



ART Threat Intelligence Guide

DeNederlandscheBank

EUROSYSTEEM

Content

1 Introduction

2 Generic threat
landscape

3 Module selection

4 TI process

5 TI report
requirements

Annex

1 Introduction

1.1 Purpose of this guide

The testing phase includes the threat intelligence (TI), red teaming (RT), purple teaming (PT) and gold teaming (GT) of an Advanced Red Teaming (ART) engagement. In this phase, the control team (CT), red team provider (RTP) or threat intelligence provider (TIP) produces a TI report tailored to the entity. Various TI modules can be selected within ART. Regardless of the module selected, a written TI report with minimum requirements will be produced as part of the ART engagement. The RTP will use this report to build an attack plan for one or more scenarios involving specified critical live production systems, people and processes that underpin the entity's critical functions (CFs). The involved Test Cyber Team (TCT) will validate whether the TI report delivered for the engagement meets the requirements outlined in this guide.

The ART TI guide aims to clarify the differences between the TI modules in ART, suggest factors to consider when selecting a TI module and outline the minimum requirements and milestones for each TI module.

Disclaimer: This guide is intended for entities within the scope of an ART test. Nothing in this guide should be construed as legal or professional advice.

1.2 Who is this guide for?

- CT of the entity undertaking the ART test
- TIP
- RTP
- TCTs of authorities involved in the ART test

1.3 Structure of this guide

- Chapter 2: Generic Threat Landscape
- Chapter 3: Module overview and module selection
- Chapter 4: TI process
- Chapter 5: Requirements for the TI report

First, this guide explains the function and use of an important component for all TI modules: DNB's Generic Threat Landscape (GTL). Next, Chapter 3 gives an overview of the different TI modules in ART and how financial entities select the most suitable one for their specific test. Following a chronological walkthrough of all major steps and milestones in the production of a TI report in chapter 4, the final chapter sets out more detailed expectations and minimum requirements for the different TI modules.



2 Generic Threat Landscape

The Generic Threat Landscape (GTL) is designed for financial sector entities within the scope of ART. It is created by the TCT and distributed to the CT as soon as the test starts. The GTL provides information about advanced threat actors that are relevant to Dutch financial entities, as well as exploring those actors' motivations to attack specific CFs within these entities.

Depending on the module selected in ART, the GTL serves as primary input for the TI report. It also includes various scenarios that can provide inspiration for a CT, RTP or TIP's scenarios in the TI report. However, it is important to emphasise that the GTL scenarios are only included as examples and should not be used in ART TI reports without modification or expansion.

The GTL contains the following elements:

1. A strategic geopolitical overview for the Dutch financial sector.
2. The most relevant advanced cyber threat actors for the Dutch financial sector.
3. An overview of CFs within Dutch financial institutions that fall within the scope of the DNB Threat Intelligence Based Ethical Red-teaming (TIBER)/ART. This element includes a detailed description of each CF.
4. Threat matrices outlining the motivation and intent of advanced cyber threat actors to conduct attacks against the various CFs outlined in the GTL.
5. Sample scenarios that could help a CT, TIP or RTP develop the scenario(s) for their ART engagement.



3 Module selection

3.1 Module overview

As part of the ART engagement, the CT must select one of the four TI modules outlined below, each of which requires the production of a TI report containing one or more threat-led scenarios. These modules vary in their requirements, cost and thoroughness. Only Module 4 includes a so-called 'attack surface analysis', which outlines intelligence gathered on the attack surface and digital footprint of the entity, which can support RTP to conduct the TI-led scenarios. This attack surface analysis outlines (when applicable) leaked credentials, publicly accessible confidential information of the entity and more.

The added value of the TI report varies per TI module. This factor should be carefully considered when selecting the most suitable module (see 3.2: How to select an ART TI module).

Module 1: Basic TI report created by internal TI expert(s) using the GTL

This module is the least time-consuming and resource-intensive option and generates a basic TI report. Module 1 has an average run time of two to three weeks. This report is drafted by one or more internal TI experts within the financial entity. For more

information, please see the clarification on page 8 entitled 'When is someone qualified as an "internal TI expert"?'

In addition to using the entity's own intelligence, resources and reports, the report also takes input from the GTL. The control team lead (CTL) and TCT will have an open discussion of the module's suitability for the entity and whether the entity's TI expert is qualified to take on the challenge. Based on the requirements in this TI Guide (see Chapter 5), the TCT verifies whether or not the TI report produced by the CT meets the requirements for an ART test. Although a Module 1 TI report will not be as extensive as the reports in Modules 2, 3 or 4, it still needs to contain elements such as an analysis of the entity's CFs, a shortlist of relevant threat actors and TI-led scenarios arising from this assessment (see Chapter 5). One element is excluded, which is the attack surface analysis.

