NORGES BANK

TIBER-NO
Targeted Threat Intelligence Report Guidance

Version 0.2

1 Introduction

This is practical guidance produced by TCT-NO to support and guide how to produce the Targeted Threat Intelligence (TTI) Report in TIBER-NO tests. The figure below shows the TTI in the TIBER-EU process.

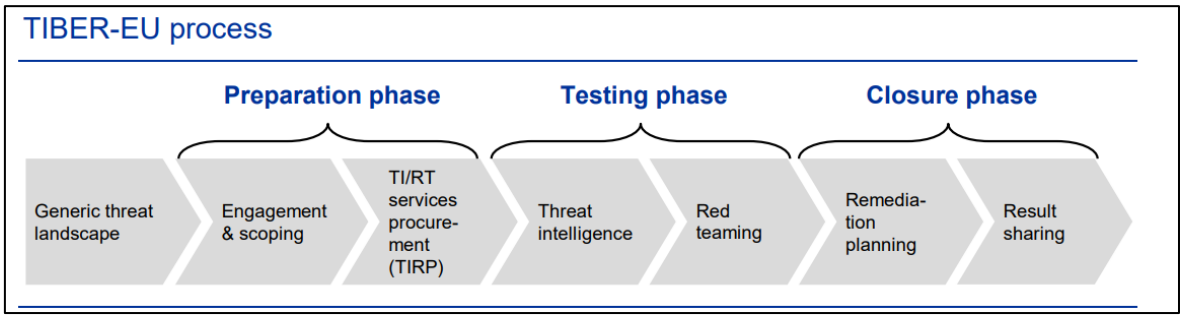

Fig: TIBER-EU process

1.1 How to use this document

This documented is intended as a supporting document to the official guidance from TIBER-EU (1), specifically catered to Norwegian TIBER tests. It is primarily intended for the Threat Intelligence team to understand the process and providing the best possible deliverable to TIBER tests.

This guide is based on:

- TIBER-EU Targeted Threat Intelligence Report Guidance document.
- TIBER-NO Operational Guide v1.2, “2. Targeted TI phase”

For more general information about TIBER-EU and TIBER-NO, see:

- What is TIBER-EU? and the TIBER-EU Framework
- TIBER-NO and TIBER-NO implementation Guide

1.2 The TTI phase in TIBER-NO

The TTI phase does not differ in any way from the way it is described in the European TIBER-EU framework. This means the official TTI guidance from TIBER-EU Framework can be used to support TIBER-NO tests. This guide is merely meant to clarify and supplement that guide. Detailed requirements are outlined in the main Framework document. The guidance is not mandatory and may be deviated from.

1.3 About the Targeted Threat Intelligence Report

The TTIR is a document to support the TIBER test and provide the entity an overview of their place in the threat landscape. The TTIR is shared with the WT and the TCT(s) for the jurisdiction the test takes place in. The WT and TCT need to agree and attest on its contents before the test can progress.

The report is also shared with the Red Team. This allows them to understand the entity, the importance of the critical functions (CFs) and relevant threats to both. The report enables them to develop the RT Test Plan and later in the attack phase, to maintain the realism for the test, and rationalize attack techniques and operational security choices during testing. The report is also shared with Entity's CTI team after test (if applicable).

