EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU

Guidance for Target Threat Intelligence Report

July 2020

Contents

1 Introduction

1.1 Purpose of this document

In the testing phase (which includes threat intelligence and red teaming), the threat intelligence provider (TI provider) prepares a Targeted Threat Intelligence Report (TTI Report) on the entity, collecting targeted intelligence on the entity, leveraging the Generic Threat Landscape report (GTL), if available and where required, and creating the threat scenarios for the test. The report will be used by the red team provider (RT provider) to carry out an intelligence-led red team test on specified critical live production systems, people and processes that underpin the entity's critical functions (CFs). The TTI Report will also have value for the entity to get visibility on its online footprint and threat landscape.

The TIBER-EU Guidance for Target Threat Intelligence Report aims to provide a standardised approach to develop the TTI Report for the entity. The TI provider should use the Scope Specification document, the GTL report if applicable, the input provided by the entity and other available intelligence on the entity and its digital footprint to create the threat scenarios. In developing the threat scenarios, the TI provider should identify the potential threat actors that may target the CFs; the motivations/intent of the threat actors; and the tactics, techniques and procedures (TTPs) of the threat actors. At the end of the TTI report, and on the basis of the threat scenarios, the TI provider and entity should re-validate the flags set out in the Scope Specification document.

The TTI report has to be agreed by the White Team of the tested entity; agreed by the TIBER Cyber Team (TCT); and shared with the RT provider in order to develop the test scenarios and test plan in the red team testing phase. For more detail on the overall processes in a TIBER test, please consult the TIBER-EU Framework[1] and related TIBER documentation.

1.2 Who is this document for?

This TIBER-EU Guidance for Target Threat Intelligence Report is aimed at:

- White Team of the entity undertaking the TIBER test;
- Threat intelligence provider; and
- Red team provider.
- TIBER Cyber Teams (TCTs) of authorities involved in the TIBER test;

[1] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

1.3 Structure of this document

This document is structured as follows:

- Section 2: Generic threat landscape;
- Section 3: Target identification;
- Section 4: Threat modelling and scenario identification; and
- Section 5: Validation of the flags, targets and objectives.

When TI providers develop the TTI Report, they should use a variety of methods in intelligence gathering, for example OSINT (open source intelligence, which is derived overtly from publicly available sources) and HUMINT (human intelligence, which is derived overtly or covertly from human sources). TI providers must always demonstrate strong ethical behaviour.

The TTI Report should also be shared with the entity's internal Cyber Threat Intelligence (CTI) team after the completion of the TIBER test to help the CTI team validate its own intelligence and reduce the targetable information discovered.

Due to the sensitive nature of the information contained within the Target Threat Intelligence report, once complete, it should be handled and treated as highly confidential and stored in a manner commensurate with this classification (e.g. TLP Amber).

2 Generic Threat Landscape

In some cases, the jurisdiction implementing the TIBER-EU Framework may have decided to produce a national Generic Threat Landscape (GTL) Report for the financial sector. The GTL Report should elaborate on the specific threat landscape of the country, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report should consider key financial market participants and their CFs, including (wholesale and retail) banks, broker-dealers, financial market infrastructures, financial market utilities, and other critical third parties, the different threat actors (including their TTPs) targeting these entities, and the common vulnerabilities.

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.

3 Target Identification

In target identification, the TI provider should provide a strategic understanding of the entity and what makes the entity an interesting target for active threat actors. TIBER-EU tests are generally conducted on critical financial sector entities, and it is therefore important that the target identification can clearly contextualise how the entity and its critical functions are vital for the sector. This will enable the threat intelligence to be put into context and will contribute to the development of relevant threat scenarios in the TTI Report. Any active activities performed by the TI provider must be approved by White Team before conducted.

3.1 Scope specification

At the stage the TI provider commences the TTI report, the White Team and TCT should have agreed on the scope of the test, as documented in the Scope Specification document.

