EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Purple Teaming Best Practices

July 2022

Contents

1 Introduction

The TIBER EU Purple Teaming Best Practices describe Purple teaming. Purple teaming is a collaborative testing activity that involves both the offensive attacker team (red team) and the defensive operator team (blue team) within a TIBER-EU test and aims to complement a TIBER-EU test in specific situations, like when a test could impact the production system or to reap further benefits when closing a TIBER-EU test.

The TIBER EU Purple Teaming Best Practices complement the Threat Intelligence-based Ethical Red Teaming (TIBER-EU) Framework, which enables European and national authorities to work with financial infrastructures and institutions to put in place a programme for controlled, bespoke tests that are based on realistic and genuine cyber threats. These tests, conducted on entities' critical live production systems, mimic the tactics, techniques and procedures of real-life threat actors with a view to improving the entities' resilience against sophisticated cyberattacks.

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. For this reason, the TIBER-EU Framework requires the White Team to conduct a risk assessment prior to the test and to put in place active and robust risk management controls, as well as monitor and adjust these controls as needed during the testing process.

These best practices for purple teaming are derived from the experience gained from numerous tests conducted under the TIBER-EU process across several jurisdictions. These insights strongly indicate the need to recognise where purple teaming could be performed in the TIBER-EU process

These best practices provide information about purple teaming in the context of the TIBER-EU Framework and can be used on a voluntary basis; they serve as guidance only and are not intended to address the specific circumstances of any particular individual or entity. They do not constitute professional or legal advice.

1.1 Purpose of this document

This document provides guidance on how purple teaming might be used in the testing and closure phases of a test conducted under the TIBER-EU process. It sets out to define what purple teaming is, together with its main principles, use cases and its potential types.

Target audience

These best practices are mainly intended to provide guidance to national TIBER Cyber Teams (TCTs), threat-intelligence (TI) and red-team (RT) providers and entities that are undergoing or planning to undergo TIBER tests, although they may also have a broader audience.

1.2 What is purple teaming?

Purple teaming (PT) is a form of collaborative activity that involves both the Red Team (RT) and the Blue Team (BT) in a TIBER-EU test and their corresponding offensive and defensive actions. Among other things, this can include insights into particular attack phases, detections, defensive actions and test reports. This increased collaboration helps to expand knowledge on the threat actors' tactics, techniques and procedures (TTPs), prevent certain risks and to identify areas and actions that can be improved at people, process and technology level. It also helps to actively pinpoint weaknesses in protection and detection capabilities so that they can be addressed and incorporated in the remediation plan. Such collaborative PT may be undertaken in various ways, ranging from desktop discussions to full-scale testing exercises.

PT is not intended to replace the red-teaming nature of a TIBER test, during which, to achieve realistic testing conditions, the test is kept confidential and the BT is unaware of the activities of the RT. Rather, it is **intended as a collaborative activity** in particular circumstances, to increase the learning experience of the test. In PT, the BT of the entity undergoing the test may be partially or fully aware of the ongoing test and possibly even cooperate with the RT during execution.

Specifically, PT can be used during the following phases in the TIBER-EU process:

In the testing phase, it is used as a last resort when circumstances arise and only once all other options have been exhausted, subject to a proposal from the White Team (WT) and the non-objection of the TCT. It can serve as a response to continue or unblock a TIBER testing phase in a situation where the test would otherwise end prematurely. In such cases, PT is considered to be of limited scope and is conducted to supplement specific parts of the attack scenarios, with the sole aim of maximising the value of the test and the return on investment in terms of learning opportunities. The reasoning and rationale put forward by the WT to continue the TIBER test requires careful assessment by the TCT to ensure alignment with the TIBER-EU requirements and the spirit of the framework. Potential types of PT during the testing phase are described in Section 5.1.

In the closure phase, it can be used to enhance the mandatory replay workshop[1] (as described in the TIBER-EU Framework) and is highly recommended. In this phase, PT consists of different review activities using specific

[1] Although in some jurisdictions, PT is specified as a mandatory element in the national implementation guide.

scenarios (which may differ from the attack scenarios) to better understand how effective the defensive controls were or would be against the offensive attacks. This helps maximise the value of the test. Potential types of PT during the closure phase are described in Section 5.2.

