TIBER-NL Threat Intelligence Based Ethical Red teaming

TIBER-NL

Purple Teaming Guide

January 2021

Version 0.9

Content

1 Introduction

1.1 Purpose of this document

The purpose of this guidance is to provide information about purple teaming within the TIBER-NL framework. It takes place after the RT phase as part of the closure and learning phase and is a mandatory part of any TIBER-NL exercise. It lays out all involved parties and their roles and responsibilities. It describes all the steps and components of the purple teaming process. For a broader picture of purple teaming within the TIBER-NL framework please refer to the TIBER-NL guide.

1.2 Legal disclaimer

The information and opinions expressed in this document are for informational purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

2 Principles of purple teaming

This chapter describes TIBER-NLs three purple teaming principles. These principles together describe the need for and purpose of purple teaming. The three principles are:

- Purple teaming is a continuation of the learning experience
- Purple teaming enhances collaboration between all parties involved
- The results of the purple team sessions are the base for the remediation plan

Purple teaming itself is defined as the external red team provider (RTP) (and external TI Provider (TIP)) and internal blue team working together to maximise the learning experience of the test and create a knowledge transfer. This purple teaming guide mainly focusses on RT and BT purple teaming.

2.1 Purple teaming is a continuation of the learning experience

TIBER-NL is meant to be a learning experience. Primarily for the tested FI. The purple teaming sessions should further enhance this learning experience by going more in depth into the TI, the attack, and play out scenario's which cannot be played out during the test. Together with the RTP minor findings and/or findings with an easy fix ('low hanging fruit') can already be remediated. This will lead to an even better learning experience for the BT. The external TI provider can likewise have sessions with the internal TI team when applicable.

2.2 Purple teaming enhances collaboration, provides deep insights and fun

The purple teaming phase forms a unique opportunity for the BT to get up and close with the Techniques, Tactics and Procedures of the TIP and RTP and learn from it to enhance their defence and extend their knowledge. All relevant parties of the FI can learn from these sessions. The intelligence team, the affected personnel, the defensive teams etc. It is the first time for all teams to come together and really get to understand what the other party knew and did at the different stages of the attack. Good purple teaming will take place in an amicable setting and can provide deep insights. It will amplify feedback cycles and professional growth. Purple teaming gives the RTP, TIP and the BT time together to exchange knowledge and help each other get better, thus enhancing the learning experience for all.

2.3 Purple teaming forms the base for the remediation plans

During the TTI phase and the red team test a lot of findings may come forward. The purple teaming phase normally offers the first opportunity for the BT to fix some of those findings and identify the feasible larger scale remediations which may need to be taken. By linking the purple team sessions and the remediation plan together, the output of the purple team sessions forms the base of the remediation plan. Also by involving a larger group of trusted employees in the purple team test, the TIBER test gets broadcasted more widely and helps get attention and traction throughout the organisation. Often this also helps to raise awareness and board level attention.

3 Purple teaming components

Purple teaming is a mandatory part of the TIBER-NL framework. To maximise the learning experience the purple teaming phase consists of four different components. This section will describe the different components.

3.1 Agree on a chronological process summary

As a base for the purple teaming both the RT and BT make a report based on their findings during the test. These reports should form condensed chronological summaries of what happened during the test on both sides. It should not contain any findings, just a factual process representation of what happened at which moment. This will be the base for the other components.

The main input for the chronological summary is the Red Team Report and the Blue Team Report (and the underlying log reports). In a first joint session the RT and BT will build a combined timeline and agree on what happened at which moment. How this timeline is presented is up to the RT and BT, but it is advised to visualise it instead of a written out timeline. A visual representation of the timeline makes it easier to understand and easier to work with during the rest of the test. The WT and TCT will deliver input as well based on their knowledge of what happened during the test.

This combined timeline will form the basis of the rest of the purple teaming activities and the remediation plan. Thus, it is of the utmost importance that WT, TI, RTP and BT agree on the timelines.

3.2 Table topping and what-if scenario's as a basis for later crisis management exercises

The confidentiality, integrity, or availability of critical systems can be tested during the TIBER-NL test. Many scenarios focused on availability are played out up to a point where a red team can prove that they would be able to hamper the availability of critical functions. In other tests a red team penetrates deep into the systems of the FI, proving the red team is able to obtain and manipulate the data. The second component of the purple teaming phase means to continue playing 'what if' scenarios where the scenario's had to stop, due to a too large impact on the FI and/or the tested critical function. This phase mostly consists of table top exercises or controlled live testing e.g. on non-production environments.

During the table top exercise the results of the scenario will be played out. For example, if the scenario was that critical payment functions were made unavailable, the exercise will focus on the consequences of that critical function not being available. The RTP together with the TIP and the WT will provide a realistic scenario. Goal of this exercise is to enhance the created awareness and to test whether the crisis scenarios for these kind of incidents are known and exercised regularly.