The Scope Specification document sets out the:

- Critical functions of the entity;
- Key systems and services, underpinning the critical functions of the entity; and
- Flags, targets and objectives of the test.

For further insight on the Scoping process, and the definitions for the above factors, please refer to the Scope Specification template.

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. The aforementioned will help inform the TI provider on the plausible threat actors targeting the entity and its critical functions, their motivations and modus operandi (i.e. tactics, techniques and procedures) to achieve the flags, targets and objectives. This analysis should be used by the TI provider to design the threat scenarios.

3.2 Business overview

This section is meant to 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. 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.

The entity and TI provider should work closely together when developing the business overview section. Although much of this information can be obtained from open source, it may be more efficient for the entity to provide this information to the TI provider, thereby allowing the TI provider to focus its efforts on conducting analysis of the information, contextualising it in terms of threat actors, motivations and modus operandi and placing more attention on the digital footprint of the entity.

Before commencement, the entity should, at a minimum, provide the TI provider with the following:

- 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 of a compromise in confidentiality, integrity and availability of the entity;
- Information about the entity's business model, its organisational setup (e.g. shareholder ownership, company structure and Board and executive management), its products and services and its key financial figures;
- The countries in which the entity has presence;
- Information about the entity's interdependencies (i.e. 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 that the entity has, which might be of interest to foreign intelligence agencies - characteristics of these clients could be shared by the entity without mentioning specific names;
- The niche markets in which the entity is active;
- High level insight on any niche Research and Development knowledge or Intellectual Property of the entity;
- High level insight on possible (future) mergers and acquisitions (M&As) of the entity which may increase the interest of certain threat actors;
- High level insight on geopolitical issues related to the entity or investments by the entity, which may impact its threat landscape;
- Details of third party involvement in critical functions; and
- Details of the entity's domains and IP addresses.

This information should be shared with the TI provider at the start of the threat intelligence phase. Some of the aforementioned information may be deemed commercially sensitive, and therefore, it important that the entity and TI provider engage constructively and take a pragmatic approach during the intelligence gathering phase.

When gathering threat intelligence on the business overview of the entity, it is critical that the TI provider does not conduct any activity which alerts the Blue Team and reveals that a TIBER test is being performed. For example, the TI provider can look up which IP addresses belong to the entity, but cannot perform port scanning which would give indication to the Blue Team that active reconnaissance is being performed.

3.3 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. This includes information that is intentionally published by the entity and internal information that has been unintentionally leaked. Such information could be customer data, staff data from social media websites, confidential material or other information that could prove to be a useful resource for an attacker.

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.

The TI provider may use OSINT, information provided by the entity, and dark web and closed sources, to gather information about the entity's digital footprint.

3.4 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 strategic[2], operational[3] and tactical[4] intelligence.

In gathering the appropriate tactical and operational intelligence, to help inform the threat scenarios, the TI provider should take into account the following:

What information can be found that threat actors would use to better understand the target network environment, specifically the CFs and systems underpinning it?

- What information could be found from network diagrams (if available) that could assist attackers in determining where CFs are located within the network and any interconnected systems and secure connections to CFs?
- What information about the systems underpinning the CFs is available that reveal potential vulnerabilities that could be exploited by actors?
- Which components of the network infrastructure of the entity have been targeted by selected threat actors before?
- What are the most prevalent and/or critical vulnerabilities for the sector that are likely to be present at the entity?

[2] Strategic intelligence refers to the contextual framework which shapes an adversary's operating environment and intended course of action. It is designed to explore the 'Who and Why' of an entity's threat landscape.

[3] Operational intelligence involves trend analysis of adversary capabilities and attack methodologies. It is concerned with the 'When, Where and How' of an attack campaign and implies an understanding of adversarial skillset. Analysing an adversary's campaign history allows one to identify characteristic attack vectors and patterns of behaviour that can be used to proactively identify the likely precursors of an impending attack and defend against it.

