NORGES BANK

TIBER-NO
Blue Team Test Report Guidance

Version 1.0

TLP:CLEAR

1 Introduction

This is a practical guide produced by TCT-NO to support and guide how to produce the Blue Team Test Report (BTTR) in TIBER-NO tests. There are no formal requirements in the TIBER framework for the contents or format of this report, just that a report shall be produced. This guidance assists the Blue Team in getting started with the report and giving ideas to areas to cover. Since the nature of a TIBER test varies considerably, there is no single “best practice” contents or structure to this type of report.

The main purpose of the Blue Team Test Report is to document what the Blue Team discovered and acted upon by the defence of the entity’s critical functions targeted by the Red Team. This will be the basis for detailed discussions in the Replay Workshop, be the basis for the Remediation Plan and Purple Teaming activities before the TIBER test concludes.

The Report must therefore analyse the actions of the Red Team and detail which activities the Blue Team detected, and which actions went without detection.

Relevant TIBER documents:

- TIBER-EU Framework
- TIBER-NO Implementation Guide
- TIBER-NO Operational Guide

2 Input to the Blue Team Test Report

Input for the Blue Team Test Report is primarily the Red Team Test Report. This again is based on multiple other documents, including the Scope Document and Targeted Threat Intelligence Report.

3 Contents of the report

The Blue Team Test Report is the Blue Team’s opportunity to show their side of the attack scenarios executed by the Red Team.

3.1 Scenarios

TIBER tests are based on multiple scenarios, there should be at least three separate scenarios and in some cases more. Each scenario is defined in the Targeted Threat Intelligence Report as separate attacks with targeting different critical or important functions and emulating multiple adversaries. Although there might be similarities or some shared aspects, the scenarios can be seen as separate attacks. Structuring the reports based on scenarios is often natural and can make the walk-through of what happened at the Reply Workshop more constructive.

3.2 Mapping with Red Team Test Report

After the execution of the test by the Red Team, the Blue Team need to map all performed steps with status for detection or lack of detection. The objective is to identify those gaps where the Blue Team can improve.

The final report should include the following information:

- Successful detections (response)
- Detections gaps (alerts)
- Visibility gaps (logging)

The mapping of attacks with detection should be based on data from the draft Red Team test report. The Red Team should help the Blue Team and explain in detail the steps taken during the testing phase. Depending upon the structure in the Red Team Test Report, the structure can be based on individual scenarios, a timeline, functional areas in scope for the test or the Blue Team's own case management. Think that this collaboration with the Blue Team will be key to improve the security posture for the test Entity and the critical functions it maintains.

If the Blue Team needs further details of the steps taken by the Red Team than what the Red Team Test Report contains, it should actively seek this information from the Red Team. The Red Team should then update the Red Team Test Report accordingly.

The Bue Team then uses the mapping of all the steps of the Red Team with the detections that they could identify, to highlight the attack techniques or steps of the attack that were not detected. If a step was detected but no alert originated, it is recommended to highlight this as an improvement area for the Blue Team. Generating a spreadsheet on each step taken by the Red Team with the related detection will help to have a quick overview of the gaps.

Based on this mapping, the Blue Team can make an analysis of the response to security incidents or simulated attacks, including response times, effectiveness of containment and mitigation measures, and any challenges or gaps identified in incident response procedures.

3.3 Other contents

Further information, such as what was logged, contents of cases from a case management system which shows what was visible to the Blue Team and how the

information was interpreted can illustrate the possible defensive position. Such information can be included inline in the report or added as appendixes to the report.

Some ideas for other areas which might be relevant:

- An outline of the Blue Team’s methodologies, tools, and techniques used by the to monitor, detect, and respond to security threats and incidents, providing insight into the Blue Team's approach and activities.
- How well were detections evaluated? Did the Blue Team give the right response given the available information?
- What Indicators of Compromise (IoCs) did the Blue Team record?
- Are the generated alerts relevant and meaningful?
- How well did escalation routines work?
- How did cooperation with other teams or subcontractors work?

3.4 Purple Teaming

Many TIBER tests end up performing some sorts of Purple Teaming during the active Red Team testing phase. This can be based on the test being discovered by the Blue Team at an early stage, or as a risk reducing measure when circumstances dictate this is needed to successfully complete the test.

Purple Teaming is also possible to perform in the Closure phase, usually in conjunction with the Replay Workshop. There might be circumstances where detection could have been avoided or exfiltration performed if the Red Team had acted slightly differently. These situations can be re-evaluated in a Purple Teaming exercise after the active testing phase is completed.

If there are areas the Blue Team see could benefit from further exploration, ideas for such Purple Teaming activities in the Closure Phase should be highlighted by the Blue Team in the report.

3.5 Recommendations to Remediation Plan

Following the Replay Workshop, the White Team is responsible for finalizing a Remediation Plan following the test. Usually, a wide range of ideas for improvements are collected during the test based on the experiences gained from the testing. This Remediation Plan shall detail what actions can be taken to improve the cyber resilience of the entity after the test is finalized.

The Blue Team are in a unique position to see what actions should be taken and should suggest detailed recommendations for the plan. This can include enhancements to security controls, and areas for further training or education. Recommendations should cover not just actions for IT systems, but also recommendations for routines, roles and responsibilities in a broad perspective. What should be done differently next time something similar occurs?

The Blue Team should also include any reflections on lessons learned during the test, including successes, challenges, and opportunities for improvement, aimed at informing future security efforts and enhancing organizational resilience.

4 Example Report structure

A suggested structure for the Blue Team Test Report can be as follows:

- Executive summary
- Observations of Red Team activities
    - Scenario 1
    - Scenario 2
    - Scenario 3
- Actions performed based on observations
- Any other relevant observations
- Suggestions for activities to investigate in Purple Teaming
- Recommendations for Remediation Plan
- Any other reflections on the test

Use appendices for larger amounts of information, such as logs or raw data.

Change log

Version	Date	Change
1.0	23.05.2024	Initial version (AH)