Norges Bank

TIBER-NO

Targeted Threat Intelligence Report Guidance

Version 1.2

TLP:CLEAR

This is practical guidance to support and guide how to produce the Targeted Threat Intelligence Report (TTIR) in TIBER-NO tests.

04.02.2026

Contents

1 Introduction

This documented is intended as a supporting document to the guidance from TIBER-EU. It is primarily intended for the Threat Intelligence Provider 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, “3. Testing phase: threat intelligence and scenarios”

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

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

1.1 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. The TTI guidance from TIBER-EU Framework can be used to support TIBER-NO tests, and this guide is 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.

1.2 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 Control Team (CT) and the TCT(s) for the jurisdiction the test takes place in. The CT and TCT need to agree and attest on its contents before the test can progress.

The report is also shared with the Red Team Testers. This allows them to understand the entity, the importance of the critical and important functions (CIFs) and relevant threats to both. The report enables them to develop the Red Team Test Plan (RTTP) 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 should also give value to the entity as a standalone product. Many entities focus on how they are perceived externally from a marketing point of view. This report should give a very different focus when an attacker with criminal intent surveys the entity. This alone can give valuable contributions to securing the entity against malicious attacks, even without any active testing performed.

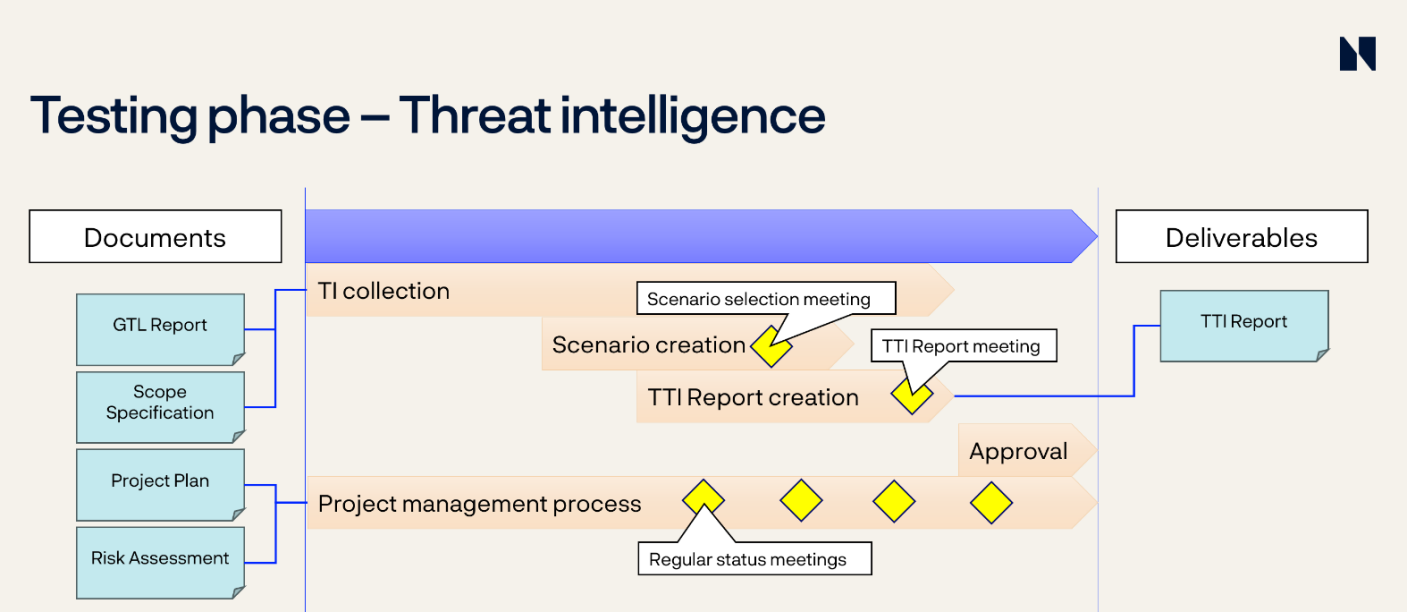

Fig: TIBER-NO TTI process

2 Input to the Targeted Threat Intelligence Report

The TTI Report requires input from a range of different sources. The Threat Intelligence Provider (TIP) 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:

