EUROPEAN CENTRAL BANK

EUROSYSTEM

# TIBER-EU

# Blue Team Test Report Guidance

January 2025

# Contents

# 1 Introduction

The Blue Team Test Report (BTTR) includes all information about the performed red teaming attack actions gathered from the Blue Team (BT) side (e.g. from logs, detections and other sources). It also highlights the reflections, agreements and disagreements of the BT on the results presented in the Red Team Test Report (RTTR). It therefore serves as part of the basis for the later conducted replay and purple teaming (PT) exercises.

## 1.1 Purpose of this document

The purpose of this document is to provide the relevant stakeholders with information on the requirements[1] for the content and format of a TIBER-EU BTTR. It also aims at providing guidance on important aspects to be considered during drafting as well as supporting material.

## 1.2 Target audience

This TIBER-EU BTTR Guidance is mainly aimed at the BT of the tested financial entity creating a BTTR in the scope of a TIBER test. Beyond that, it is useful to read for all stakeholder of a TIBER engagement to understand the nature of its content.

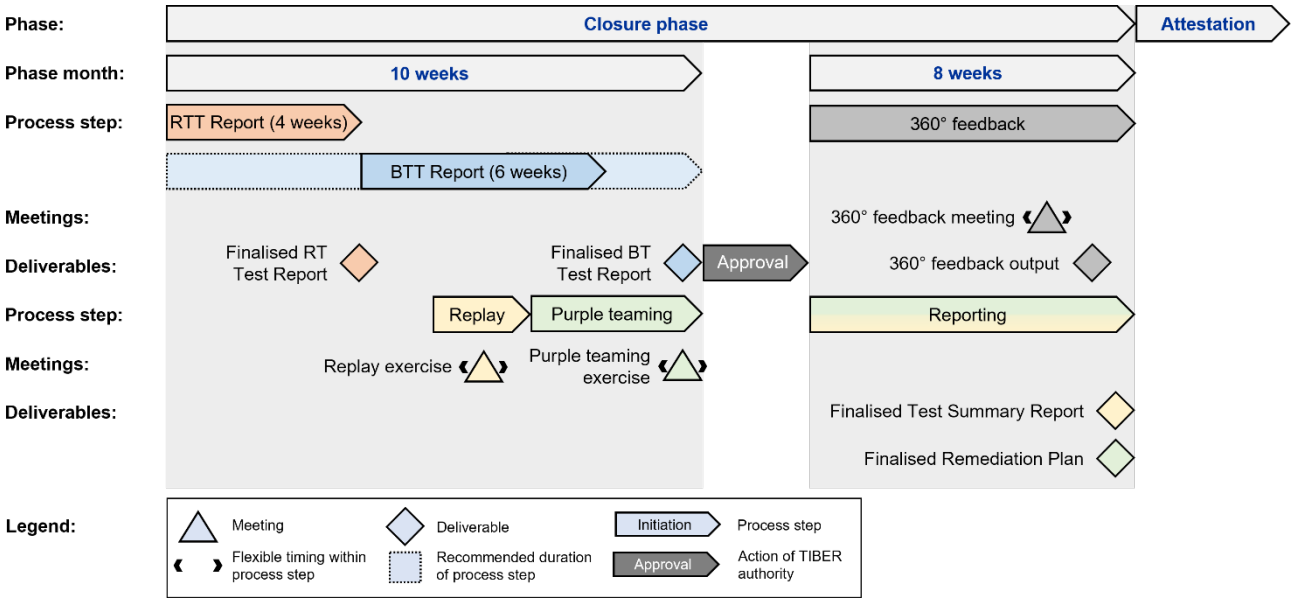
## 1.3 Location within testing process

The BTTR is to be written by the BT during the first process step of the closure phase, after having received – at a minimum – a draft of the RTTR, and before the replay and purple teaming exercises will commence.