Definitions of the TIBER Cyber Team (TCT), White Team (WT), Blue Team (BT), Red Team (RT) and Threat Intelligence (TI) providers can be found in the TIBER-EU Framework.

1.3 Structure of the best practices

The remainder of this document is structured as follows:

- Section 2 – High-level overview of purple teaming
- Section 3 – Purple teaming in the testing phase
- Section 4 – Purple teaming in the closure phase
- Section 5 – Types of purple teaming

2 High-level overview of purple teaming

2.1 General principles

Purple teaming (PT) – whether conducted in the testing phase or to enhance the replay workshop during the closure phase – needs to follow some fundamental principles, as outlined below.

2.2 Scope and objectives

For PT to be successful, the stakeholders involved must clearly define the scope, goals, objectives, timing and rules for the actual activity. These aspects should be first discussed during engagement and scoping of the TIBER-EU preparation phase to form a preliminary understanding of where PT could be anticipated. The risk management controls should be reviewed and where necessary adapted, as it is possible that different and more elaborated attack scenarios can be tested under PT.

2.3 Cooperative attitude among stakeholders

During PT, the TCT should continue to provide advice to the WT to support its management of the test. The objective should be to continue deriving the maximum possible value. The WT should also approach PT with an exploratory mindset to delve deeper into the attack scenarios and examine additional techniques and possibly additional attack scenarios. These scenarios may have a forward-looking, outside-the-box perspective that is extreme but plausible and should resemble attacks which could occur in the (near) future.

For PT to be successful, the BT and RT are expected to forge a different working relationship and maximise their collaboration throughout, to create a unique learning experience and enhance each other's understanding. It should also take into account barriers between the various stakeholders that may hinder understanding due to different types of knowledge and expertise. Since information must flow between the different teams, language should be adapted so that all stakeholders have a common understanding. Stakeholders should be open-minded and mindful so as to create a bridge for open discussion and model this cooperative behaviour. To facilitate such behaviour, the RT should lead by example, clearly explaining its tactics and objectives to the BT, acknowledging the areas of strength and gradually opening up the conversation to the areas that need to be improved. This can be done by conducting live remediation to refine existing controls or implement new ones, for example.

The TCT and WT should approach PT with an exploratory mindset and retain a constructive attitude throughout. Close cooperation between the WT, RT and BT is crucial for the success of any PT. The BT and RT should have regular check points

so that they can confirm their understanding of each other's actions. The WT is instrumental in establishing a good basis for cooperation and needs to make explicit the roles and responsibilities within the PT setting.

2.4 Communication channels between stakeholders

For communication channels to be efficient and effective and to avoid misunderstandings, the WT should clearly define communication frequency and secure channels in advance, as foreseen in the TIBER-EU Framework. Formal (real-time) communication via secure channels (e.g. involving end-to-end encrypted email and chat) may not be in place between the RT and BT in the context of PT and should be implemented. Effective, efficient and transparent communication among stakeholders is a critical success factor for any TIBER test, and all the more so for PT.

2.5 Roles and responsibilities

The stakeholders involved in PT remain the same in both the testing and the closure phases.

The TIBER Cyber Team (TCT) serves as an adviser for all parties during PT. In particular, the TCT should ensure that the spirit, principles and processes envisaged in the TIBER-EU Framework are maintained and observed. Moreover, the TCT as a whole, and the TIBER test manager (TTM) in particular, has the power to invalidate a test if they assert that it has not been conducted in line with both the requirements set out in the TIBER-EU Framework and the spirit of the framework. Additionally, the TCT can object to using PT during the testing phase and suggest alternatives to overcome any hindrances encountered.