Suitable for:

- Entities that do have an internal TI experts, but do not have the capability to digest large amounts of threat intelligence;
- Engagements to be completed in a limited number of weeks;
- Entities that have limited resources available for this engagement.

Limitations:

- This option is generally not as thorough as Modules 3 and 4;
- Module 1 gives very limited external insights into crown jewels and opportunities for threat actors to target an entity;
- This module is the least costly option for entities. However, the attack surface analysis – which is not included in this module option – is very beneficial to the RTP's situational awareness. Although choosing this module could save time and money, making this economic decision could potentially lead to adverse consequences during the RT phase;
- Not all entities have the required in-house TI expertise to deliver the high-quality TI report needed for this module.

Module 2: Limited TI report created by internal TI expert(s) using a previous TI report

In this module, the internal TI expert – who is part of the CT – delivers a TI report based on input from the GTL and an 'old' TI report with content that can still be used in the ART TI phase. The expected average duration of this TI module is between three and four weeks. The existing TI report must have been produced specifically for the entity by an external cyber security provider and should be no more than 24 months old. As well as the GTL, a pre-existing report with detailed and specific

intelligence gives the TI expert easily accessible and targeted information about the entity that can be used in the ART TI report.

The TCT and CT should discuss the extent to which the TI report is applicable to the ART test. In some cases, for example where the entity has undergone substantial organisational changes, a report that is only 12 months old may be obsolete, while for other entities a 25-month-old report could still contain useable intelligence. This must be assessed on a case-by-case basis. (For more guidance on whether or not an existing report can be used, [please see the clarification](#)).

The main difference from Module 1 is that in Module 2 the internal TI expert has more information/documents/analyses to base the ART TI report on, making the TI report more valuable to the red team and therefore also to the ART test. On average, this also means the TI expert will need more time to digest all the input.

Suitable for:

- Entities that do have an internal TI experts, but do not have the capability to digest large amounts of threat intelligence;
- Engagements to be completed in a limited number of weeks;
- Entities that have limited resources available for this engagement;

- Entities that have not undergone restructuring or major infrastructure changes since the publication of the previous report used for the coming ART engagement.

Limitations:

- This module is not as thorough as Modules 3 and 4;
- It provides only very limited external insights into crown jewels and opportunities for threat actors to target an entity;
- The cost of this module is lower than for Modules 3 and 4. However, the attack surface analysis – which is not included in this module – is very beneficial to the RTP's situational awareness. Although choosing this module could save time and money, this economic decision could potentially lead to adverse consequences during the RT phase;
- Not all entities have the required in-house TI expertise to deliver the high-quality TI report needed for this module;
- The older the existing report is, the less operational and strategic value it is likely to have;
- The CT will still need to translate the older report into an up-to-date TI report/TI-based scenarios.

When is an 'old' TI report suitable for use in an ART engagement?

ART allows entities to use a previous TI report to enrich the TI report created for Module 2. Whether or not a previous report can be used for this engagement depends on the following characteristics:

- The report is no older than 24 months (the TCT retains freedom to allow older TI reports to be used);
- The intelligence in the report is still relevant to the entity being tested;
 - The CT is able to explain the extent to which the internal organisation has changed since the creation of the report;
 - The current threat landscape has not changed significantly since the report was shared;
- The report includes sufficient in-depth intelligence on the entity and the applicable threat landscape. A one- or two-page document is not sufficient and does not count as a previous report;
- The 'old' report should be of good quality and be suitable to serve as starting point for a new report. This means that it should have been produced by a reputable external TIP.

Module 3: Limited TI report produced by a RTP

Some entities choose to take a different path during TI phase by commissioning a TI report from an external vendor. A TI report produced by a third party can give the entity a new perspective. In Module 3, a TI report is created by the RTP. The average duration of this TI phase is between three and five weeks. Several RTPs are capable of producing TI reports in addition to their RT services. The Module 3 report would include all the elements of a full (Module 4) TI report, with the exception of an attack surface analysis. This means that a limited TI report still contains an analysis of the scoping document, thorough business overview, an analysis of the current cyber threat landscape, relevant threat actors and one or more TI-led scenarios based on the previous information. The RTP is free to include an attack surface analysis in the TI report if it would improve the quality of the threat-led scenarios.

A Module 3 report is more detailed and comprehensive than the TI reports created for Modules 1 and 2. For more information on the requirements for this module, please see Chapter 5.

Suitable for:

- Entities that want to benefit from a fresh external TI assessment;
- Entities with no internal TI expert to produce an ART TI report.

