



TIBER-WATER

Implementation Guide

How to conduct a TIBER-Water test

Content

1
[Introduction](#)

2
[TIBER-WATER Overview](#)

3
[Managing a TIBER-WATER Test](#)

4
[Generic Threat Landscape](#)

5
[Preparation Phase](#)

6
[Test Phase](#)

7
[Closure and Learning Phase](#)

Annex I
[Abbreviations](#)

Annex II
[Relevant documentation](#)

1 Introduction

1.1 Background

Entities that comprise the Dutch water sector must continuously work on their resilience against cyberattacks causing systemic impact. The Dutch water sector consists of drinking water companies (united in Vewin), water management (united in hetWaterschapshuis and CertWM), the Dutch Ministry of Infrastructure and Water (I&W) and Rijkswaterstaat as well as municipalities that manage objects relating to water management.

The decision was made by CertWM, I&W and Steering committee BCM to develop a Red Teaming methodology for the water sector, based on a proven methodology and which should align with Red Teaming initiatives within the Dutch government. The best in class proven methodology is TIBER-EU and it's Dutch counterpart TIBER-NL. The latter is also being adapted for use by the Dutch government, which is named TIBER-Rijk.

TIBER-NL was chosen as the basis for defining a Red Teaming methodology for the water sector. It has been adapted in workshop sessions with security representatives from the water sector. TIBER-WATER follows the TIBER-NL approach, but adds specific focus points and changes for the water sector, such as the real-world risks involved with testing Operational Technology (OT). This document has been reviewed by De Nederlandsche Bank ("DNB") to assure alignment to TIBER-NL.

Within the TIBER-WATER guide, Entities hire cyber security providers to deliver intelligence and controlled simulated attacks on their live critical production systems. Procedures and safeguards will be put in place to minimise the risk to the integrity, confidentiality and availability of the operational processes.

TIBER-WATER tests mimic potential attacks from real threat actors. The test emulates high level threat groups only (organised crime groups / hackers/ state proxy/ nation state threat actors) and thereby tests whether defensive measures taken are effective (capability assessment), supplementing the present work done by supervisors and overseers (compliance assessments). The tests also supplement current penetration tests, red teaming exercises and vulnerability scans executed within entities. Test scenarios will draw on current commercially obtained threat intelligence. This testing method aims to determine, and importantly serves to improve the cyber resilience capabilities of targeted entities. The TIBER-WATER framework is intended to improve their cyber operational resilience and ultimately, the cyber operational resilience of the water sector as a whole. TIBER-WATER testing will be a recurrent exercise. A TIBER-WATER test can therefore be defined as: the highest possible level of intelligence-based red teaming exercise using the same Tactics, Techniques and Procedures (TTPs) as real

adversaries, against live critical production infrastructure, without the foreknowledge of the organisation's defending Blue Team (BT). As such, the BT is unaware of the TIBER-WATER test. The actual test consists of time boxed phases (in, through, out).

As a consequence, existing controls, prevention measures, and security detection and response capabilities against advanced attacks can be tested throughout all phases of the attack. It also helps identify weaknesses, errors or other security issues in a controlled manner.

The test phase is followed by full disclosure to the BT and a replay (which has to include purple teaming) between the Threat Intel Provider (TIP), Red Team Provider (RTP) and the entity's BT to identify gaps, address findings and improve the response capability. During the test a White Team (WT) consisting of only the smallest necessary number of people from the entity security and business units will monitor the test and intervene when needed, e.g., when the test seems to lead to critical impact. During a test business impact is allowed to a level agreed on beforehand, critical impact is not. The WT will be in close contact with the from the TIBER-WATER Cyber Team (TCT), who conveys the TIBER-WATER test process.

Collaboration, evidence and improvement lie at the heart of TIBER. What differentiates TIBER-WATER from other security tests is its intelligence-led holistic approach and water sector's focus in which collaboration and learning are central elements. This means that entities can improve their resilience based on proven relevant weaknesses rather than on perceived / possible weaknesses. Hence TIBER-WATER delivers a higher return on security investments than solely working from a compliance-driven risk framework and defending against perceived risks. In addition, the central role of the TCT enables comparison and the distillation of best practices in the water sector.

1.2 When to use TIBER-WATER

There is no formalised checklist your entity can use to determine whether it has reached an optimal level to start a TIBER test. However, having an operational SOC / Blue Team with a basic set of use cases is strongly recommended to measure the detection capabilities.

Entities that have not yet reached a certain level of cyber maturity will likely benefit more from a gradual increase in the level of security testing, making the recommendations more manageable. See the 'WATER Red Teaming Light' document for an intermediate level approach. Once more accessible forms of security testing have been successfully conducted, the following aspects might be taken into account to determine whether your entity is ready for a TIBER test (an extract from [TIBER Short Read](#)):

- **Your entity should be of critical importance to the lives of citizens and/or the functioning of systemic entities.** Since a TIBER test requires a significant amount of resources, entities undergoing such a test should be of a certain size and/or importance for citizens and/or the functioning of the water sector, or possess 'crown jewels'. Without these characteristics, the most skilful actors operating in the digital threat landscape would, in general, be less interested in breaking your defence.
- **The culture within your entity should be open to learning experiences.** Red teaming, especially TIBER, is primarily a learning exercise. In this learning process, it should be acceptable for the blue team (the entity's cyber-defenders) to make mistakes and learn from them. Without a fair level of openness and willingness to learn and improve, a TIBER test will likely be found to be very difficult.
- **Your entity is highly recommended to conduct traditional red teaming, scenario-based testing or other security evaluation tests before participating in TIBER.** A basic cyber maturity should be established within your entity to maximize the learning effect of a TIBER test. Traditional security evaluations such as smaller red teaming tests or scenario-based tests can help achieve such maturity.
- **In order to conduct a TIBER test, your entity should have sufficient resources and personnel available.** A TIBER test is demanding in terms of resources as well as staffing. Without a structured, well-functioning blue team, it will be very hard to gain enough learning experience to enhance your entity's cyber defence. Without a properly staffed white team, the safe and efficient conduct of the test might be in jeopardy.

- **If you are interested in conducting a TIBER test, you should have the support of your entity's board.** Support from at least one board member is needed for multiple reasons:
 1. The board of your entity should take ownership of the entity's cybersecurity and should be sensitized towards related risks and weaknesses.
 2. TIBER tests are a resource-consuming effort. The board should allocate the resources needed to conduct this test.
 3. Testing on live production systems poses a certain – although very limited – risk to the continuity of business processes and should therefore be authorized by the board as the risk owner.
 4. TIBER tests will likely result in findings on the capabilities of the cyber defence of your entity. In order to properly follow up on these findings, the respective willingness and budget is required to address shortcomings. Support of your board can ensure that the necessary improvements can indeed be implemented, making the TIBER test a worthwhile exercise.

1.3 When to repeat the TIBER-WATER test

Ideally, a TIBER-WATER test should be repeated periodically, e.g. every 2-3 years. If no fixed schedule is followed, the following may be reasons to execute a new test:

- Important recommendations for improvements or additional security measures have been implemented.
- Monitoring capabilities of the Blue Team/SOC have been greatly improved.
- Significant changes have been made that affect the attack surface of the organisation.
- Cyber threats have been significantly increased.

1.3 Purpose of this guide

This guide has been developed by the Dutch Ministry of Infrastructure and Water (“I&W”) in close cooperation with all participants of TIBER-WATER and is a derivative of the TIBER-NL framework. It is meant to serve these TIBER-WATER participants and their cyber security service providers. It explains the key phases, activities, deliverables and interactions involved in a TIBER-WATER test.

This document is a guide rather than a detailed prescriptive method. It should therefore be consulted alongside other relevant TIBER-WATER, TIBER-XX and TIBER-EU materials which will be provided by the TCT to TIBER-WATER participants. This guide only details the TIBER-WATER test process. The TCT is available to answer any questions that entities or cyber security service providers might have on the TIBER-WATER test process or the TIBER-WATER program.

1.3 Legal disclaimer and copyright notice

The information and opinions expressed in this document are for information 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. This document, the “TIBER-WATER Guide”, contains material to which the European Central Bank and the Bank of England (“BoE”) own the

copyrights, as licensed by BoE under the Creative Commons Attribution 4.0 International License (i.e., the Bank of England’s CBEST Intelligence-Led Testing document, the “Licensed Material”) - a copy of which can be found on <<http://creativecommons.org/licenses/by/4.0>>. This license granted by BoE inter alia contains a disclaimer of warranties.