[4] Tactical intelligence refers to visibility of the tools and hacking methodologies used by cyber adversaries to breach victim networks. High quality, actionable tactical intelligence gives a unique insight into hackers' methods/capabilities and forms the basis for understanding intent at an operator level. It is concerned with the 'How and What' of an attack.

What information would threat actors be able to obtain in order for successful social engineering to be performed to gain initial access to the infrastructure (when applicable in the scenarios)?

- What personnel could be targeted by threat actors based on the job roles and assumed levels of privileged access to key technologies or CFs?
- What contact details and credentials belonging to key personnel can be found that could assist threat actors in their attacks?

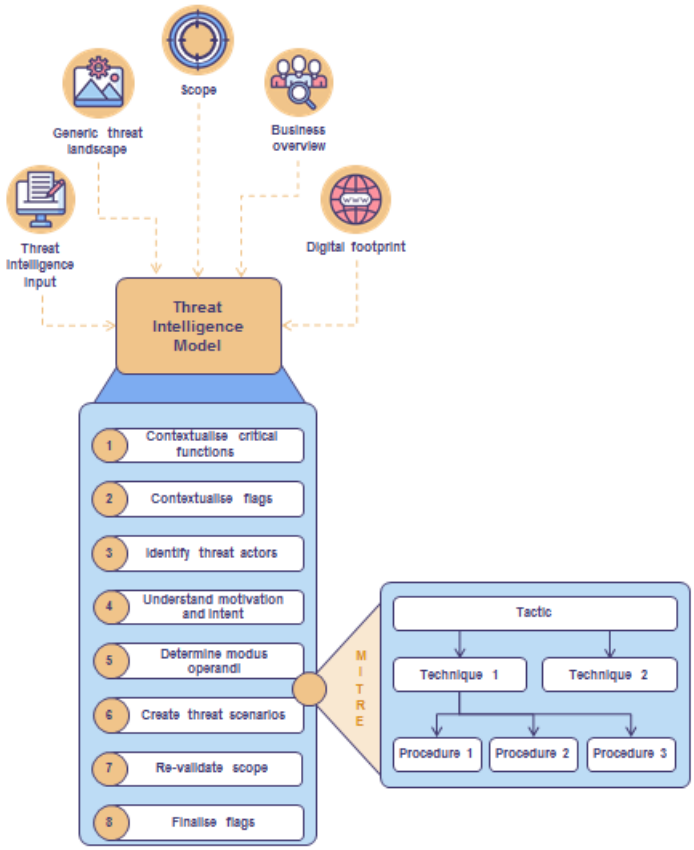
How do third parties/managed service providers affect the security posture of the entity, and how would these parties be used by threat actors to attack the entity?

- Which of the entity's third party/managed service providers have been compromised before and how could this provide opportunities for actors to compromise the entity?
- Which of the entity's third party/managed service providers could be compromised and how could this provide opportunities for actors to compromise the entity?

In general, the 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 components should not be analysed in silos.

4 Threat modelling and scenario identification

Once the TI provider gathers the information in Sections 2 and 3, they should use it to help develop the threat scenarios, in line with the **'TIBER Threat Intelligence Model'** set out below as an eight step approach:



4.1 Contextualise critical functions

The information gathered in Sections 2 and 3 should provide the TI provider 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. For example, the Scope Specification template may list the critical functions as below:

Critical Function	Sub-categories	Justification for inclusion
Deposit taking and savings	Current accounts	Deposit taking and savings services are a core function for the real economy, and any disruption to these would have a detrimental impact on the customer base. Customers of a disrupted deposit taker may lose immediate access to their deposits, and thus are not able to execute payments. In the event of disruption to a significant deposit taker, the resulting liquidity shortage could have serious adverse effects on activity in the wider economy.
	Savings accounts	
	Retail internet banking	
	Debit cards	
	ATM cards	
	Credit cards	
	Mortgages	
	Home equity loans	
	Personal loans	

The information gathered from the Generic Threat Landscape, business overview, digital footprint and threat intelligence input should enrich the understanding of the TI provider and provide more robust, specific intelligence to determine the threat actors that would target the critical functions and their modus operandi.