Limitations:

- Although a limited TI report produced by the RTP can provide excellent value, the exclusion of an attack surface analysis can hinder the RT phase later on;
- Using the same provider for both the TI and RT may compromise the separation of duties.

Example from a real ART test

In one of the ART tests conducted, an attack surface analysis was not included in the TI phase. Although excluding this analysis from the TI phase saved financial resources that would otherwise have been spent on this module, the lack of an attack surface analysis negatively affected the RT phase. The RTP experienced a serious setback due to a lack of progress during the through phase of the test, as it was unaware of the entity's infrastructure. It was later found that this information was available online and would probably have been collected if a more extensive TI module had been selected.

The main takeaway from this example is that an investment in the TI phase can often have a beneficial effect on the overall quality and effectiveness of the RT phase.

Module 4: Extensive TI report produced by a TIP

Module 4 is the most extensive TI module available in ART. For this module, a professional and experienced TIP must be engaged to produce a full TI report, similar to TIBER. The average duration of a TI report for this module is between six and eight weeks. The TI report includes an elaborate analysis of the CFs and underpinning systems in the scoping document, an elaborate business overview and threat landscape assessment. These provide the basis for identifying the actors that pose the greatest threat to the institution. The TI report produced as part of this module contains an extensive attack surface analysis. Cyber threat actors are identified and scenarios are developed. These scenarios should make it possible to use the findings outlined in the attack surface analysis in the RT phase. The TIP is expected to present the findings of the attack surface analysis in such a way that the RTP can readily incorporate it into the test plan.

Suitable for:

- Entities that want a thorough deep dive into their business/ crown jewels, their potential adversaries, their online presence and the threat landscape.

Limitations:

- Of all the TI modules, this module requires the greatest investment of time, people and resources from the entity;

- It can demand considerable resources for the entity to process the lessons learned from a full TI report with an attack surface analysis.

3.2 How to select an ART TI module

The selection of the right TI module for an ART engagement depends on the requirements specific to the engagement and the entity. The balance between costs and rewards of selecting a certain TI module also varies between entities.

As every TI module requires different capabilities from the entity conducting the test, this guide cannot provide a complete overview of all the factors to consider when selecting a suitable module. However, the below points outline several considerations for a CTL selecting the TI module in an ART engagement.

- *Internal TI expertise*

Not every financial entity has the time or resources to maintain internal TI expertise or resources, the entity cannot produce the TI report for Modules 1 or 2 (please see the clarification).

- *Need for external TI reporting to validate internal TI assessments*

Some entities have their own TI capability or preferred suppliers to provide TI-related services. External TI in ART could help validate or challenge the entities' insights and understanding of the current

threat landscape and how this applies to their situation. Collaboration between both internal and external TI teams could be advantageous for the most advanced ART entities. It should also be noted that this approach goes beyond the minimum requirements of all TI modules in the ART framework.

- *The availability of a previous TI report*

Some entities may recently have received an external TI report which can partially be used in this ART engagement. If the entity wishes to select Module 2 for the ART engagement, this depends on the availability of an 'old' TI report – this module cannot be selected if the entity does not have such a report. Even if an existing TI report was written in the last 24 months, various factors can determine its current usability. More information can be found in the clarification. All the criteria mentioned in the clarification should be discussed by the TCT and CTL to gain sufficient insight into the usability of the report for the ART TI phase.

The brief descriptions given above can help entities decide which module is the best fit for their specific ART engagement. Ultimately, the TCT has the final say in whether the TI module proposed by the entity is suitable for use in a specific ART engagement.

When is someone qualified as an 'internal TI expert'?

The assessment of whether someone within an entity qualifies as an internal TI expert is not an exact science. However, the following characteristics offer a basic guideline to determine if the internal TI expert is qualified to write the ART TI report:

- The internal expert has an educational background in the field of threat intelligence;
- The internal expert has TI certifications mentioned in the TIBER-EU Procurement Guidelines;
- The internal expert knows the financial entity well;
- The internal expert has a role within the entity that focuses at least partially on TI;
- The internal expert has several years' hands-on experience with TI and has demonstrated working experience or professional interest in the field of TI in the financial services sector.

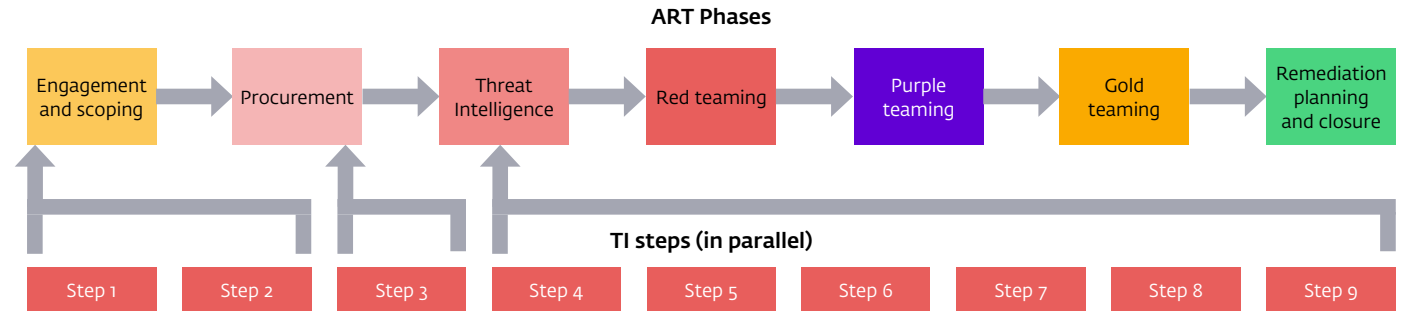
When in doubt about whether an employee qualifies as an internal TI expert, the CTL should consult the TCT.

4 The TI process

This section of the TI guide uses nine chronological steps to outline milestones and tips to help CTs, RTPs and TIPs progress through the TI phase in a structured way. While some steps can run in parallel, others do not and these require a go/no-go meeting with the TCT to assure quality and alignment. Although all the steps influence the TI process, not all the steps in the process take place during the Test phase (as can be seen below).

Steps

- Step 1: Module selection [Engagement & scoping phase]
- Step 2: Scoping [Engagement & scoping phase]
- Step 3: Procurement [Procurement phase]
- Step 4: Launch meeting [Test phase]
- Step 5: Business specialist meeting [Test phase]
- Step 6: Draft report and feedback [Test phase]
- Step 7: Revision of the TI report [Test phase]
- Step 8: Involvement of the RTP [Test phase]
- Step 9: Finalisation of the TI phase [Test phase]



Step 1: Module selection

As mentioned in earlier chapters, the first step in any ART TI process is determining which TI module best fits the entity. This decision follows from a discussion between the TCT and CTL but is ultimately the responsibility of the CTL. For more on module selection and requirements, see Chapters 3 and 5.

If Module 1 or 2 is selected, the CT incorporates an internal TI expert. Chapter 3 provides more information on selecting a suitable TI module.

Milestones

- Selection of the TI module that suits the learning objectives and capabilities of the entity;
- Involvement of an internal TI expert who is familiar with the deliverables for this ART engagement (necessary for Modules 1 and 2).

Step 2: Scoping process

Once all the modules for the testing phase (TI/RT/PT/GT) have been selected, the entity can start the scoping process. This process is important for the TI phase, as it is when the entity's CFs, services and underlying processes are identified. 'Flags' to be captured can be placed on these key systems and services. The scoping document is a key pillar that supports the TI report.

Milestone

- C-level and TCT approval obtained for the scoping document (go/ no go).

Step 3: Procurement

In the procurement phase, the CTL reaches out to several TIP/RTP to request quotations for the TI module in this ART test as defined during the engagement and scoping phase. The CT clearly describes the expectations regarding the TI phase and makes clear that the external provider will provide a TI report. TI report requirements (outlined in Chapter 5 of this guide) are also shared in the request, making it more likely that the proposals received will match the entity's needs.

Milestone

- Procurement of a TIP/RTP that aligns with the TI module selected for this ART engagement (for Modules 3 and 4).

Step 4: Launch meeting

Once the procurement is finalised, it is time to plan a launch meeting. The launch meeting marks the start of the actual TI phase. This is when various practical agreements are made regarding the frequency of meetings during the TI and RT phases, communication channels, documentation and responsibilities. After the launch meeting, the TCT, CT and (if applicable) TIP or RTP hold weekly meetings to discuss the progress of the TI module. Regardless of the module selected, a TI report is created that includes one or more threat-led scenario(s).

Milestones

- Launch meeting is planned by the CT;
- Launch meeting between CT, TCT, TIP and RTP has taken place;
- Weekly meetings are planned between TCT, CT and (if applicable) TIP and RTP.

Step 5: Business overview meeting

If the entity selects Module 3 or 4, one of the first actions in the TI phase is for the CT to organise a meeting with a business specialist. The CT can also arrange this meeting if Module 1 or 2 is selected and the internal TI expert has insufficient insight into the entity's business operations and client base. Modern entities are often highly specialised, which means that business operations and client base are often difficult for an external provider to understand and assess. It is of the utmost importance that the TIP/RTP understands not only the technical components of the financial entity, but also its business processes. During this meeting, a business specialist from within the entity will help give the RTP/TIP a better understanding of the CFs and underpinning systems in the scoping document. This will allow the RTP/TIP to make a better assessment as to which threats are applicable to the entity.

Milestone

- A business overview meeting has taken place (mandatory for Modules 3 and 4).

Step 6: Draft report and feedback

During the TI phase, it is advisable to share a draft version of the TI report with the TCT. This way, the TCT is able to provide feedback on whether the report aligns with the ART requirements. Getting feedback at an early stage in the TI phase makes it easier for the CT/RT/TIP to adjust course if necessary and significantly increases the likelihood that the final report will meet the ART requirements. In Module 4, the CT plans a scenario workshop with the TIP at which the team outline the longlist of scenarios and discuss these with the CT and – ideally – with the C-level sponsor. This ensures that the entity's stakeholders are kept informed about the scenarios selection process and gives them the opportunity to share feedback.

The draft TI report is reviewed by the TCT and the CT, who give feedback including the following points:

1. Does the report meet the requirements outlined in Chapter 5?
2. Are the findings of the report in line with the TCT's perspective on the cyber threat landscape? If not, does the CT/RTP/TIP back up its alternative perspective with credible, publicly accessible sources?

The TCT provides only one set of comprehensive feedback.

The production and delivery of a TI report that meets all the ART criteria remains the responsibility of the CT/RT/TIP.

Milestones

- [optional] Interim draft versions of the TI report have been shared with the TCT;
- Draft TI report has been shared with the TCT;
- TCT has shared feedback on the draft TI report;
- A scenario workshop meeting has taken place (mandatory for Module 4);
- Weekly update meetings between the TCT, CT and (if applicable) TIP or RTP have taken place.

Step 7: Revision of the TI report

Based on the feedback provided, the CT/RT/TIP updates and finalises the TI report. It is important to keep all the stakeholders informed on the progress of the TI report during the weekly updates to avoid 'surprises' when the finished report is presented.

Milestone

- Feedback from the TCT has been processed by the stakeholder responsible for the creation of the TI report.

Step 8: Involvement of the RTP

The CT can choose to involve the RTP at any moment during the TI phase. This involvement will help create a smooth transition between the TI and RT phases. For example, the draft TI report could be shared with the RTP to enable the RTP to start drafting the RT attack plan and preparing for the RT phase. However, the

responsibility for the decision to use a draft report before it is finalised lies with the RTP.

Milestone

- [optional] Draft TI report has been shared with the RTP.

Step 9: Finalisation of the TI phase

Once the feedback from the TCT and CT has been processed, the revised document will be formally decided upon at a go/no-go meeting. During this meeting, the TCT, CT (including C-level), RTP and TIP (if applicable) discuss the final document. If all parties agree on the quality and content, the C-level sponsor gives a 'go' on the TI-led scenarios and the test can now progress to the next stage: drafting the RT attack plan. The final TI report is handed over to the RTP. The TI-based scenarios serve as the foundation for the RT attack plan. The TIP and RTP discuss how they will communicate if questions arise from the TI report.

Milestones

- Final TI report and incorporated threat-led scenarios have been approved by the TCT and C-level (go / no go);
- Final TI report has been handed over to RTP.







5 Requirements for the TI report

All TI modules will ultimately lead to a TI report. Whichever module is chosen, the resulting TI report contains at least a number of recurring elements. The minimum requirements for these elements vary per module and are outlined in this TI guide.

Commercial creativity is encouraged in ART when delivering the TI, RT and GT activities, as this fuels innovation and encourages providers to meet customers' individual needs. The recommendations in this guide are not set in stone. However, the ART framework does set minimum requirements in terms of standards and elements to safeguard the quality of the TI report.

5.1 Overview

The table below gives an overview of the differences between the minimum requirements for each module. This chapter also contains an explanatory section for each of the required elements for the various TI modules.