The White Team (WT) is responsible for making all the necessary decisions as circumstances arise and for ensuring that proper risk management controls are in place for the test to be conducted in an appropriate manner. In addition to making sure that risk management controls remain effective in PT, the WT must also ensure that:

- stakeholders fully comprehend the agreed scope, goals and objectives when switching to PT during the testing or closure phases;
- stakeholders are aware of and agree on the communication channels to be used, including between the RT and BT (under WT supervision);
- appropriate arrangements are in place to facilitate the shift to PT and provide the clarity required by the RT and BT to be able to adapt to this new collaborative way of working;
- the RT and BT adapt their behaviour when initiating and executing different types of PT, and cultivate cooperation and mutual support.

The Threat Intelligence (TI) provider provides expert judgement on the scenarios and the tactics, techniques and procedures (TTPs) to be used in PT. The involvement of the TI provider in PT is crucial in both testing and closing phases, as scenarios may need to be adapted. Additional and more advanced scenarios or TTPs may be added, depending on test specificities and planning, resourcing and timing.

The Red Team (RT) carries out the simulated attack by attempting to compromise live production systems of the entity by mimicking the TTPs of threat actors, as described in the TIBER-EU Framework. In PT, the RT is responsible for the offensive aspects. The expert judgement of the RT should also be sought when considering and planning PT. The RT should work with the TI provider to validate the plan and provide a list of TTPs to be used during PT.

The Blue Team (BT) acts out, or is actively in charge of, all the defensive aspects of the scenarios being executed. The BT may also contribute to additional scenario types and variations by providing interesting leads and feeding information back to the RT in the course of PT. During PT, the BT might have difficulty shifting to a more cooperative attitude, particularly if the actions it has to engage in may not be clear. The WT should communicate with the BT regularly to ensure the constructive nature of PT is maintained.

3 Purple teaming in the testing phase

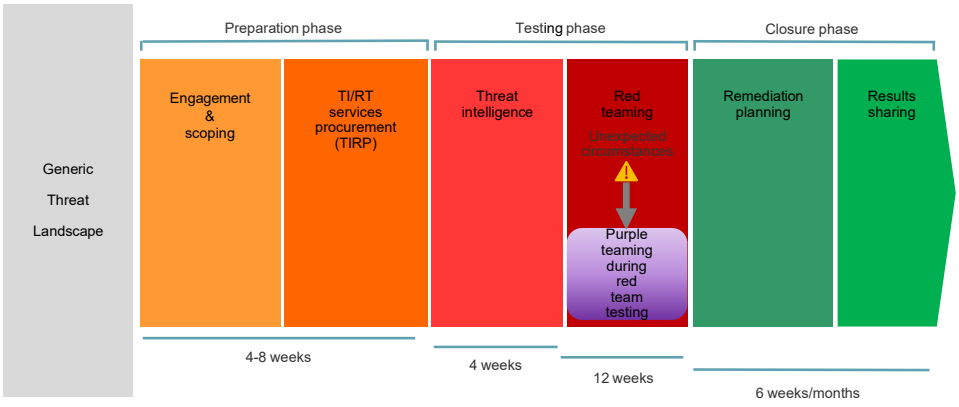
3.1 Rationale

While the TIBER-EU methodology ensures thorough planning, circumstances may arise during a live test that force the stakeholders to act pragmatically to balance the objective of maximising the learning outcome against maintaining a strict interpretation of the framework.

A considerable amount of time, cost and effort goes into planning and executing a TIBER test. So, the invalidation of a TIBER test is not desirable, unless the test fails to meet the requirements and spirit of the framework. Hence, it is reasonable that in certain circumstances, it is possible to carry out PT during the testing phase in order to continue the TIBER test and to maximise the return on investment.

It is recommended that a scenario-based approach be employed for PT within a TIBER test. When planning for or transitioning to PT during the testing phase, it is always advisable to re-evaluate the attack scenarios to ensure they fit the PT setting while still remaining close to the TTPs of the simulated threat actor (see Figure 1). The PT activity may cover one or more of the attack scenarios, depending on the situation; however, it is conceivable that PT will be applied to a specific attack scenario whereas other attack scenarios will continue normally under red teaming.