De Nederlandsche Bank (“DNB”) has made changes to the Licensed Material, to which changes DNB owns the copyrights. DNB also owns the copyrights to (other) additions made by DNB as contained in the NL Guide, which works are together licensed under the Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).

The Dutch Ministry of Infrastructure and Water (“I&W”) has made changes to the Licensed Material, to which changes I&W owns the copyrights. I&W also owns the copyrights to (other) additions made by I&W as contained in the TIBER-WATER Guide, which works are together licensed under the Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).



To view a copy of this licence, visit <<https://creativecommons.org/licenses/by-sa/4.0/>> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Summary of license conditions with regard to the TIBER-WATER Guide

You are free to:

- Share — copy and redistribute the material in any medium or format.
- Adapt — remix, transform and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- Attribution — you must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- Share Alike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
- No additional restrictions — you may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

- You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.
- No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy or moral rights may limit how you use the material.

2 TIBER-WATER Overview

2.1 Summary

The main goal of this chapter is to give a broad overview of the most important elements of TIBER-WATER. It describes a general process overview where all phases and the goal of TIBER-WATER is explained, it gives a brief explanation of the most important stakeholders during a test and it describes the role of the TIBER-WATER Cyber Team.

2.2 Process overview

The main goal of TIBER-WATER is to give the tested entity a learning experience as to how resilient they are against attacks from high end adversaries such as nation states and organised crime groups. This is achieved by performing a scenario based red team test based on recent intelligence as to which adversaries would be most likely to target the entity. The Red Team is then tasked to follow the tactics, techniques and procedures of the relevant actor.

The process is divided into four phases:

- **The Generic Threat Landscape phase** shows which threat actors are relevant for the entities within the TIBER-WATER scope and reflects on the motivations of these actors to attack the critical functions of the entity.

- **The Preparation phase**, during which the TIBER-WATER test is formally launched, the WT is established, the test scope is determined, critical functions (which products/ services are delivered by the organisation) are defined and approved by the board, and a TIP and a RTP are procured. If the RTP is capable of providing target intelligence and producing intelligence led scenarios to the highest standards, then procuring a separate TIP is not mandatory. The RTP in that case needs to comply with the requirements of 'Chinese walls' in scenario development between threat intelligence and red teaming phases. Note: procurement of a TIP might differ between an organisation's first TIBER-test and consecutive tests.
- **The Test phase**, during which target intelligence is gathered and intelligence led scenarios are produced, and the RTP prepares (writes a test plan) and executes an intelligence-led red teaming test against a specified target (systems and services that underpin one or more critical functions). Note: gathering of TI and development of scenarios might differ between an organisation's first TIBER-test and consecutive tests. See 6.2.1.
- **Learning and Closure phase**, during which a replay of the executed scenarios will take place between the BT, the TIP and the RTP. The TIBER process is reviewed and the entity remediation plan is finalised. Good practices will be shared with peers by the entity if the benefits of sharing sensitive

information are greater than the risks. The entity may inform their respective supervisor and / or overseer about the TIBER-WATER test in their regular meetings based on their remediation plan following the test.

The process model below is a logical depiction of the TIBER-WATER process. However, in reality the process is not such a neat linear sequence of steps: some activities may start earlier and run in parallel with others in order to increase efficiency given the limited timescales of the test. The TCT will help by advising the WTL on the timing of the test phases in order to generate synergy.

The first phase, the generic threat intelligence process, will be executed by the TCT for all of the tests. The output (Generic Threat Landscape) will be shared with the entities. The next three phases (Preparation, Testing and Closure & Learning) will be dealt with separately per entity.

2.3 Stakeholders

The most important stakeholders during a test are the following:

- White Team and their Lead (WT and WTL)
- TIBER Cyber Team (TCT)
- Board of directors of the entity
- Blue Team of the entity (BT)
- Threat Intelligence Provider (TIP)
- Red Team Provider (RTP)

2.3.1 White Team and their Lead

The White Team is the team managing the test from the entity's side. They are the only few people fully aware of the test. The White Team consists of a White Team Lead and its backup, a board member, the CISO, subject matter experts, if necessary, and a member from third parties, if necessary. For a full description of the White Team please consult the [TIBER-EU White Team Guidance](#).

As a minimum, an employee with knowledge about Operational Technology (OT) affecting the entity should be part of the WT to assess risks during the test.

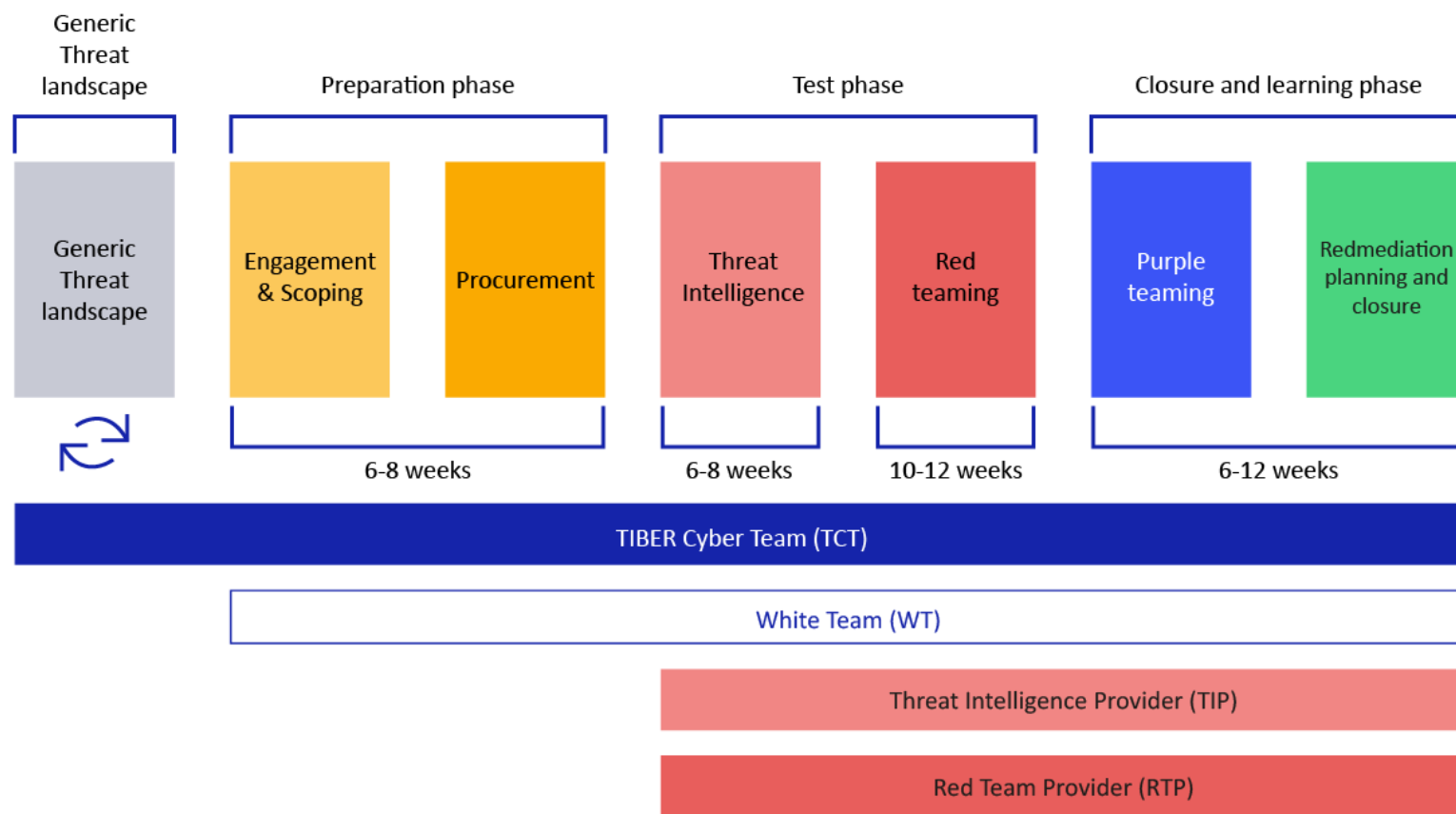
2.3.2 The TIBER Cyber Team

The role of the TCT is to make sure entities undergo tests in a uniform and controlled manner. During all phases of the TIBER-WATER process, the entity's WT closely cooperates with the TCT. The TCT conveys the WT through the TIBER-WATER phases, but can in no way be held accountable for the WT's actions or any TIBER-WATER test consequences. The TCT has a close relationship with the WT but is not formally part of the team.