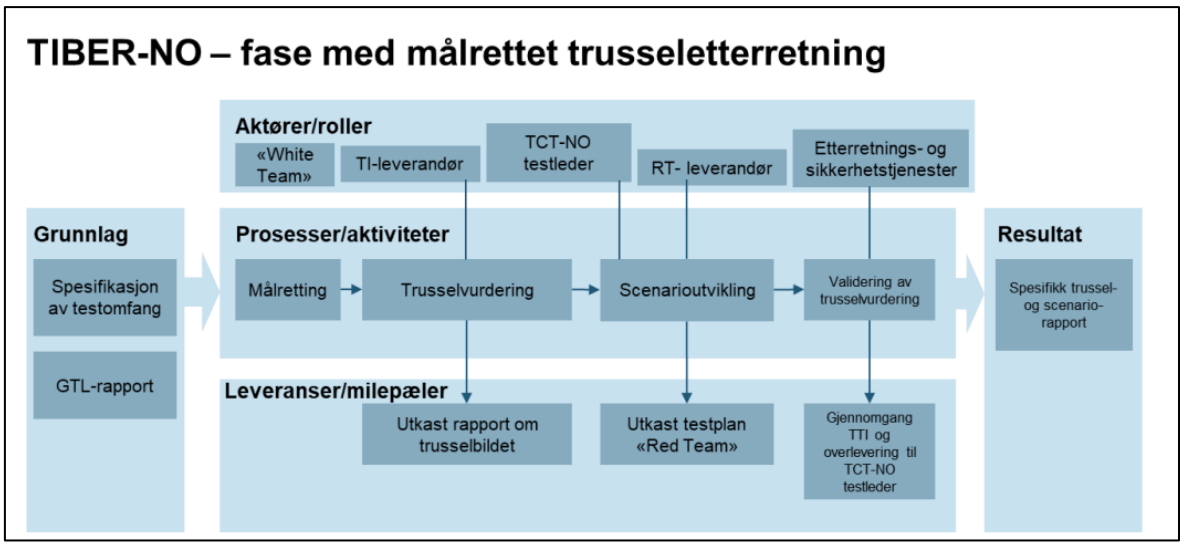

Fig: TIBER-NO TTI process

2 Input to the Targeted Threat Intelligence Report

The TTI Report requires input from a range of different sources. TI provider should use information related to the scope, business overview, digital footprint, and threat intelligence input in an interconnected manner, as they all inform and influence each other, and provide a broader and holistic picture of the entity's threat landscape.

These include:

- Generic Threat Landscape report (GTL) produced by Nordic Financial CERT for Norway and Denmark
- Scope Specification document produced by the WT.
    - Should include Critical Functions, underlying key systems and services, flags, targets, and objectives of the test. This allows the TI provider to increase its knowledge of the entity and to focus its threat intelligence for the TTI Report towards the Entity.
- Business overview
    - Provide a strategic understanding of the entity's organization and business, its current and planned activities, and further context of the entity's role within the financial sector. The overview can include:
        - Business structure
        - Key countries or geographic locations
        - Short- and long-term strategic goals
        - Executives and other key employees
- Possible further documentation provided by the WT.

3 Content of Targeted Threat Intelligence Report

This section describes the contents and development of the TTI Report.

3.1 Business overview from an intelligence perspective

This section should provide a strategic understanding of Entity as an organization and the specified critical functions from a threat intelligence perspective. It should provide an assessment of the possible business consequences the Entity could face as a result of potential cyber-attacks, as well as the potential systemic risk to the broader National financial sector in the event of a compromise to the assets in scope of the test.

This section should include:

- Overview of the organization and their business
- Supply chain or third-party support, both in technology and processes
- Mergers and acquisitions (if relevant)
- Investments and geopolitical issues associated with the Entity
- Business and system consequences, i.e., describing the potential impact of a cyber-attack

3.2 Digital footprint

The output of this activity is the identification, on a CF-basis, of the attack surfaces of people, processes and technologies relating to the Entity. The digital footprint operation should identify:

- Intelligence of interest

- External facing systems
- Internal systems
- Security functions and systems
- Critical systems (related to CFs)
- Outsourced or third-party functions.

3.3 Threat actor assessment

Assessment of which threat actors are relevant for targeting the Entity. The TI provider should list the categories of threat actors and threat actors ranked by intent and capability to attack the entity and/or a specific critical function of the test Entity.

They should then describe how threat actors would target the Entity's Critical Functions and focus their efforts on achieving the objectives/flags.

Should include:

- Threat actor longlist, including a rationale for their inclusion. This list can contain a range of threat actor across all threat categories specified in the GTL, such as hacktivist, Organized Crime Group, Nation State Groups, etc.
- Rationale for the exclusion of long list actors, resulting in three concrete threat actors for the profiling part of the TTIR.

3.4 Threat actor profiling

After the threat actor longlist has been reduced to three concrete threat actors, a description of a profile for each of them. The TI provider should elaborate on the threat actor's motivations, i.e., what they seek to gain from the attack. This section should include a threat profile for selected threat actor, describing:

- Motivation – what is the motivation of the threat actor towards this specific Entity? E.g., financial gain, geopolitical advantages, or other.
- Goals / purpose / intent – what is the concrete goal or achievement of the threat actor?
- Sophistication – how sophisticated is their operation, their techniques and their knowledge of the target and the financial sector. Ranging from script kiddie to nation state.
- Agility – how the threat actor would adapt to changing circumstances and how they would do this, and how quickly are they able to adapt. Ranging from inflexible to adaptable.
- Perseverance – How sustained is the threat actor in their comment to their cyber-espionage and attack campaigns. How much resources and long-time interest do they have in their target. Ranging from opportunistic to motivated.
- Purpose - how targeted they are towards their end goal. I.e. do they go directly to the CF or firstly provide a broad presence within the network and/or roam around to look for opportunities? Ranging from meandering to direct.

3.5 Develop threat scenarios

TIBER-EU requires a minimum of three scenarios, emulating three different and specific threat actors. We recommend initially identifying around six scenarios which later can be reduced down based on discussions between the TTI provider and WT.

Each scenario should be described with:

- A descriptive scenario name, ideally specifying both threat actor and goal or motivation. See the naming convention suggested in the Scope Specification guidance.
    - E.g: *Scenario SC-A: Lockbit gang targets BigBank Payment Service for financial gain*
- Capability, intent and overall threat level for the selected threat actor and scenario
    - E.g. *"Capability: Very high, Intent: High, Threat: High"*
- Describe the preparation, infiltration, entrenchment, and execution of the scenario.
    - Identify the TTPs that the threat actor would employ all the way from no access to a full compromise of the critical functions and achievement of the objectives/flags for the scenario.