Figure 1
Indicative PT timeline in the testing phase



3.2 Circumstances leading to purple teaming

Alternative ways of progressing are thoroughly examined before the WT proposes moving to PT. For example, pausing the test should be considered to see if this would be an equally suitable measure to maximise the lessons learnt. It is then up to

the TCT to evaluate each case individually, in close dialogue with the WT, RT and TI providers, and assess whether PT is an option.

The WT is also encouraged to consider, within the risk management controls of the test, any circumstances that may lead to PT. For this reason, it is advisable for the WT to plan to execute the most daring or noisiest attack scenarios last in order to avoid the BT detecting RT activities during the early stages of the test.

Some potential circumstances that may lead to PT during the testing phase are described below.

- When the BT has detected the RT in such a way that the secrecy of the test is irreparably compromised. Note that it is possible that during a test, the BT may detect some RT actions; however, this alone does not necessarily mean that PT is the right way forward, and it is possible to still continue the test in its original RT manner using a cover story (e.g. a local penetration test) to explain certain detections to the BT or to only introduce PT for the detected attack scenarios. In addition, it may be possible that a test is partially detected by the BT and the WT can then instruct a freeze on RT activities to allow the elevated threat level to subside. In such cases, it is crucial to have alternative approaches and techniques at hand, as it is a common mistake to pause only to reuse the same attack vectors that have already been detected.

- In difficult to foresee situations where there is a high degree of confidence that the emulated attack on specific systems that underpin critical functions could lead to a substantial disruption. In these cases, it is advisable to discontinue testing and to introduce PT for these systems instead. This would enable the BT, once informed, to take timely action to prevent and minimise any impact.

- In the case of a parallel real cyberattack (i.e. outside of the TIBER test) where the BT has to fully shift its focus to disruption prevention and containment. This may result in the TIBER test being revealed in order to transparently help the BT differentiate TIBER activities from the genuine attack. Among other possibilities, the test may be postponed to a later date, possibly utilising PT.

- When there is a high probability (e.g. derived from clear signs) that the response of the uninformed BT to contain the detected emulated attack will have a critical impact on systems underpinning critical functions. This potential overreaction might be appropriate in the event of a real attack, but not in the context of a TIBER test, given that the RT will never deliberately cause disruption. If the BT is not aware of the TIBER test, they have no way of knowing if their response is adequate.

- To prevent situations that can lead to the BT straying from normal response procedures. This would be counterproductive and both reduce the realism of the test and hamper its learning outcome. This can happen when the BT, suspecting that the attack is not genuine, changes its attitude and response mechanisms.
- When the WT is unable to stop escalation by the BT and the BT has involved external parties such as the police, intelligence services, government authorities, industry bodies or financial institutions, for example, due to the perceived severity of the incident. Involving these parties will put an unnecessary strain on those authorities and could have a severe impact on current and future testing activities. The test should be halted immediately and PT may be considered.

3.3 Minimum requirements in the testing phase

It is not possible to provide an exhaustive list of circumstances that could result in shifting to PT during the testing phase. However, one of the main criteria should be that the testing phase cannot continue in a secret and/or secure manner due to an event outside of the control of the WT, RT or TCT.

Including PT in the testing phase needs to be discussed and agreed. This should involve:

- the WT formally proposing PT, detailing specific scope and objectives;
- the TCT agreeing to PT and not raising an objection;
- the test still being conducted in accordance with the spirit of the framework (i.e. PT should be considered an option of last resort rather than a relaxation of the TIBER-EU requirements), focusing on maximising the learning experience and outcome;
- the WT liaising with the TI and RT providers as necessary to adapt existing scenarios or implement alternative scenarios so as to maximise the value of the test for the tested entity;
- agreeing in advance on expectations regarding the outcome, communication channels, response and recovery activities, confidentiality boundaries, start and end, escalation paths, allocated resources (including budget) and reporting formats;
- agreeing that the outcomes of PT be clearly documented and form an integral part of the remediation plan.

