EUROPEAN CENTRAL BANK

EUROSYSTEM

# TIBER-EU

# Guidance for the Red Team Test Report

August 2020

# Contents

# 1 Introduction

## 1.1 Purpose of this document

The closure phase (which includes remediation planning and result sharing) allows all relevant stakeholders to reflect on the outcome of the test and make improvements to further enhance the cyber resilience of the entity. In this phase, the red team (RT) provider will draft a Red Team Test Report, which will include details of the approach taken to the testing as well as the findings and observations from the test.

The output of this activity is a draft version of the Red Team Test Report produced by the RT provider for delivery to the entity. The entity's Blue Team are informed of the test and will use the Red Team Test Report to deliver their own Blue Team Report.

The TIBER-EU Guidance for the Red Team Test Report aims to provide RT providers with a standardised approach and structure for producing the Red Team Test Report, focusing on: setting out the summary of the test with accompanying evidence; detailing the findings and root cause analyses; determining the key discussion points for the replay with all the relevant stakeholders; and finalising the remediation plan.

The Red Team Test Report is a key document that helps inform the White Team, Blue Team and TIBER Cyber Teams (TCTs) involved in the TIBER test of the test and its outcome, and sets the basis for future improvements to the entity's cyber resilience posture.

Where necessary, the Red Team Test Report will include advice on areas for improvement in terms of technical controls, policies and procedures, education and awareness, as well as highlight any strong control areas that the RT provider was unable to circumvent. On the basis of the draft Red Team Test Report, there will be a Replay Workshop in which the executed scenarios will be replayed and the issues uncovered during the test discussed, after which the RT Provider shall finalise the Red Team Test Report.

It is clear that there will be several possible iterations of the Report, and the final Report should be fully accurate, reflective of the discussions at the Replay and agreed upon by the entity (including the final recommendations and potential remediation actions). The entity will then take on board the findings, and agree and finalise a Remediation Plan (including planning for follow-up testing) with the authorities (i.e. the supervisors more specifically); the testing process will be reviewed, and the entity's protection, detection and response capabilities discussed.

## 1.2 Who is this document for?

This TIBER-EU Guidance for the Red Team Test Report is aimed at:

- Red team provider.

- White Team of the entity undertaking the TIBER test and;
- Threat intelligence provider; and
- TIBER Cyber Teams (TCTs) involved in the TIBER test;

## 1.3 Structure of this document

This document is structured as follows:

- Section 2: Report Structure;
- Section 3: Discussion and Replay workshop;
- Section 4: Remediation Plan; and
- Section 5: Approach of the RT provider.

Due to the sensitive nature of the information contained within the Red Team Test Report, it should be handled and treated in a manner commensurate with this classification (e.g. Traffic Light Protocol Red). Further information can be found in Section 5. It is the responsibility of the entity to retain the Red Team Test Report, and at the discretion of the entity whether to share the report digitally with the TCT. At the very least, the TCT must be permitted to visit the entity onsite to review the entire report.

# 2 Report Structure

While strict template(s) are not provided for the Red Team Test Report, in order to give flexibility and allow RT providers to use their own creative licence, the RT provider should ensure that at a minimum they incorporate sections as documented below.

If the RT provider wishes to include more information and/or address more aspects either within the sections or in additional sections then the RT provider can do so.

## 2.1 Executive Summary

The RT provider should draft a short narrative in business language, suitable for consumption by senior management and higher level governance bodies (such as a Board of Directors), in order to:

- Explain what critical functions and underlying systems were tested;
- Give a high level timeline of the test and provide an overview of the scenarios tested (including references to mimicked threat actors) and context of the successful and unsuccessful attack methods employed;
- Highlight the main findings (based on criticality) and possible root causes based on the attack methods used;
- Give insight into the main categories of recommendations to address the findings and possible root causes; and
- Note any significant notable observations and exceptions in the test.

## 2.2 Storyline

The RT provider should draft a storyline of the test, end to end, which is to be consumed by middle management and experts, to outline:

- The critical functions and underlying systems that were tested;
- Any deviation from the Red Team Test Plan;
- The attack scenarios that were utilised, in line with the MITRE ATT&CK Framework, including the flags and objectives (i.e. CIA triad);
- Any leg-up or allowance made by the White Team of the entity undergoing the test to facilitate the test and/or action by the Blue Team of the entity affecting the test;
- What was compromised and the attack path;

- The main findings and associated recommendations; and
- Any insight the RT provider wishes to provide on the cybersecurity posture of the entity undergoing the test, including further exploitation that could have taken place if the RT provider had more time and resources like a real life attacker, and areas of strength and/or weakness.

## 2.3 Findings

The RT provider must document extensively the findings identified in the testing process. The RT provider must categorise each finding in accordance with the NIST functions (i.e. Identify, Protect, Detect, Respond, and Recover) or other suitable standards such as the Eurosystem Cyber Resilience Oversight Expectations (Governance, Identification, Protection, Detection, Response and Recovery, Situational Awareness, Testing and Learning and Evolving); each finding must be categorised by criticality and complexity; and each finding must contain a clear description on how the entity was compromised and the impact of the compromise (including also the real impact if there were no limitations of a test). The findings should be both technical and non-technical, if applicable.

This categorisation does not need to be based on a single dimensional technical aspect only, such as the Common Vulnerability Scoring System (CVSS) rating, but also taking into account multiple factors including but not limited to the “location” of the finding in the infrastructure and proximity/effect on a critical system, the impact on the critical function if compromised and what further compromise this can lead to.

## 2.4 Provisional root cause analysis

The RT provider must use their experience and expert judgement to determine whether they can draw conclusions on root causes of the findings outlined above. In order to do this the RT provider needs to consider people, processes and technology holistically and not limit their view on the technological aspect alone.

Using these root causes, the RT provider must also extrapolate from their actions what could have been further done to take further the attack on the entity and what the possible impact could have been. Based on this analysis and the findings from the root cause, as well as the RT provider’s expert opinion, the root causes need also to be categorised per criticality.

It should be noted that the provisional root cause analysis will be judgement based and only preliminary; the aim of such preliminary analysis is to provide the basis for the Blue Team to reflect and to facilitate a robust discussion in the Replay workshop. This section of the Red Team Test Report should be more analytical in nature, and aims to facilitate the Replay workshop being more forward thinking, rather than solely technical and retrospective.

## 2.5 Recommendations

The red team test results should deliver meaningful output to drive decisions and actions. This means that the RT provider should develop clear conclusions and identify concrete recommendations that can lead to future action. The RT provider must document extensively the recommendations on the findings in the following manner:

- The recommendation prioritisation must be commensurate to the finding it aims to address; and
- The recommendation must be adequately described so that the entity undergoing the test is able to determine its objective and how they would be able to implement the actions under each recommendation.

The RT provider must document extensively the recommendations on the root causes in the following manner:

- The recommendations of root causes must be separate from those of the findings;
- The recommendation prioritisation must be commensurate to the root cause it aims to address;
- The recommendations on root causes should be drafted at a level that provides options and guidance to the entity undergoing the test, given that there may be alternative ways to eradicate the root cause.

## 2.6 Artefacts

The RT provider, in the main body of the Red Team Test Report or in appendices to the report, must include any artefacts that could plausibly remain on the systems of the entity undergone the test. These artefacts are, for example, toolsets that may remain on compromised hosts/systems. This section should list and allow these remaining artefacts to be removed by the entity as they may pose a risk to the systems or interfere with any future incident investigations or security assessments. Typically these artefacts are described using filenames, paths, hashes, hostnames, IPs, email addresses, email subjects, email domains and web domains.

On the whole, the RT provider must substantiate all of the above with clear evidence (e.g. log files, screenshots, etc).

# 3 Discussion and Replay workshop

The draft Red Team Test Report is used as a basis for the preparation of the Blue Team Report. After the RT provider and Blue Team deliver their reports, the entity must arrange a replay workshop. The goal of this workshop is to learn from the testing experience in collaboration with the RT provider. During the workshop, a replay is organised in which the Blue Team and the RT provider review the steps taken by both parties during the test.

Additionally, a purple teaming element can be added, in which the Blue Team and the RT provider work together to see which other steps could have been taken by the RT provider and how the BT could have responded to those steps.

When conducting the replay, the RT provider should state how well the testing team managed to progress through the targeted attack life cycle stages of each scenario. The RT provider should also offer an opinion as to what else could have been achieved with more time and resources given that genuine threat actors are not constrained by the time and resource limitations of TIBER-EU.

Using the Red Team Test Report, the RT provider and relevant teams from the entity undergoing the test are expected to discuss:

- The overall test and the success and/or failure points within it;
- The findings documented by the RT provider and their criticality;
- The root causes of the findings, as provisionally determined by the RT provider, and confirmed by the entity and their possible recommendations;
- The RT provider's recommendations for the findings;
- Any other Red Team observations regarding the entity's cybersecurity posture including possible defensive actions that could be taken by the Blue Team; and
- Any other insight from the RT provider regarding what further action could have been taken if more resources and time were available.

The RT provider should ensure that the Red Team Test Report adequately contains details around the findings, provisional root cause analyses and further issues, which will form the basis for the Replay workshop.

# 4 Remediation Plan

The Red Team Test Report should contain the findings, root causes and possible recommendations for the entity to address in order to mitigate the identified weaknesses, and thereby become more resilient to plausible future cyber attacks.

The entity is expected to acknowledge the findings and consider the recommendations offered by the RT provider in the final Red Team Test Report and draft a remediation plan in order to address the following:

- Assign overall ownership of the remediation plan to an individual;
- List findings by criticality and assign ownership for each;
- Have a detailed action plan; and
- Set timeframes and closure dates to remediate the findings based on their criticality.

It is important that the remediation plan not only focuses and addresses technical findings but, where applicable, also the root causes of the findings, which may encompass aspects related to people, process and technology. For example, specific unpatched systems (as identified in the test) must be patched but the overall patching process must also be strengthened to ensure that systems are patched in a consistent and routine manner across the entity as a whole.

The Red Team Test Report and the Replay Workshop are critical components of the TIBER-EU process, and both provide the basis for a comprehensive reflection and robust discussion between all the stakeholders, respectively. The outcome should be meaningful remediation plans. Consequently, it is important that the RT provider provides sufficient detail and evidence, and provisional root cause analyses, in the Red Team Test Report, for the entity to develop such meaningful remediation plans.

# 5 Approach of the RT provider

The Red Team Test Report is a critical report for the overall TIBER testing process, and will be read by stakeholders at different levels. As such, the RT provider should ensure that it is clear, concise and accurate. It should provide maximum value to the entity undergoing the TIBER-EU test.

RT providers will differ in their approaches and their documentation. The TIBER-EU Guidance for the Red Team Test Report does not aim to prescribe how RT providers should format their reports, but aims to provide a structured approach to producing the Report, whilst allowing each RT provider its own creative licence.

The RT provider should be aware that the Red Team Test Report (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 RT provider 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 codename as a filename;
- Removal of any mention of the entity in the Red Team Test Report contents or its filename (this can be accomplished by using an appropriate codename);
- Very clear labelling in electronic and physical copies of the security label (e.g. Highly Confidential); and

The draft report must be issued within two weeks of test completion. This is because the Red Team Test Report forms the basis of the subsequent discussions with the entity with respect to the findings and possible recommendations, as well as root cause analysis; and helps inform the Replay Workshop (and possible Purple Teaming) between the TCT, Red, Blue and White teams, which constitute the “Closure” phase of the TIBER-EU Framework.

It is clear that there will be several possible iterations of the Report, and the final Report should be fully accurate, reflective of the discussions at the Replay and agreed upon by the entity (including the final recommendations and potential remediation actions).

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