The TCT will:

- Align closely with the WTL to make sure the test follows the agreed procedure and meets the right quality level for a TIBER-WATER test.
- Make sure the individual tests fit the function of the entity, the threat intelligence and high-level scenarios provided.

Figure 2.1 TIBER-WATER test process model



- Assess the level of the cyber security service providers, and the level of the work of the RTP and possibly the TIP during the test.
- Facilitate sharing and learning between the entities participating in TIBER-WATER.
- Maintain cooperation with other TIBER(-like) programs regarding testing, including TIBER-Rijk.
- R&D regarding intelligence, testing and talent development.
- Continuously develop the TIBER-WATER framework based on experiences during the tests.

2.3.3 The board of directors of the entity

The board of directors is an important stakeholder throughout the test and in various ways. One of the board members is part of the White Team and has to formally give a go on the start of the test. They will be aware of the test and what is happening and can, if necessary, take decisions with regards to events during the test. It is the responsibility of the WTL to keep the board member involved and up to date during the test.

The other board members are not aware of the test and thus only involved during the closure and learning phase. This can either be during the purple teaming sessions when the tabletop exercises take place, or when the test is finished.

After each test it is mandatory for the WT and the board to allocate time for the WT to present the findings and proposed remediations of the test.

2.3.4 Blue Team of the entity

The Blue Team (BT) is the defending team. They should not be aware of the test until the test is finished. However, due to circumstances it might be that they find out earlier about (parts of) the test, which the entity should try to prevent at all costs. After the test phase has ended the BT can be made aware of the test to its full extent. Together with the Red Team they will evaluate the findings of the test and create their learning experience during the purple teaming session.

The BT is not just limited to technical personnel such as a (outsourced) Security Operations Center (SOC) or IT administrators. The BT consists of everyone who is not part of the WT and therefore is not informed about the ongoing test. This ranges from the person receiving the phishing e-mails to personnel whose accounts might be compromised during a test.

2.3.5 Threat Intelligence Provider

The Threat Intelligence Provider (TIP) is responsible for providing the Targeted Threat Intelligence during the test phase and provide additional intelligence if necessary, during the Red Team. The TIP should provide a team with a Threat Intel lead and one or more analysts. The main product of the TIP is the TTI-report which contains a company overview, a threat landscape for the entity and scenario's to be played.

They are also part of the purple teaming sessions. For more information see the [EU services procurement guideline](#) and the [targeted threat intelligence report format](#).

2.3.6 Red Team Provider

The Red Team Provider (RTP) is responsible for executing the Red Team test based on the earlier made scenarios. For this the RTP should provide a team of a Red Team Lead and one or more red teamers who specialise in various fields of red teaming. The main products delivered by the RTP are the Red Team test plan and the Red Team report. They are the main drivers behind the purple teaming sessions. For more information see the [EU services procurement guideline](#), the [Red Team Test Plan format](#) and the [Red Team report format](#).

Selecting a RTP which has technical experience with security testing of Operational Technology used by the entity (e.g. SCADA and PLCs) is imperative for managing the risk of the TIBER-WATER test.

If the RTP has generic OT-knowledge but does not have specific expertise on the brands and types of OT used by the entity, technical manuals and data may be provided by the WT, and/or an OT-specialist from the entity may be added to the RT. The WT should ensure the RT is able to carry out attacks against the OT without exceeding the risk boundaries of the TIBER-WATER test.

3 Managing a TIBER-WATER test

3.1 Project management

The WTL is responsible for managing the project of the TIBER-WATER test. This means that it is responsible for planning the mandatory meetings, agreeing on secure communication channels, and draft a high-level overall planning for the entire test. Part of the project management is also making sure internal stakeholders such as the board are onboarded to the test in a timely manner and make sure that the external parties deliver according to the planning or make sure the planning is adapted in case of changes.

While a formal project plan is not a necessity, it is advised to create one to keep things clear. A planning is mandatory to create and communicate with all parties involved.

3.2 Risk management

There are risks associated with a TIBER-WATER test for all entities due to the criticality of the target systems, the people and the processes involved in the tests.

Before an entity engages in a TIBER-WATER test they should conduct thorough due diligence of (possible) in scope systems to ensure that at least backup and restoration capabilities are in place. Furthermore, it is advised that the entity conducts a risk assessment with regards to the risks a TIBER-WATER test poses and that these risks are taken into consideration and handled.

The entity makes sure when hiring cyber security service providers (whether a RTP and/or a TIP) that there is mutual agreement on at least the following aspects: the scope of the test, boundaries, timing and availability of the providers, contracts, actions to be taken and liability (including insurance where applicable). A check with the TCT on previous experiences with the cyber security service provider(s) involved in a TIBER-WATER test, is another measure designed to further mitigate the risk of damage to critical live systems. In addition, close involvement of the TCT in each TIBER-WATER test makes sure that the test proceeds according to the agreed test scope, scenario, planning and process as described in the cooperatively developed framework documents. Minimum requirements for cyber security service providers, both TIP and RTP, are described in the [TIBER-EU Services Procurement Guidelines](#).

Risks are also reduced by planning, informing only a select group of people in higher management about the test and the scope of the test, a clear definition of the scope and predefined escalation procedures. It is important to note that the entity remains in control of and responsible for the test. At any time, the WT can order a temporary halt if concerns are raised over damage (or potential damage) to a system or business processes. Trusted contacts within the WT positioned at the top of the (security) incident escalation

chain help prevent miscommunication and knowledge about the TIBER-WATER test leaking out.

To prevent TIBER-WATER tests from leaking out, code names are used. These code names should be used throughout all documentation related to the TIBER-WATER test as best as possible but at least in document titles and throughout the documents. Elements where codenames can't be used (such as, but not limited to URL's, screenshots etc) are exempt and the full name of the entity can be used. Codenames will be assigned by the entity. It is important to make sure one codename is used throughout all documentation.

The testing should be flexible enough to mimic the (seen, current and potential future) actions of a real threat actor *and* is to be performed in a planned and controlled manner in order to (amongst other things) ensure uniform testing, protect those involved (e.g. indemnifications) and prevent damage. These elements are essential in order to make sure the entity and its peers can learn and evolve, not only using their own but all relevant results and findings.

As a result of the test, it is possible that during a test the BT has reached a level of escalation where it starts to inform relevant authorities such as, but not limited to, police, intelligence agencies or data-protection agencies. The WT should at all times try to prevent this from happening. Authorities should not be burdened by a TIBER-WATER test. In case the WT is informed of an active escalation to third authorities, the test should immediately be paused and measures should be taken to prevent the authorities to act on the incident escalation.

The following is prohibited in TIBER-WATER (not an exhaustive list):

- Unauthorised destruction of equipment
- Uncontrolled modification of data / programs
- Unauthorized jeopardizing continuity of critical services
- Extortion
- Threatening or bribing employees
- Kidnapping
- The use of names, logos or otherwise identifiable information of real people or companies

4 Generic Threat Landscape

4.1 Summary

The Generic Threat Landscape (GTL) is a document describing the threat landscape of the entities within the TIBER-WATER scope. It is created by the TCT and distributed to the WT as soon as the test starts. It shows which threat actors are relevant for the entities within the TIBER-WATER scope and reflects on the motivations of these actors to attack the critical functions of the entity.

4.2 Process

The TCT continuously monitors cyber threats using various internal and external sources and creates a GTL every year. The basis of this GTL is a generic threat report for the Dutch vital sectors created by The General Intelligence Agency (AIVD), which is enriched, refined and made specific for the water sector.¹ The results are combined into a threat landscape which shows the main threat actors targeting the critical functions of the Dutch water sector.