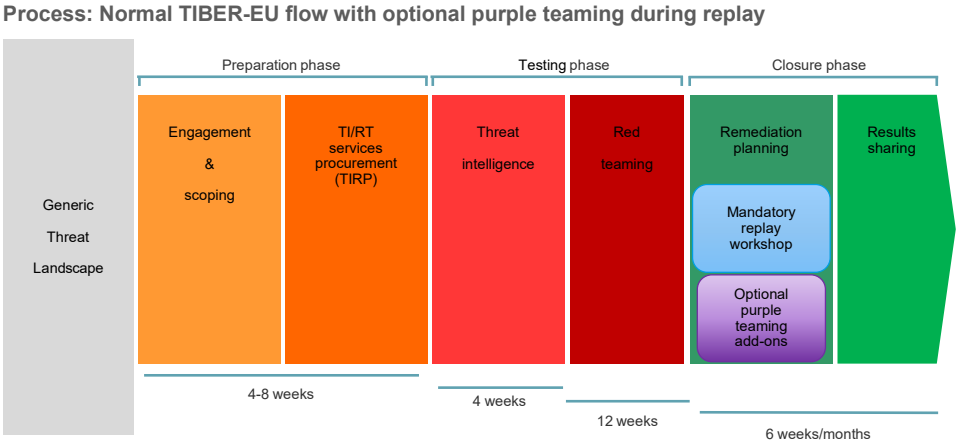
4 Purple teaming in the closure phase

4.1 Rationale

As described in the TIBER-EU Framework, it is optional but highly recommended that PT be performed on top of, or in combination with, the mandatory replay workshop.[2] PT in the closure phase helps to optimise RT and BT collaboration and maximise learning opportunities, defence capabilities, situational awareness and ultimately the return on investment of the whole test.

A well-executed PT activity in the closure phase (see Figure 2) can provide the entity with a comprehensive review of the effectiveness at each layer of its infrastructure in scope and improve the detective controls that are crucial to shed light on suspicious activity.

Figure 2
Indicative PT timeline in the closure phase



4.2 Planning

If planned for the closure phase, PT should ideally be scheduled to take place shortly after the delivery of the final RT and BT reports, close to, or in conjunction with, the replay workshop. This timeline ensures that PT is carried out while the details and observations noted during the testing phase are still fresh in the minds of the BT and RT.

There are no uniform PT duration or scope requirements as PT is tailored individually for each test. However, it is strongly recommended when selecting the appropriate PT type in the closure phase, to consider:

[2] In some TIBER-EU jurisdictions, PT forms an integral part of the mandatory replay workshop.

- that PT will vary, depending on the specific nature of a test;
- further strengthening the collaborative engagement between BT and RT to identify alternative attack steps that could have been taken by the RT and potential ways of detection and response by the BT;
- the effectiveness of the defensive controls against offensive actions and how to maximise the value of working closely together during PT specific to the closure phase.

4.3 Results

PT in the closure phase allows for more detailed examination and evaluation of particular aspects of a TIBER-EU test, without the constraints present in the testing phase, such as BT detection, limited amount of participation and so on. In particular, it makes it possible to directly leverage the expert knowledge of the RT to revisit and address specific areas deemed important by the tested entity.

PT can therefore result in a deeper understanding of the interconnections and implications of the most relevant offensive and/or defensive measures for the tested entity. It might help to demonstrate and highlight the potential consequences from both a technical and a business perspective (e.g. remediation, recovery time, business continuity, etc.) and hence inform considerations beyond the technical realm. As a result, PT might facilitate a better understanding of the consequences of an attack, further proliferation of an attack and alternative ways to enhance protection and detection.

The results of PT will greatly benefit the further refinement of recommendations and remediation planning, which will in turn enhance the cyber resilience of the tested entity. In addition, they might feed into other operational resilience exercises and improve the entity's operational risk and information security/cyber resilience programme or framework. One such example is to utilise the scenarios in crisis simulation and coordination exercises.

5 Types of purple teaming

PT types can vary in their purpose, learning experience, form, level of BT involvement and specificities. Most importantly, proper consideration needs to be given to when (test phase) and why (specific situation) they might be applied.