3.6 Re-validate scope and flags

The TTI provider should propose possible changes to the Scope Specification and its flags based on the information collected in the phase. The WT, TI provider and TCT should together review the TTI Report, and then revise and finalise the Scope Specification and flags based on this input.

4 Example TTI report structure

This is just an example of some components of what a TTIR should include, not an exhaustive list. TIBER-NO does not provide a template for the report itself.

- Executive summary
- Business overview from an intelligence perspective
- Intelligence on Entity's digital presence
- Threat actors
    - Threat actor assessment
    - Selected threat actor profiling
- High-level threat scenarios - for each scenario:
    - Threat level for actor and scenario
    - Attack flow, including TTPs
- Appendices
    - For larger amounts of information, TTP tables, OSINT raw data, or similar.

5 TIBER-EU recommendations for TTI Report

These are not strict *requirements*, but recommendations from the TIBER-EU guidance for the TTI report.

- GTL or similar is used to develop TTIR.
- Entity provides scope and information to TI provider.
- Target identification follows the Scope Specification.
- CFs and flags are contextualized to link entity and CT to threat landscape, categories and actors.
- An assessment of threat groups relevant for Entity is included.
- Threat actor motivations, capability and intent are documented.
- Selected threat scenarios are developed based on all the above points.

Checklist for the TTIR from TIBER-EU

These are recommendations extracted from the TIBER-EU guidance for the TTI report. This can serve as a checklist for the TI team when developing the TTI report to ensure they include the minimum information. TCT-NO encourages the TI team to use this table in that manner.

Category	Element	Desc.
Generic Threat Landscape	Develop GTL or apply it to TTIR	In cases where the TIBER-XX jurisdiction has developed a GTL, the TI provider should make use of it as a valuable input in developing the TTI Report. If the TIBER-XX jurisdiction has decided not to provide a GTL Report, then the TI provider should develop a view of the general threat landscape for the entity as part of the TTI Report.
Target identification	Scope specification	The TI provider should use the critical functions, underlying key systems and services, and flags, targets and objectives of the test to increase its knowledge of the entity and to focus its threat intelligence for the TTI Report.
Target identification	Business overview	This section is ideally to be provided by the entity. The TI provider should use this information to help identify the plausible threat actors targeting the entity and its critical functions and to help design the threat scenarios.
Target identification	Digital footprint	The TI provider, as part of its threat intelligence gathering, should assess the entity's digital footprint as best as possible. The output of this activity is the identification, on a CF-basis, of the attack surfaces of people, processes and technologies relating to the entity.

Category	Element	Desc.
Target identification	Threat intelligence input	The TI provider should use the information from the Scope Specification document, which outlines the key systems and technologies used by the entity, to collect strategic2 , operational3 and tactical4 intelligence.
Threat modelling and scenario identification	Contextualise critical functions	The information gathered by the TI provider should provide them with more detailed background information on the entity and provide the basis for further contextualisation of the critical functions set out in the Scope Specification template.
Threat modelling and scenario identification	Contextualise flags	The information gathered by the TI provider should provide them with more detailed background information on how threat actors would target the entity's critical functions and focus their efforts on achieving the objectives/flags, as set out in the Scope Specification template.
Threat modelling and scenario identification	Identify threat actors and understand motivation and intent	The information gathered by the TI provider and the contextualised critical functions should allow the TI provider to conduct its own assessment on which threat actors are relevant for the entity. The TI provider should list the categories of threat actors and threat actors ranked by intent and capability to attack the entity and/or a specific critical function of the entity
Threat modelling and scenario identification	Determine modus operandi	Once the TI provider has adequately linked the critical functions, flags, threat actors and motivations/intent, based on the evidence gathered during the reconnaissance (i.e. sections 2 and 3), they should determine the modus operandi (i.e. TTPs) that the threat actor would employ to compromise the critical functions and achieve the objectives/flags.
Threat modelling and scenario identification	Create threat scenarios	Based on the information gathered and the analysis undertaken, the TI provider should clearly document the threat scenarios for the TIBER test. The threat scenarios should be intelligence-driven and evidence based. The TI provider should elaborate on the threat actor's motivations, i.e. what they seek to gain from the attack.
Threat modelling and scenario identification	Re-validate scope and finalise flags	Once the TI provider completes the TTI Report and determines the threat scenarios for the test, they should liaise with the entity to review the Scope Specification document. Based on the TTI Report and the threat scenarios, the Scope Specification should be validated and revised, if necessary (including the flags).

Change log

Version	Date	Change
0.2	17.10.2023	Updated version
0.1	05.09.2023	Initial version