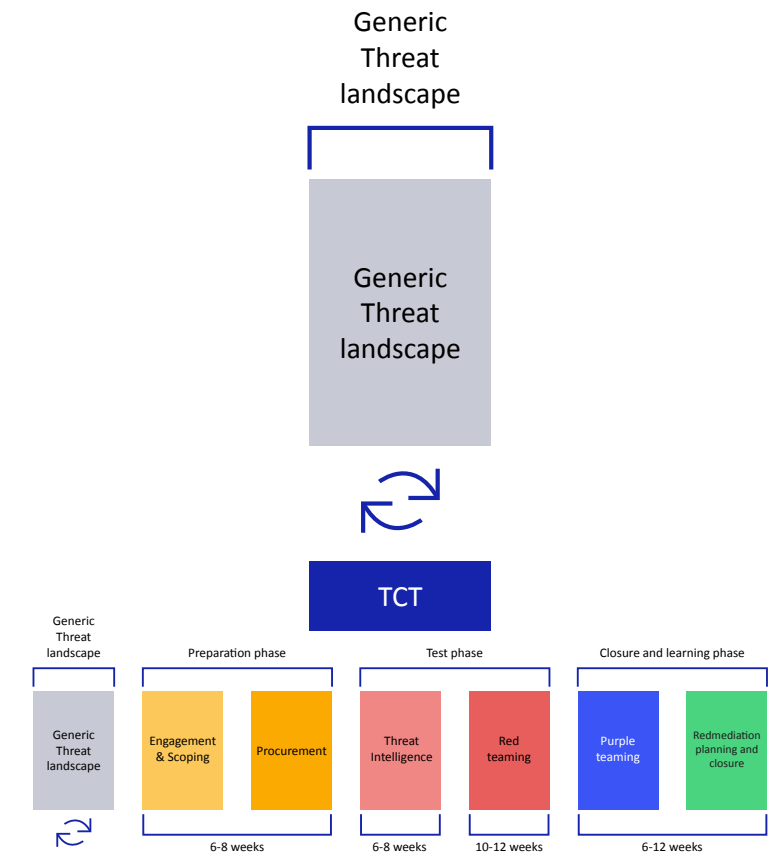
4.3 Meetings

During the GTL-phase there are no mandatory meetings.

4.4 Deliverables

The main deliverable is the Generic Threat Landscape. The document is delivered yearly and distributed on demand each time a test starts and the TIP and RTP have been procured.

Figure 4.1 Generic threat landscape overview



¹ This is currently in development. The first report is expected to be delivered by the end of 2023.

5 Preparation Phase

5.1 Summary

During the TIBER-WATER Preparation Phase the TCT starts engaging with the entity and the project is formally launched. The scope is established, and the entity procures the cyber security service provider(s). The duration of this phase of work is approximately 4–6 weeks, not including the duration of the entity procurement process. The goal of the preparation phase is to deliver the scoping document, procure the providers and formally launch the TIBER-WATER test.

5.2 Process

5.2.1 Engagement

The Pre-Launch meeting marks the start of the planned and agreed on TIBER-WATER process for the entity. The entity establishes a WT. This comprises a select number of senior individuals who are experts and/or are positioned within the security incident escalation chain. The WTL will make sure they are aware of the TIBER-WATER test, the need for secrecy and the process the team should go through in case the BT detects and escalates a TIBER-WATER related incident.

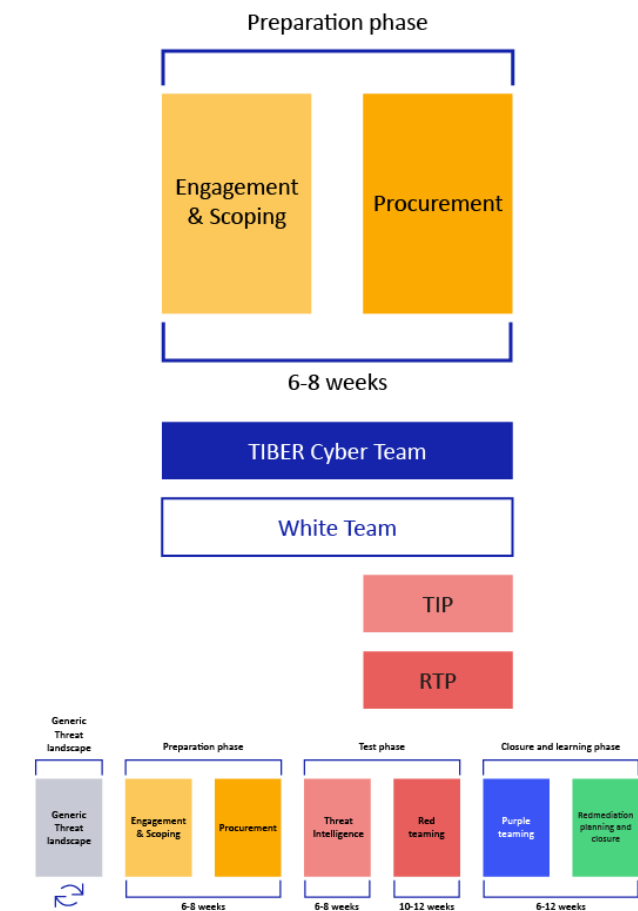
5.2.2 Scoping

During the launch, the TCT provides the entity with the latest version of the TIBER-EU Scope Specification format. The entity then starts work on a draft version. The TCT is available during the scoping process to clarify the requirements and is available to give feedback.

The TIBER-EU Scope Specification defines the scope of the TIBER-WATER test, specifically the critical functions involved. Critical functions are defined as the people, processes and technologies required to deliver a core service which, if disrupted, could have an impact on the Dutch water sector, the organisations safety and soundness, the organisations customer base or the organisations market conduct.

Entities across the water sector support and deliver these functions in different ways via their own internal processes and outsourced services, which are in turn underpinned by critical systems. It is these critical systems, processes, and the people surrounding them, that are the focus of TIBER-WATER threat intelligence and Red teaming. Flags are placed on the critical systems in the [TIBER-EU Scope Specification document](#). These flags form the goal for the later test scenarios which are based on relevant threat intelligence.

Figure 5.1 Preparation phase overview



The entity is allowed to involve the RTP and TIP in the scoping process.

During the scoping process, the entity must complete the [TIBER-EU Scope Specification](#) document. The TIBER-EU Scope Specification sets out the scope of the TIBER-WATER test, and lists the key systems and services that underpin each CF. This information helps the WT set the “flags” to be captured, which are essentially the targets and objectives that the RTP must strive to achieve during the test.

The WT should discuss the flags with the TCT. Although the flags are set during the scoping process, on some occasions they can be changed following the threat intelligence gathering and as the test evolves.

Specific learning objectives for the entity should also be defined and documented by the WT as part of this phase. For instance, ‘Identifying blind spots of security monitoring of our OT and response’.

5.2.3 Procurement

With regard to contractual considerations, smooth delivery of a TIBER-WATER test requires that the process is transparent and appropriate information and documentation flows freely between the relevant parties. To facilitate the free flow of information, Non-Disclosure Agreements (NDA) can be used.

The necessary elements for a RFP (Request for Proposal) used to procure a TIP and an RTP, can be found in the [TIBER-EU Services Procurement Guidelines](#).

After the Pre-Launch meeting, the entity starts its procurement process. The entity then selects a RTP and a TIP to perform the test. Importantly, the entity offers a shortlist of potential providers to the TCT and receives feedback regarding the providers from the TCT.

During procurement the entity undertakes the following activities:

- Procures and takes on board a RTP and a TIP, ensuring that it has incorporated the NDA clauses into its cyber security service provider contracts.
- Completes the TIBER-WATER Test Project Plan, including the schedule of meetings to be held between the entity, TIP, RTP, and TCT.

Note: the requirements for a TIP might differ between the first test and consecutive tests at the same entity. These requirements need to be agreed upon by both the WT and the TCT. Paragraph 6.2.1 will go into detail about potential differences.

5.2.4 Go/No go

After all steps have been completed there will be a formal go/no go moment where WTL will decide whether the Preparation phase has been completed, the quality has been sufficient according to TIBER-WATER, all meetings have taken place and all deliverables have been delivered. The WTL will inform the TCT about the outcome and any deviations. The TCT will review and provide guidance where necessary.