- Nordic Generic Threat Landscape (GTL) report produced by Nordic Financial CERT
- Scope Specification Document produced by the CT.
    - Should include Critical and Important Functions, underlying key systems and services, flags, targets, and objectives of the test. This allows the TIP 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 organisation 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 CT.

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 organisation 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 CIF-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 CIFs)
- Outsourced or third-party functions. (service providers, etc.)
- High value targets
- Buildings and premises, including data centres, etc.

3.3 Threat actor assessment

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

They should then describe how threat actors would target the entity’s Critical and Important Functions and focus their efforts on achieving the objectives and 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 TIP 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 CIF or firstly provide a broad presence within the network and/or roam around to look for opportunities? Ranging from meandering to direct.

When mapping the Threat Actors to Critical and Important Functions (CIFs), see the example in the TIBER-EU TTIR Guidance chapter 3.3.3. The Nordic GTL 2026 pages 54-61 also describes how mapping of CIFs can be performed.

3.5 Develop threat scenarios

The threat scenarios are written from an attacker's point of view and emulate the attacker's capabilities. This means a detailed description of the emulated threat actor's preferred tactics, techniques and procedures, using the MITRE ATT&CK framework. To avoid the threat scenarios from being too much backward-looking, the TIP should enhance each threat scenario with forward-looking plausible TTPs emulating what relevant attackers might be capable of in the foreseeable future. However, there should be a clear distinction between the evidence-based backward-looking scenarios vs. the hypothetical forward-looking TTPs in the described threat scenarios.

A maximum of one scenario per TIBER test may be non-threat-led, allowing for the investigation of future or otherwise relevant attack vectors. Such a scenario is referred to as scenario-X. If no scenario-X is specified during the threat intelligence phase, a maximum of one scenario may be transformed into a scenario-X during the active testing phase, after agreement of the TM, CT and

RTT. A scenario-X can include some more flexibility than the traditional scenarios in TIBER while keeping to the overall approach and learning value of the test. A scenario-X may be threat lead, such as when combining multiple Threat Actors. It is also possible to experiment with new approaches and technologies not yet observed used, such as AI, Quantum computing, deepfakes etc.

In case of a multi-party test involving an ICT third party provider, at least one of the selected scenarios should cover the ICT third party providers' systems, processes and technologies supporting the CIFs of the entities in scope.

The proposed scenarios shall differ with reference to the identified threat actors and associated tactics, techniques and procedures and shall target each critical or important function in the scope. There shall be a scenario long list of around six to ten scenarios which later will be reduced based on discussions between the TIP, CT and TM.

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 the threat actor would employ all the way from no access to a full compromise of the critical and important functions and achievement of the objectives and flags for the scenario.

3.6 Re-validate scope and flags

The TIP should propose possible changes to the Scope Specification and its flags based on the information collected in the phase. The CT, TIP and TCT should together review the TTIR, and then revise and finalise the Scope Specification and flags based on this input.

4 Example TTIR 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 TTIR

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

- GTL or similar is used to develop TTIR.
- Entity provides scope and information to TIP.
- Target identification follows the Scope Specification.
- CIFs and flags are contextualized to link entity 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.

Changelog

Version	Date	Change
1.2	04.02.2026	Updated visual layout of document (AH)
1.1	14.04.2025	Updated TIBER terminology and removed the outdated TIBER-EU checklist (AH)
1.0	09.04.2024	Minor updates, ready for publication (AH)
0.2	17.10.2023	Updated version (AH)
0.1	05.09.2023	Initial version