This section describes some possible types and examples of such PT, which might be used alone or in combination. However, since each TIBER test is different, they might be expanded or adapted according to the specific circumstances of a given test. The best approach when deciding which type of PT to select is for the relevant stakeholders to openly discuss the different alternatives. A detailed description of each type of PT is provided in Sections 5.1 and 5.2.

Because the selection of PT type is strongly dependent on the nature of the TIBER test in question, some of these types may only be suitable in specific situations. Used elsewhere, they might lead to invalidation of the test. This is crucial for the testing phase, as the TIBER-EU Framework requires the BT to be unaware of the engagement during this phase.

When planning PT, the following general aspects should be considered:

- the purpose and learning experience for the entity, bearing in mind all the specificities of the entity and the test;
- clear agreement on how to carry out PT;
- the BT's level of knowledge about the test;
- the level of communication and bilateral channels between RT and BT;
- the involvement of other stakeholders, such as the WT, TCT or even (additional) board members of the entity concerned.

5.1 Types of purple teaming in the testing phase

The types of PT during the testing phase are typically limited to activities conducted on the technical systems themselves, since tabletop activities are usually conducted in the closure phase and do not necessarily justify informing the BT about the ongoing test. Potential types of PT specific to the testing phase are described below.

5.1.1 Catch-and-release

"Catch-and-release" is a useful way of testing an entity's defensive capabilities when there have been **repeated detections by the BT during the final stage** of a test. Because of such detection and consequent blocking of the accounts and tools involved, further progress in testing activities might not be possible without a

significant change in TTPs. While different TTPs, such as choosing alternative routes into or through a network or different attack techniques, could be employed in the early stages of a test, this might not be feasible during the final stage. For example, if production systems have been successfully breached but exfiltration or modification of data is still outstanding, or when a route to the critical functions cannot be identified by the RT, a sudden change in TTPs might be counterproductive. In such situations, a catch-and-release approach might be carried out, enabling lessons to be learnt about very specific aspects of an attack that could not otherwise be achieved.

Catch-and-release is initiated by revealing to the BT that a test is being performed on its systems and installing a dedicated communication channel between the RT, BT and WT. In the event of any further detection within well-defined boundaries (e.g. certain machines or subnets), the BT uses this channel to report the detected Indicators of Compromise (IoC) to the RT, which confirms or refutes those as being part of their test. Note that special care should be taken by the WT to ensure that the BT blocks out confidential information that might not be related to the TIBER test. Should the identified IoCs indeed be part of the TIBER test, the BT will then perform the agreed measures to allow the test to continue (e.g. releasing an isolated machine or account). Alternatively, other previously agreed actions might also be taken, such as shutting down a machine, escalating the incident or starting a forensic investigation with the aim of evaluating these processes as part of the test.

The BT documents the events, together with all countermeasures or releases, for later reproduction and discussion. Importantly, specific guardrails should be defined in advance, specifying which machines (or subnets) are in scope of such types of PT as well as which responses actions cannot or should not be skipped.

Although the BT is aware of a test being performed on its production systems, this does not necessarily mean that the BT is aware that it is a TIBER test or what scenarios are covered by the test. During the complete PT phase, regular updates should take place to ensure adequate risk control and facilitate mitigation measures.

5.1.2 Collaborative proof-of-concept

“Proof-of-concept” can be a very helpful activity to provide evidence of a weakness discovered during TIBER tests in situations where practical testing on the production systems by the RT alone is not feasible (e.g. because of being out of scope, unjustified high risk of impacting critical systems, etc.). In some settings, a proof-of-concept might require the explicit involvement of the BT to provide a particular part of infrastructure expertise or risk control, for example. A collaborative proof-of-concept offers a very detailed learning experience related to a particular attack step or vulnerability.

Executing a collaborative proof-of-concept includes collecting all the evidence required to illustrate the feasibility of a certain attack vector without actually fully performing such an attack. This might include a theoretical discussion of the expected outcome of executing a given step as well as the protective measures in

place. A practical test of partial aspects of the attack is usually also carried out (e.g. sub-steps, using dummy data, execution on testing systems, etc.).