5.3 Meetings

During the preparation phase the following meetings are mandatory:

- Pre-launch meeting
- Launch meeting
- Scoping meeting

Apart from the mandatory meetings it is advised that the TCT and the WT have regular meetings to discuss progress. The TCT can, whenever needed, support the WT in the procurement process or participate in workshops to create a scoping document.

It is of the utmost importance that both the RTP and the TIP understand the scope of the test, not only the technical components but also the business processes. If the WT feels this isn’t the case, it is advised to have a meeting where the scoping document is explained by the WT to the RTP and the entity.

Special attention should be paid to ensuring the RTP has a full understanding of the real-world impact and risks for the objects linked to the Operational Technology in scope of the test.

5.3.1 Pre-Launch Meeting

The pre-launch meeting finalises the pre-launch phase. A WT is established, and it marks the start of procurement of the TIP and RTP. The framework is explained to the WT and expectations are exchanged between the WT and the TCT. After the pre-launch meeting the risk register can be created and a planning can be made. It is a preparation for the launch meeting in which also the providers will be present.

The participants of the Pre-Launch meeting are:

- WT
- TCT

5.3.2 Launch meeting

The launch meeting is the formal launch of the TIBER-WATER test. During the launch meeting the following topics are discussed:

- the TIBER-WATER process and documentation
- stakeholders, roles and responsibilities
- contractual considerations
- project planning
- preparation of leg-ups

After the launch meeting the TIBER-WATER test is formally started. The launch meeting can be combined with the scoping meeting.

The participants of the Launch meeting are:

- WT
- TCT
- RTP
- TIP

5.3.3 Scoping meeting

During the scoping meeting the scoping document is agreed upon by the TCT and the entity. More importantly this is the meeting where the scoping document is approved by one board member of the entity.

The participants of the scoping meeting are:

- WT
- TCT
- RTP
- TCTP
- C-level member of the entity

The launch meeting and the scoping meeting can be combined for efficiency.

5.3.4 Business Overview Workshop

To support the TIP and RTP in their understanding of the entity, a workshop is planned to discuss the activities of the entity and how this would impact its threat landscape.

The WT should prepare the following for this meeting:

- explanation about the core business of the entity, what is most critical for them and why is the entity vital for the broader landscape of entities.
- a business and technical overview of each CF-supporting system in scope.
- the current threat assessment and/or threat register.
- Importance of objects and associated OT in scope, including risks and real-world impact.
- examples of recent attacks.

The participants of the scoping meeting are:

- WT (including a business expert)
- TCT
- RTP
- TIP

5.4 Deliverables

The main deliverables of the preparation phase are that

- a WTL is appointed and a WT is formed;
- a RTP and TIP have been procured;
- a scoping document is delivered;
- the scoping document is approved by a C-level executive of the entity;
- communication protocols are established and relevant communication groups are created; and
- file sharing policies are established.

6 Test Phase

6.1 Summary

During the Test phase target intelligence on the entity is gathered. This results in intelligence-led test scenarios. These scenarios will be expanded by the RTP into a Test Plan. If urgent findings are found to be relevant to other entities, these will be shared. How extensive the 'intelligence gathering' needs to be depends on a number of factors. Is this the entity's first TIBER-WATER test or a successive test? How much time has there been between tests? How much has the entity changed between tests? And how much has the threat landscape changed between tests?

6.2 Process

6.2.1 Threat Intelligence phase

6.2.1.1 Threat intelligence gathering and reporting

In this phase, during the first TIBER-WATER engagement of the entity, the TIP executes an initial furtive, broad, intelligence-based targeting exercise of the kind typically undertaken by threat actors as they prepare for their attack. The objective is to draw a picture of the entity as a target from the threat actor's perspective. The use of various methods (including OSINT, TECHINT, and intelligence-based initial targeting) is encouraged. It cannot be stressed enough that this phase is a passive phase. No active reconnaissance should be undertaken. All reconnaissance should be performed in close cooperation with the RTP.

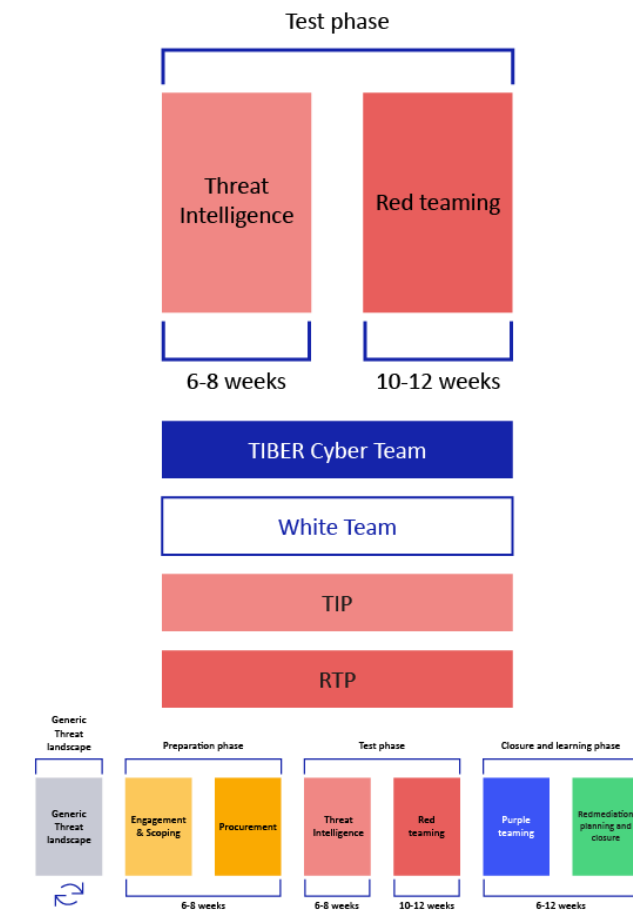
The targeted threat intelligence (TTI) process results in the production of a TTI-Report, which is a bespoke, focused threat intelligence report for the entity being tested. It consists of three parts:

1. A business overview from an intelligence perspective. This section is meant to provide a strategic understanding of the business of the entity and its current and planned activities. It also gives a more detailed insight into the business and systemic consequences of compromise of the critical functions. This is primarily based on the information gathered in the business overview workshop as discussed in 5.3.4.

2. Actors and high-level scenarios. For relevant threat actors it will be determined how likely and capable they are to attack the CFs of the entity. This will lead to a list of most likely and capable threat actors. The TIP can use the GTL as a starting point, but it is possible to motivate which additional threat actors would be relevant from the TIP perspective. These actors will form the basis for the scenarios. The TIP will write a high-level scenario of how an attack by the specific threat actor would take place including with which motivation and intent the threat actor would attack specific CFs. Based on this the enrichment of the TTI-Report contains the following items:

- Most likely threat actors to target the CF of the entity.

Figure 6.1 Test phase overview



- A motivation as to why exactly these threat actors are relevant.
- Most likely targets for each threat actor based on the scoping document.
- High level scenarios for the most likely threat actors.

3. Intelligence on entity's (digital) presence to support the scenarios. In this part the TIP provides the RTP with (passive) intelligence that relates to the scenarios that are drafted. For example: a scenario of an OCG attacking via RDP vulnerabilities is only relevant if the entity is vulnerable to these kinds of attack. This part of the TTI-report serves mainly to provide more detail on how the proposed threat actor would potentially attack the entity, given the real-life opportunities found in the entity's (digital) footprint. The entity can provide information to help focus the search of TIP. It is not the intention of this section of the TTI-report to provide a broad data dump on everything that there is to find about the entity. This is done by the RTP. The intelligence should, as mentioned, relate to the proposed scenarios.

The target intelligence delivered by the TIP will contribute to the further development of the test scenarios.

Some key considerations for the TIP:

- TI providers must engage with the entity to obtain useful context for conducting the threat analysis. To facilitate this the business overview workshop (5.3.4) is planned.

Although the entity may not always be able to share the details of sensitive incidents with the TIP, it should still be possible to learn about the entity both through engagement gathering and evidence of previous breaches from public sources. The TIBER-EU Scope Specification can be a basis for this.

