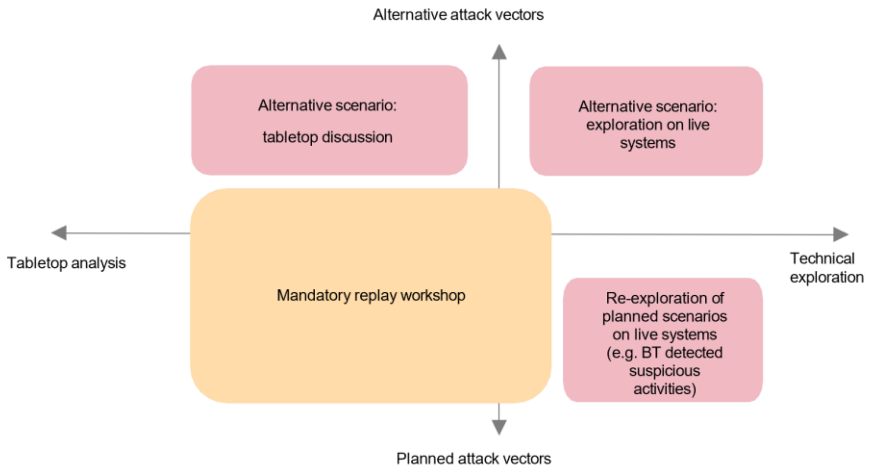
[14] Section 5.1 of the PT Best Practices Publication.

[15] Section 5.2 of the PT Best Practices Publication.

• RT and BT are fully aware of each other's respective goals • Different from a normal TIBER-EU test, during a war game the BT knows what the RT flags are; flags are strategically placed in systems underpinning critical functions	• These attack vectors can then be explored during the closure phase in collaboration with the BT • Alternative scenario explorations on live systems can include: a) a technical exploration of attack scenarios deviating from those conducted during testing phase; b) a technical exploration of attack scenarios applied to alternative target environments (e.g., execution in a Citrix environment instead of on a company laptop); c) proof-of-concept (e.g., scenarios not conducted during testing due to a high risk of BT detection or system damage); d) a technical exploration of novel TTPs which have emerged but could not be tested on the technical system during testing phase

The following graphic is Figure 3 as set out in the ECB's PT Best Practices Publication.

Types of PT in the Closure Phase


Alternative attack vectors
Alternative scenario: tabletop discussion
Alternative scenario: exploration on live systems
Tabletop analysis
Mandatory replay workshop
Technical exploration
Re-exploration of planned scenarios on live systems (e.g. BT detected suspicious activities)
Planned attack vectors

Outlook and next steps

As discussed above, an implementation of PT in the TIBER-EU process aims to support the maximisation of the learning experience and outcome of TIBER-EU tests and the ECB is of the view that using a PT appropriately is highly recommended to further those aims. While the ECB's Best Practices provide detailed instructions when and how to make use of PT, it still needs to be discussed on a case-by-case basis prior to an implementation in a TIBER-EU test. This is especially the case so as to ensure a non-disruptive safe testing environment for the tested entity generally but also that entity's business as usual engagement with counterparties, clients and customers for its regulated activity (in particular critical economic functions – if any) are not disrupted in an adverse manner. Evaluating such risks will likely also require the input from various control functions within the financial services firm being tested, including from a governance, risk, compliance and legal perspective.

Ultimately, a controlled wall-crossing of information barriers between the RT and BT and fostering controlled collaboration between those teams in special circumstances may increase the overall learning experience and make the outcome of TIBER-EU tests more valuable to the tested entity. When the red and blue teams meet in the middle to form a joint purple team, this provides new insights into strengths and weaknesses of the testing process and might eventually lead to finding the "truth", i.e., the detection of core cyber-resilience issues of the tested entity.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these proposals.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's EU RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com

In this document, "PwC Legal" refers to PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft, which is part of the network of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.

www.pwclegal.de