As for other, similar activities, close cooperation between RT and BT (also including relevant business areas where appropriate) is required to consider all offensive and defensive aspects of an attack. In most cases, proofs-of-concept are conducted during the closure phase to avoid undesired effects during the test itself, such as putting the BT on high alert. However, at a very late stage of testing, the remaining activity might depend on a particular proof-of-concept. BT staff might thus be informed about the test and asked to contribute when drawing up the proof-of-concept.

Other stakeholders, such as the WT and the TCT, should be closely involved to ensure the proof does indeed provide evidence of a weakness.

5.1.3 War game

A war game is an activity in which RT and BT are fully aware of each other's respective goal to capture the respective flags (RT) or to protect the entity's critical assets and terminate the attackers' access to the network (BT). As such, war games differ from the spirit of a normal TIBER test in the sense that the BT knows what the RT flags are. If a war game is performed, flags are usually placed in systems underpinning critical functions included in the test scope.

In very particular situations, such as when a TIBER test is known to the BT at a very early stage of the RT, a war game might be a suitable option to continue the test and still enable a learning experience.

5.2 Types of purple teaming in the closure phase

Under the TIBER-EU Framework, the mandatory replay workshop is a chronological walk-through of each scenario. It serves to detail and discuss the actions of the RT, together with the relevant responses of the BT, step by step at an appropriate level of technical detail based on the RT and BT reports and logs, but without necessarily actively using the systems themselves (i.e. the replay is often conducted in the form of a tabletop discussion, see Figure 3).

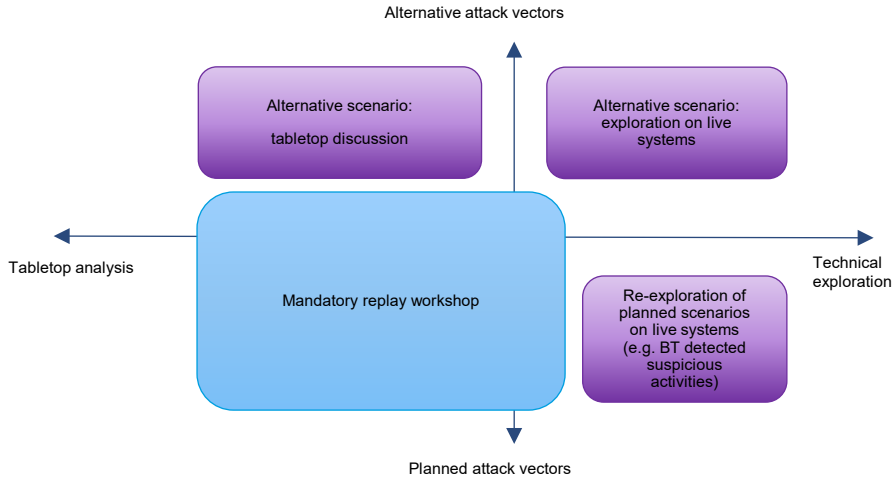
In practice, the replay workshop is often complemented by additional types of PT to investigate selected aspects of a test in more detail and hence maximise the learning experience.[3] As such, different types of PT can either be combined with the mandatory replay workshop or carried out in separate workshops.

PT activities in the closure phase might focus on attack scenarios planned and executed during the testing phase or on alternative, more explorative approaches.

[3] In some jurisdictions, PT is specified as a mandatory requirement in some national TIBER implementation guide.

They can take the form of tabletop discussions as well as activities on the technical systems.

Figure 3
Types of PT



Deciding on which types of PT are best suited for a particular test depends on many factors, such as the results of the test, risk considerations, the intended type of learning experience and available resources. The types of PT described below can serve as a reference to ensure the consistent use of terminology by all parties involved. These are likely to be combined and blended in a way that best fits the situation at hand and the specificities of the entity being tested. Additional stakeholders, such as the internal RT of the entity tested, might also be included in a passive or active role. This can lead to additional learnings for all parties.