- Cyber security service providers should have adequate language support. Languages play an important role in providing cyber threat intelligence. Cyber threats are a global phenomenon, and a TIP that offers little linguistic coverage of online threats will potentially miss a significant proportion of relevant information.
- TI providers should be able to use a variety of methods in intelligence gathering, for example OSINT (which is derived overtly from publicly available sources).
- TI providers must always demonstrate strong ethical behaviour.
- TIP and RTP must work together in a collaborative, transparent and flexible manner. A TIP must demonstrate willingness and the ability to work in this way, sharing its deliverables with its RTP counterpart for review and comment. The TIP should also demonstrate a willingness to work with the RTP during the remainder of the test. This includes the creation of testing scenarios, as well as any new intelligence requirements that occur as the test progresses. The TIP is expected to provide input into the final report issued to the entity.
- Should the TIP and the RTP be separate parties, it is essential that the RTP is involved during the TI phase.

Differences between TI reports for first and successive TIBER-tests

The standard requirement for every TIBER-WATER test is a full TTI-report, created according to the TIBER-EU TTI-framework and the guidance of the TCT. In some instances, the standard TTI-requirement may not be in the best interest of the participating entity. For the consecutive TIBER-WATER test, the organisation or its threat landscape may have stayed largely the same since the foregoing test. In these cases, creating a full TTI-report may lead to a significant overlap in TTI-reports. In case the standard TTI-requirement offers too little added value for a participating entity, the WT may decide to procure an update to the last TTI-report if legally agreed with the first TTI provider.

The following non-exhaustive list of factors is relevant for this decision:

- a. The degree in which the threat landscape has changed since the start of the TI-phase of the foregoing TIBER-WATER test (geo-political changes, new threat actors, modus operandi, etc.).
- b. The degree in which the profile of the entity has changed (reorganisations, mergers, change in customers & services offered, system changes, etc.).
- c. The report that is updated cannot be older than 24 months. The WT may deviate from this term in case of special circumstances.

Additional information delivered by the entity

The entity delivers additional information for the TIP on the scenarios chosen including on people, (business) processes and systems targeted in the scenario. The level of detail of this information is up to the entity to decide.

The TIBER-WATER process is designed to create realistic threat scenarios mimicking possible (future) attacks against the entity. Real-world threat actors may have months to prepare an attack. They are also able to operate free from some of the constraints that cyber security service providers must observe, such as the time and resources available – not to mention the moral, ethical and legal boundaries¹. This difference can cause challenges when attempting to create realistic scenarios as knowledge about the internal network is often the hardest to gain using morally, ethically or legally justified techniques.

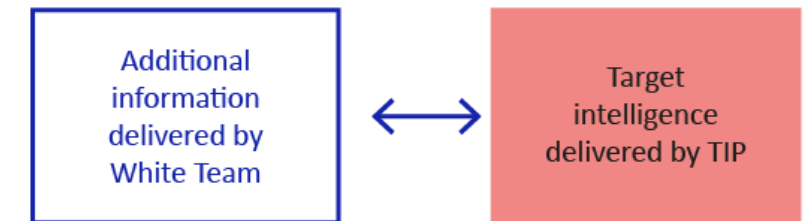
A similar constraint relates to the systems underpinning the CF's which typically do not have a large footprint on the public internet. Whether they are internal bespoke systems or external systems that span multiple organisations with common connecting infrastructure, the knowledge of the functioning of these systems with an RTP may be limited in comparison to those threat actors with the capacity and time to study these extensively.

Therefore, it depends on the entity how much information it is willing to give to make sure the RTP is on the right level of knowledge to mimic advanced attacks. This way, TIBER-WATER reflects a 'grey box' testing approach in contrast with the 'black box' approach. The RTP receives support from the entity itself in order to balance out the smaller number of possibilities it has compared to high end attack groups. Experience shows that the more relevant information an entity gives to the RTP the more the entity will gain from the test. Of course, there will be a balance to observe. The claim may never be made in hindsight that the test was manipulated and a real threat actor could not have gotten that information. Therefore, it should be evident that the information given to the RTP could have been obtained by an advanced threat actor, given more time, different known techniques etc. Whether this information is provided by the entity or delivered by a TIP, is up to the entity.

Figure 6.2 shows the balance between target information delivered by the entity or TIP. More of one means less is needed from the other, and time can be spent elsewhere (for the RTP this will mean relatively more actual test time).

The WT should give the TIP access to the previous TTI-report to prevent overlap and to ensure the new report is drafted as efficiently as possible. The updated TTI-report should be created in accordance with the TIBER-EU TTI-format. It is the responsibility of the WT to ensure that both the previous and the current TIP agree with this approach. After the TTI-Report is finished there is a formal handover from the TIP to the RTP.

Figure 6.2 Balancing information entity and TIP



6.2.1.2 Go/No go

After the TTI-report has been delivered there will be a formal go/no go moment where the White Team together with the TCT will determine whether the TTI has been completed, quality standards are met, meetings have taken place and deliverables have been delivered.

¹ It is up to the entity to set up contractual agreements with the RTP regarding e.g., the inviolability of their employees' privacy. It is, however, important to note that privacy related information is left out from test reports under all circumstances.

6.2.2 Red Teaming phase

6.2.2.1 Red Team test plan

In the Test Plan, the RTP will put together scenarios for the TIBER-WATER test which:

- uses the TTI-Report (entity + RTP/TIP) and aligns these into credible attack scenarios.
- provides background to the tradecraft of the type of threat actor that is mimicked in the test.
- gather OSINT information that would help the threat actor achieve its goal.
- would, if occurring in real life, have impact on the Dutch water sector.
- provide some elements which test the response of the entity, including evidence on whether the compromise action would be immediately detected or could have a fair chance of succeeding.

Attack scenarios

The scenarios are written from the threat actors' point of view and are intelligence-led. The RTP indicates various creative options in each of the test phases based on various TTPs used by advanced threat actors, to anticipate changing circumstances or if the first option does not work. The RTP should also indicate where a leg up might be needed if the attack is not successful and what this leg up will entail. The scenario writing is a creative process.

The TTPs do not only mimic those seen in the past, but can combine techniques of various relevant threat actors thus saving resources. The RTP should motivate why threat actors' techniques could be combined in the scenario.

Rules of engagement

Part of the test plan should be the rules of engagement. This is a part of the test plan where the RTP lays down the rules they will abide to during the engagement. The rules of engagement should contain at least the following:

- High level description of the techniques being used during the attack.
- List of excluded techniques.
- Detailed description of scenario's used for social engineering.
- How privacy of both voluntarily and involuntarily participants is being safeguarded in compliance with rules & regulations.

The boundaries defined in the scoping document are input to these rules of engagement.

Operational Technology

For TIBER-WATER special attention should be paid to testing of Operational Technology (OT) due to the real-world impact that manipulation could cause. OT devices may malfunction or be rendered inoperable by even simple port scans, so extreme care must be undertaken. As a minimum, an OT subject matter expert (SME) should be part of the WT and any actions against OT should be approved by the WT (right) before they are executed by the RT. If the operational impact cannot be assessed, the risk is deemed to be unacceptable and an alternative solution must be used. In this case, the WT and RTP could consider:

- Switching to purple teaming once access to OT has been proven by the RT, accepting that incident response is no longer assessed during the TIBER-WATER test.
- Accepting screenshots as proof of access to OT systems.

- (Scheduled) maintenance on OT that may impact availability or redundancy requirements.

Detailed out phase plan

Before the start of the out phase, a plan has to be delivered by the RTP on how they will approach the out phase. This plan should contain at least the following elements:

- Detailed description of the objective on the out phase and the scope of the out phase.
- Detailed description of the TTP's being used during the out phase.
- An overview of business knowledge needed to perform the out phase.
- A list of possible specialists needed to perform the out phase.
- Risks to be managed during the execution of the out phase.
- Possible leg-ups for the out phase.

It is up to the WT to supply the required business knowledge and the specialists. The TIP has to judge whether the required knowledge by the RTP is realistic in comparison to the simulated threat actor. If it is not deemed realistic it is advisable that the WT makes a judgment call on whether to supply the information or not. This depends on the risk for the continuity of the business of the proposed actions.

Approval of the RT test plan

At two points during the test there will be a formal approval of the RT test plan:

- Before the test phase starts the RT test plan is approved by the WT (including the board member), TCT, TIP and RTP.

