TLP:AMBER

RTL-WATER
Implementation Guide

Options for a Red Team Light test

Version 1.00 Release date 21-03-2023

Content

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 parties in the Dutch water sector have jointly developed a mature Red Teaming methodology for the water sector, based on the proven methodology of TIBER-NL and which is aligned to the methodology for the Dutch government (TIBER-Rijk). The resulting methodology has been defined in the TIBER-WATER Implementation Guide.

1.2 RTL-WATER

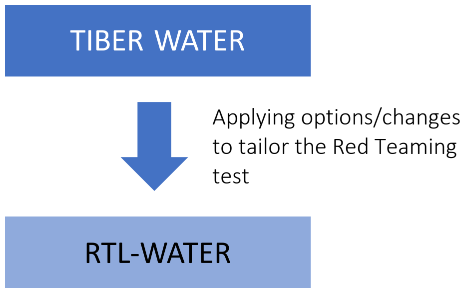
The goal of the water sector as a whole is to perform TIBER-WATER tests to improve cyber resillience. While a TIBER-WATER test is the most mature Red Teaming methodology for the water sector and should be used where possible, the entity may decide that a lighter or more focussed approach is more appropriate based on the maturity of the organisation its state of security.

A Red Teaming Light test (RTL-WATER) is not a TIBER-WATER test and should not be presented as such. However, it can be seen as a stepping stone to performing full TIBER-WATER tests in the future.

The options for performing a RTL-WATER test as listed in this document have been chosen and defined by the working group Red Teaming for the water sector.

Note: At the time of the publication of this document, De Nederlandse Bank is developing a similar methodology called “Advanced Red Teaming (ART)”. The RTL-WATER approach for the water sector may be aligned to ART at a later time.

Figure 1.1 RTL-WATER is derived from TIBER-WATER



1.3 Purpose of this document

This document lists the recommended options for performing a Red Teaming Light test while adhering to the overall TIBER-WATER test process as much as possible.

This document is a guide rather than a detailed prescriptive method. It should be consulted alongside TIBER-WATER and other relevant TIBER-related documents.

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.

2. RTL-WATER: Red Teaming Light for the water sector

The recommended changes and choices that can be made by the entity for RTL-WATER are described in this chapter. All of these choices should be made during the preparation phase.

It is important to note that the RTL-WATER test must not be limited to technical security tests, since that would limit the test and makes it a penetration test.

The three key areas in which a RTL-WATER test could deviate from a full TIBER-WATER test are:

- Purple Teaming
- Replicating an Existing Scenario
- Reducing Scope

2.1 Purple Teaming

The full test may be conducted as a purple teaming test. In this case the BT is informed on each step the RT executes. The BT analyses if it could detect the attack, but does not interfere with or stop the attack.

Since the BT is aware of the test, the RT does not have to build a hidden infrastructure that makes attribution difficult. Purple teaming does not exclude the use of social engineering, misuse of systems or configurations. Purple teaming greatly reduces the risk but does not test realistic response and escalation processes.

2.2 Replicating an Existing Scenario

The entity may build on information about recent attacks in the sector or comparable organisations to to define an attack scenario.

Since this scenario replaces the TTI report, it should as a minimum contain the following elements:

- Definition of the attack objectives
- Explanation of the threat actor, its maturity and TTPs used
- High level attack scenario
- Type of OSINT relevant to this scenario (e.g. the names of HR managers or OT-brands used)

The RTP builds a Red Team Test plan based on this scenario. In this case the RTP should conduct OSINT to complete the scenario.

2.3 Reducing Scope

The scope of a TIBER-WATER test includes the full organization and all of its assets. During a RTL-WATER test, the entity may decide to perform a more focused test by reducing the scope to:

- Gaining access to the office infrastructure only. This is possible if the objectives of the simulated actor are within the office infrastructure (e.g. CRM or financial systems).
- Gaining access to the office infrastructure up to OT gateways. The test may then continue with purple teaming in the OT infrastructure.
- Compromising Operational Technology (OT) only. Assumes that the office network has been breached as a starting point for attacking OT.

RTL-WATER
Implementation Guide