	Module 1	Module 2	Module 3	Module 4
Executive summary	Included	Included	Included	Included
Business overview	Basic (description of company activities).	Basic (description of company activities).	Limited (description of company activities + analysis of interesting aspects).	Extensive (description of company activities, locations and particularities including detailed analysis).
Analysis of scoping document	Basic	Basic	Limited	Extensive
Analysis of threat landscape	Basic analysis with a generic threat landscape analysis.	Basic, but complemented with threat intelligence from the 'old' TI report.	Basic, but more tailored to the entity and gives a clear picture of the implications of the threat landscape for the entity.	Extensive analysis of the threat landscape with a strong focus on the implications for the entity.
Number of threat actors				
Long-/shortlist of scenarios	Shortlist	Shortlist	Shortlist	Longlist and shortlist
Level of detail in the scenarios	Basic level of detail. RTP will provide detailed attack plan.	Basic level of detail. RTP will provide detailed attack plan.	In-depth description of scenario(s) outlining threat actor behaviour following a logical narrative.	In-depth description of scenario(s) outlining threat actor behaviour following a logical narrative.
Attack surface analysis	Not mandatory	Not mandatory, but can incorporate attack surface analysis findings from old report, if any.	Not mandatory, but possible if the RT sees opportunities.	Extensive
Staff needed	Regular CT + Internal TI expert(s) + Business specialist (optional)	Regular CT + Internal TI expert(s) + Business specialist (optional)	Regular CT + Business specialist + Internal TI expert(s) (optional)	Regular CT + Business specialist + Internal TI expert(s) (optional)

5.2 Executive summary

Modules 1, 2, 3 & 4

All TI reports created for an ART engagement start with an executive summary that briefly outlines the report in clear language that resonates with C-level management. At a minimum, the summary should include the chosen scenario(s), selected actor(s), goals and motivation of the threat actor and targeted systems and flags.

5.3 Analysis of the scoping document

A scoping document is created for every ART engagement. This document, with all critical processes and systems within the financial entity, is then analysed during the TI phase. The analysis focuses on the processes and systems that align with both the learning goals of the entity and the available threat intelligence.

Module 1

The analysis generates a shortlist of the most important systems that fall within the scope of the test. No detailed description is required. The scoping document can help the RTP clarify why each system was included.

Module 2

In the TI report, the CT provides a shortlist of the most important in-scope systems for this engagement. If any vulnerabilities/weaknesses were identified in the previous TI report regarding the in-scope systems, these are outlined in the new TI report.

Module 3

As in Module 1, the shortlist can be limited to the most important systems identified for the threat-led scenario(s) of the test. No detailed description is required. Based on this shortlist of systems, the RTP conducts an analysis to create TI-based scenarios for the report.

Module 4

The TIP provides an extensive analysis of a longlist of systems, which is then distilled down to a shortlist. Assumptions and uncertainties about the in-scope systems should be included in the analysis and used to explain the inclusion of systems in the shortlist of the TI report. This makes the subsequent analysis of threat actor behaviour against this specific entity more robust.

5.4 Business overview

This section provides a strategic overview of the entity and its business, together with extra context relating to the entity's role

within the financial sector. The purpose of the business overview is to gain insight into how key components of the entity and its activities may be of interest to criminals and state actors, or how these aspects could be affected by an advanced cyber-attack. For example, if the entity has interests, customers or offices in China, the business overview section should reflect this. This kind of information could be important in deciding which threat actors are most relevant to this ART test. The business overview will be more or less thorough depending on the module selected for the engagement, but this section is an integral part of any TI report. The characteristics of the entity outlined in this section are linked to the threat landscape analysis later on in the TI report.

Module 1

In Module 1, the business overview can be limited to a basic description about the core characteristics of the entity being tested. The analysis provides insights into the core business of the company and its crown jewels (as described in the scoping document). The starting point for this analysis is provided by the scoping document. If the CT has sufficient business knowledge, there is no need to involve additional business specialists to enrich the business overview.

Module 2

In Module 2, the business overview is limited to a basic description of the core characteristics of the entity being tested. The analysis provides insight into the core business of the company and its crown jewels (in terms of systems or processes operated and special data held). The starting point for this analysis is provided by the scoping document. The difference from Module 1 is that insights and information from the existing TI report can be incorporated into the new report. A business specialist can be included in the CT to help to enrich the business overview in the new TI report.

Module 3

The business overview section in Module 3 gives a limited overview of the business of the entity being tested. The analysis should include insights into the core business of the company and its crown jewels (in terms of systems or processes operated and special data held). The starting point for this analysis is provided by the scoping document that is shared with the RTP by the CT. No detailed description is expected of aspects such as the different business units, controversies or upcoming mergers/acquisitions. However, the CT does organise a business overview meeting for the RTP. This meeting helps provide insight into the entity being tested in order to increase the quality of the TI assessment.

Module 4

The business overview section in Module 4 gives an extensive overview of the entity's business. The CT organises a business overview meeting for the TIP to increase understanding of the entity. Input by the tested entity on the points outlined in Annex 1 can serve as a starting point for the TIP to write a business overview. This information can be both requested from the entity and complemented by the TIP's own Open Source Intelligence (OSINT) efforts to draft an extensive business overview. The TIP ensures that the insights outlined in the business overview are integrated into the broader TI assessment.