- After eight weeks the RT test plan is finalized and approved again when the detailed plan for the out phase is added.

6.2.2.2 Go/No go

After the Red Team test plan has been delivered there will be a formal go/no go moment where the WT will determine whether the quality of the Red Team test plan is sufficient.

6.2.2.3 The Red Team test

The RTP now moves into execution of the TIBER-WATER test during which it performs an intelligence-led red teaming exercise on the target systems. The scenarios are not a prescriptive runbook which must be followed precisely during the test. If obstacles occur the RTP should show its creativity (as advanced threat actors would) to develop alternative ways to reach the test objective. This is always done in close contact with the WT and the TCT. All actions of the RTP are logged for replay with the BT, evidence for the RTP report and future reference.

The test objectives (compromise actions) are the ‘flags’ that the RTP must attempt to capture during the test as it progresses through the scenarios. Of course, all captures are in close cooperation with the WT and the overall aim is to improve the BT capabilities. The scenario is to be played out from beginning to end. The RTP may need some help to overcome barriers, it may be discovered etc. but the scenario must continue to make full use of the TIBER-WATER exercise within the given timeframe and test all phases of the test (in, through, out).

RTP are constrained by the time and resources available as well as moral, ethical and legal boundaries. It is therefore possible that the RTP may require occasional steers from the WT to help them progress. Should this happen, then these steers are duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

At all times the RTP liaises closely with the entity’s WT and with the TCT. RT and WT should have daily meetings to discuss the upcoming attack activities and an instant messaging channel for quick discussions and approvals. The RT should always obtain approval before executing an attack step (especially when attacking OT) so that the WT is able to assess the associated risk.

The TCT is updated at least once a week by the RTP and WT on the progress. Physical meetings between the WT, TCT and RTP during this phase are strongly encouraged since the discussions add significantly to the quality of the test. Also, entities have had very positive experiences when a member of the WT is onsite with the RTP for some time during the engagement.

During week six of the test there is a cut-off point. If after 6 weeks the Red Team has not been able to complete the “in phase” the RTP will be provided with realistic leg ups so the rest of the scenario can be played or, in case the RTP has gained foothold in another scenario, it can be allowed to use that path for the rest of the scenario where the “in phase” failed.

6.2.3 Removing the TIBER-WATER label of a test

As the TCT is not part of the commercial relation between the RTP and the entity, it cannot stop the test. It however has the power to remove the TIBER-WATER label. Which means the test is not recognized as a TIBER-WATER test. The TCT is therefore very careful in its decision to remove the TIBER-WATER label. The quality and safety of the exercise should always be at the heart of the test.

The TCT can remove the TIBER-WATER label in the following situations (this is not an exhaustive list). The decision will always be made in consultation with the WT unless the situation doesn’t permit this:

- Either the TIP or the RTP has (repeatedly) shown it cannot live up to the standards laid out in the TIBER-WATER framework
- The test has been compromised by the RTP, TIP or the entity either intentional or as a result of (gross) negligence
- When there is foul play by the WT/BT
- All other situations which compromise the quality, safety or the secrecy of the test

Should the TCT decide to remove the TIBER-WATER label, the entity can choose to continue the test gaining the learnings from the test but without it being recognized as a TIBER-WATER test, or the entity can consult with the TCT what steps have to be undertaken to make the test a TIBER-WATER recognised test.

6.3 Meetings

The following meetings are mandatory during the test phase:

- Weekly update meetings
- Approval of the TTI-report
- Approval of the RT test plan
- Formal handover workshop from the TIP to the RTP

Weekly update meetings

During the complete test phase, both the threat intelligence part and the Red Team test part, there will be weekly update meetings where the TIP and/or the RTP gives an update on the weeks progress and discuss next week's activities. This is to keep all parties involved and up to date with the test and to ensure quality standards are met.

The participants of the weekly update meetings are:

- WT
- TCT
- TIP
- RTP

While not mandatory it is advised that both TIP and RTP are present throughout all the update meetings, whether they are during the intelligence phase or the Red Team phase of the test.

6.3.2 Approval of the TTI-report

After the TIP delivers the TTI-report there is a meeting to give formal approval of this report. This is done to make sure that

the TTI-report meets the quality standards of TIBER-WATER and contains all the components of the [TTI-report](#).

The participants of the approval of the TTI-report are:

- WT
- TCT
- TIP
- RTP

6.3.3 Formal handover TIP to RTP

After the TIP delivers the targeted threat intelligence report there is a workshop with the TIP and the RTP where the TIP explains the scenarios to the RTP so they can modify the scenarios into a RT test plan.

The participants of the handover are:

- WT
- TCT
- TIP
- RTP

This meeting can be combined with the approval of the TTI-report.

6.3.4 Approval of the RT test plan

After the Red Team has created the RT test plan there is a meeting to give formal approval of the RT test plan and start the Red Team phase of the test. This is to ensure that the RT Test Plan meets to quality standards of TIBER-WATER and contains all components of the [Red Team Test Plan format](#).

The participants of the approval of the RT test plan are:

- WT
- TCT
- RTP

6.4 Deliverables

The main deliverables of the test phase are that:

- a TTI-report has been approved based on the [Targeted Threat Intelligence Report Format](#)
- a RT test plan has been approved based on the [Red Team Test Plan format](#)
- the Red Team test has been completed

7 Closure and Learning Phase

7.1 Summary

The closure and learning phase starts when the test is finalised. Reports are written, learning experiences are capitalised through purple teaming, results are communicated to the board and the test summary is written. The phase consists of different elements each having a different goal. The closure and learning phase takes approximately 6-8 weeks.

7.2 Process

7.2.1 Purple teaming

7.2.1.1 Red Team test report and Blue Team report

The output of this activity is a draft version of the Red Team Test Report produced by the RTP for delivery to the entity. The draft report must be issued within two weeks of test completion. The report must give an overview of the whole TIBER-WATER process, including the CFs in scope, the threat intelligence base of the test, the scenarios planned, the scenarios executed, the findings of the test and the advice of the RTP to the entity. For the RT report the [RT test report format](#) should be used.

The key members of the entities' BT are informed of the test and will write their own report ahead of the purple teaming session. Should, due to findings or omissions in the monitoring the BT not be able to write a full report, the RT report can be supplied to them to help them in procuring the

report. Both RT and BT reports are input for the purple teaming session.

7.2.1.2 Purple teaming

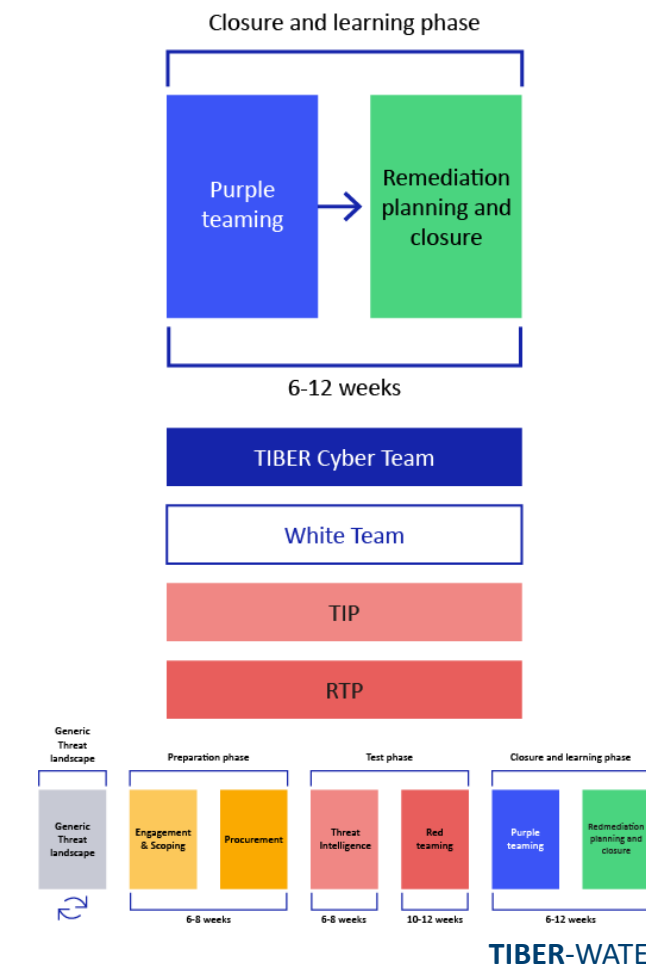
After the RTP delivers its report, the entity arranges a purple teaming workshop. This workshop lasts at least a full day. Often this phase is perceived as the most educational and hence more days are being used. The goal of this workshop is to enhance the learning experience. During the purple teaming workshop, the RTP and entity should replay the attack and collaborate with each other to enhance specifically the defensive capabilities of the entity, as a spin off the attacking capabilities of the RTP will grow. The TCT should be present during parts this meeting. Purple teaming and who should be involved and participate will be described in more detail in the [TIBER purple teaming best practices](#). Purple teaming in TIBER-WATER is an expansion of the replay where the learning experience for both the BT and the RTP is enhanced.