4.2 Contextualise flags

The information gathered in Sections 2 and 3 should provide the TI provider 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. For example, the Scope Specification template may list a flag as below:

Critical function *(sub-category)*	Deposit taking and savings *(Retail internet banking)*
Target System / Service name	Internet banking, consisting of: Customer Data Maintenance; Customer View; Front-end Payments; TradeBox; User Data Maintenance; and Logon
Information Assurance threat category (Confidentiality, Integrity, Availability)	Integrity

Description of system/service function	Core payment service
Objective - i.e. testing activity required to demonstrate compromise (e.g. Exfiltration, Insertion, Privilege Escalation)	Ability to initiate unauthorised credit transfer of X amount

The Scope Specification template lists the critical functions, their underlying systems and services, and the objectives/flags that the RT provider will look to compromise. The information gathered in Sections 2 and 3 helps inform the TI provider with more specific details how the threat actors would look to compromise the critical functions, the underlying systems and services and achieve the objectives/flags. The TI provider should incorporate this specific information in the TTI Report to contextualise the flags by developing more concrete threat scenarios that will allow the RT provider to build the attack scenarios and help compromise the flags/objectives during the test.

For example, the digital footprint may provide the TI provider with important information from staff profiles on social media or the threat intelligence input could reveal vulnerabilities related to the underlying systems and services, which could be used to exploit the entity.

4.3 Identify threat actors and understand motivation and intent

The information gathered in Sections 2 and 3, the contextualised critical functions (section 4.1) and flags (section 4.2) 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.

The assessment of the TI provider should be based on specific actors. The TI provider can firstly use a categorization of threat actors, and assess how each of these categories relates to the entity. When the categories are assessed and listed, then the TI provider should determine which threat actors are deemed most relevant to the entity and why.

For each of the threat actors listed, the TI provider should provide analysis on their motivations and intent, and explain clearly why they would specifically target the critical functions and attempt to achieve the objectives/flags. This analysis must be evidence based and demonstrate strong analytical reasoning in terms of motivation and intent. For example:

"APTXX has long targeted European countries. It is strongly believed to be operating for country X. In recent years tensions have risen between country X and European countries which has led to a rise of disruptive operations against critical infrastructure in Europe. Until recently these operations were limited to non-financial sector. However in June this year the central payment processor neighbouring country Y was target of APTXX and caused an outage of two weeks.

After this successful operation APTXX has been ordered by country X to investigate whether they can find a way into European payment institutions in order to shut down operations when geopolitical tensions rise even further. They are likely to use both physical and digital, as shown by incidents 1 and 2 in Europe this year."

During these steps, the TI provider can map the threat actors to the Critical Function(s) and the underlying motivation and intent. For example:

	Asset Management	**Payment processes**	**Processing of PII**
TA-505 (Organised Criminal Group)	Financial gain – Theft of Money	Financial gain – Fraudulent transfers	Financial gain – Theft and selling of PII
Cobalt group/Money taker/ FIN7 (Organised Criminal Group)	Financial gain – Theft of Money, Theft and selling or use of Market sensitive information	Financial gain – Theft of Money	Financial gain – Theft and selling of PII
APTxx (Nation State)	Espionage – Theft of confidential information		Espionage – Monitoring Opponents

Furthermore, the TI provider should also provide an explanation as to why other threat actors are excluded.

4.4 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.

It is important that the TI provider sets out a detailed analysis of the TTPs that the real life threat actor would use – in this regard, it is highly recommended that the TI provider uses the **MITRE ATT&CK Framework** as the model[5].