5.5 Threat landscape analysis

This section of the TI report outlines the threat landscape relevant for the tested entity. A threat landscape analysis translates the financial sector's overall threat landscape into a tailored threat assessment for the entity being tested. It is important for this threat assessment to incorporate the entity's core business characteristics into the analysis. Where possible, claims made in the TI report are backed up using publicly accessible references. This makes it easier for the TCT and CT to validate the quality of the report.

Module 1

The GTL serves as the main input for the threat landscape analysis in this TI module. This section can be a fairly short analysis showing

how the threat landscape in the GTL applies to the entity in question. A shortlist of threat actors can be clearly distilled from this analysis.

Module 2

The threat landscape analysis in this report is basic. Where possible, intelligence from the old TI report is re-used in this TI module. Care is given to describe how the threat landscape has evolved since the publication of the old TI report. The CT uses the old TI report, GTL and insights gained during the business overview meeting to analyse how the threat landscape for the financial sector applies to the entity being tested. A shortlist of threat actors who are most likely to conduct an attack against the tested entity can be distilled from this analysis.

Module 3

Threat landscape analysis in this TI module is limited. The RTP is expected to conduct an analysis based on the GTL, the business overview meeting and the RTP's own intelligence sources. Based on these insights, the threat landscape analysis for this specific entity is presented in a concise, limited manner. The threat landscape analysis should clearly explain why certain threat actors are most likely to conduct an attack against this specific entity.

Module 4

For Module 4, the TIP is expected to provide an extensive threat landscape analysis, similar to TIBER. The TIP first gives a holistic picture of the cyber threat landscape and relevant cyber threat actor categories. Next, the TIP is expected to assess how cyber threat actors' motivation and intent relate to the entity being tested, with this assessment being based on an analysis of the intelligence collected, the GTL and contextualised critical functions. The TIP assesses which cyber threat actors are most likely to attack the entity and explains why. This assessment is based on a clear and coherent analysis, which should be included in the report.

5.6 Scenarios

The threat landscape analysis, business overview, GTL and – if applicable – attack surface analysis provide the basis for drafting various TI-led scenarios for the engagement. The level of detail in the scenarios varies according to the module selected, but all TI-led scenarios drafted for ART engagements should emulate a specific advanced threat actor and follow a clear narrative. The different phases (in/through/out) should also be clearly distinguishable. The minimum requirements for scenarios in the TI modules are set out below.

Module 1 & 2

Based on the threat assessment in the TI report, the CT drafts a shortlist of one or multiple scenarios. The level of detail in the scenarios is limited, but there should be enough information for the RTP to develop an in-depth attack plan. The scenarios do not need to elaborate on the TTPs used during the engagement. Regardless, the CT should outline the elements that shape the overall narrative of the scenarios. In addition to providing a clear narrative including a selected threat actor, its motivation and its goal(s), the following questions must be answered: 1) How does the threat actor gain access to the network? 2) What systems are being targeted? and 3) What is the action on the objective?

Module 3

RTP drafts a shortlist of one or multiple scenarios based on the intelligence analysis conducted. The RTP uses its creative freedom and knowledge of trends to forecast upcoming attacks for the selected threat actors. These scenarios are threat-led and follow a clear narrative with a distinguishable in/through/out phase. Targeted systems and actions for the objective are specified. The TI report includes an overview of Tactics, Techniques and Procedures (TTPs) used by these threat actors. Unlike Modules 1 and 2, Module 3 carries an expectation of more detailed scenarios in the TI report.

The RTP is expected to consider:

- The level of sophistication of techniques the actor may use and the agility of the threat actor (how does the threat actor respond to changing circumstances?);
- How targeted the threat actor's behaviour is towards reaching its end goal (does the actor directly move to the CF, or first establish a broad presence within the network and/or explore the network to identify new opportunities?);
- The threat actor's knowledge of the financial sector, its CFs and the systems being used (has the actor targeted the financial sector or similar industries before?).

Module 4

During the TI phase, the analysis of the available intelligence leads to the creation of a longlist of high-level scenarios. The TIP uses its creative freedom and knowledge of trends to forecast potential upcoming attacks for the selected threat actors for the entity being tested. This longlist is outlined in the TI report. The longlist of scenarios and a proposed shortlist are presented to the CT, and ideally also to the C-level sponsor, during the scenario workshop in the TI phase.

A shortlist of scenarios is agreed upon in the scenario workshop. These scenarios are threat-led and follow a clear narrative with a distinguishable in/through/out phase. Targeted systems and actions for the objective should be specified. To complement the extensive threat-led scenarios, the TI report includes an overview of TTPs used by the threat actors. Unlike Modules 1 and 2, this module carries an expectation of more detailed scenarios in the TI report.