5.2.1 Alternative scenario: tabletop discussion

A tabletop discussion can provide valuable learning experiences where technical systems are not required or available for the review. This type of activity allows a less technical audience, including management, to be included more widely in the discussion. While the planned attack vectors have already been analysed in the mandatory replay workshop, a tabletop discussion is a great way to investigate alternative attack vectors and discuss or simulate the “what ifs” without a strict focus on technical systems. For example, a simulation might be used to discuss the entity’s response in case the method or pathway used by the attacker to infiltrate the system was successful. Such tabletop discussions offer high flexibility with regard to the tools used.

A tabletop discussion can be carried out in a variety of ways. These might include:

- a role play to discuss and simulate alternative offensive and defensive measures and their consequences;

- the theoretical evaluation of scenarios that are closely related but out of scope of a TIBER test;
- the simulation of potential consequences reaching far beyond the test (e.g. restoring business continuity after a successful ransomware attack);
- the inclusion of senior management.

Tabletop discussions might include many different stakeholders (such as business process owners) and therefore require thorough planning and moderation. However, they facilitate an all-round view of the wider aspects of an entity's security and can even go far beyond the initial scope of the test.

5.2.2 Re-exploration of planned scenarios on live systems

A technical re-exploration of the attack vectors planned and executed during a TIBER test is an effective way to combine the expertise of the RT and the BT to practically show the offensive and defensive potential of an attack step or attack chain. Although this type of activity is quite resource-intensive in terms of preparation, it can deliver a highly comprehensive and detailed hands-on learning experience for the BT. For example, it might be very helpful in cases where the BT struggled to detect RT activities during a test. In this case, the RT and BT might engage in a collaborative attack recollection. Running through a chosen attack sequence step by step, the RT executes the respective TTPs while the BT can simultaneously provide corresponding defensive information (e.g. event notifications received, alerts, blocked executions, etc.). The two teams can together discuss (and document) the consequences of such an attack sequence and draw up preventive and/or reactive measures from their respective points of view.

This type of activity might include:

- walking through an RT activity that was not visible in the BT logs during the testing phase;
- walking through an RT activity that was visible in log entries, but the malicious activity was not detected by the BT during the testing phase;
- walking through an RT activity that triggered an alert during testing but was not triaged properly;
- walking through activities to which defensive responses were ineffective during testing;
- walking through activities that triggered a defensive response that effectively closed the attack vector but was unable to prevent the attackers from meeting their objectives.

Alternative defensive measures and potential offensive countermeasures might be discussed and practically evaluated to achieve a good understanding of the different

possibilities of attack and defence. This type of activity requires close cooperation between RT and BT as well as an open and explorative spirit.

5.2.3 Alternative scenario: exploration on live systems

Technical explorations of relevant attack scenarios during the closure phase might not be limited to merely evaluating scenarios conducted during the test phase. Variations of tested attack scenarios as well as novel or more elaborate scenarios are constantly inspired during a TIBER test. These can often not be comprehensively evaluated during the testing phase due to time and other constraints. For example, there might not be sufficient time to test a potential attack vector due to its late point of discovery during the testing period or a high risk of system damage or BT detection.

This attack vector might be explored during the closure phase, since more time is available and the close cooperation with the BT could significantly reduce the identified risks. Although such reviews could be done in a theoretical manner, more detailed insights are often gained when testing is carried out on the actual systems. Alternative scenario explorations on live systems might contain:

- a technical exploration of attack scenarios deviating from those conducted during the testing phase;
- a technical exploration of tested attack scenarios applied to alternative target environments (e.g. execution in a Citrix environment instead of on a company laptop);
- proof-of-concept (e.g. scenarios not conducted during testing due to a high risk of BT detection or system damage);
- a technical exploration of novel TTPs which have emerged but could not be tested on the technical systems during the testing phase.
- The technical exploration of alternative attack scenarios makes it possible to take an in-depth look at the consequences, potential detection and response measures for novel kinds of attacks. Since this is done in a collaborative manner, even aspects entailing a high degree of risk can be investigated to obtain very realistic results with a high level of technical detail.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).