[1] In addition to the minimum requirements for complying with the TLPT obligations under DORA, this document also includes operational TIBER-EU guidance based on best practices, knowledge and experience from numerous previous tests.

**Figure 1**[2]

Closure phase process overview




[2] Note that only the actions of the TIBER authority are included in the figure that have an impact on the timelines of the test. The figure is not an exhaustive overview of all actions to be undertaken by the involved stakeholders.

# 2 Required content of the Blue Team Test Report

The BTTR shall include information on at least the following:

- for each attack step described by the red team testers (RTT) in the RTTR:
    - a list of detected attack actions;
    - Threat hunting activities and configuration changes (FW rules, detection rules, hardening …) performed during or after the active RT phase (independently from the recommendation plan)
    - log entries corresponding to these attack steps or detections (if any);
    - a timeline mapped with RTT and BT actions;
- Remaining RTT artefacts found by the BT, including information on when and where they were found and if the BT was informed about the artefact by the RTT (if applicable);
- an assessment of the findings and recommendations of the RTT;
- evidence of the RTT attack collected by the BT;
- BT root cause analysis of successful attacks by the RTT;
- a list of lessons learned and identified potential for improvement;
- a list of topics to be addressed in the PT exercise.

# 3 Considerations when drafting the Blue Team Test Report

The BTTR will be read by various stakeholders at all organisational levels within the tested entity. As such, the BT should ensure that the BTTR is clear, concise and accurate. The BTTR should aid the entity in understanding its current security posture and identify areas for improvement in order to strengthen cyber resilience. In particular, it is highly recommended for the BT to draft an executive summary suitable for consumption by senior management and high-level governance bodies (such as a Board of Directors).

## 3.1 BT context

In the BTTR, it may be helpful to include general information on the structure and composition of the BT, the responsibilities of the internal BT during the active test phase (e.g., Level-1, Level-2, Level-3), outsourced responsibilities of BT and which service providers are used. In addition, it may be useful to provide a general overview of the sources of information available to the BT (e.g., particular type of logs or other reporting systems, human observations, etc.).

## 3.2 Timeline of events

A timeline of events constitutes the basis of the BTTR and the subsequent replay exercise. Therefore, the BT should use the timeline of events in the RTTR provided by the RTT and map all its own actions alongside it.

In case of a detection of the RTT activities, the detection and escalation activities performed against the different stages of the RTT attack timeline should be outlined. In particular, the BT should highlight which controls detected the RTT and, if necessary, automatically stopped them (e.g., EDR, SIEM, IPS, FW, Proxy, DLP). In addition, the BT should highlight which measures were taken to manually stop the activities, remediate the attack paths taken during RTT activities, and escalate the incident internally or externally. Moreover, the BTTR may describe to which extent the organisation's regular processes were adhered to or deviated from.

In a similar manner, the BT should map the undetected activities of the RTTR timeline against its own logs and explain why existing controls did not take effect or why they could be circumvented by the RTT. For this purpose, it can be helpful to systematically search all log databases based on the attack steps of the RTT to identify cases in which the attacks appeared in the logs but were not detected. For example, because of the systems not yet being connected to the internal monitoring processes or due to a lack of use cases.

The BT may also outline threat hunting activities and configuration changes (e.g. FW rules, detection rules, hardening, etc.) performed during or after the active RT phase. The BT should substantiate all of the activities with clear evidence (e.g. incident ticket number including timeline of the ticket creation, detection status, log references, alerts triggered, escalation measures taken, reports, countermeasures taken, etc.) in the BTTR.

## 3.3 Findings and recommendations for remediation

The BT should draft a response to the RTT findings and recommendations as outlined in the RTTR. The BT may challenge the findings, for instance by accepting, partially accepting, supplementing, or rejecting them. In case of rejections, these should always be clearly justified and discussed with the RTT in the replay exercise.