Another part of this phase is the playing out of what-if scenarios. This means the TIP and the RTP prepare for a scenario what the emulated actor could have achieved other than their primary goals. This will be played out on the day itself either in the form of a live test or a table top, whatever is deemed most suitable and effective by the WT, RTP and TIP. The TCT can advise on this if needed. The findings of this part of the PT session can provide input for a crisis management exercise for the FI. Where they play a critical function actually getting hit and the consequences of that in relation to reputational damage, press coverage, loss of trust etc. Experience learns these scenarios, which are following a realistic and detailed flow tailored to the organisation are much more meaningful than a made up scenario as are generally used in crisis management exercises.

3.3 Purple teaming

The purple teaming part is where the collaboration between the TIP, RTP and the BT is at its highest. Per phase the reconnaissance (preparation) and the attack will be replayed step by step and the teams will be working together to enhance the BT's Intel detection and defences capabilities,.

The TIP will assess the Threat Intelligence capabilities and the digital footprint of the organisation and will, together with the BT, see what possibilities there are to enhance the threat intelligence capabilities and influence their own digital footprint.

In a protected environment -and with the help from the RTP- the BT will be exposed to different TTP's the red team used during the actual test. This gives the blue team full insight in the TTP's used and should help them to enhance their defences. Each scenario (following the MITRE (pre)ATT@CK framework) should be played out phase by phase, starting with the recon phase and ending wherever the attack ended for the played scenario. Of course there is room for variation and playing additional scenario's when this seems meaningful.

Each phase should focus on the attack scenario used. For instance, if an in-phase was heavily focused on phishing, the purple teaming should focus on how the

Blue Team could have prevented the phishing attack. The session should be attended by all participants in that part of the scenario, not only the SOC but also the compromised users. The purple team sessions should not only focus on the technical aspects of the test but cover the full people, process and technology stack.

Participants differ for each purple teamed phase depending on the TTP's used and the people who were part of the test (knowing or unknowing) should take part in the purple teaming of the phase they were part of. A recommended list of participants per phase can be found in chapter 4.

3.4 Remediation Plan

After all the components of purple teaming have been completed, there will be enough input to start/continue writing the remediation report -no TIBER format is provided for this as it is quite specific- and a summary making use of the MITRE ATT@CK scheme. The purple teaming phase should lead to a learning experience for all those involved in the test as well as a draft version of the remediation report. Together with all those involved the most important learnings should be either solved directly during the purple teaming ('low hanging fruit'). Other, larger or more complicated remediations put in a draft remediation plan which will discussion remediation options and feasibility. Together with the attack summary this remediation report be the product of the purple teaming phase.

4 Participants, roles and responsibilities

Given the various phases within the purple teaming phase, it is only logical that per phase the participants differ. The main goal of the purple teaming is the learning experience which means that as much voluntary and involuntary employees of the tested FI should participate. This chapter will give an indication of the participants for each component.

4.1 Participants

The table below is to give an idea of all participants for the purple teaming phase. It is not an exhaustive list. The general recommendation is, especially for the purple teaming component to invite as many relevant participants as possible to get the most value out of it. Per part of the purple teaming component the list of attendees should be adapted to the phase which is being purple teamed.

Participant	Chronological summary	Table topping	Purple teaming	Remediation plan
WT	M	M	M	M
RTP	M	M	M	M
TIP	M	M	M	M
TCT	M	R	R	-
SOC/CDC	M	M	M	R
Senior Management	-	R	-	-
IT Administration	R	M	M	R
Compromised users	-	-	R	-
Business Analysts	R	M	M	-

M=Mandatory R=Recommended

4.2 Responsibilities

Apart from the content, the organising of the purple teaming phase lies with the WTL. Regarding content, both the RTP and the TIP have a joint responsibility of preparing and facilitating the first three sessions. The BT will in almost all cases be divided over several departments. To prevent groups from becoming too large for some subjects separate sessions have to be organised to make sure to get the maximum learning experience. The WTL is responsible for facilitating the remediation plan.

5 Planning of the purple teaming phase

5.1 Scheduling of the Purple Team phase

The purple team phase should be scheduled after the red team report and the blue team report are in their final draft stages. The start of the PT should be very closely to the end of the test. Preferably within two weeks after the release of the draft red and blue team reports.

5.2 Planning of the phases

The main goal of purple teaming is to further enhance the learning experience of the test. Therefore there is no standard planning or mandatory time expense for the purple teaming phase. The purple teaming phase should be tailored for each individual test. The purple teaming and all components are mandatory however. Therefore it is strongly recommended to allocate at least two days for it. An estimated allocation of time for each phase can be found in the table below:

Purple teaming component	**% of time allocated.**
Chronological summary	15%
Table topping	20%
Purple teaming	45%
Remediation plan	20%