7.2.2 Remediation planning and closure

7.2.2.1 360-Feedback

During the 360-feedback meeting, the entity (WT and BT), TCT, TIP and RTP will come together to review the TIBER-WATER exercise. The TCT arranges and facilitates the workshop. In the 360-feedback report all parties deliver feedback on each other. Goal is to further facilitate the learning experience of all those involved in the process for future exercises.

Figure 7.1 Closure and learning phase overview



The 360-feedback meeting is a review of the process and performance of all parties involved. It is not meant to discuss findings of the test. The learnings are to be used for all parties involved to make the next TIBER-WATER test they are part of an even better learning experience.

During the feedback meeting, the WT also provides feedback on how well the learning objectives have been met during the TIBER-WATER test.

For the meeting the [360-feedback format](#) could be used.

7.2.2.2 Remediation plan and TIBER-WATER Test Summary

Based on the test outcomes the entity should work on a remediation plan. The TIBER-WATER documentation can be used to support the business case for implementing improvements to mitigate the vulnerabilities identified during the TIBER-WATER test. Input for the remediation plan can be the TIP report, the RT report, the BT report, input from the WT and organisational findings.

The TIBER-WATER Test Summary summarises the TIBER-WATER process and should draw upon the delivered documentation such as the RT and BT reports, the Targeted Threat Intelligence and when available its remediation plan(s). For this the entity should use the [Test Summary format](#).

The gathered intelligence and lessons learned from the test will be input for the Generic Threat Intelligence Report used in future tests.

7.2.2.3 Result sharing

1. Board level executives

It is of the utmost importance that the board level of entity is informed on threats, test results and the remediation plan (risk mitigation measures). The TCT will be attending the presentation of the results and findings to board level and the TCT will stress the importance of board attention, support and accountability in executing the remediation plan.

2. White Team Leads

Since the TIBER-WATER test focuses on the Dutch water sector as a whole, sharing of information between the entities is an important part of the TIBER-WATER framework. As one of the main goals of TIBER is enhancing the sector's operational resilience against advanced threat actors, the entity shares effective remediation solutions and best practices with relevant peers promptly to enhance the cyber resilience of the sector. The entity can share more general lessons learned via the anonymized test summary. The TCT and the WT can discuss the forum for sharing the information, and the level of detail. In general, results are shared during the WTL meetings in which the White Team Leads of the different entities.

3. External parties

The decision to share information with external parties resides entirely with the entity. The RT test report and other sensitive documents belonging related to the TIBER-WATER process will remain on premise of the entity. The TCT will not share TIBER-WATER related information or documentation regarding a specific entity. The TCT is available to give an explanation regarding the TIBER-WATER program at the request of the entity.

7.2.2.4 Finalising the test

After the test is finished, results have been shared and after the purple teaming is finished the WTL should make sure that all remains of the test are cleaned up. This means that eg: all traces of malware used during the test should be cleaned up, all data dealing with the test is removed at the participating teams. The RTP should assist the WTL, all communication groups be closed down unless still needed. After all this is done the WTL make the formal decision that the TIBER-WATER test has ended.

7.3 Meetings

The most important meetings during the closure and learning phase are:

- Kick-off purple teaming
- Board meeting
- 360-feedback session

7.3.1 Kick-off Purple Teaming

The kick-off for the purple teaming session marks the start of the purple teaming. The first component of purple teaming usually is creating a chronological summary. After that the none of the elements are mandatory. It is however recommended to follow all stages of purple teaming and allocate enough time for it to maximise the learning experience. The recommendation is to allocate a minimum of 2 full days of effort and to decide on the duration between the WT and RT. The purple teaming is where most of the learning experiences are gained.

During the purple teaming the kick-off the following are present:

- WT
- TCT
- RTP
- TIP
- BT

7.3.2 Board meeting

After the purple teaming session and finalisation of both BT and RT reports a board meeting is used to communicate the results and the impact of the test. It is important that the board understands the full extent of the results of the test and the impact it had on the organisation.

During the board meeting the following are present:

- WT, including the involved board member
- Board of the entity
- TCT
- The TIP and RTP are optional participants.

7.3.3 360-Feedback session

During the 360-feedback session all parties actively involved evaluate the test. The evaluation is done on the TIBER-WATER process and not on the actual results of the test. The evaluation focuses on how all parties involved performed in light of their role in the process.

During the 360-feedback session the following are present:

- WT
- TCT
- RTP
- TIP
- Optional: key persons from the BT (e.g. when purple teaming has started early)

7.4 Deliverables

The main deliverables of the closure and learning phase are that:

- A RT report is delivered based on the [TIBER-EU Guidance for the Red Team Test Report format](#).
- A BT report is delivered.
- The board is informed on the results of the test.
- A 360-feedback report is delivered, which may be based on the [TIBER-NL 360-Feedback format](#).
- A TIBER-WATER Test Summary is delivered based on the [TIBER-NL Test Summary format](#).
- The entity has started to work on addressing and remediating the findings.

Annex I Abbreviations used in this document

<u>Term</u>	<u>Explanation</u>	<u>Term</u>	<u>Explanation</u>
BT	Blue Team	SCADA	Supervisory Control and Data Acquisition system
CBEST	The Bank of England cyber resilience program on which TIBER-WATER is based	TCT	TIBER-WATER Cyber Team
CF	Critical Functions	TECHINT	Technical Intelligence
GTL	Generic Threat Landscape	TI	Threat Intelligence
IOC	Indicators of Compromise	TIA	Threat Intelligence Advisor
I&W	Ministry of Infrastructure and Water Management	TIP	Threat Intelligence Provider
MO	Modus Operandi	TIBER	Threat Intelligence Based Ethical Red teaming
NDA	Non-Disclosure Agreement	TTI	Targeted Threat Intelligence
OSINT	Open-Source Intelligence	TTP	Tactics, Techniques and Procedures used in a cyber attack
PLC	Programmable Logic Controller	WT	White Team
RT	Red Team	WTL	White Team Lead
RTP	Red teaming Provider		

Annex II Overview of relevant documentation

All documents are 'living' documents. After the first TIBER-WATER testing period drafts have been developed for the second testing round that have been aligned with the TIBER-EU and TIBER-NL documentation. Each future round or development will possibly lead to revision of the TIBER-WATER documentation. The TIBER-WATER process must always be agile enough to adapt to the evolving threat landscape.

Please note that most the documents listed on this page are developed for TIBER-NL and TIBER-EU and will therefore use terms from the financial sector. Even so, these documents are applicable to TIBER-WATER until specific templates for TIBER-WATER have been developed.

Background

[TIBER Short Read](#)

Implementation Guide

[TIBER-NL Implementation Guide](#)

Preparation Phase

[TIBER-EU White Team Guidance](#)

[TIBER-EU Services Procurement Guidelines](#)

[TIBER-EU Scope Specification template](#)

Test Phase

[TIBER-EU Guidance for Target Threat Intelligence Report](#)

[TIBER-EU Guidance for the Red Team Test plan](#)

[TIBER-EU Guidance for the Red Team Test report](#)

Closure Phase

[TIBER-NL Format 360-Feedback Report](#)

[Format TIBER-NL Test Summary](#)

[TIBER-EU Purple Teaming best practices](#)

[TIBER-EU Attestation Template](#)

If any of these links no longer work, please consult the [TIBER-EU](#) and/ or [TIBER-NL](#) page(s).

TIBER-WATER
Implementation Guide