The TIP is expected to consider:

- The level of sophistication of techniques the actor may use and the agility of the threat actor (how does the threat actor respond to changing circumstances?);
- How targeted the threat actor's behaviour is towards reaching its end goal (does the actor directly move to the CF, or first

establish a broad presence within the network and/or explore the network to identify new opportunities?);

- The threat actor's knowledge of the financial sector, its CFs and the systems being used (has the actor targeted the financial sector or similar industries before?).

5.7 Attack surface analysis

An analysis on the digital footprint and attack surface can significantly enrich TI reports created for TI-led RT engagements. This approach involves discovering the entity's attack surfaces related to people, processes and technologies. The attack surface analysis could include customer data, staff data from social media websites, confidential material and other information that could be a useful resource for an attacker. This intelligence can be collected from the darkweb and public – and closed sources. In ART, findings from the attack surface analysis can be used to support scenario development. It is important to note that collecting this intelligence is a resource-intensive endeavour. Within ART, the attack surface analysis is only mandatory in Module 4, but entities are free to integrate relevant findings drawn from an earlier report (Module 2) or conduct a – limited – attack surface analysis for the creation of a TI report (Module 3). Whichever module is selected, it is important to note that only passive scanning is permitted in this phase. Active scanning activities can alert the blue team or reveal the engagement altogether.

Module 1

An attack surface analysis is not mandatory for Module 1. However, if the internal TI expert has recently come across valuable insights that would be beneficial to the report, it is advisable to include this information.

Module 2

An attack surface analysis is not mandatory for Module 2. However, if an attack surface analysis from the old report is still relevant and accurate, it is advisable to incorporate this information into the new TI report created for this engagement. The CT and TCT will have a discussion in advance of the engagement to determine whether the old TI report is still relevant.

Module 3

Although an attack surface analysis is not mandatory for Module 3, the RTP may consider that this intelligence adds value to complement the analysis and support the creation of TI-led scenarios. In this case, it is advisable for the RTP to include this in the TI report for this engagement.

Module 4

Module 4 is the most detailed module and includes an extensive attack surface analysis. The TIP assesses the (digital) footprint of the entity and conducts an analysis focused on the relevance for the entity's CFs. The TIP uses these insights to support its overall intelligence assessment, similar to TIBER. The TIP is expected to collect intelligence from a range of public – and closed sources, such as the darkweb, social media websites and internet fora. Relevant intelligence includes – for example – customer data, staff data, floor plans and more which can provide useful for an attacker. Findings from the attack surface analysis help to design the threat-led scenarios for this ART engagement. The TIP should never conduct active scanning to prevent detection during this part of the test. Only passive scanning is allowed.



Annex 1 Business overview information

To enable the TIP to draft a TI report for the entity, the entity should provide the following information (selected based on the criteria set out in the [TIBER Guidance for Target Threat Intelligence Report](#)) at the start of the TI phase:

- An explanation of the entity and its critical functions and their significance for the broader financial sector;
- The entity's own threat assessment, including examples of recent adverse cyber events;
- The potential systemic implications if the entity's confidentiality, integrity and availability are compromised;
- Information about the entity's business model, its structure (e.g. shareholder ownership, company structure, board and executive management), its products and services and its key financial figures;
- The countries in which the entity operates;
- Information about the entity's interdependencies (both financial and operational) and disclosure of countries from which the entity receives significant supply chain support (e.g. IT support is outsourced to country X);
- The types of clients the entity has that might be of interest to foreign intelligence agencies – the entity could share characteristics of these clients without mentioning specific names or providing traceable information;
- The niche markets in which the entity is active;
- High-level insight into any niche research and development knowledge or intellectual property held by the entity;
- High-level insight into possible (future) mergers and acquisitions involving the entity that may increase the interest of certain threat actors;
- High-level insight into geopolitical issues related to the entity or investments by the entity that may impact its threat landscape;
- Details of third-party involvement in critical functions;
- Details of the entity's domains and IP addresses.

Annex 2 List of abbreviations

ART	Advanced Red Teaming
CF	Critical function
CT	Control team
CTL	Control team lead
GT	Gold teaming
OSINT	Open Source Intelligence
RT	Red teaming
RTP	Red team provider
PT	Purple teaming
TCT	Test cyber team
TI	Threat intelligence
TIBER	Threat Intelligence Based Ethical Red-teaming
TIP	Threat intelligence provider
TTP	Tactics, Techniques and Procedures

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0)20 524 91 11
dnb.nl/en

Follow us on:



DeNederlandscheBank

EUROSYSTEEM