There may be situations where the BT accepts the RTT assessment but does not support the recommended suggestions for improvement. For example, there may be internal reasons (unknown to the RTT) why certain technical controls did not work, are not (yet) implemented, should be altered before implementation, or cannot be implemented. It is possible that identified problems have already become known through other (internal) tests and the processing is still ongoing.

In case of agreement with the findings and recommendations of the RTTR, the BT should take up these recommendations, further substantiate them and derive adequate mitigation measures.

## 3.4 Root cause analysis

The RTT may determine, on the basis of their experience and professional assessment, whether conclusions can be drawn as to the causes of the reported findings. To this end, the RTT holistically include people, processes and technologies in their considerations and do not limit themselves to the technological aspect alone. Using these and/or additionally identified root causes, the BT should extrapolate lessons learned and potential mitigations to detect/prevent such activities in the future. Weaknesses in the existing governance processes should also be considered in this regard.

The elaboration of the BT on findings, root cause analysis and recommendations may be more analytically oriented to help ensure that the replay exercise is not only technical and retrospective, but also enables a forward-looking view.

## 3.5 Artefacts

The BT should highlight any remaining RTT artefacts in the BTTR. Especially those artefacts which cannot be easily removed by the RTT, due to practical considerations, should be thoroughly checked and deleted in consultation with the

RTT. These artefacts may pose a risk to the systems or may affect future incident investigations or safety assessments. Artifacts are usually described using file names, paths, hashes, hostnames, IPs, email addresses, email subjects, email domains, and web domains.

## 3.6 Topics for the purple teaming exercise

The BT must make a list of topics to be addressed during the purple teaming exercise, which may be supplemented by the TM. In the purple teaming exercise, the BT and the RTT will work together, for instance to see which other steps RTT may have taken, and how the BT can detect and respond to such actions.

## 3.7 Confidentiality

The BT should be aware that the BTTR (including the annexes) is highly sensitive and therefore must be treated with the highest level of confidentiality in line with the TIBER-EU framework. Consequently, the BT must ensure the following:

- strict control of the production of any copies and a register of all and any copies with the recipients;
- restricted access control to any copies;
- use of the allocated codename throughout the report;
- removal of any mention of the entity in the BTTR contents;
- very clear labelling in electronic and physical copies of the security label (e.g. highly confidential);
- where appropriate, requirements from national security legislations.

Due to the sensitive nature of the information contained within the BTTR, it should be handled and treated in a manner commensurate with this classification (e.g. TLP Red). It is the responsibility of the entity to retain the BTTR, and to share the report with the TM. At the very least, the TM must be permitted to visit the entity onsite to review the entire report.

The TM may request to receive a report without any sensitive information[3].

[3] Sensitive information is defined as information that can readily be leveraged to carry out attacks against the ICT systems of the financial entity, intellectual property, confidential business data and/or personal data that can directly or indirectly harm the financial entity and its ecosystem would it fall in the hands of malicious actor.

# 4 Drafting format

The BTTR might be drafted in any preferred format, provided that all required information is included. Particular attention needs to be dedicated to the timeline, where the BT maps its actions alongside the actions of the RTT, which will be used as a mutually agreed basis for the Replay and PT exercises. Example templates (if any) to be used on a voluntary basis are provided in the annex and might prove helpful for better formalisation.

# 5 Annex

## 5.1 Annex 1 – Possible representation of RT activities

| **Name of the RT activity**<br>e.g., Use of Kerberoasting | **Identifier/TTP**<br>e.g. (T1558.003 Kerberoasting) |
|---|---|
| **Description** | For example, attackers can abuse a valid Kerberos ticket (TGT) or spy on network traffic to obtain a ticket for the ticket-granting service (TGS) that could be vulnerable to brute force. |
| **Recent detection** | |
| **Possible detection** | |
| **Possible prevention** | |

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).

PDF ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-N
HTML ISBN 987-xx-xxx-xxxx-x, ISSN xxxx-xxxx, doi:xx.xxxx/xxxxxx, QB-xx-xx-xxx-EN-Q