The MITRE ATT&CK Framework sets out detailed and prescriptive TTPs, and provides a robust and comprehensive basis for the TI/RT providers to plan the threat and attack scenarios. The TI provider should map the critical functions, objectives/flags and threat actors to the TTPs that would most likely be used by the real life threat actor. For example:

Threat Actor	Objective/Flag	Tactic	Technique	Procedure(s)
APTxx (Nation State)	**Exfiltration of sensitive data**	**Exfiltration** - The adversary is trying to steal data.	**Automated Exfiltration** - Data, such as sensitive documents, may be exfiltrated through the use of automated processing or Scripting after being gathered during Collection.	**Machete** - Machete's collected files are exfiltrated automatically to remote servers. **USBStealer** - USBStealer automatically exfiltrates collected files via removable media when an infected device is connected to the second victim after receiving commands from the first victim

Whilst this provides a good basis for the test, the RT provider should be flexible and ready to change course during the test and apply other TTPs.

4.5 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. The number of threat scenarios will differ by test, depending on the nature of the entity, the scope, flags and the overall information gathered during the reconnaissance.

[5] https://attack.mitre.org/

Based on the detailed reconnaissance of the information, the TI provider should build threat scenarios, focusing on the specific intent of the threat actor for attacking a specific CF of the entity, and taking into account what TTPs a threat actor would employ when attacking the entity.

The threat scenarios should not be based on historical data only. Rather, the TI provider is expected to think about where the threat actor is going next and what new avenues the threat actor would explore. The TI provider should also take into account:

- the sophistication of techniques the actor would use;
- the agility of the threat actors (i.e. how the threat actor would adapt quickly to changing circumstances and how would they do this);
- how targeted they are towards their end goal (i.e. do they go directly to the CF or firstly provide broad presence within the network and/or roam around to look for opportunities); and
- their knowledge of the financial sector, its functions and the systems being used (i.e. have they targeted the financial sector or similar systems before).

The TI provider can use its creative freedom and knowledge of trends to forecast upcoming attacks for the selected threat actors.

It is highly recommended that the TI provider uses the **MITRE ATT&CK Framework** as the model to support the threat scenarios.

The TI provider should, based on the intelligence gathered, make a list of draft threat scenarios that are rated based on capability of the actor and intent. These should thereafter be discussed by the entity's White Team and TCT, and be approved by both stakeholders. The TI provider should produce enough threat scenarios to stimulate a substantiated debate between the White Team and TCT, and provide a sufficient basis for the RT provider to develop attack scenarios in the Red Team Test Plan.

4.6 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).

It should be noted that finalising the flags should be a fluid process, and whilst the TTI Report helps inform this, they should be finalised in the Red Team Plan. The finalisation of the flags should be a multilateral discussion between the White Team, TCT, TI and RT providers.

5 Approach of the TI provider

The TIBER-EU Guidance for Target Threat Intelligence Report aims to provide a standardised approach to develop the TTI Report. The TI provider should use the Scope Specification document, the Generic Threat Landscape report (GTL) if applicable, and the guidance set out in this document to prepare the TTI Report.

TI providers will differ in their approaches and their documentation. The TIBER-EU Guidance for Target Threat Intelligence Report does not aim to prescribe how TI providers should format their reports, but aims to provide a structured approach to the TI phase.

The **Threat modelling and scenario identification** section (Section 4) aims to provide a logical approach to determining the threat scenarios, and ensure that the output is detailed and useful for the entity and the RT providers.

The final TTI Report should provide detailed sections on: business overview; digital footprint; threat intelligence input; and a clear rationale for the threat actors relevant to the entity, their motivations and intent, and the TTPs that they would employ to target the critical functions and achieve the set objectives/flags (i.e. the threat scenarios).

The threat intelligence phase will take approximately 6-8 weeks, and must be conducted by TI providers that meet the requirements set out in the TIBER-EU Services Procurement Guidelines.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu