jamk

TIBER-EU Preparation Phase Framework

Case study Nixu: optimizing TIBER-EU engagements

Tuukka Valkeasuo

Master’s thesis
March 2023
Information and communication technology
Master's Degree Programme in Information Technology
Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Valkeasuo, Tuukka

TIBER-EU Preparation Phase Framework

Jyväskylä: JAMK University of Applied Sciences, March 2023, 71 pages.

Master's Degree Programme in Information Technology, Cyber Security. Master's Thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

TIBER-EU is an industry-specific framework for entities part of the European core financial infrastructure to plan and execute threat intelligence-based red teaming exercises. The goal of TIBER-EU is, through a standardized approach, to ensure the quality of the security tests and gain consistent results, improving the cyber resilience of the European financial sector.

The development of TIBER-EU was completed by the European Central Bank and European Union national central banks, and the framework was published in May 2018. As TIBER-EU is a relatively new concept, financial institutes lack experience in initiating TIBER-EU projects. Similarly, red teaming and threat intelligence service providers have potential to optimize their methodologies to plan and execute their assignments. The research focused on understanding if it is possible to develop a framework and a tool to enhance the quality of cyber security service provider Nixu's TIBER-EU project planning and scoping, considering that the information received from the target entity may be limited.

To implement a framework that provides value for real-life engagements, the research started with a series of interviews to analyze the current state of the TIBER-EU engagement methodology and to gather improvement requirements. Co-creation methodology was used to design the data models and business logic of the tool implemented using a selected low-code platform.

The research outcome was that the scope for a TIBER-EU engagement can be conducted from well-structured threat intelligence, target entity characteristics, and red teaming scenarios. Tool implementation demonstrated this in practice, and the final evaluation survey confirmed the findings. However, deployment of the framework into use was found to require adjustments in how the needed data is generated and managed by the organization.

Keywords/tags (subjects)

Cyber security, TIBER-EU, Red Teaming, Cyber Threat Intelligence, Co-creation

Miscellaneous (Confidential information)

No confidential information.

jamk

Description

Valkeasuo, Tuukka

TIBER-EU -valmisteluvaiheen viitekehys

Jyväskylä: Jyväskylän ammattikorkeakoulu, maaliskuu 2023, 71 sivua

Master’s Degree Programme in Information Technology, Cyber Security. Opinnäytetyö YAMK.

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

TIBER-EU on toimialakohtainen uhkatietoihin perustuva hyökkäävän tietoturvatestauksen toimintamalli eurooppalaisen finanssialan kriittisen infrastruktuurin toimijoille. TIBER-EU -toimintamallin tarkoitus on vakioida ja siten varmistaa laadukas sekä yhdenmukainen tietoturvatestaus.

Euroopan keskuspankki on johtanut yhdessä Euroopan Unionin keskuspankkien kanssa TIBER-EU -viitekehyksen kehitystä, joka julkaistiin toukokuussa 2018. TIBER-EU -toimintamallin ollessa suhteellisen uusi, finanssitoimialan yrityksillä ei ole vielä merkittävästi kokemusta TIBER-EU projekteista ja niiden käynnistämisestä. Vastaavasti, tietoturvatestaus- ja uhkatietopalveluita tarjoavilla yrityksillä on mahdollisuuksia kehittää heidän metodologioitaan suunnitella ja toteuttaa toimeksiantoja. Tutkimus keskittyy määrittämään onko mahdollista tuottaa viitekehitys ja työkalu kehittämään tietoturvayhtiö Nixun TIBER-EU projektien suunnittelun ja laajuuden määritystä, huomioiden, että asiakasyritys saattaa toimittaa vain rajallisesti tietoa suunnittelun tueksi.

Tutkimustyö aloitettiin haastattelemalla Nixun tietoturva-asiantuntijoita. Tarkoituksena oli ymmärtää TIBER-EU -hankkeiden nykytila ja -toimintamalli, sekä kerätä kehitysideoita. Nykytilan ymmärtäminen tuki myös tutkimuksen lopputulosten soveltamista käytäntöön. Kehitystyö tehtiin yhteiskehittämismetodologialla, ja lopputuotokset toteutettiin valittua matalan koodin alustaa hyödyntäen.

Tutkimuksen tulokset osoittivat, että TIBER-EU -hankkeiden suunnittelua ja laajuutta voidaan määrittää uhkatietojen, kohdeyrityksen ominaisuuksien, ja tietoturvatestausskenaarioiden rakenteellisella mallilla. Toteutettu työkalu osoitti tämän käytännössä, lisäksi kyselytutkimuksen vastaukset vahvistivat havainnot. Kehitetyn työkalun käyttöönoton havaittiin kuitenkin vaativan organisaation toimintamallien kehitystä, mukaan lukien rakenteellisen mallin vaatiman datan tuottamiseksi.

Avainsanat (asiasanat)

Kyberturvallisuus, TIBER-EU, Red Teaming, Kyberuhkatiedot, Yhteiskehittäminen

Muut tiedot (salassapidettävät liitteet)

Ei salassapidettäviä tietoja.

Contents

Figures

Tables

Terms and Abbreviations

API	Application Programming Interface
APT	Advanced Persistent Threat
ERD	Entity Relationship Diagram
ENISA	The European Union Agency for Cybersecurity
GTL	Generic Threat Landscape
HUMINT	Human Intelligence
MITRE ATT&CK	Globally accessible knowledge base of adversary tactics and techniques
OSINT	Open Source Intelligence
RT	Red Team
RTTP	Red Teaming Test Plan
RQ	Research Question
TCT	TIBER Cyber Team
TI	Threat Intelligence
TKC	TIBER-EU Knowledge Center
TIBER	Threat Intelligence Based Ethical Red-Teaming
TIBER-EU	The European framed for Threat Intelligence Based Ethical Red-Teaming
TTI	Targeted Threat Intelligence
TTIR	Targeted Threat Intelligence Report
TTP	adversary Tactics, Techniques, and Procedures

1 Introduction

1.1 Introduction and business context

Red teaming as a means to decrease enterprise risks across strategic, operational, and tactical levels was referred to as an existing concept by the Department of Defense (2003) almost two decades ago. Military forces are considered the early inventors of red teaming, initially used to find weaknesses in their strategies. Over time other industries, both in the private and public sectors, have adopted the methodology intending to improve their security posture by understanding how adversarial and malicious actors could breach their services, infrastructure, or organization (TechTarget, 2021). The scope of red teaming has developed to focus on cyber security. In this context, a red team has against them often a blue team, the company's internal IT and security persons defending against attacks (National Institute of Standards and Technology, n.d.-a).

The need for industry-specific frameworks and regulations arises since not all industries are equal for cybercriminals. One of the most targeted industries is finance and insurance, overtaken by last year by the manufacturing industry (IBM Security, 2022). TIBER-EU's goal is as an industry-specific intelligence-led red teaming framework to strengthen the security resilience of the European financial sector. It also addresses the risk of the possible use of conflicting frameworks and introduces a set of rules for cross-authority cooperation reducing regulatory complexity and efforts required (European Central Bank, 2018).

As a case study, I will research and develop TIBER-EU engagement improvements for Nixu, a leading cyber security services company. Nixu has already established a presence using the TIBER-EU framework across European financial institutions and is looking for possibilities to optimize its use further to benefit Nixu and its customers.

1.2 Business challenge, research questions, and objective

TIBER-EU is a framework for entities being part of European core financial infrastructure to, so far, voluntarily plan and execute threat intelligence-based red teaming exercises. The goal of TIBER-EU is through a standardized approach to ensure the quality of the security tests and gain consistent results. The framework being relatively new, even though it contains details of the end-to-end

TIBER process (see Figure 1) and its phases and actors, service providers still have potential to optimize the methods to apply it across the TIBER-EU engagements.

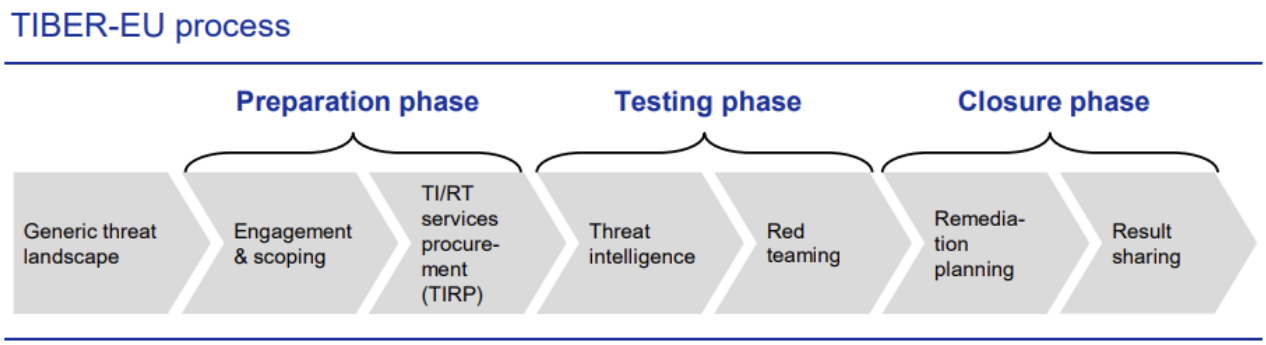

Figure 1. TIBER-EU process (European Central Bank, 2018, p. 20)

In the initial scope definition of the research, Nixu's key stakeholders and I identified the importance of the TIBER-EU preparation phase. Even if optimization areas could also be found from the later phases of the process, efficiently and consistently defining and communicating the scope to the customer already in the procurement phase is a crucial success factor of an engagement. Thus, the research questions were defined as follows:

- RQ1: Is it possible to improve TIBER-EU engagement scope definition, communication, and effort estimate accuracy with a threat intelligence-based framework?
- RQ2: What kind of threat intelligence-based framework would improve TIBER-EU engagement scope and effort estimate accuracy?
- RQ3: Can a tool be implemented for such a threat intelligence-based framework?

The logical structure of the framework can be illustrated (see Figure 2) as a chain of input information leading to the required output. In practice, the final output is the relevant attack scenarios

for a particular financial institute, which Nixu then uses to organize in an optimal way for the engagement.

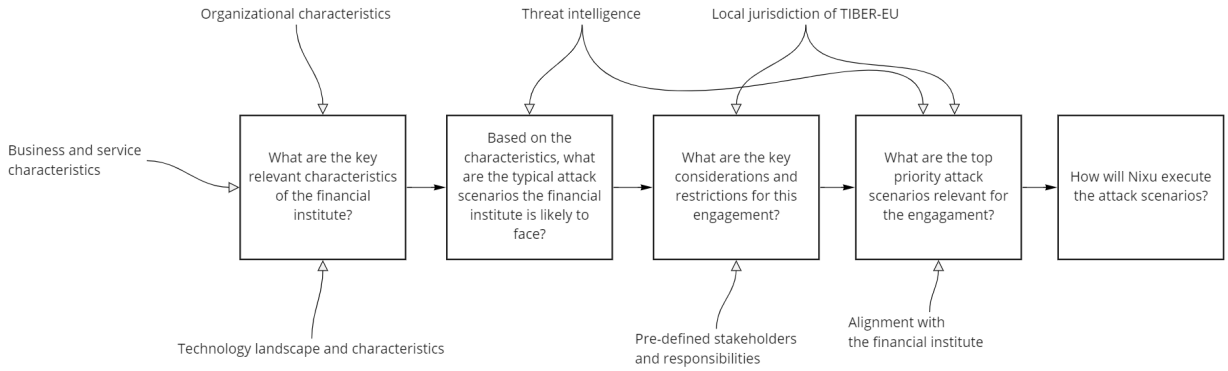

Figure 2. The logical structure of the researched TIBER-EU Preparation Phase framework

Suppose I am able, with my research, to define the framework that is proven to work. In that case, the expectation is that a more relevant engagement scope will further improve Nixu's operational efficiency when delivering TIBER-EU services. In addition, one of the goals is to strengthen dialogue with customers' non-technically savvy stakeholders leading to better customer satisfaction and less obscurity.

1.3 Thesis structure

The TIBER-EU Preparation Phase framework research is done in collaboration with Nixu's TIBER subject matter experts. This process is iterative, which is also reflected in the thesis structure.

The first Chapter introduces the business context, research questions, and expected outcomes. A brief history of red teaming is followed by introducing the significance of the financial industry for cyber criminals and the TIBER-EU framework as an industry-specific framework to address it. The reader is also introduced to the highest level of process description of TIBER-EU to set the context for the research focusing on the preparation phase and the logical structure of the framework to be researched and developed. The Chapter is finalized with a description of the research methods.

The second Chapter contains the literature review and previous research in red teaming, cyber threat actors and intelligence, financial industry cyber security, and TIBER-EU. As the developed framework aims to define the relevant attack scenarios for a given financial institute, this chapter emphasizes research on attack scenarios and their evolution in the finance sector. MITRE ATT@CK

framework as a recommended adversary tactics and techniques knowledge base is also researched.

Chapters 3, 4, and 5 focus on the implementation of the research. The implementation begins with the current state analysis, including knowledge base and data gathering, followed by the analysis of the data and key findings summary in Chapter 3. The fourth chapter builds on the essential findings and develops the first hypothesis of the framework to be iteratively enhanced during the implementation. The fifth chapter contains all the iterations of the actual framework development. The primary research method in this phase is co-creation workshops. Each workshop's outcomes and impact on the framework are documented. The final proposal of the framework is presented, including the feedback for ongoing development.

Chapter 6 analyzes the research results, including the co-creation workshops and the survey as a triangulation method. After the analysis, conclusion of the key results, findings, and additional benefits is presented. Finally, Chapter 7 discusses the critique and reflections on the research, as well as ethics, reliability and further research topics.

1.4 Research methods

1.4.1 Research Design

To implement a framework that provides practical value and can be used in real-life engagements, I start the research by analyzing the current state of Nixu's TIBER engagement processes. By understanding the key improvement areas and gathering the knowledge base from the stakeholders, the research can continue to the implementation planning phase in which the initial framework is designed, and co-creation workshops are planned to improve it. To prove the results of the framework, the results assessments phase completes the research. This research process is illustrated in Figure 3.

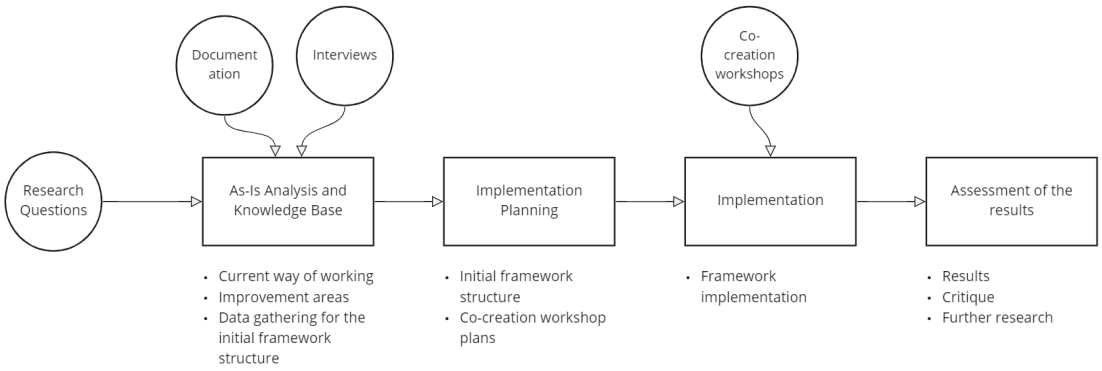

Figure 3. The research phases

The approach is designed to provide precise phasing and defined outcomes for each while providing the flexibility that is expected to be needed based on the results of the interviews and co-creation workshops.

1.4.2 Research Approach

The phased approach I chose requires different research methods across the phases. The as-is analysis differs from the implementation phase, and applicable methods must be used for each.

Initially, I planned to use the *observation* method for the as-is analysis and knowledge base phase. An observation method is a qualitative data collection method based on empirical understanding. This method is particularly well suited for researching phenomena that evolve over time, possibly even several years (Szajnfarber & Gralla, 2017). To understand the feasibility of an observation method for the research, it must be applicable for a part of a long-lasting process, as my thesis aims to improve a planning phase of a red teaming engagement. University of Jyväskylä (2012) states that observation as a data collection method should focus on human behavior, including verbal and non-verbal expressions, and how the phenomenon is used and interacted with. Szajnfarber & Gralla (2017) discuss the observation method also in the context of a product development process, possibly to be used only for a particular milestone of it. These definitions are encouraging; the observation research method could be applied in the research context.

Obstacles in applying the observation method result from challenges of confidentiality and limiting exposure of unexpected events to a researcher. This may expose a risk that cannot be accepted in

cyber security engagements. In addition, as the stakeholders of the research are working in multiple countries and often remotely, observation would need to be executed in an online environment. Lack of visibility to human interactions and being able to see only through small lenses of web cameras hinder the data collection. Due to these factors, the interview method was chosen instead of observation. An interview method, a non-qualitative data collection method relying on note-taking and recordings as well, focuses on gathering data only during the duration of the interview session. In an interview, a researcher is clearly present, and the observation method differs from it by having options of being executed as overt or covert research. I do not consider being present an issue for the research questions as the actual human behavior is not essential, rather only the logic of decision-making when planning the TIBER-EU engagements.

Since in interviews the interviewees are being guided through the session with a set of questions and effectively limiting their thought process, it is not an optimal method for generating new inventions. A method that fits better for capturing new ideas is *co-creation*, a creative process that involves all the stakeholders in problem-solving. (Benson et al., 2021). Co-creation is categorized as Participatory Action Research, having typical elements of being targeted for a defined need and executed in an iterative manner (Institute of Development Studies, n.d.). I deemed these characteristics to be the right ones, considering the research questions to be solved and the stakeholders participating in the research.

1.4.3 Data Collection

The data collection plan for the research is illustrated in Figure 4, divided according to the research process phases. I structured the data collection based on the Six Sigma data collection plan, as one of its primary goals is to ensure everyone participating in the data gathering has the same understanding of the plan (Juneja, n.d.).

	Purpose of the data gathered	**What?** in terms of measurements and ways to collect	**Type of Data** continuous or discrete	**Who** are involved in the data collection	**Where** in the process, not physically	**Frequency** of the data collection	**How to display** the collected data
As-Is Analysis and Knowledge Base	• Stakeholder map and engagement • Understanding the current process • Identifying improvement areas • Initial idea gathering	• A pre-defined set of interview questions • Unstructured follow-up questions for details or topics of importance	• Discrete: interview discussion, notes and recording	• Pre-defined set of stakeholders	• TIBER-EU planning phase expertise gathered from the stakeholders in the as-is analysis phase of the research	• Interviews are executed once • Possibility to request clarifications or details requested from interviewees	• Workshop notes • Recording • As-is analysis highlights documented
Implementation	• Ideas and feedback for iterative framework development • Input for answering the research questions	• Co-creation workshops according to the plan developed in the Implementation Planning phase	• Iterative process of co-creation workshops	• Pre-defined set of stakeholders	• TIBER-EU planning phase expertise gathered from the stakeholders in the implementation phase of the research	• Two iterative co-creation workshops	• The developed framework • Documented further improvement areas
Assessment of the results	• Triangulation to validate the implementation results and research question answers	• Survey to gather data of the implementation results	• Discrete: one time survey	• Pre-defined set of stakeholders	• Stakeholder input and expectations for the framework in the assessment phase of the research	• One survey	• Survey results chart

Figure 4. Data Collection Plan

While in my research, contrary to Six Sigma projects, I will be planning and executing the data gathering by myself, the structure provides solid grounds for verifying the completeness of the plan and communicating it to the stakeholders.

The stakeholders of the research project are categorized based on their expertise and responsibility areas in TIBER-EU engagements, as illustrated in Figure 5.

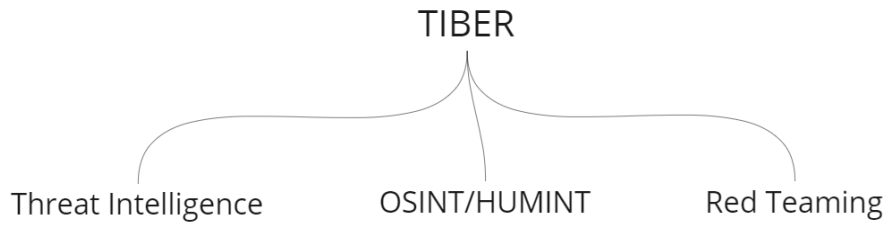

Figure 5. Stakeholder map

As the categorization above does not reflect the actual organization in place, it aids in defining the relevant expertise needed for TIBER engagements and mapping them to the expert group of our research. The definitions for the categories:

- **Threat Intelligence**: A person whose primary expertise and typically organizational position is in the domain of threat intelligence. The expected role in a TIBER engagement would be as a Threat Intelligence Provider.
- **OSINT/HUMINT**: A person whose primary expertise is in OSINT (Open Source Intelligence) and HUMINT (Human Intelligence) and typically works across the engagements providing insights across an engagement lifecycle. The expected role in a TIBER engagement is to execute and aid in social engineering scenarios and part of penetration test scenarios.
- **Red Teaming**: A person whose primary expertise is in assessing vulnerabilities in people, a physical and a technical landscape of a target, and executing scenarios gaining initial access and expanding presence in the target entity. The expected role in a TIBER engagement is to execute the scenarios defined by the scope.

- **TIBER**: A person with expertise across the three other domains and combining them to a threat intelligence-based ethical red teaming. The expected role in TIBER engagements is in business development, sales support, project management, and potentially the execution of the scenarios defined by the scope.

The planning of data collection needs to consider an individual having expertise in more than one category.

2 Literature Review

2.1 Scope of the Literature Review

TIBER-EU is an outcome of cyber security evolution from general defense mechanisms to an industry-specific detailed offensive security framework. While I don't study general cyber security trends, it is essential to understand why the shift from defensive to offensive has taken place, the importance of the financial sector specifically, and related terms and frameworks recommended by TIBER-EU. Building on research on blue, purple, white, and red teaming gives us the stepping stone to understanding how adversary attacks are modeled using the MITRE ATT@CK framework. I continue to study the importance of cyber security for the financial industry and the most relevant threat actors, namely the APTs (Advanced Persistent Threats). This relates to understanding and researching the concept of Threat Intelligence, which is at the heart of the Threat Intelligence Based Ethical Red Teaming (TIBER).

2.2 Red Teaming

The concept of using colors to indicate teams and their position in an attack scenario can be traced back to the military. The US military is the originator of the term "Red Team" during the Cold War during the 1960s. At the time, red color represented the Soviet Union and has evolved to represent any actor in an adversarial position. (Zenko, 2015). Similarly, the term "Blue Team" has been established for the defending forces.

Red Teaming in the field of cyber security has the same ultimate purpose as in the military, improving the readiness and skills of the defending organization (National Institute of Standards and Technology, n.d.-a). The Blue Team, typically a group of people defending the information systems, is challenged by a group of internal or external people emulating a potential attack scenario

(National Institute of Standards and Technology, n.d.-b). A red team naturally has permission for the emulation, and a small group of people in the target organization know and plan the assignment. Rules of Engagement are carefully documented to define the legality of the actions as well as ensure the proper scope for the tests to provide the expected outcomes for the organization. In more extensive engagements, the task of defining the rules of engagement and monitoring the red teaming exercise, a "White Team" can be established. This group of people acting as referees will ensure the rules are obeyed, communicate with the red and blue teams in case of questions or issues, and typically be responsible for post-engagement activities, including documenting the results and lessons learned. (National Institute of Standards and Technology, n.d.-c). Quite recently, the colors red and blue have been brought closer together to form Purple Teaming. In this concept, the two teams, instead of working against each other, do collaborate with the goal of improving cyber security as one team. This approach is considered a better fit for companies with varying sizes and cyber security maturity, granted that enterprises with larger budgets are claimed to get better results and also bring speed and cost efficiency in the execution and learning (Godyla & Hickey, 2021; Olsen, 2022).

Red teaming and penetration testing are both offensive cyber security tests, but there are inherent differences between the two. The purpose of the penetration test is to find vulnerabilities in the target organization, but this is done for a set of defined technical assets or systems within a given time frame. This is often used interchangeably with the term ethical hacking. However, ethical hacking is an umbrella term, including penetration testing. In a penetration test, a single application might be tested, while ethical hacking does not explicitly define the assets to be tested; its goal is to penetrate into the organization by leveraging a comprehensive set of assets in the network. (Fox, 2021; Narang, 2023). Red teaming further builds on the concept of ethical hacking by adding attack surfaces and methodologies and expanding the duration of the testing. While there seems not to be a well-defined difference between red teaming and ethical hacking, red teaming can be considered long-lasting or continuous testing not only concentrating on technical assets but including, for example, Open Source Intelligence, Threat Intelligence, social engineering, and physical penetration testing (Das, 2019; Synopsys, Inc., 2022). Furthermore, TIBER is an evolution of red teaming, defining in detail the actors, processes, and responsibilities of red teaming for the financial industry in Europe. Figure 6 depicts the high-level relation of these concepts, notably the TIBER partial circle illustrating it is originally not meant to be industry-agnostic.

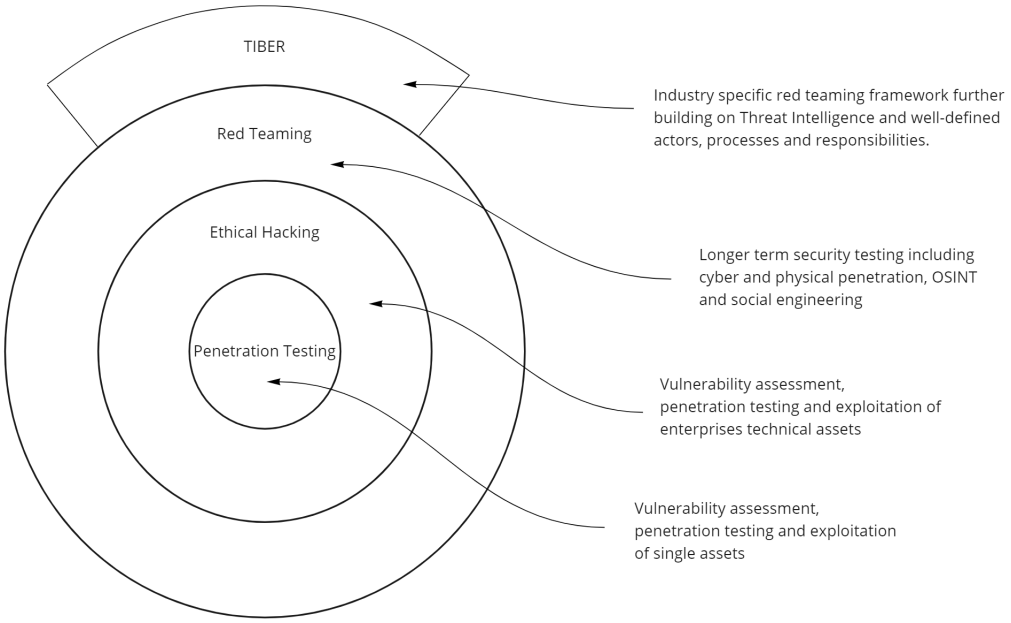

Figure 6. High-level relation of penetration testing, ethical hacking, red teaming and TIBER

Next, I continue the literature study with the concept of threat intelligence. This fundamental concept sets TIBER apart from red teaming, where threat intelligence if used, is on a more generic level.

2.3 Cyber Threat Intelligence

The purpose of threat intelligence is to provide evidence-based data for an organization to improve its security posture. It is information collected by the organization itself, shared by the organization, or received by the organization from a third party. For it to be intelligence, it must have relevance and priority indicators to the organization, which must be able to take actions based on the information. (Liska, n.d.).

As an industry, cyber threat intelligence is relatively young, as the first threat intelligence report with extensive media coverage is generally considered to be the Mandiant APT1 report issued in 2013 (Roberts, 2021). However, the sole purpose of threat intelligence is not to provide publicly available information and reports. The industry today consists of human intelligence services and providers, threat data feed providers, threat intelligence platforms, and complete threat intelligence solutions (InfoSecurity, 2020). The vendors provide commercial services, and threat intelligence can be highly confidential.

All threat intelligence is not equal; the typical classification is to divide them into strategic, operational, and tactical intelligence. Strategic threat intelligence is used for organizational planning and long-term goals, operational intelligence concentrates on day-to-day operational activities. Tactical intelligence can be based on real-time data sources, including intelligence provider data feeds (Gourley, 2018). Baker (2022) further defines more specific use cases for each classification.

- **Tactical**: threat feeds, real-time alerts, automated malware analysis
- **Operational**: threat monitoring, patch prioritization, actor profiling, incident response, operational intelligence reporting
- **Strategic**: campaign tracking, insider threat, threat research, deception operations, strategic intelligence reporting

In the context of TIBER-EU, the threat intelligence significance is two-fold. The threat reports' structure and contents are an integral part of the TIBER-EU -framework and thus also have a considerable role in enhancing Nixu's TIBER-EU planning process. On the other hand, I will research the existing threat intelligence in the context of the financial industry and relevant threat actors, ultimately leading to the birth of the TIBER-EU.

Roberts (2021) suggests that threat intelligence reports generally have the same structure, including key points, summary, details, recommendations, and appendices. Since the contents are defined on a high level, I need to look at public threat reports for the details. I chose three well-known public threat report providers: Crowdstrike's 2022 Global Threat Report (Crowdstrike, 2022), ENISA Threat Landscape 2021 (The European Union Agency for Cybersecurity, 2021), and National Cyber Security Centre Finland's Information Security 2020 Annual Report (Finnish Transport and Communications Agency National Cyber Security Centre, 2021). Consequently, these three sources represent global, European, and country-specific annual threat intelligence reports.

ENISA and Crowdstrike follow the structure proposed by Roberts (2021). A notable difference between the reports is that only ENISA and Crowdstrike provide intelligence on active cyber threat actors.

Finnish Transport and Communications Agency National Cyber Security Centre has in addition introduced a concept of *cyber weather*. This is a form of a summary of the information that can be easily understood by non-technology savvy readers, following the trend of the reports evolving to

become more engaging for the readers and dynamic in their structure for ease of use (The European Union Agency for Cybersecurity, n.d.).

2.4 Cyber Threat Actors

Individuals, groups of individuals, or states with malicious intent, potentially having an impact on an organization's security, are called cyber threat actors (CubeCyber, n.d.; Haber, 2017). Cyber threat actors' motivations, goals, and capabilities vary, and they can be classified according to them (CircleID, 2019; Redlegg, 2020):

- **Nation-states / advanced persistent threats:** Funded and sponsored by nations with extraordinary resources. Typically targeting intellectual property, sensitive information, and money, as well as supporting their nation's espionage goals.
- **Cybercriminals / organized crime**: Targeting confidential data and personal information for financial gains, or stealing money directly or indirectly, for example, leveraging ransomware.
- **Hacktivists**: Driven by political or socially motivated purposes, often targeting to raise awareness for their cause
- **Terrorist groups**: Driven by ideological violence targeted to cause destruction to critical services and infrastructure
- **Thrill-seekers / script kiddies**: Typically using tools developed by others or exploiting known vulnerabilities to attack networks for the thrill or personal satisfaction of their achievement.
- **Insider threats**: Employees who have infiltrated an organization for malicious purposes, or existing employees who have been persuaded to turn against their organization, or often due to dissatisfaction, want to cause harm for their employer.

Ola (2019) summarizes the actors, their attacks, attack significance, and complexity in a six-tier model illustrated in Figure 7.

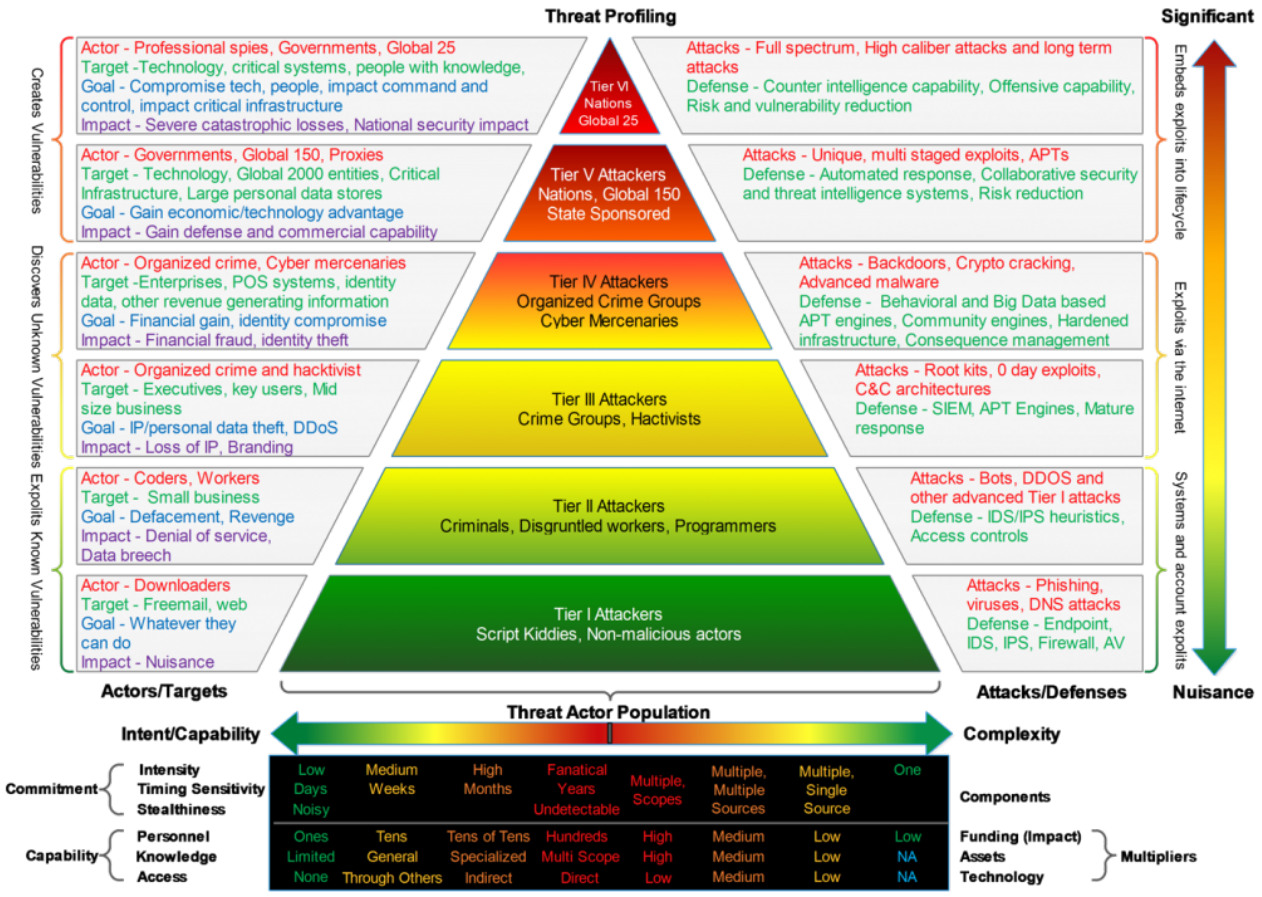

Figure 7. Threat actor tiers (Ola, 2019)

In the context of TIBER-EU and cybercrimes against European financial institutions, the relevant tiers are tiers IV to VI. Nation states / advanced persistent threats and organized cyber criminals can be considered to pose the most relevant threat scenarios against strong cyber defenses.

Several cyber security organizations track APTs. Steffens (2020) claims that adversaries form patterns of habit over time to gain higher productivity. These behavioral and technical clues are used to attribute attacks to threat actors.

APTs are not named after a standard naming convention. For example, Mandiant uses a numbering scheme and lists 37 APTs in their catalog (Mandiant, n.d.), and Crowdstrike uses animals in the naming convention and lists 10 APTs (Crowdstrike, n.d.). MITRE maintains an APT list that does its best to combine the naming convention into a single table (The MITRE Corporation, n.d.-b). In July 2022, the table consisted of 133 adversary groups, including 17 APTs, and the numbers are expected to grow as Crowdstrike named 21 new adversaries in 2021 (Crowdstrike, 2022, p. 7). Steffens (2020) states that over 130 APTs have been named over time.

Analyzing adversaries has led to the conclusion that there is an extensive but confined amount of tactics, techniques, and procedures attacks consist of. MITRE ATT@CK framework has been established to document these and is generally considered the de facto repository for the information (Routin et al., 2022, p. 267).

2.5 MITRE ATT@CK

Understanding adversary actions, analyzing intrusions, and preparing for attacks have required a way to document the threats. An early pioneer in establishing a standardized documentation methodology was Lockheed Martin with their Cyber Kill Chain. This adaptation of the military kill chain concept into cyber security was considered a success in raising awareness of such documentation frameworks. (Orchilles, 2022). Two years later, in 2013 US Department of Defense released the Diamond Model of Intrusion Analysis. As Cyber Kill Chain is based on the concept of interrupting an adversary's playbook of steps, it is a concept of linear steps attackers are expected to take. The Diamond Model, on the other hand, emphasizes four key features of an intrusion: adversary, infrastructure, capability, and victim (Caltagirone et al., 2013).

The Cyber Kill Chain and the Diamond Model have not disappeared; however, the cyber security industry currently relies mainly on the MITRE ATT&CK framework (see Figure 8). The ATT&CK framework has been developed since 2013 to document threat tactics and techniques to explain how an attacker has or may be exploiting a target company. The MITRE ATT&CK consists of threat matrices, categories, and techniques with additional information on how attackers use the techniques and how to detect and mitigate them (The MITRE Corporation, n.d.-a).

Figure 8. ATT&CK Matrix for Enterprise (The MITRE Corporation, n.d.-a)

In addition to containing a catalog of TTPs, the MITRE ATT&CK can be used to document intrusions and plan red teaming scenarios, as illustrated in Figure 9.

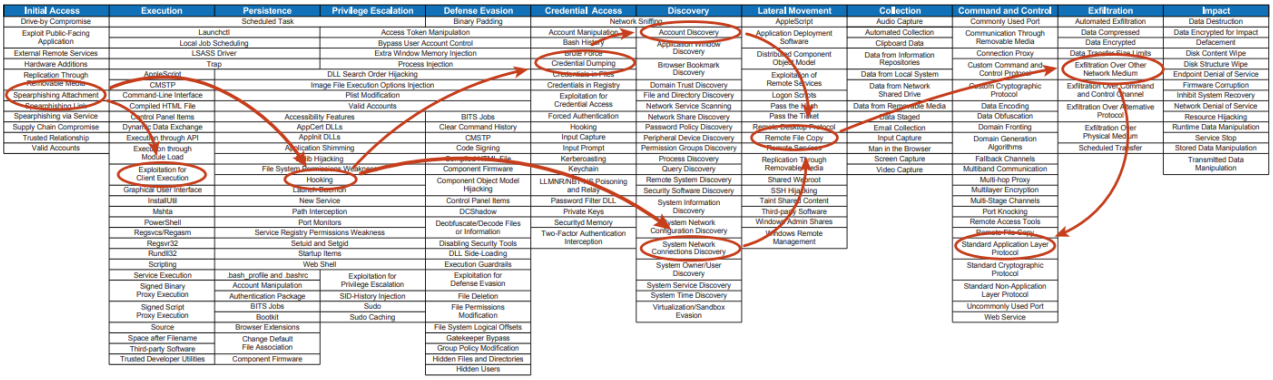

Figure 9. ATT&CK for Adversary Emulation and Red Teaming (The MITRE Corporation, 2020)

Furthermore, as demonstrated in Figure 10, the APT characteristics can be mapped on ATT&CK for documentation purposes or comparison of an attack against an APT for threat actor attribution.

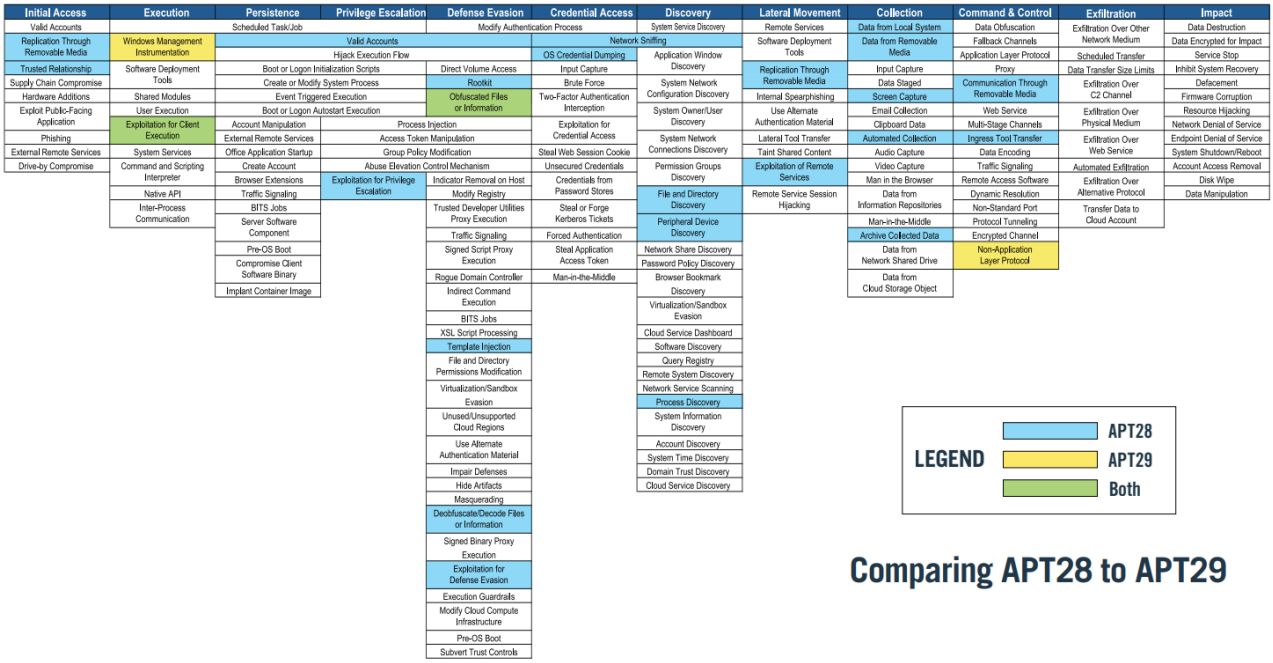

Figure 10. ATT&CK for Threat Actor Analysis (The MITRE Corporation, 2020)

ATT&CK has also been recognized by several significant cyber security companies extending the framework as third-party projects (Strom, 2021). A framework with remarkable adoption in the cyber security industry supports the goal of TIBER-EU to harmonize the red teaming approach and methodology, and the constant pace of improvement of ATT&CK provides a reliable platform to rely on. While not explicitly requiring it, TIBER-EU highly recommends that the threat intelligence is based on the MITRE ATT&CK framework (European Central Bank, 2020a, p. 13).

2.6 Financial Industry Cyber Security

The growth of cybercrimes has been severe by any metric measured during the last years, and Cybersecurity Ventures forecasts the growth of costs to increase yearly by 15 percent. Today, cybercrime, if measured as an economy, would be the world's third largest, trailing only the U.S. and China, and the expected growth leads the yearly costs to 10.5 trillion USD by 2025. (Morgan, 2022).

The financial industry, defined by Beck et al. (1999) as *central banks, deposit money banks, and other financial institutions such as financial intermediaries and insurance companies, pension funds, and investment schemes*, is a lucrative target as the primary goal of cyber security adversaries is a monetary gain (Verizon, 2020). The focus on financial institutions is further amplified by

the migration to online banking, digital payment wallets, peer-to-peer transactions, digital currencies, and the use of the Society for Worldwide Interbank Financial Telecommunications (SWIFT)-based transaction system (Creado & Ramteke, 2020). World Economic Forum's report (2015) on disruptive innovation financial services functions painted a picture (see Figure 11) of the rapidly evolving industry and reasoning for the expansion of attack surfaces for adversaries, leading to the growth in cyberattacks.

Figure 11. Financial Services functions and innovation (World Economic Forum, 2015, p. 12)

The financial industry also suffers non-industry-specific attacks, such as ransomware. This form of malware encrypts files rendering them unusable until the malicious actor is paid a ransom for possible decryption. The attack does not rely on any industry-specific technologies or processes. These kinds of attacks cannot be underestimated as damages of ransomware across industries is expected to grow from 20 billion USD in 2021 to 42 billion USD in 2024, to a large extent due to a combination of significant profits, low probability of getting caught, and relatively low skills needed for the attacks (Morgan, 2022; Müller et al., 2022).

In my research, the focus is on direct attacks against financial institutes, not attacks against their customers, in which the adversaries often exploit the implicit trust of customers to banks causing monetary losses for individuals or companies through for example watering-hole attacks, wire

transfers and home equity loan frauds, social engineering attacks, and banking trojans (Kellermann & Young, 2019). Verizon analyzed in their Data Breach Investigation Report (2022) 2527 incidents in the financial and insurance industry globally. The most prevalent types of attacks representing 79% of breaches in the financial sector are *basic web application attacks*, *system intrusion,* and *miscellaneous errors*. These are followed by *social engineering*, *privilege misuse,* and *lost and stolen assets*, as depicted in Figure 12.

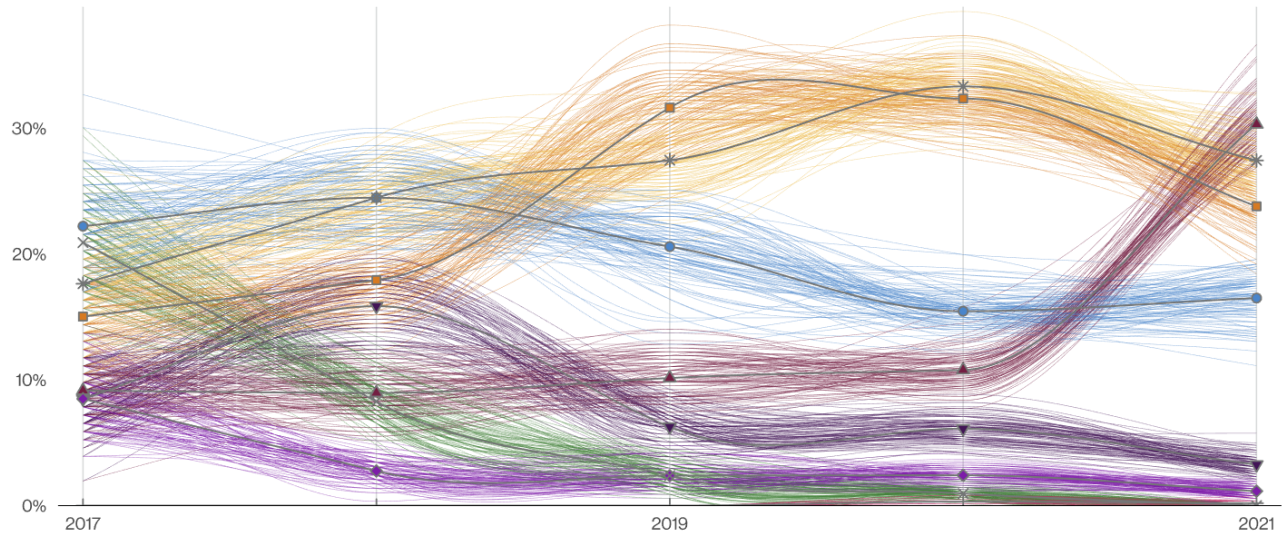

Figure 12. Patterns over time in Financial and Insurance industry breaches (Verizon, 2022)

An interesting trend in the report is that Actor disclosure has grown from 5% in 2016 to 58% in 2022. This is mainly due to ransomware attacks, which by nature require some form of Actor disclosure for the ransom payment.

Due to the growth trends in combination with cybercrime in financial services companies costing more than in any other industry (Accenture Security, 2018), companies and regulators have taken action to improve the situation. In Europe, the TIBER-EU framework has been established to aid the core financial infrastructure entities, as of now voluntarily, to enhance their security posture.

2.7 TIBER-EU

European Central Bank (2018) defines TIBER-EU as

> *a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led red team tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities*. *An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems.*

Ultimately TIBER-EU's goal is to improve the cyber resilience of the financial sector while responding to the trend of a growing number of frameworks, which may lead to incompatibility issues, inconsistent results, and a heavy burden to organizations, by providing a harmonized model across the EU. The framework is based on De Nederlandsche Bank's initial implementation of TIBER-NL in 2016 (Breachlock, 2020). The development of TIBER-EU was completed by the European Central Bank and European Union national central banks, and the framework was published in May 2018. In April 2022, twelve countries have implemented or are in the process of implementing the framework. (European Central Bank, 2022).

Comparing TIBER-EU to non-industry specific frameworks such as the Penetration Testing Execution Standard pre-engagement phase (Penetration Testing Execution Standard, 2014) or Open Source Security Testing Methodology Manual (Institute for Security and Open Methodologies, 2010), the latter are more operational, focus on execution of specific tests and their stakeholder management concentrates on infrastructure and supplier management, while TIBER-EU is designed to be European level multi-stakeholder process allowing collaborative cross-authority testing. This is supported by Saarainen's model to classify red teaming frameworks into high, mid, and low-level ones, and TIBER-EU scored high in all the categories of overall regulation, service provider regulation, and result-sharing regulation (2021, p. 51). Saarainen also claims that the frameworks with high governance are less agile. While this is true to a certain extent, TIBER-EU as a framework allows country-specific implementations to adapt to local circumstances.

At its highest level, the TIBER-EU defines the end-to-end test process to include three mandatory phases (European Central Bank, 2018):

- **Preparation phase**: Initiation of the test, including scope definition and procurement.
- **Testing phase**: Executing the planned tests, including red teaming and threat intelligence.
- **Closure phase**: Reporting of the results and planning the improvements.

In Finland, the TIBER-FI process created by the Bank of Finland has been defined to be executed in seasons lasting from six to twelve months, and the process has an initial step of *decision to participate* as the participation is voluntary for Finnish financial institutions (Finlands Bank, n.d.). In Denmark, the TIBER-DK goes into even more detail, defining the duration of each phase in weeks, for example preparation phase to last approximately 16 weeks (Danmarks Nationalbank, 2020, p. 12). Furthermore, the organizational charts and stakeholders are defined by each country as applicable to them.

TIBER-EU breaks down each phase into the more detailed process, actor and role, and deliverable definitions. Figure 13 depicts the details of the preparation phase in the focus of the research.

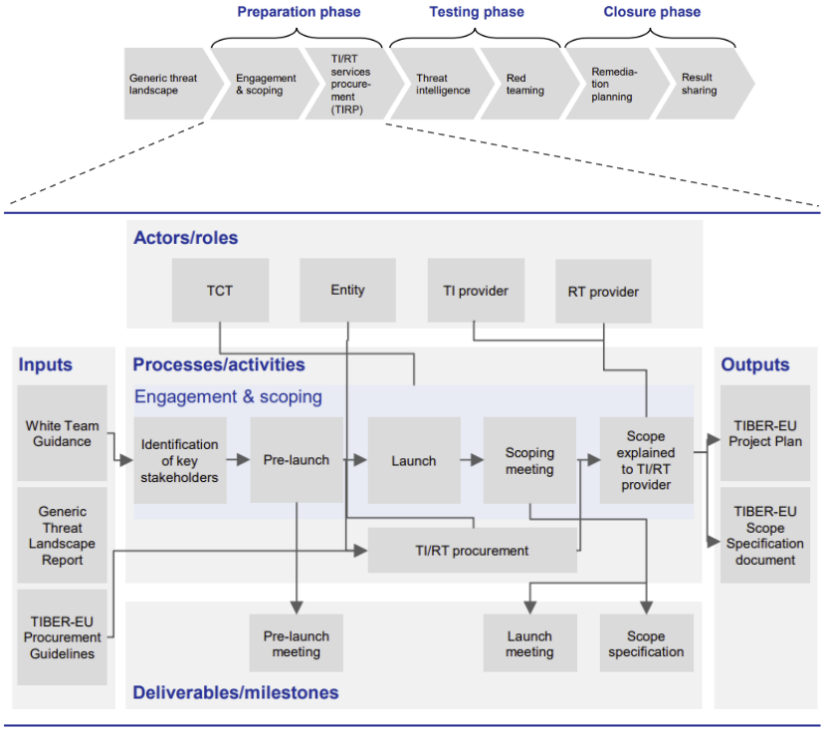

Figure 13. Overview of the TIBER-EU Preparation phase (European Central Bank, 2018)

As the execution of the tests is done in live environments instead of the test environment, TIBER-EU engagements carry an inherent risk. This is mitigated by unambiguously defining the roles and responsibilities and setting a standard set of requirements for the threat intelligence and red team provider companies and team members:

- **TIBER Cyber Team (TCT)**: Centralized body formed by the authorities bringing together the TIBER knowledge and capabilities at the national or European level. TCT works across all the TIBER tests in the sector. Led by a Team Test Manager (TTM).
- **TIBER-EU Knowledge Center (TKC)**: European Central Bank hosted body to improve collaboration of the national and European TCTs.
- **White Team**: coordinates the activities, including external parties providing red teaming and threat intelligence. Led by a white team lead (WTL).
- **Blue Team**: All the staff of the entity not belonging to the White Team. Blue Team is not informed about the test before the Closure phase.
- **Threat Intelligence Provider**: Provides threat intelligence and targeted threat intelligence reports to the tested entity. Must be an independent third party and meet the qualification criteria.
- **Red Team Provider**: Plans and executes the tests for the entity being tested. Must be an independent third party and meet the qualification criteria.
- **National cyber security center** or **governmental intelligence agency**: Provides relevant input and insights to the testing process and reports.

In TIBER-EU, the word *Entity* is reserved to represent the financial institute being tested.

For my research questions, it is important to analyze not only the preparation phase but also the first part of the testing phase *Threat Intelligence* (see Figure 14).

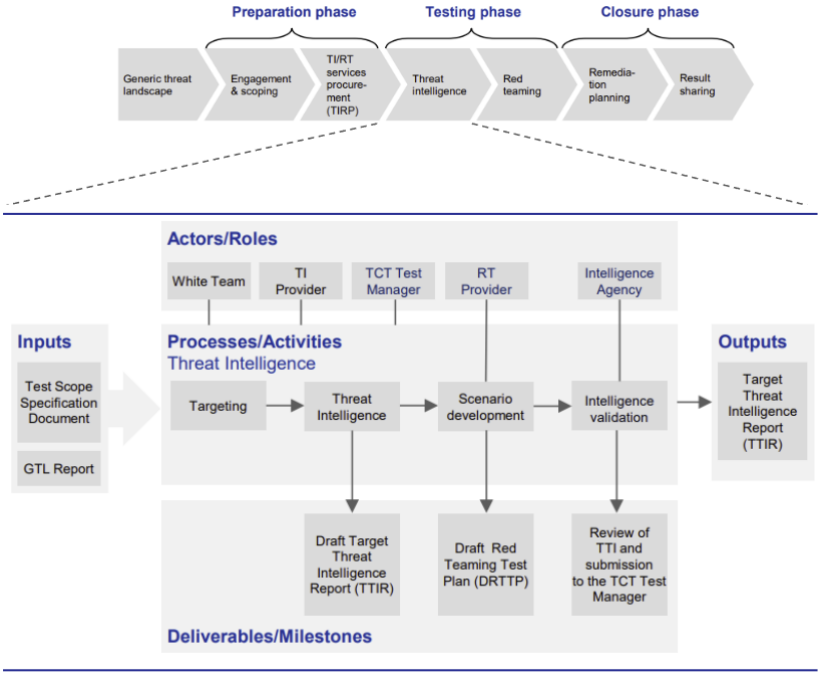

Figure 14. Overview of the TIBER-EU Threat Intelligence phase (European Central Bank, 2018)

Initial steps of the Threat Intelligence phase focus on having a Targeted Threat Intelligence Report (TTIR) in place. Targeted Threat Intelligence contains a set of attack scenarios that are the most relevant for the entity based on solid facts. Next, handover to the red teaming provider is done in the Scenario Development phase, in which the red teaming provider integrates the defined attack scenarios into the Red Teaming Test Plan (RTTP). These scenarios are at the core of the test execution, defining the actual test goals described from the adversary's perspective. (European Central Bank, 2018).

The fact that Scenario Development is done as part of the Testing Phase poses the challenge of *how a service provider is capable of planning, estimating, and proposing a meaningful scope with commercially sustainable terms while the details of the scope will be agreed considerably later in the process*? The research questions aim to study how the Preparation phase can be executed with information as close as possible to the final TTIR and RTTP.

3 Current State Analysis

This section presents the detailed execution of the current state analysis phase and the findings. For the findings, a hypothesis of a development initiative is formed to act as the initial ideation for the enhancements.

3.1 Overview of the current state analysis stage

The current state was analyzed through semi-structured interviews. The goal was to identify the current operating model in red teaming engagements, findings based on the TIBER engagements executed so far, and to define the strengths to build on and develop initiatives.

I formed the interview questions based on the literature review and a hypothesis of the criteria that impact a TIBER-EU engagement preparation and scope definition. For the high-level concept illustrated in Figure 2, my goal was to gather data to understand the existence of relevant assets and information to be re-used, the TIBER-EU experience and insights of the interviewees, and the key factors that impact red teaming and TIBER-EU engagements.

3.2 Data collection for the current state through interviews

For the interviews, I met professionals across all the areas of TIBER, including Threat Intelligence, Penetration Testing, OSINT, and business development, including sales. Due to the variety of backgrounds and extensive scope to be interviewed, I developed an initial list of interview questions that contained a set of fundamental questions and specific discussions for each interviewee's area of expertise. This structure of interview questions was achieved by categorizing them into base questions, TIBER-EU questions, specific questions for red teaming and threat intelligence depending on interviewee expertise, and finally, feedback for an initial framework structure (see Figure 15). The questions are listed in Appendix 1.

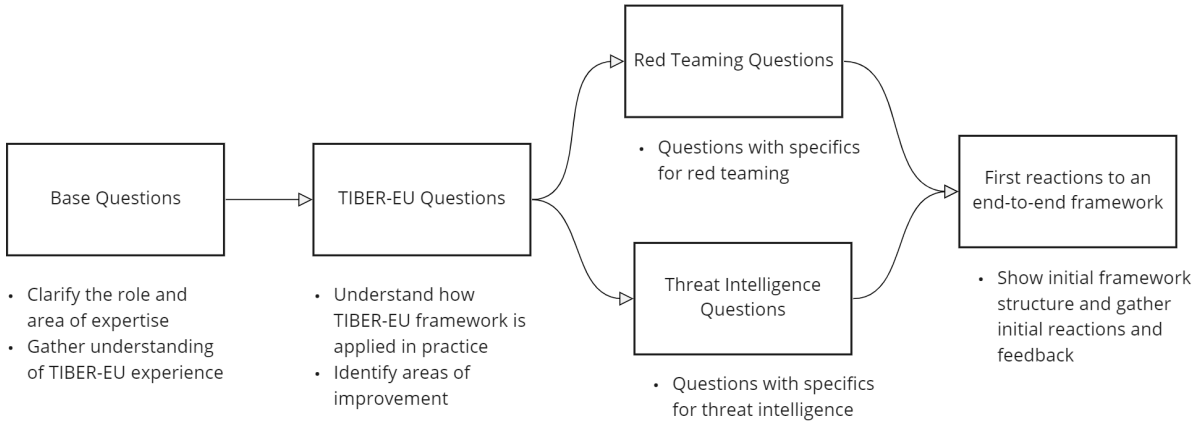

Figure 15. Interview question process

One-hour interviews were scheduled across several weeks to accommodate the times of the work schedules of each person. The anonymized interviewees are listed in Table 1.

Table 1. Interviewed persons and the schedule

#	Role / area of expertise	Key topic	Interview date
1	Cyber security consultant	OSINT	17.5.2022
2	Business unit lead	Sales and organizational efficiency	27.5.2022
3	Practice Lead, threat intelligence	Threat intelligence	17.6.2022
4	Senior security specialist	Penetration testing	17.6.2022
5	Security specialist, Red Team	TIBER, red teaming	21.6.2022
6	Product manager, threat intelligence	Threat intelligence	1.7.2022
7	Cyber security consultant	Penetration testing	1.7.2022
8	Principal security consultant	TIBER	5.7.2022
9	Senior security consultant	Penetration testing, tools and frameworks, MITRE ATT@CK	5.7.2022

I recorded the interviews and took hand-written notes to start forming the reoccurring findings across the interviews. These are described in detail and enriched with my analysis in the following sections.

3.3 Analysis of the data collected through interviews

After the interviews, I started to analyze the data. Dawson (2009) uses four categories for qualitative data analysis: *thematic* analysis, *comparative* analysis, *content* analysis, and *discourse* analysis. My chosen analysis method is a combination of thematic analysis and comparative analysis.

In thematic analysis, the analysis is done by themes derived from the data gathered from the interviews and the literature review. As this type of analysis is *inductive*, the themes are not enforced by me but rather surface from the data. (Dawson, 2009). As the data was gathered, the key findings were tested with other interviewees, and the interview outcomes were compared. This

comparative analysis was used to avoid an individual's point of view becoming a fact without testing it with others.

Altogether thematic analysis consists of six steps: familiarize yourself with the data, assign preliminary codes, search for patterns or themes, review themes, define and name themes, and produce the report (Mortensen, 2020). The themes and their implications are described in Table 2. Each of the themes is categorized as follows:

- **People and processes**: Findings related to people, their skills, way of working, and processes having a potential impact on the research questions.
- **Capabilities and tools**: Findings related to existing or potentially developed technical capabilities, tools, and frameworks having a potential impact on the research questions.
- **TIBER-EU**: Findings related to the TIBER-EU -framework and having a potential impact on the research questions.

Table 2. Thematic analysis themes

#	Category	Finding	Implications
1	People and processes	TIBER-EU engagements require even closer cooperation between the threat intelligence and the red team organizations	Instead of considering threat intelligence as a separate service for customers and general public, the way of working should bring the teams closer together.
2	People and processes	While threat intelligence and red teaming are require different skills and ambitions, in an optimal situation people in TIBER-EU engagements have understanding of both	In the TIBER-EU Procurement Guidelines the list of recognized certificates is geared towards penetration testing, having only few threat intelligence certificates. To accommodate this the more likely scenario is to expand threat intelligence people knowledge towards penetration testing.
3	People and processes	Typical nature of threat intelligence service is long lasting with periodic (e.g. quarterly) peaks in demand to generate the threat intelligence reporting. The processes and resourcing may need to consider project-based allocation of people in to TIBER-EU projects.	Define a standard team structures for TIBER-EU engagements and plan resourcing in such way that at least one TIBER-EU team can be re-allocated to a new project with short notice.
4	People and processes	Understanding financial industry's business and operating model is needed to plan and design relevant engagements as well as execute the red teaming phase in a meaningful way.	Request TCT to prepare a standard material shared with the engagement participants. Initiate development of internal documentation covering the industry specifics as well as different types of financial industry actors.
5	People and processes	TIBER-EU as a concept is relatively new and there is limited amount of experience in the industry for scoping, estimating, and executing TIBER-EU engagements	A framework for enhanced TIBER-EU engagement planning is to large extent for the purpose of definition of data that needs to be collected in the future engagements, to enable data-driven decision making in the future.
6	People and processes	The scope definition in TIBER-EU engagements is more formalized than in typical penetration tests. A penetration test scope defined as a flag, such as 'gain Active Directory domain administrator privileges', leaves more room for team members to execute the engagement based on their own methodology, while staying within the budget boundaries.	The framework to define the scope and scenarios must guide and support the team to greater extent than in many penetration test and red teaming engagements. This is likely to require a mindset change also from the team members.
7	People and processes	Often the customer is expected to be able to define a red teaming engagement scope. In complex engagements such as TIBER-EU their expertise does not necessarily be sufficient to define the scope in details.	As the customer expectations and TIBER-EU procurement guidelines require the TI and RT provider(s) must have a robust methodology in place. While the TIBER-EU customer may define part of the scope, the service provider must be able to guide the scope definition based on their expertise.
8	Capabilities and tools	Red teaming and penetration test execution expects and requires high level of professionalism and experience from the team members. There is potential to gain benefits in customer communication (including sales) by having a structured framework that gathers the best practices across the engagements.	To raise the bar across the organization, not to have dependencies on individual persons and their skills and preferences, and to enable more efficient onboarding of new team members the methodology throughout TIBER EU -engagements needs to be thoroughly documented.
9	Capabilities and tools	As TIBER-EU is relatively new concept, the current threat intelligence reporting and reporting process has not been designed TIBER-EU in mind, and there is improvement potential to make information exchange and reporting structure fit better for TIBER-EU engagaments	Threat intellgence reports and related tools need to be, considering the confidentiality of the information, accessible for wider audience in addition to the threat intelligence team.
10	Capabilities and tools	MITRE ATT&CK framework that is integral in TIBER-EU is also used in red teaming engagements. Details of its use are often depending on the team members.	For efficiency and consistency a standardized methodology to use MITRE ATT@CK framework as part of the TIBER-EU engagement needs to be in place.
11	TIBER-EU	TIBER-EU adaptations across the countries have differences. This includes the early phases of the engagement including scoping. Some countries have defined a specific number of attack scenarios to be included in the scope while there is no such definition in place. In addition the expected duration of TIBER-EU engagement phases vary across the countries.	The scenarios to be proposed for the customers need to have flexibility and variance in their complexity and granularity to accommodate different requirements and constraints.
12	TIBER-EU	The concepts in TIBER-EU are not inherently specific to financial industry.	The planning of tools and capabilities as well as organizational development can consider TIBER approach to be used across industries.
13	TIBER-EU	While TIBER-EU is more a guideline currently, and it is expected to be a mandatory concept in financial industry.	Volume of TIBER-EU engagement across Europe can be expected to grow.
14	TIBER-EU	The scope of TIBER-EU engagements is largely driven by the active APTs and their TTPs, and the geographical presence of the entity.	The planning and scope definition process begins with only few factors.
15	TIBER-EU	Factors that may impact and provide details to a TIBER-EU engagament scope such as details of technical landscape are not known during the early phases of the engagement planning.	The process of scope definition and related frameworks are and must support iterative way of working.

The themes will be used to define the initial guidance for the goals, dependencies, and constraints of the TIBER-EU standardized planning framework, further developed in the co-creation work-shops with the core expert team.

4 Ideas for the TIBER-EU preparation phase framework

The current state analysis revealed improvement potential in the TIBER-EU engagement prepara-tion phase, providing an encouraging answer to RQ 1*: it is possible to improve TIBER-EU engage-ment scoping and scope communication*. Furthermore, such a framework can also enhance effort estimations. Due to TIBER-EU being relatively new, leading to a lack of baseline data, the purpose of the framework in the short term is to initiate the collection of the relevant data.

To form the initial framework, I categorized the current state analysis themes into *requirements* listed in Table 3. These high-level requirements define the needs that the framework should be able to provide to Nixu, providing answers to the research questions RQ2 and RQ3.

Table 3. TIBER-EU standardized framework high-level requirements

#	Requirement
Req.1	The framework must contain the attack scenarios executed to the Entity
Req.2	The scenarios are defined by the Entity or Nixu threat intelligence
Req.3	The scenarios must be linked to the MITRE ATT@CK techniques
Req.4	The scenarios are high level descriptions of the attack. Scenario execution can be done by various techniques depending on the particular Entity.
Req.5	The framework must propose the most likely scenarios for an Entity depending on the characteristics of the Entity
Req.6	The scenarios that are relevant for an Entity are either defined by the Entity itself or derived from the threat actors and threat actor preferences
Req.7	Threat actors are either Groups in MITRE ATT@CK -framework or custom threat actors
Req.8	Threat actors are linked to an Entity by threat actor geographical activities (countries) and threat actor preferred Critical Functions. These must match to the Entity.
Req.9	The general structure of the framework can be optimally also used for any industry, not only for the TIBER-EU engagements
Req.10	The framework needs to be based on three types of data; input from threat intelligence organization, input from red teaming organization, and input from external sources such as MITRE ATT@CK

The requirements contain a set of objects and object relations. The framework's ultimate purpose is to connect an Entity object to a Scenario object for a given Engagement. This connection is established through several relations, for which the objects are:

- **Engagement**: An object to which the other objects are tied for the purpose of having an engagement-specific scope.
- **Entity**: The target financial institute(s) for which an engagement is scoped.
- **Entity Country**: The country or countries in which an entity has a presence and within the scope of the engagement.
- **Entity Critical Function**: Critical functions that an entity possesses and are in the scope of the engagement.

- **Threat Actor**: APT, other type of threat actor, or custom threat actor created for the scope of the engagement.
- **Threat Actor Country**: The countries in which the threat actor operates in for assessing if it overlaps the countries in which the Entity operates in, in the engagement scope.
- **Threat Actor Critical Function**: The critical functions the threat actor typically attacks to for assessing if it overlaps with the critical functions the Entity in the Engagement scope has.
- **Threat Actor Techniques**: the techniques as defined in MITRE ATT@CK that a threat actor uses in its attacks.
- **Scenario**: a textual description of an attack, including all its steps.
- **Scenario Techniques**: the techniques as defined in MITRE ATT@CK that can be used to execute the steps in a Scenario.
- **Scenario Estimate**: work estimate tied to the phases of a scenario, considering the scenario techniques, to define the needed team and capacity for the execution.

The objects and their relations are graphically represented using object modeling techniques.

4.1 Object Modeling

For modeling the objects and their relations, I use an entity relationship diagram (ERD). It serves my need to unambiguously define how the objects are related to each other and graphically represent the objects and relations. Initially, I created a logical data model containing key objects and relations but not including the final details of a physical data model, which could be directly translated to a database structure for implementation. (Biscobing, 2019).

Song et al. (1995) researched and identified a variety of ERD notations. Their conclusion is that differences in notations typically appear in how n-ary relationships of objects are allowed, how and where cardinalities and constraints are represented, and to what extent foreign keys are modeled. To avoid confusion, I use Crow's Foot Notation, invented by Gordon Everest, a modeling notation close to a physical data model. It also uses a verb as a relationship name, which improves the clarity of how objects are associated (Chawla, 2013).

The logical entity relationship diagram for the identified objects is illustrated in Figure 16.

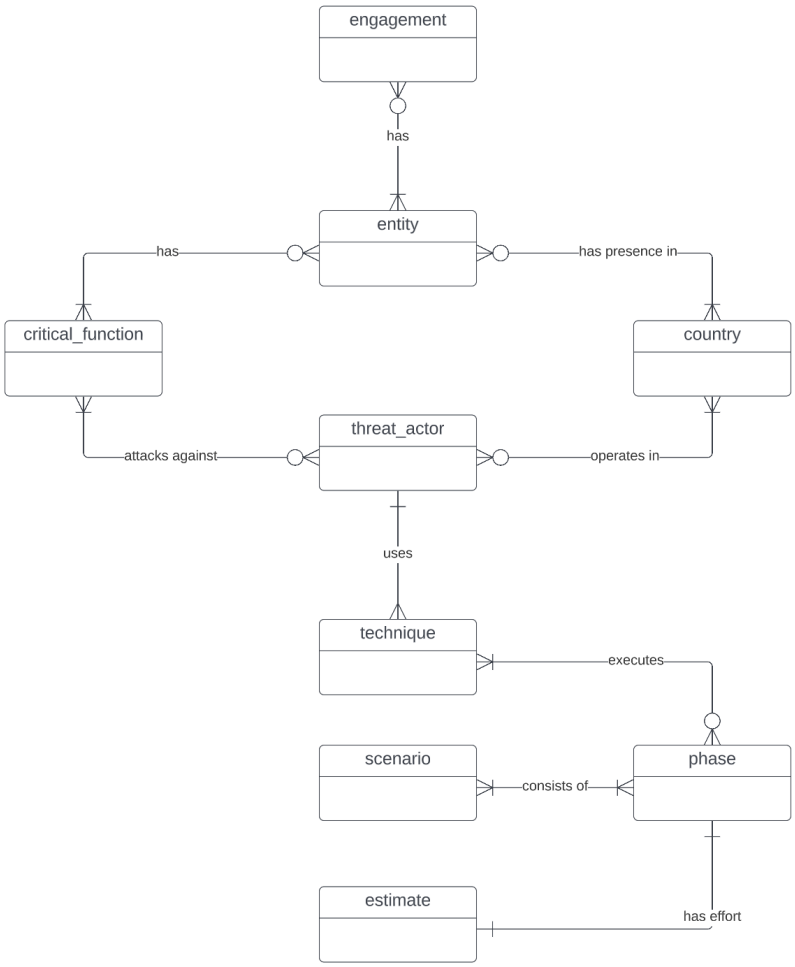

Figure 16. Framework logical Entity Relationship Diagram

4.2 Framework technical implementation

The current state analysis revealed that the framework would bring the organization's teams closer together and, with the new ways of working, facilitate more seamless information exchange. Third research question is about if it is possible to implement the framework in a tool, which would also provide elements of automation, data storage, and enforced rules on how the objects can be interacted with.

To define the initial application architecture fulfilling the requirements, I developed a hypothesis using a three-tier architecture. Dividing the application into three separate tiers is a commonly used approach (IBM Cloud Education, 2020):

- **Presentation tier**: The user interface for human users to interact with the application.
- **Application tier**: Uses and modifies data in the data tier. Processes the information received from the presentation tier and executes the business logic accordingly.
- **Data tier**: The back-end of the application for storing and managing the data needed for the application to function.

The requirements in Table 3 can be mapped to the tiers providing me with a logical architecture of the application, illustrated in Figure 17.

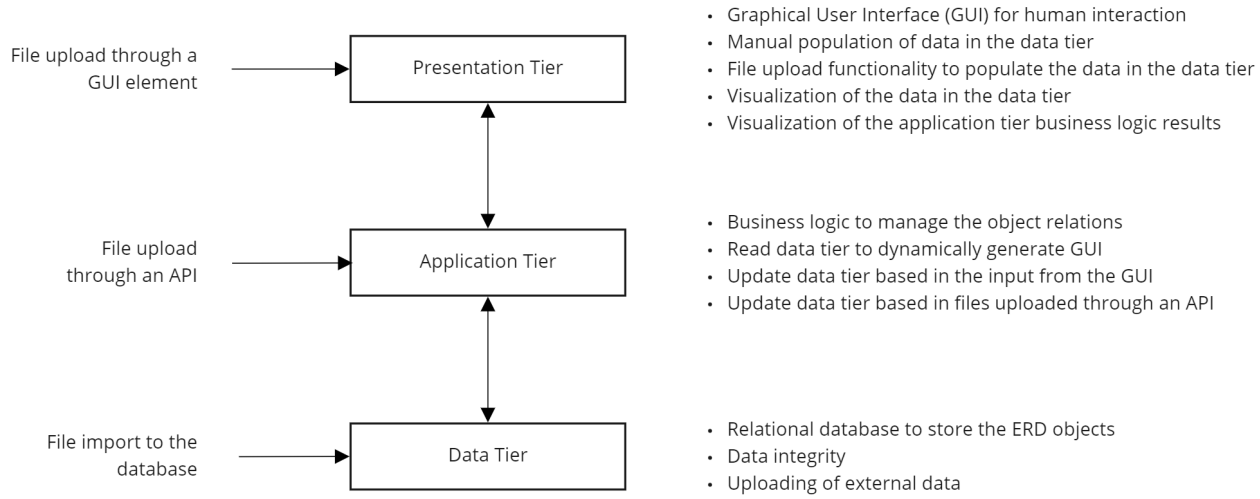

Figure 17. Three-tier-model mapped to high-level requirements

As the framework implementation is an iterative process and the needed functionalities are expected to change considerably during the process, flexibility is a high priority when choosing the technology for the implementation. I chose Retool web-based low-code platform for the presentation and application tiers. After exploring the use of Google BigQuery as the technology for the data tier, it was rejected due to its complexity for a relatively simple relational database. Instead, a cloud-hosted PostgreSQL database was selected for the data tier.

5 Implementation of the TIBER-EU preparation phase framework

5.1 Overview of the implementation

The initial ideas of the framework need to be transformed into the final version capable of answering the research questions. The chosen methodology is co-creation workshops.

Co-creation, as the definition implies, is about creating new together. Practical methods vary significantly, and De Koning et al. (2016) state that co-creation methods can be categorized based on the co-creation spectrum, types, and steps. I define the method used in my research using these categories to plan co-creation that meets the requirements of the research questions.

The spectrum of the co-creation varies from open innovation to participatory design method, with an additional dimension of how much collaboration the co-creators have. *Co-creation types* define in which parts of the process co-creation takes place and the scale of direct value created. Finally, the *co-creation steps,* by definition, are the steps executed in the co-creation process. (De Koning et al., 2016). Based on the categorization, I use the guiding principles in Table 4 for my co-creation workshops.

Table 4. Co-creation workshop guiding principles

	Guiding principle	Instead of
Spectrum of co-creation	Co-creation as a design method with high level of collaboration	Co-creation as an innovation approach with high level of collaboration, or low level of collaboration close to traditional business approach
Type of co-creation	Co-design with high level of collaboration	Personal offering with no collaboration or community design with open collaboration
Steps of co-creation	Define and Design phases of innovation approach	Early steps of Identification or Analysis, later phases of Realize or Evaluate.

Using the co-creation workshops for design rather than innovation implies that each workshop is expected to have a well-defined scope. Building on the TIBER-EU framework leaves very little room for open innovation, and my approach is, rather than starting from an empty canvas, to present a solution in each workshop for gathering design improvements. Regardless, as the workshop participants will be the core persons in using such a framework in the future, their design input is critical for achieving business benefits.

The implementation step of the research process is divided into three phases, as illustrated in Figure 18.

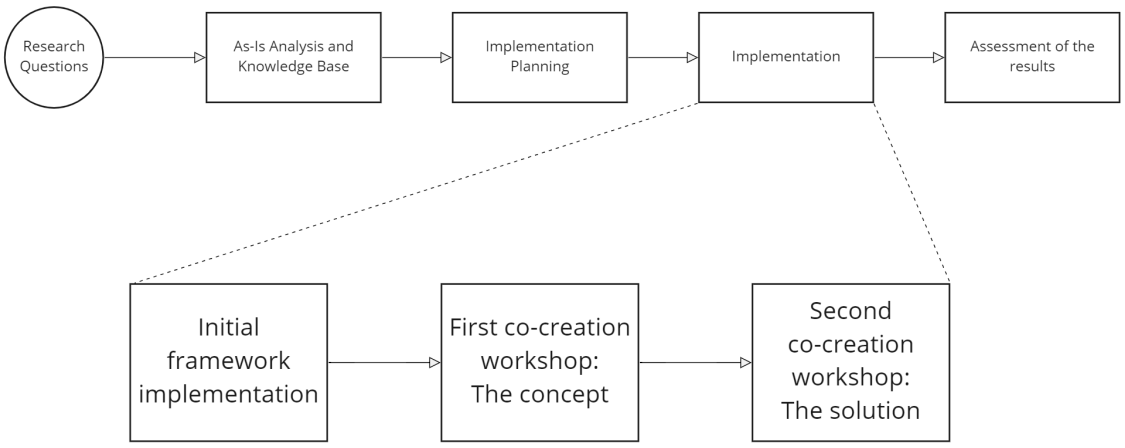

Figure 18. Implementation phase structure

The first co-creation workshop verifies and gathers feedback for the concept of the standardized framework. The focus is on the objects, how they relate to each other, including the ERD, and the information available to populate the model with data. The initial framework implementation user interface is demonstrated to the extent it supports understanding the concept.

The second co-creation workshop focuses on the implementation of the standardized framework and physical representation of the object and their relations in the three-tier architecture. The user experience is not a high priority, nevertheless the implementation needs to demonstrate the capabilities of the standardized framework to be evaluated against the research questions.

5.2 Initial framework implementation

Based on the literature research, current state analysis, and initial framework ideation, I implemented the first version of the standardized framework. The implementation consisted of the phases:

- **Design and implement the physical data model**: Transformation of the logical data model to the physical data model and implement it on the selected PostgreSQL database
- **Design of test data:** Set of representative data for each object that allows demonstrating and testing the implementation and not limiting the audience due to confidentiality requirements
- **Design and implement the business logic and user interface**: Transforming the functional requirements to business logic and implementation on the selected low-code platform.

The initial implementation is completed to the extent required to demonstrate the concept in the first co-creation workshop.

5.2.1 Physical data model

When I initiated the physical data model design, I aimed to use data as much as possible publicly available to populate the database tables. The tables and their source of data are:

- **tb_engagement**: engagements as populated by the user.
- **ecb_entity:** financial institutes as defined by European Central Bank.
- **tb_engagement_entity**: mapping table to define the entities in the scope of a particular engagement, as populated by the user.
- **Tb_critical_function:** critical functions as defined by various TIBER-EU countries or custom critical functions if added by the application user.
- **tb_engagement_entity_critical_function:** mapping table to define the critical functions of the entities in the scope of the engagement, as defined by the application user.
- **tb_country:** table with all the countries in the world and their standardized naming conventions.
- **tb_threat_actor:** mapping table for MITRE defined and custom threat actors.
- **mitre_group:** threat actors as defined in MITRE ATT@CK.
- **tb_custom_group:** custom threat actors as defined by the user.
- **mitre_group_techniques:** techniques threat actors used as defined in MITRE ATT@CK.
- **tb_scenario:** attack scenario as defined by the application user.
- **tb_scenario_step:** steps within an attack scenario as defined by the application user.
- **tb_estimate:** work effort estimate range for an attack scenario as defined by the application user.

The physical model with tables and attributes is depicted in Figure 19.

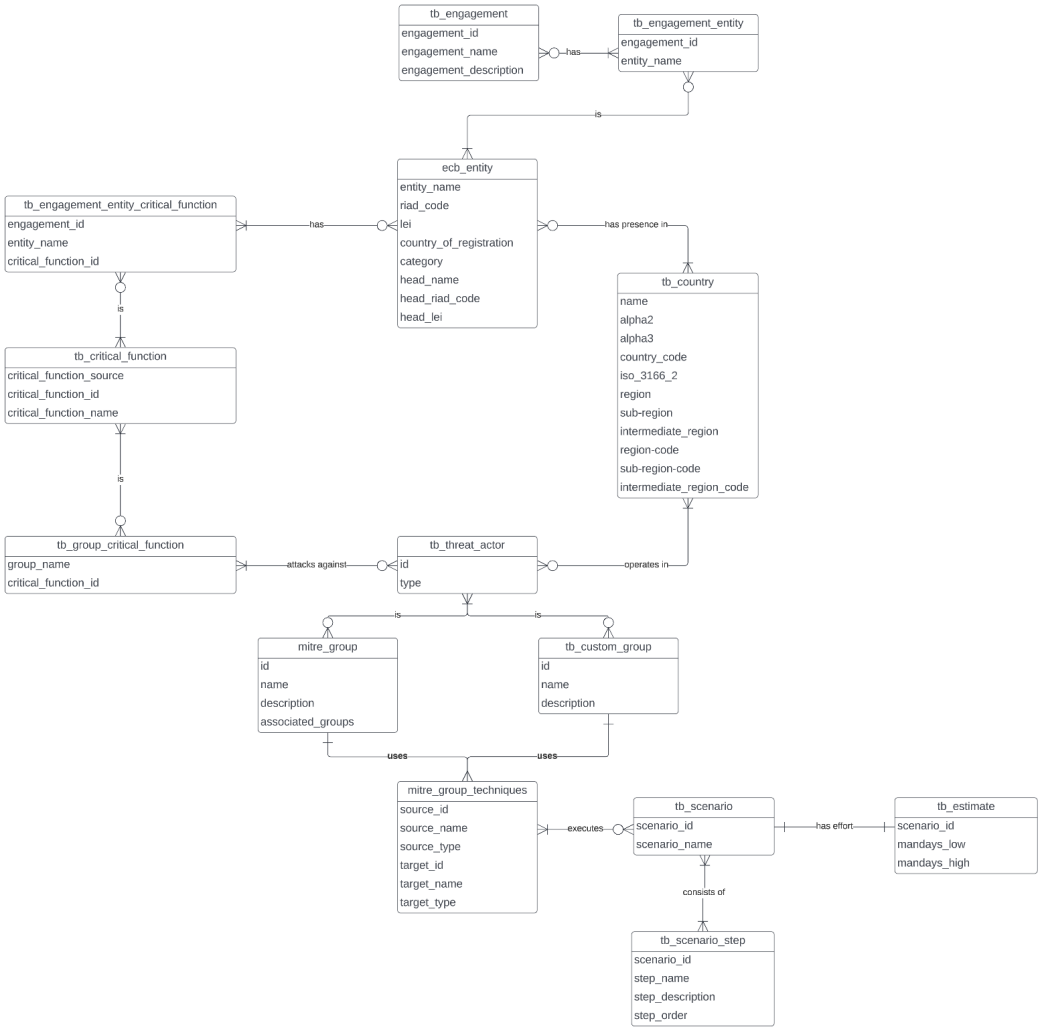

Figure 19. Initial physical data model

The following section illustrates the framework business logic and how the data model implements it.

5.2.2 Illustration of the entity relationship with test data

The functionality of the data model is demonstrated by populating it with imaginary data. Such data is planned to emphasize the relations of the objects to gather feedback if the design represents real-life scenarios.

The modeling begins with defining an engagement and an Entity for its target, a payment gateway provider located in Denmark, Germany, Netherlands, Norway, Sweden, and Finland, as illustrated

in Figure 20. A straightforward business model of this imaginary company states that it only uses one critical function.

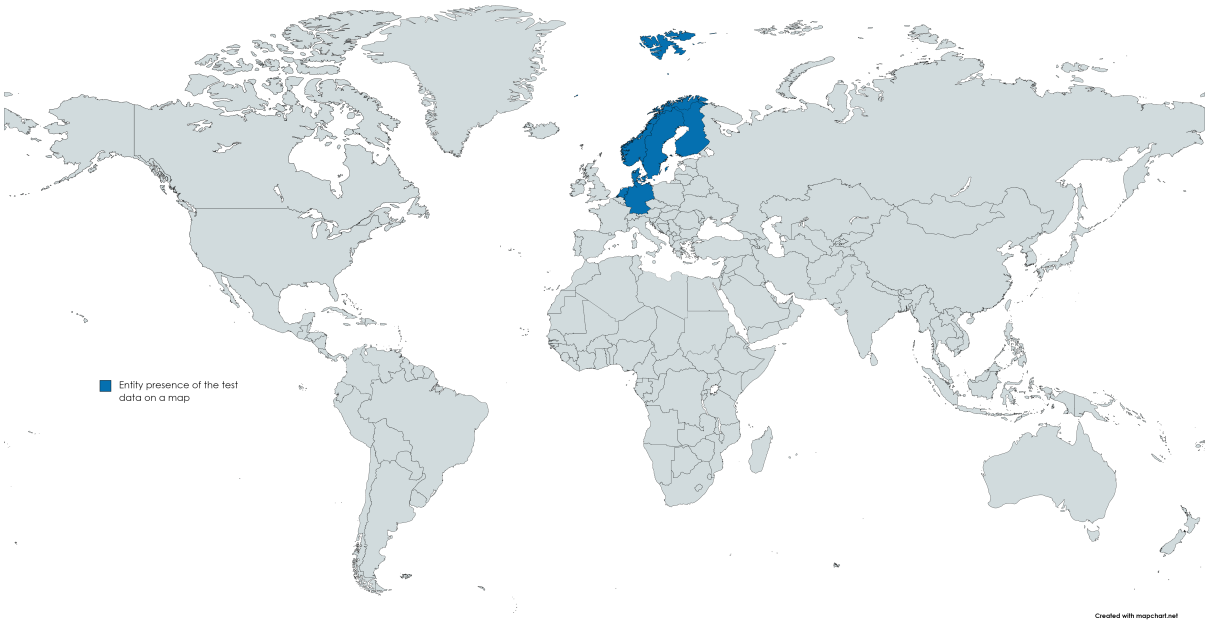

Figure 20. Entity presence of the test data on a map

Next, the data model is populated with three threat actors. As illustrated in Figure 21, an APT that operates solely in China, another in Central Europe, and a third one is active in Finland, Sweden, Norway, and Denmark. First two threat actors are specifically targeting payment gateway providers as well as cash supply systems, while Threat Actor three focuses on wholesale funding frauds.

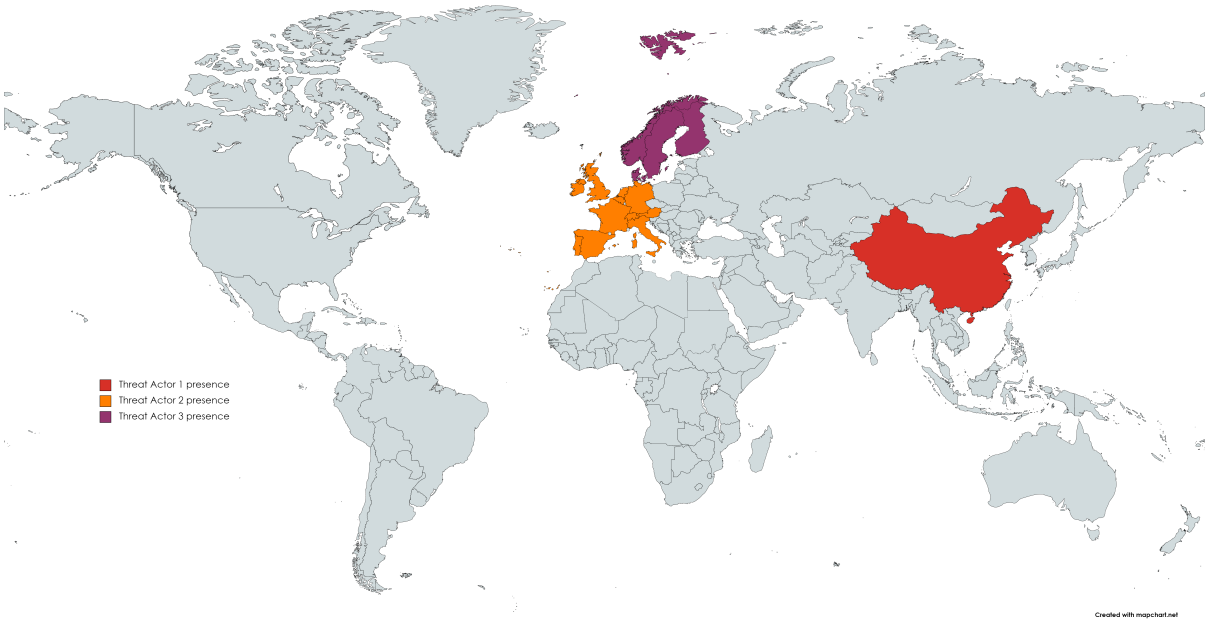

Figure 21. Threat actor presence of the test data on a map

The purpose of the model is first to filter threat actors that are active in the countries with Entity's presence. In the test data, both Threat Actor two and Threat Actor three have a presence overlapping with the Entity presence.

Next, relevant threat actors are filtered based on their target critical functions matching the Entity's critical functions (see Figure 22). Based on this filtering, Threat Actor three is not relevant for the Entity.

	Entity	Threat Actor 1	Threat Actor 2	Threat Actor 3
Deposits				
Wholesale Funding				X
Cash supply systems		X	X	
Payment gateway	X	X	X	

Figure 22. Test data threat actor filter based on critical functions

According to the filtering based on the geographical presence and critical functions, the scenario design is based on only the techniques of Threat Actor two.

5.2.3 Business logic and user interface

The presentation layer of the three-tier model provides the business logic execution capability. Primary use is to define the engagements and their scope, based on which the filtering of threat actors, their techniques, and subsequently, the relevant scenarios for the Entity are executed automatically. The secondary use is to insert and modify data to the physical data model. While to some extent the data is populated through APIs and data imports, custom data may also be generated through the presentation layer.

The logic of the graphical user interface is initially divided into four sections:

- **Projects**: Create, modify and view engagements and their scope
- **Critical Functions:** Create, modify and view critical functions that can be mapped to an Entity
- **Threat Actors**: View threat actors from MITRE ATT@CK, as well as their presence and target critical functions
- **Scenarios:** Create, modify and view scenarios to test Entities with

Each section is implemented as a dedicated graphical user interface and business logic.

Projects

The first step in managing the engagements is to create a project. In addition to the basic information of name and description, the scope is defined by selecting the Entities that are targets of the engagement. Each Entity must also have critical functions defined. The graphical user interface for these is depicted in Figure 23.

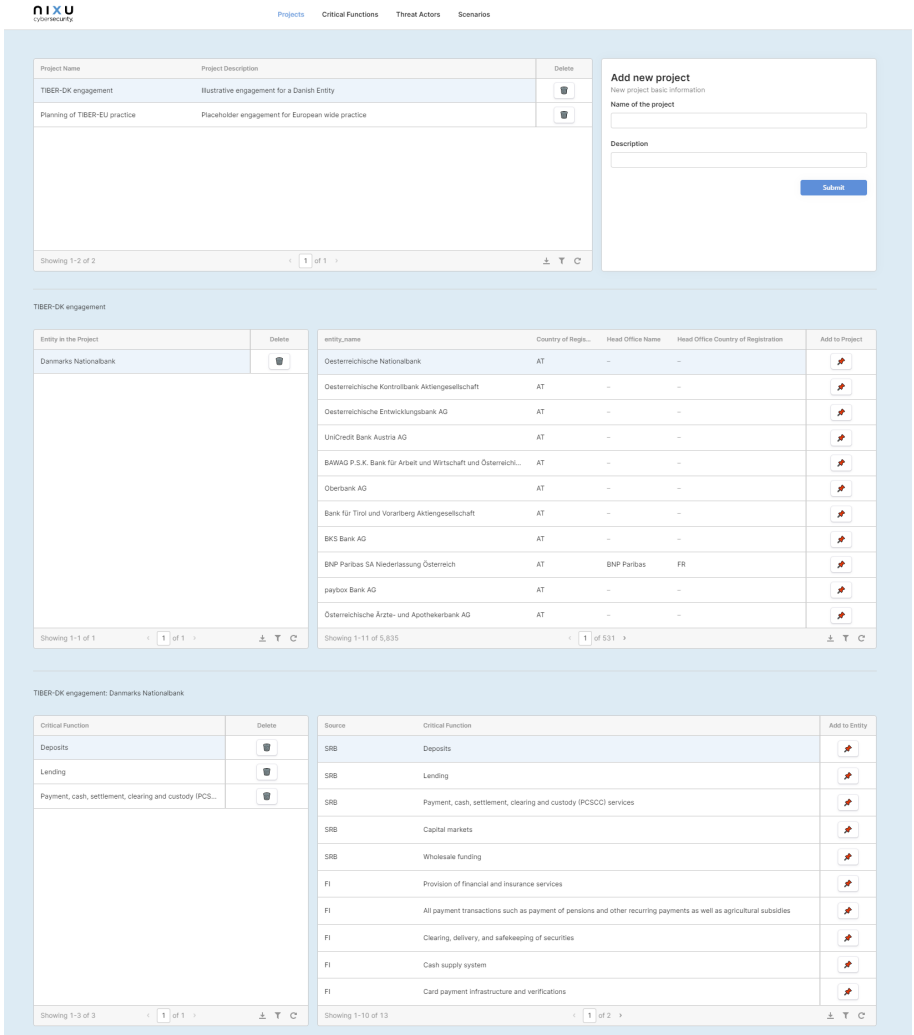

Figure 23. Presentation layer to manage engagements and their scope

After the scope is defined, the threat actors with matching geographical presence and focus on the Entity's critical functions are presented (see Figure 24).

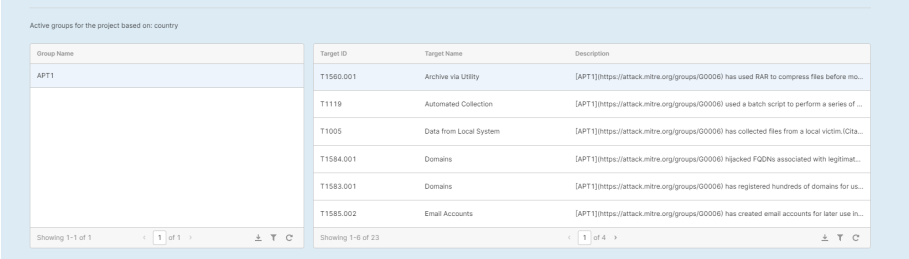

Figure 24. Most relevant threat actors and their techniques for the Engagement

The entities are imported to the database from the list of financial institutes publicly available from the European Central Bank. Critical Functions, on the other hand, need to have custom entries added. For this, a graphical user interface is provided.

Critical Functions

In European Union, the need to define critical functions of banks is based on situations where a bank may fail and is not able to go through normal insolvency proceedings. To manage these situations where financial stability must not be harmed, authorities have defined tools for resolution, which ensure the critical function continuity (European Commission, n.d.). The central authority for these resolutions is the Single Resolution Board (European Union, n.d.). Figure 25 depicts the critical functions defined by the Single Resolution Board (Single Resolution Board, 2017).

			Name entity 1	Name entity 2	Name entity 3	Name entity 4	Name entity 5
Deposits	F.1	Households	■	■			■
	F.2	Non-financial corporations - SMEs	■	■	■		
	F.3	Non-financial corporations - non-SMEs			■		
	F.4	General Governments					
Lending	F.11	Households - lending for house purchase		■			
	F.12	Households - other lending	■				
	F.13	Non-financial corporations - SMEs		■	■		
	F.14	Non-financial corporations - non-SMEs			■		
	F.15	General Governments					
Payment, Cash, Settlement, Clearing, Custody	F.21	Payment services to MFIs				■	
	F.22	Payment services to non-MFIs	■	■			■
	F.23	Cash services	■	■			
	F.24	Securities settlement services				■	
	F.25	CCP clearing services					
	F.26	Custody services				■	
Capital Markets	F.31	Derivatives held for trading - OTC					
	F.32	Derivatives held for trading - non-OTC					
	F.34	Secondary markets / trading (held-for-trading only)				■	
	F.35	Primary Markets / underwriting				■	
Wholesale Funding	F.41	Borrowing				■	
	F.42	Derivatives (assets)					
	F.43	Lending				■	
	F.44	Derivatives (liabilities)					

Figure 25. Mapping of critical functions to example entities (Single Resolution Board, 2017)

TIBER-EU uses critical functions to define the scope of an engagement. The list of the Single Resolution Board forms the basis of the critical functions, and the list is expanded by the country-specific TIBER implementations. For this reason, the list is not static, and functionality to easily view, create, and modify critical functions is implemented (see Figure 26).

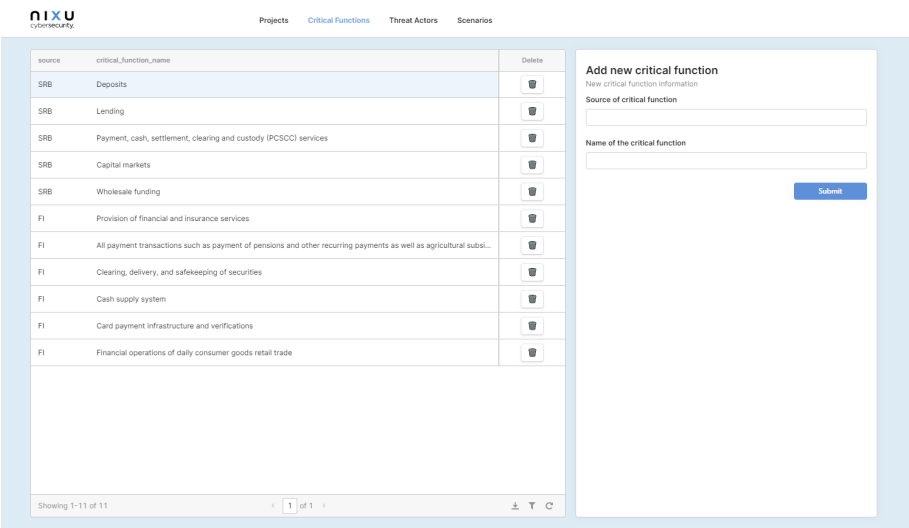

Figure 26. Presentation layer to manage critical functions

Threat Actors

Information on threat actors is relatively complex and not easily configurable through a graphical user interface. Consequently, as depicted in Figure 27, the information is only viewable.

The physical data model is designed to be compatible with the MITRE ATT@CK framework extracts of threat actors, and all the inserts and updates of data are done via database imports.

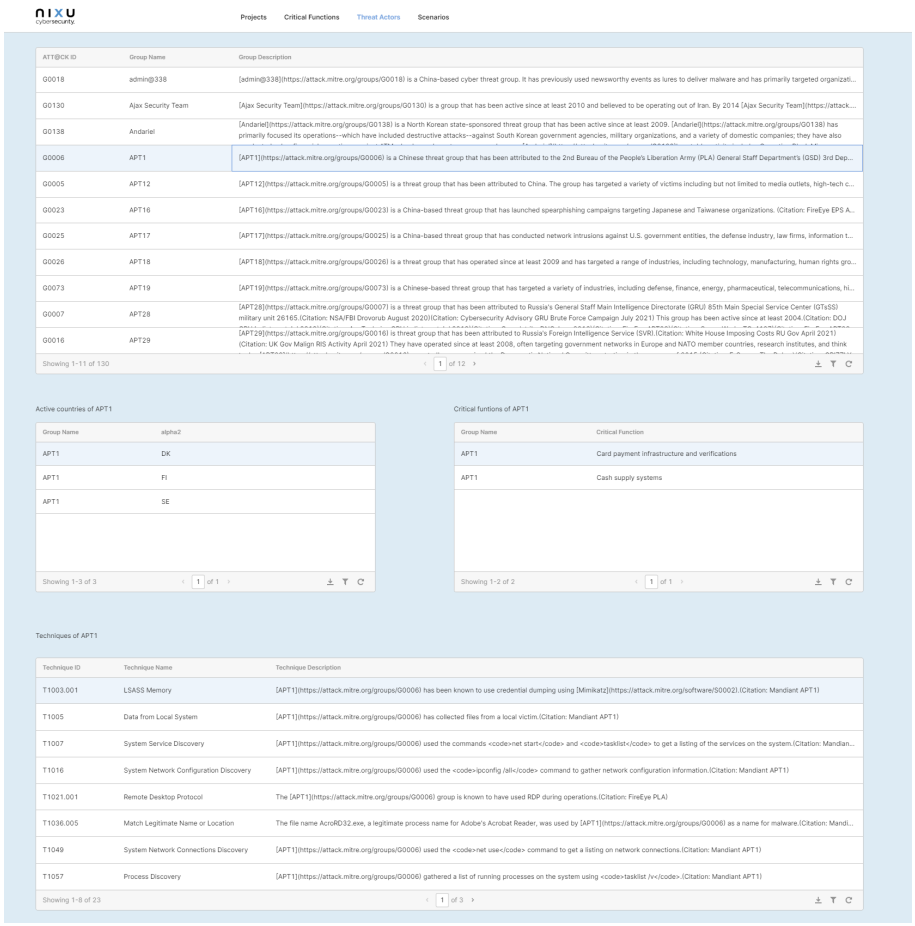

Figure 27. Presentation layer to see threat actors

Each threat actor has a set of techniques mapped to it. The scenarios relevant to an Entity are designed to match those techniques.

Scenarios

The final executable scenarios are defined through the graphical user interface (Figure 28). Each scenario has a name and high-level description and consists of steps. The step definitions are free text.

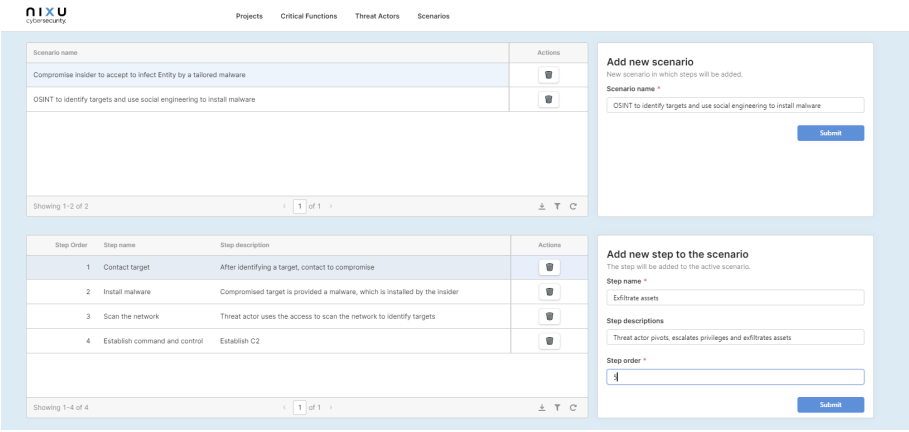

Figure 28. Presentation layer to manage scenarios

I have recognized scenario modeling as one of the critical enhancement needs in the later phases. The first co-creation workshop focuses on gathering feedback for the model, after which the scenario design can be finalized.

5.3 The first co-creation workshop

In the first co-creation workshop, I wanted to present and validate the initial framework design. The combination of the literature study and interviews established a good understanding of the desired framework. However, I expected to receive further improvement ideas from the workshop participants as I was able to present a concrete and detailed design and business logic.

To ensure tight collaboration, the number of participants was kept to a minimum. On the other hand, having both red teaming and threat intelligence present in the workshop was a high priority. The selected participant profiles are presented in Table 5.

Table 5. The first co-creation workshop participants

#	Role / area of expertise	Key contributation area
1	Practice Lead, threat intelligence	Threat intelligence
2	Security specialist, Red Team	TIBER, red teaming
3	Product manager, threat intelligence	Threat intelligence
4	Principal security consultant	TIBER

I divided the workshop into three parts:

- **Initial view of the presentation layer implementation logic**: Brief presentation of the framework's business logic and user interface. The purpose was to help workshop participants to understand the end goal of the entity relationship diagram.
- **Logical entity relationship diagram and data model co-creating**: Explanation of the logical layer of the design for a higher abstraction level first and improve it together with the workshop participants.
- **Physical entity relationship diagram and data model co-creating:** After the logical layer was clarified, the details of the physical level design were explained and improved together with the workshop participants.

An active discussion was facilitated throughout the workshop to encourage participants to share all their ideas. Furthermore, the workshop material was shared well in advance. This pre-read time allowed the participants to prepare questions and improvements ideas in advance.

In general, the framework was considered logical and relevant for the purpose it is developed for. The workshop deemed the optimal use for the framework is in the early stages of the TIBER preparation process. This is because the less information about the Entity Nixu has, the more relevant the framework is. In the later stages of TIBER-EU preparation and during the execution phase, more detailed information is gathered through OSINT or shared by the Entity. With this information, the scenarios may change or become very detailed compared to what the framework provides in its current state. These findings are input for future research areas and will be discussed more in section 7.3.

The outcomes of the co-creation workshop are gathered in Table 6. There are two categories of items in the table. Some items can be directly implemented into the framework; on the other hand, some items are informative and used when considering framework design decisions.

Table 6. First co-creation workshop feedback items

#	Feedback Item
F.1	Engagement definition should have an attribute defining to which TIBER country it is for, for example TIBER-FI.
F.2	Engagements should have also engagement level flags. A flag could be *stay undetected* which is applicable across the scenarios.
F.3	Engagement level flags impact the effort estimates.
F.4	Often a threat actor presence cannot be defined on a country level. An option to define regions such as *Europe* should be added. Also some threat actors act globally.
F.5	Scenarios may contain other activities in addition to red teaming, for example joint purple teaming excercise executed after red teaming.
F.6	There are also catch all scenarios, for example achieving domain administrator privileges may be relevant to Entities regardless of other factors.
F.7	A catch all scenario may be also a scenario the Entity provides themselves, and is to be executed regardless of other factors.
F.8	Threat actors defined by MITRE ATT@CK are not always up-to-date. There are threat actors that MITRE ATT@CK does not contain.
F.9	There is a need to create custom threat actors, as well as general threats that can be a combination of multiple threat actors.

An updated framework with the co-creation feedback items implemented is presented in the second co-creation workshop.

5.4 Improved framework implementation

All the improvements to the framework are based on the co-creation feedback items in Table 6. Analyzing the items, they can be grouped based on the functionality they impact. For each grouping, a change is implemented in the logical and physical entity diagram models and in the presentation layer.

5.4.1 Improved Engagement object and presentation layer

The co-creation workshop items F.1 and F.2 are directly linked to the Engagement definition, adding new attributes to the data model and respective user interface items. As estimation data is not

available for the scenarios, requirement F.3 will impact the process of using the tool rather than having a technical implementation in place.

The physical data model requires the following updates:

- **tb_tiber_country: A** new table including the set of TIBER countries, for example, TIBER-FI.
- **tb_flag:** A new table including the set of flags that can be linked to an engagement Entity level.
- **tb_engagement**: A reference to tb_tiber_country added to represent which country's TIBER framework is used.

A flag as a TIBER-EU engagement goal is also included in the TIBER-EU project scoping guide (European Central Bank, 2020b), see Figure 29. The implementation is designed to be compatible with the TIBER-EU framework for easy adoption of such flags in actual engagements.

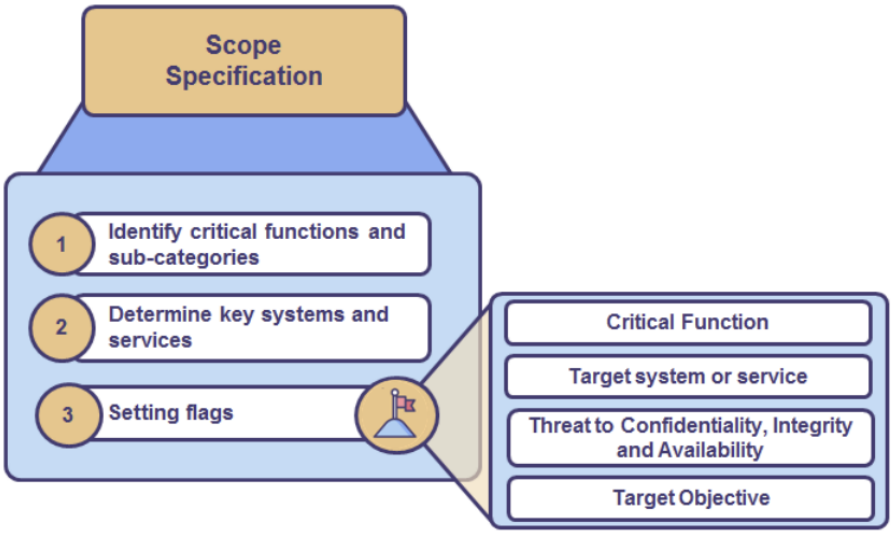

Figure 29. TIBER-EU scope specification high-level structure (European Central Bank, 2020b)

The physical model including these improvements is depicted in Figure 30.

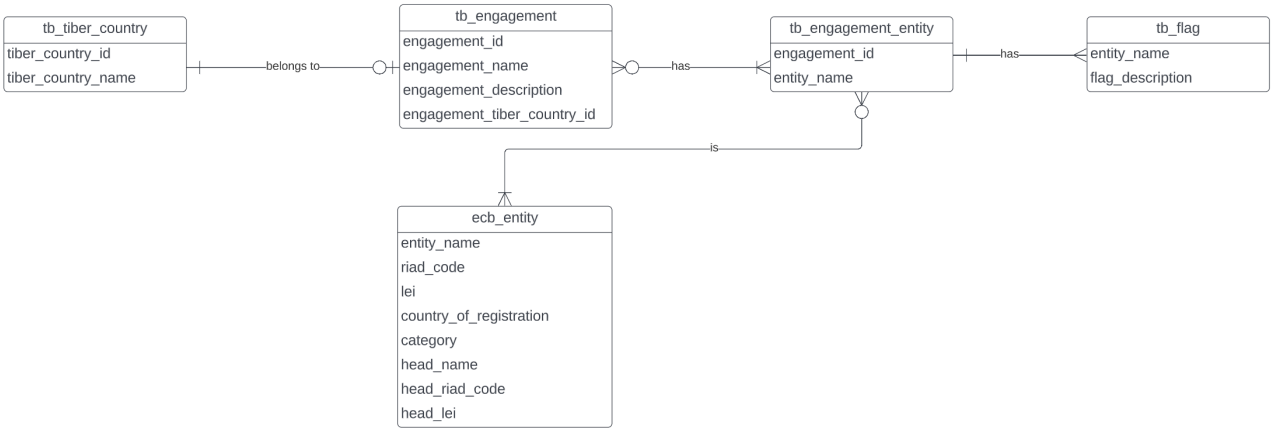

Figure 30. The improved physical data model of Engagement

The improved functionality on the presentation layer requires updates on the existing Engagement user interface and new user interface to manage engagement level flags.

The administration user interface for the engagement level flags is depicted in Figure 31. Creating, modifying, and deleting flags is done utilizing a similar look and feel as other entities in the framework.

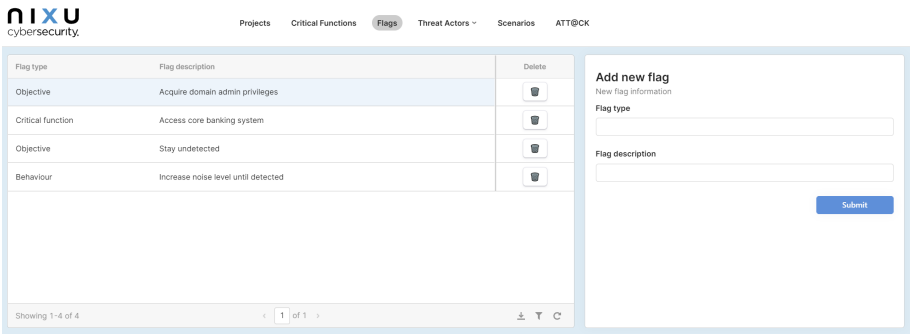

Figure 31. Presentation layer to manage engagement level flags

The TIBER-EU countries, while evolving, are relatively stable. For this reason, no administrative user interface was developed to administrate them. Instead, direct database updates are used.

Once both objects, flags, and TIBER-EU countries are implemented, the final stage is to improve the Engagement user interface to use them. An extract of the improved presentation layer to manage Engagements is depicted in Figure 32.

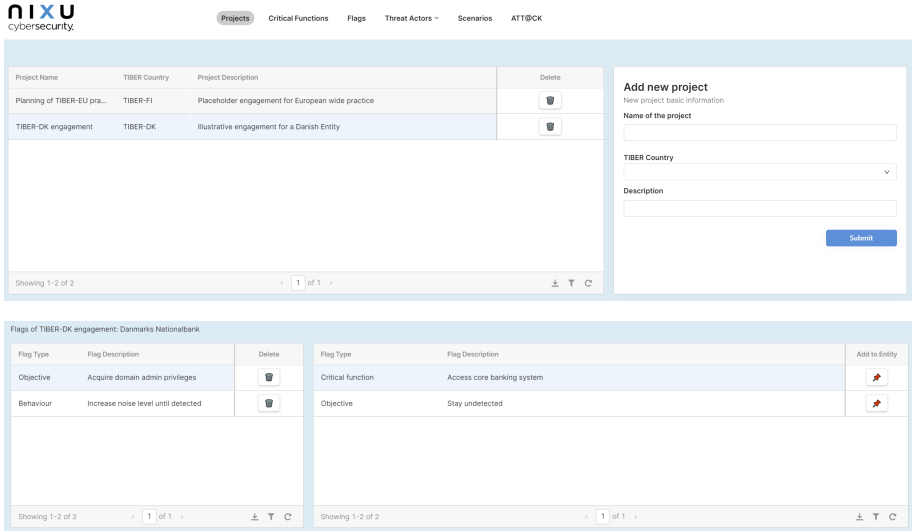

Figure 32. Improved presentation layer to manage engagement and scope.

5.4.2 Improved Threat actor object and presentation layer

The initial implementation of threat actors relied extensively on existing data of MITRE ATT@CK -framework. However, the initial set of requirements already brought up the need for custom threat actors, and in the co-creation session, more detailed requirements were gathered.

Requirements F.8 and F.9 are related to the fact that there is a need in practice to create custom threat actors. Either this is due to ATT@CK not including a known threat actor, or project needs can only be fulfilled by modeling a custom threat actor.

In addition, as requirement F.4 states, it is often impossible to define threat actor presence on a country level. A geographical presence in all of Europe or globally needs to be used in those cases.

As the physical data model supports these requirements, the improved functionalities are implemented on the presentation layer. Managing the threat actors is enhanced by two key capabilities, the first being creating and managing custom threat actors, as illustrated in Figure 33. Each threat actor is defined with a country-specific and regional presence.

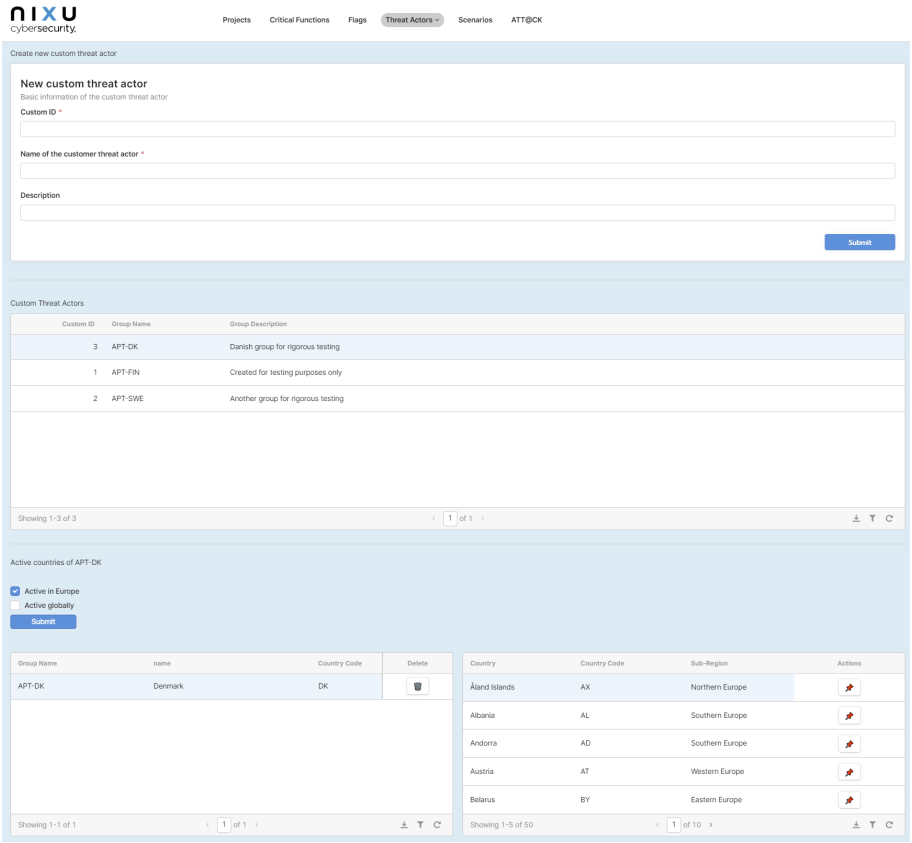

Figure 33. Presentation layer to create and define presence for custom threat actors

The modeling of techniques used by a custom threat actor is done using MITRE ATT@CK Navigator, a tool provided by the ATT@CK framework for annotating and exploring ATT@CK matrices (see Figure 34).

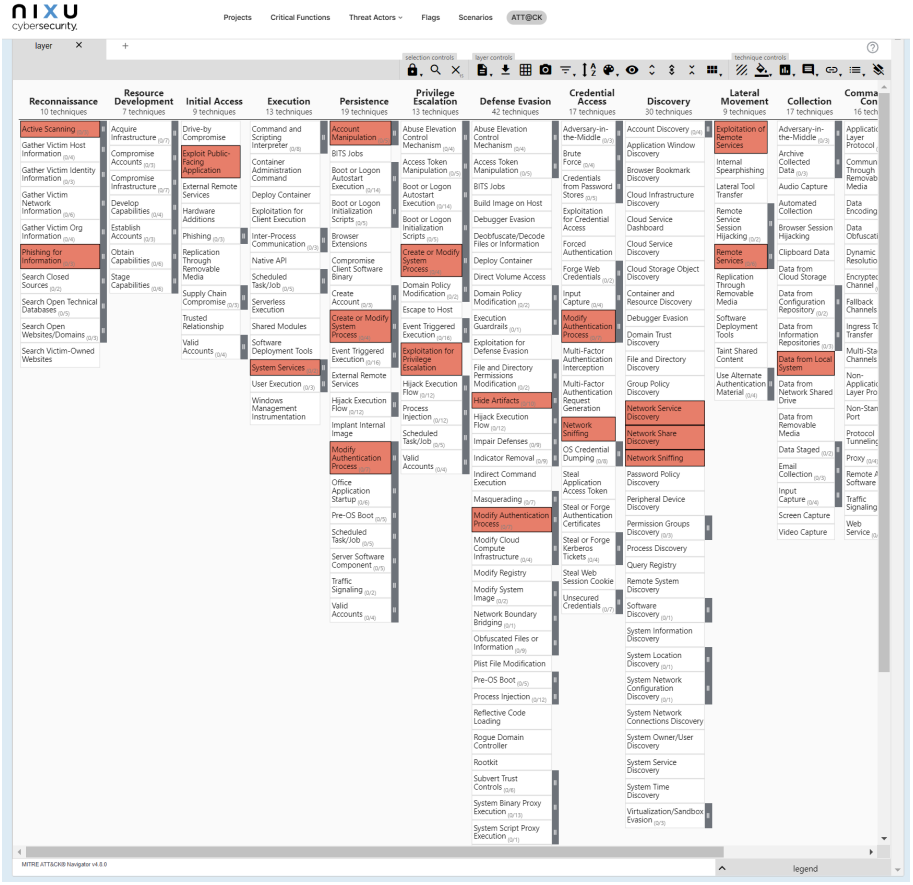

Figure 34. Presentation layer to define custom threat actor techniques

In the Navigator tool the selected techniques represent the behavior of a threat actor and can be attached to a created custom threat actor.

5.4.3 Improved Scenarios object and presentation layer

Scenario capabilities in the initial implementation were limited on purpose. One key outcome of the co-creation workshop was to confirm the end-to-end logic of the framework, after which more substantial effort is worth being used for the scenario modeling.

Requirements F.5, F.6, and F.7 highlight the need for flexibility in scenario modeling. The presentation layer must not set too strict boundaries. The concept of each scenario consisting of steps that can be defined independently supports this approach, illustrated in Figure 35.

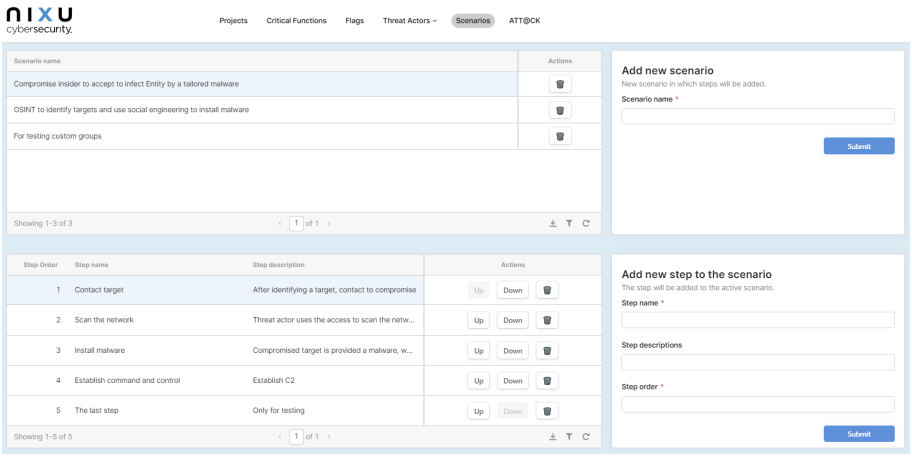

Figure 35. Improved presentation layer to manage scenarios and steps

The functionality is also enhanced by linking the step description to the ATT@CK techniques needed to execute the step (Figure 36).

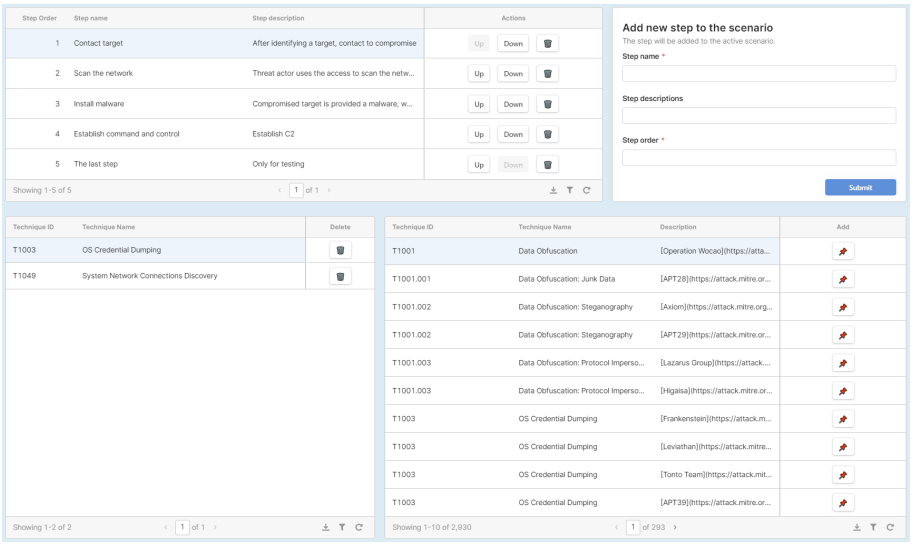

Figure 36. Presentation layer for defining techniques used for a step

Mapping techniques to scenarios is essential to complete the model. The scenarios relevant for an Entity are identified based on matching threat actor's and scenario's techniques.

5.5 The second co-creation workshop

As defined in the implementation plan steps (see Figure 18), in the second co-creation workshop I presented the overall solution in the form of implemented end-to-end framework. To achieve this, I have improved the framework based on the feedback from the first co-creation workshop and expanded the capabilities to answer the research questions.

To validate the improved implementation and build on the jointly gathered understanding of the research questions and the framework implementation to address them, it is essential to continue with the same group of workshop participants.

The research is concluded after the second co-creation workshop with the assessments of the results. This step is executed as a survey, as illustrated in the data collection plan (Figure 4). I leveraged the co-creation workshop to introduce the questionnaire used to provide input for the assessment of the results.

Based on these goals for the workshop, I defined the structure to present the solution, gather co-creation feedback, and introduce the survey for the framework results:

- **Presentation layer implementation:** Presentation of the business logic and the user interface with a set of test data. Test data is designed to illustrate key data dependencies as defined in the entity relationship diagrams. Business logic demonstrates how the framework is used by the solution end user.
- **Entity relation diagram and data sources:** Explanation of the logical and physical data models with a focus on iterative improvements.
- **Introduction to the questionnaire:** Explanation of the purpose of the questionnaire and instructions of the survey tool.

Even though the workshop structure is built on the solution presentation, the participants are requested to share their feedback for further improvements. As with the first co-creation workshop, the pre-read material is shared in advance, allowing the participants to prepare their comments.

I expect most feedback items to be logical or functional improvements or topics for future research. However, the workshop being the final one for the research, my goal is also to understand if the comments directly impact the research questions. To validate this, for each feedback item, the following question will be asked:

- Is the feedback to improve the framework logic, capabilities, or functionality, or will you consider it as a blocker for the framework being applicable for its purpose?

Categorizing the comments during the workshop provides me immediate feedback if the core stakeholders have identified any significant obstacles to the framework. This information will be gathered in the framework results survey. However, understanding critical items during the workshop gives us time to co-create a possible solution. Furthermore, considering the scope and plan of the research, I am not implementing the improvement ideas into the framework. Follow-ups

may be considered only for the blockers to ensure the framework has been given sufficient attention to answer the research questions.

The co-creation feedback items are presented in Table 7. They were categorized as improvement ideas, future research ideas, or blockers for the framework's applicability.

Table 7. Second co-creation workshop feedback items

#	Feedback Item	Type
F.10	Increase the automation of data imports to minimize manual effort	Improvement idea
F.11	Analysis if custom TTPs are needed, in addition to the ones MITRE ATT@CK provides. Related functionality implementation.	Improvement idea
F.12	Secure hosting considerations, also to have good compliancy and related documentation for customers	Improvement idea
F.13	Functionality to export the created scenarios could provide additional value in using them in customer communication	Improvement idea

A significant outcome of the categorization is that no blockers are identified. While the research question finalization can be completed after the survey results have been analyzed, the results are encouraging.

6 Research Results

6.1 Co-creation Workshop Results

To answer the research questions, I started by understanding the business challenge and establishing an entity relationship diagram to prove that the required relationships can be modeled. Having a positive answer to the first research question, if a framework to improve TIBER-EU engagements can be achieved, I could continue to the following research questions.

The entity relationship diagram provided grounds for the answers to research question two. Being able to be more concrete in defining what kind of framework would improve TIBER-EU engagements, I chose to implement the logical models into a tool. The first co-creation workshop was used to present and co-create the implementation to a desired direction, providing the answers to research question two, in the form of requirements and definitions for an end-to-end threat intelligence-based framework.

To answer research question three, if the framework can be implemented into a tool, I continued to enhance the capabilities of the initial implementation. The main goal of the co-creation workshop two was to present a complete end-to-end implementation of the tool and to find any show-stoppers that would prove the tool unusable. As the feedback was very positive and there were no findings rejecting the tool, the third research question was answered positively.

6.2 Survey Results

In addition to the co-creation workshops and their feedback, I used a triangulation method to add a level of control and test the consistency of findings. Surveys are a *methodological triangulation*, as they add more techniques to gather data. Furthermore, a survey can validate results and enrich and provide more insights. (Triangulation, n.d.). In my research, I wanted to ensure all the co-creation workshop participants had sufficient time and place to voice their input and feedback. Sometimes working in a group suppresses some opinions, or the participants may be shy to provide negative feedback to the researcher. There was no particular reason to believe this we the case. However, I sent out an anonymous survey to collect more data to verify the research question answers. The survey goal was also to provide insights for Nixu on how they could benefit from the tool and considerations for deploying it into use.

Chauncey (2013) advises keeping the survey concise, as respondents have more time for each item, although very short questionnaires may not be deemed credible. Following this guidance, the survey consisted of nine questions with multiple-choice answers. Standard Likert scales were used to avoid inconsistency. When Likert was not applicable, the response categories were designed to be exhaustive. (Chauncey, 2013). The respondents were given the option to provide additional free text comments to ensure all insights were included.

As the number of respondents was limited to the relatively small audience participating in the co-creation workshops, the answers are not statistically significant. Instead, the results are analyzed if any of the survey answers contradict the positive responses for all research questions.

The first question confirms that the participants see value in a structured framework (Figure 37).

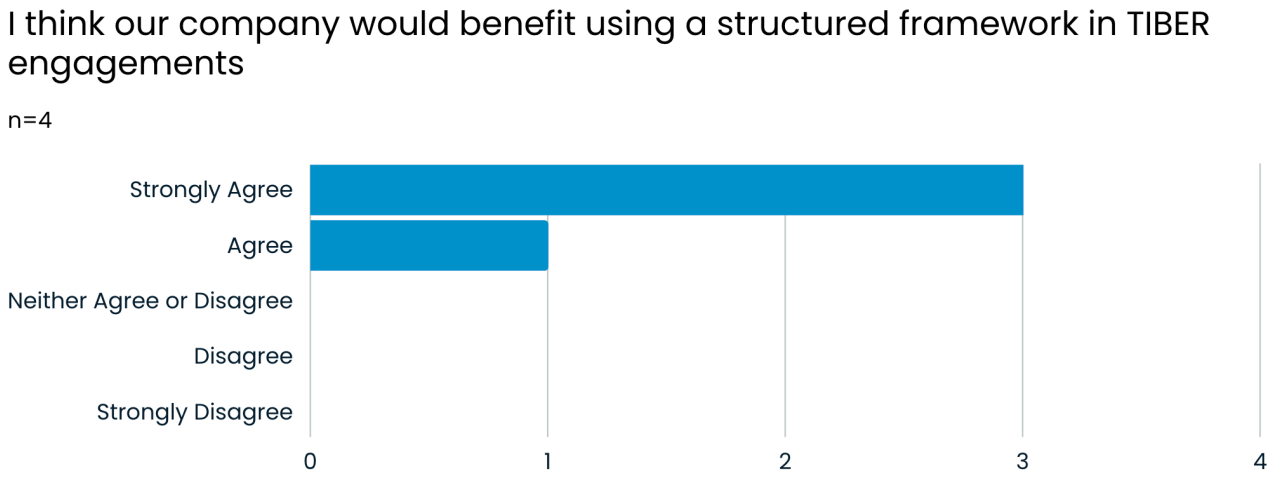

Figure 37. Question 1: I think our company would benefit using a structured framework in TIBER engagements

The respondents believe it is possible to design a framework applicable to real-life engagements (Figure 38). Agreeing answers to this question support a positive response to research question one.

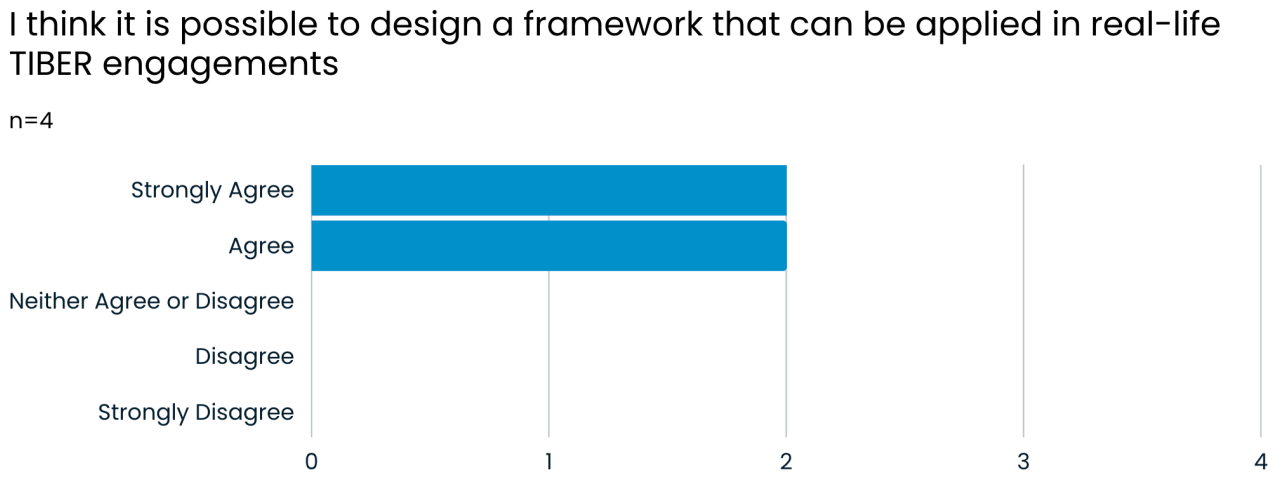

Figure 38. Question 2: I think it is possible to design a framework that can be applied in real-life TIBER engagements

The third question is for insight into how much the participants have benefited from being part of the research projects (Figure 39).

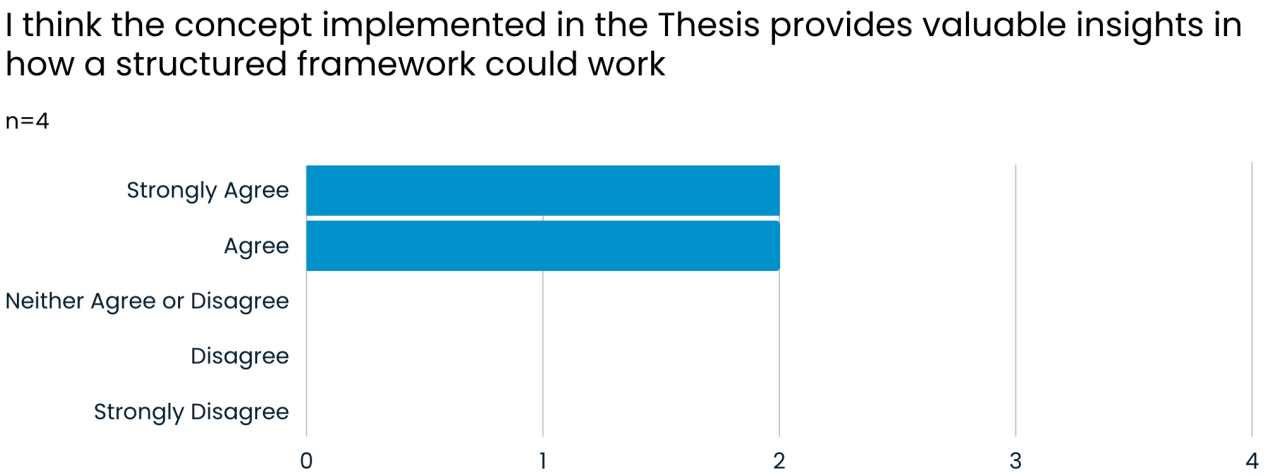

Figure 39. Question 3: I think the concept implemented in the Thesis provides valuable insights in how a structured framework could work

Asking respondents' opinions of the tool selection and implementation demonstrates agreement with its applicability (Figure 40). The research project goal was not to implement a production-ready tool, but if responses were disagreeing, that would indicate negative answers to research questions two and three.

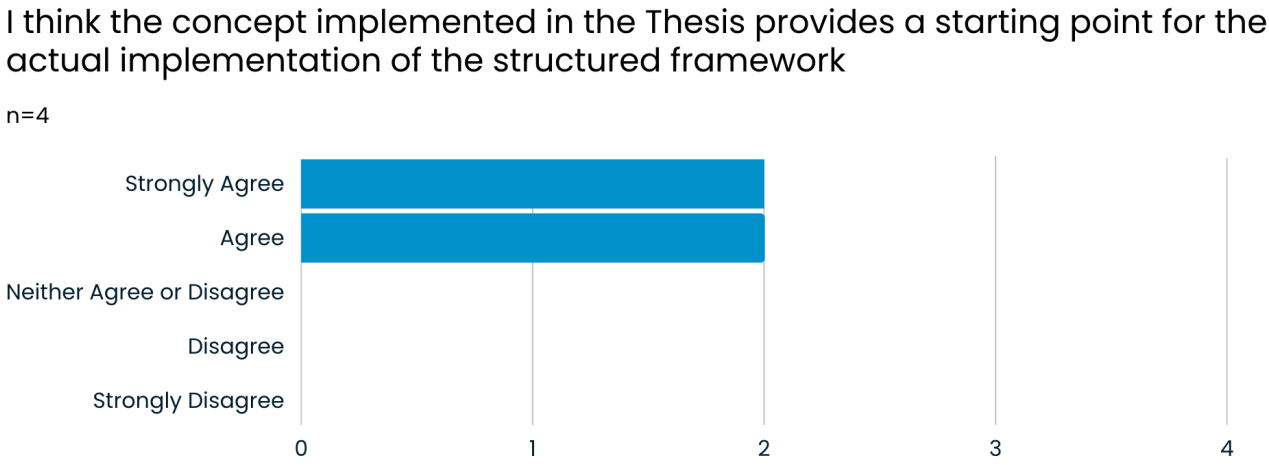

Figure 40. Question 4: I think the concept implemented in the Thesis provides a starting point for the actual implementation of the structured framework

For added insight, the respondents were asked if they see it feasible to expand the framework to industries other than the financial sector. This answer does not impact the research questions but indicates future research possibilities due to varying answers, as depicted in Figure 41.

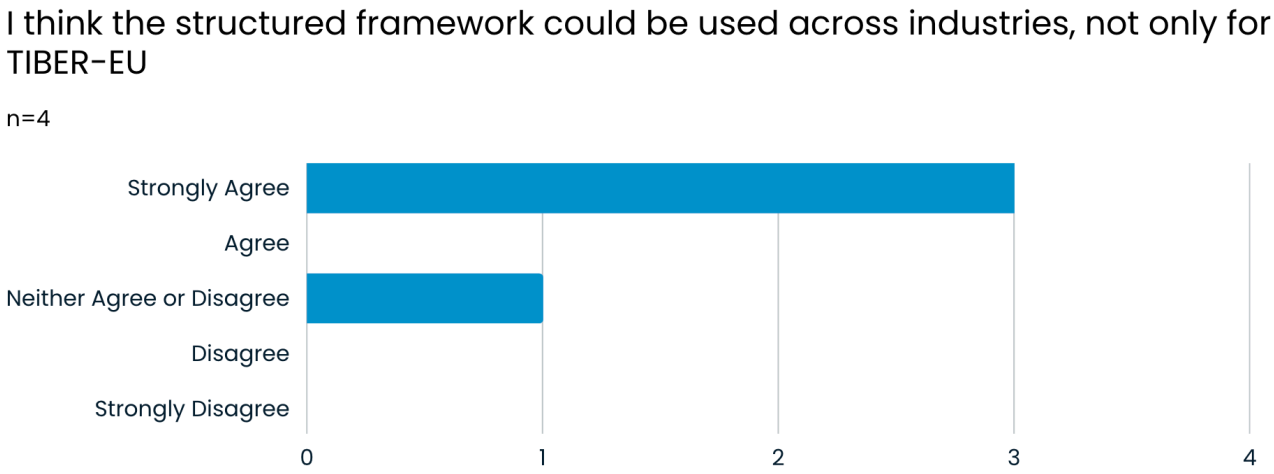

Figure 41. Question 5: I think the structured framework could be used across industries, not only for TIBER EU

Further testing the readiness of the implementation for real-life engagements shows some neutral positions (Figure 42). Combining this question with the following one provides an understanding of the hesitation.

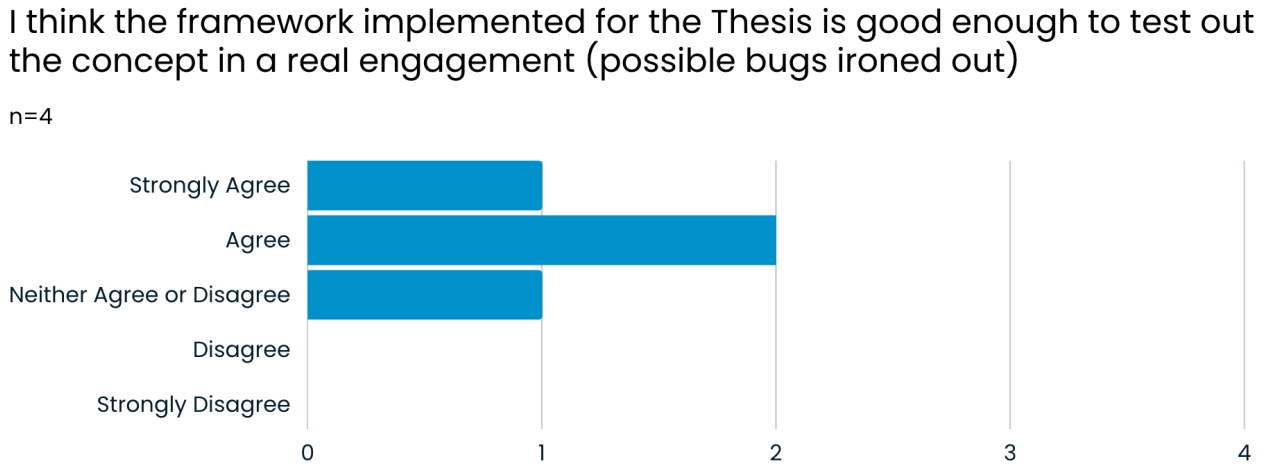

Figure 42. Question 6: I think the framework implemented for the Thesis is good enough to test out the concept in a real engagement

The respondents believe the tool has reasonable readiness for real-life engagements, but the data needed to populate the tool needs some effort. Neutral answers in Figure 43 illustrate this.

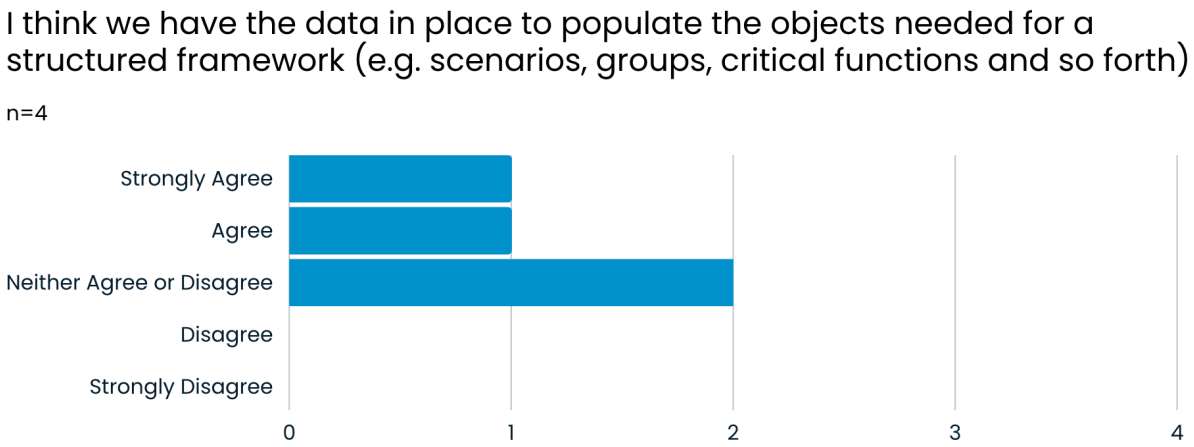

Figure 43. Question 7: I think we have the data in place to populate the objects needed for a structured framework

The key benefits the respondents saw the framework could bring are (Figure 44):

- Facilitates information sharing and understanding
- Harmonizes processes and ways of working
- Improves quality of customer engagements
- Improves profitability of customer engagements
- Improves communication with customers
- Improves company's credibility in TIBER engagements
- Makes my work more efficient
- Makes my colleagues work more efficient
- Speeds up the process to initiate engagements (written comment)
- Makes it easier to estimate engagements (written comment)

As the respondents saw benefits in using the framework, it is not only possible to implement but has the potential to impact the business positively.

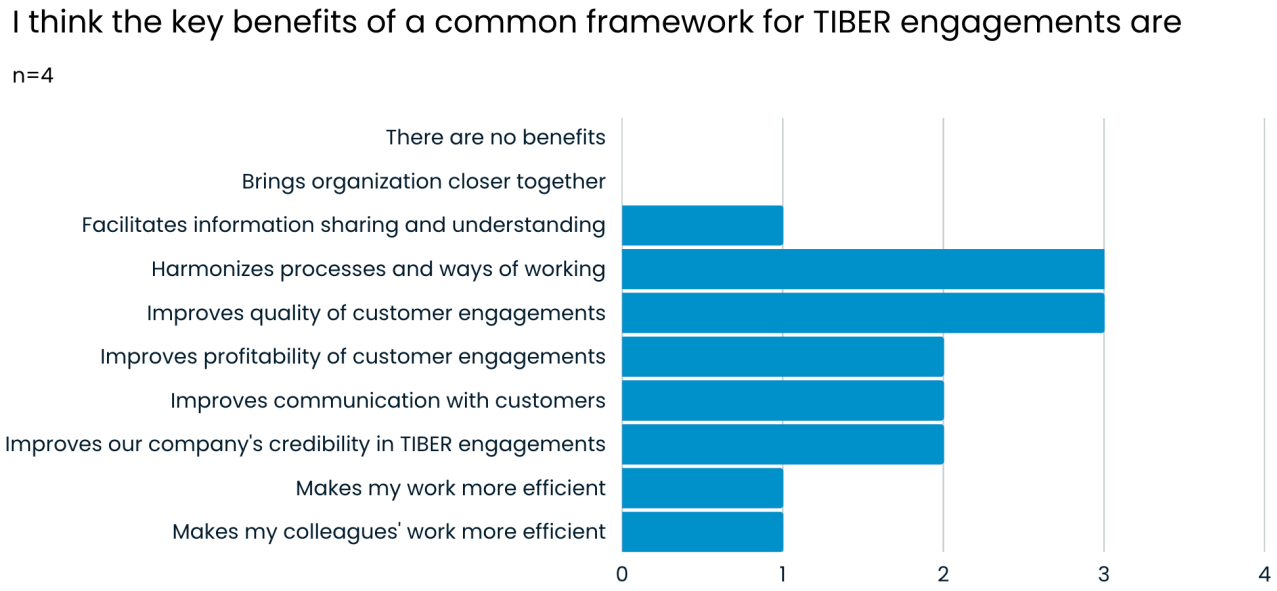

Figure 44. Question 8: I think the key benefits of a common framework for TIBER engagements are

Finally, for Nixu internally to plan their activities in continuing with the framework, the key actions chosen by the respondents were (Figure 45):

- Our company needs to establish an implementation initiative to have a production-ready framework in place
- Our company needs to establish a rollout initiative to deploy the current framework in use
- Our company needs to adapt processes to use the framework efficiently
- Our company needs to increase resources to use the framework efficiently
- Our company needs to adapt our existing resource availability to use the framework efficiently
- Our company needs to further evaluate the framework fit through real-life TIBER engagements (written comment)

The answers option *we should not proceed with this* would have been a strong indication of a lack of belief in the framework and consequently impacted the answers to the research questions.

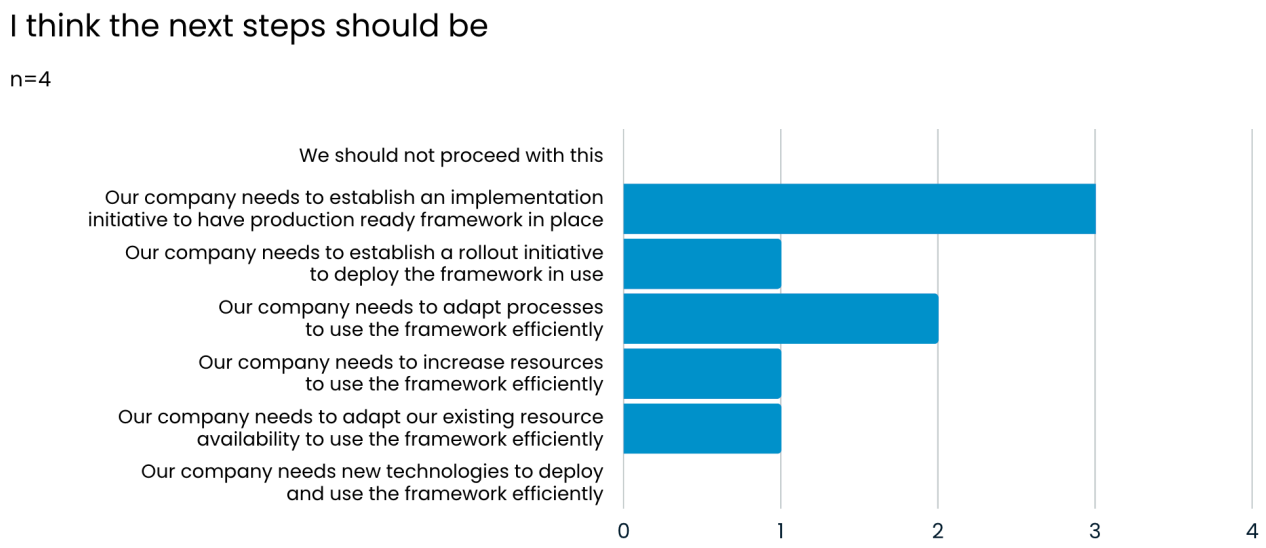

Figure 45. Question 9: I think the next steps should be

The survey analysis concludes that the answers are in line with the results and the research questions answers that were deducted based on the co-creation workshops.

6.3 Conclusion

The goal of the research, as discussed in section 2.7, is to address the challenge of TIBER-EU engagement scoping and the fact that the information required for a detailed scope is not available in the early stages of customer engagement. The positive answers to all three research questions as well as the survey results supporting the framework's applicability in real-life engagement and improving the scope definition and its effort estimation strongly indicate that using the developed framework can result in enhanced preparation phase accuracy.

Even with the framework, expecting the initial scope not to be adjusted during engagement is unrealistic. However, having a data-driven scope definition avoids scope creep. Lack of planning, clarity, foresight, and inaccurately defined requirements are among the top reasons why the original scope may extend beyond the initially agreed (Larson & Larson, 2009). Furthermore, agreeing on the scope changes and their impact can be done credibly and justifiably. As the scope is based on well-defined threat intelligence and customer entity characteristics, changes in the initial attributes can be modeled and discussed with the customer.

An additional benefit of the framework is that it improves scalability, repeatability, and continuous improvement of the engagement preparation process. Instead of depending on individual persons' experiences and preferences, the framework provides consistent outcomes regardless of the user. It must be noted that while the results are consistent, they must also be high quality. Thus, the experience of the subject matter experts needs to shift from running the preparation process to ensuring data quality.

Finally, the deployment of the framework requires an initiative of its own. It consists of finalizing the framework to be production ready and, even more importantly, ensuring the relevant roles and responsibilities, resource availability, and processes are adapted to take full advantage of the framework. An organizational structure and capacity for an operational, up-to-date, and continuously improving framework is the basis for successful engagement and realized benefits.

7 Discussion

7.1 Research Critique

7.1.1 Stakeholders

The research was set to answer questions related to an industry-specific framework, which has existed only for five years. Based on these grounds, selecting the subject matter experts to participate in the interviews and co-creation workshops was not possible from a vast group of people. Instead, the selected individuals were few with extensive experience in cyber security in general, combined with some coverage of TIBER-EU-specific experience.

The limited number of persons does not invalidate the answers to the research questions. I proved that a standardized framework can be implemented for TIBER-EU engagements. The structure of the framework, effectively answering my research question two, is however based on limited innovation. As such, it can provide a competitive advantage for Nixu.

The research could be even more impactful. TIBER-EU is bringing together financial institutes, authorities, and significant cybersecurity companies across Europe. The research questions could be answered by a consortium of people from all the stakeholders. Bringing the concreteness of TIBER-

EU to the next level could improve the efficiency and results of the engagements, benefiting all the parties.

7.1.2 Implementation

To answer the research questions, I defined the research plan keeping in mind the high level of confidentiality also limiting the information available for the research. The details of threat intelligence or TIBER-EU projects cannot be shared for research purposes. For these, a set of representative information was generated, and its applicability for the purpose is the responsibility of the information provider. On the positive side, a significant portion of the implementation is based on publicly available information, such as MITRE ATT@CK -framework.

Information sharing with the stakeholders was generally done in scheduled meetings, interviews, and co-creation workshops. With good preparations from all the parties the results were good, but having more informal information exchange could have provided more insights and feedback for the implementation. The expectation is that the results of the implementation also serve as the next baseline for further improvements, as now the stakeholders have a concrete framework and tool to use and improve. This includes the technologies used to implement the tool. Having a more mature framework structure, it is easier to evaluate possible technologies that may fit Nixu's existing technology landscape and hosting options.

7.1.3 Reflections on the Research

When initiating the research, I admittedly did not fully understand how multi-dimensional research area TIBER-EU is. Red teaming, threat intelligence, financial sector security considerations, and cyber security industry frameworks are all brought together, and it has been fulfilling to contribute while being educated by professionals.

During times when cyber security resources are scarce, being proactive and thorough in planning and preparations are essential. I also needed to be aware of changes in people's availability. Developing methods to decrease the time required from the stakeholders did pay off and ensured the focus was on producing valuable results.

As an outcome, I was able to answer the research questions. Moreover, I appreciate the wealth of information gathered and generated has grown me as a cyber security professional. And not only me, but based on the feedback, also the stakeholders gained insights to take with them in their future endeavors.

7.2 Ethics and Reliability

As the research involved a relatively small group of stakeholders, and the research methodology required human interpretation of the gathered data, it is essential to ensure the ethics and reliability of the results. I implemented four methods to avoid any unconscious bias and improve research repeatability:

- **Data gathering plan aligned with Six Sigma**: a plan that defined the data gathering methods and the use of data to avoid ad-hoc adjustments that could lead to poor accuracy or unrepeatable process.
- **Thematic and comparative analysis of the interviews:** Structured analysis of the interviews to avoid bias, as well as testing individual's point of view with other interviewees.
- **Co-creation requirement gathering and implementation with a feedback loop:** Feedback for the Entity Relationship Diagrams and the tool implementation was collected from all the co-creation workshop participants. Implemented changes were presented to the participants in a subsequent session to avoid misinterpretations.
- **Triangulation with a questionnaire:** The research questions were derived from the co-creation workshops, and triangulation was done using a questionnaire. As in the co-creation workshops the participants' identities were known the questionnaire was anonymous to lower the barrier for the respondents to provide feedback.

As a guiding principle, the material was shared in advance for all the interviews and co-creation workshops. Preparation time minimizes situations where valuable feedback is not received as participants have not been prepared for the topic.

When evaluating the reliability of my research, the limited number of stakeholders must be kept in mind. Even if each stakeholder was an expert in their field of cybersecurity, the data gathered depended on the organization's current state and the needs of the individuals. While I don't expect the research results to change entirely if the stakeholders were different persons, there can be variations in the tool implementation.

7.3 Further research

My research focused on answering the foundational questions if a standardized framework benefits TIBER-EU engagements and if such a framework can be implemented as a tool. The research was scoped to the TIBER-EU preparation phase. Building on the positive results achieved, future research can expand the research questions in three alternative dimensions: TIBER-EU process coverage, the framework user experience and usability, and an industry-agnostic framework.

7.3.1 Expand the framework to TIBER-EU testing and closure phases

The current framework covers one of the three TIBER-EU process phases, the preparation phase. With the help of the framework, the initial scope definition can be done efficiently, and the scope has improved relevance for the Entity. A natural next step is to expand the framework to the testing phase to follow up on the scenario execution and results.

Understanding the success of the defined scenarios and possible adaptation to the scope during the execution can be assumed to be interesting for all stakeholders. Furthermore, the TIBER-EU closure phase, including results sharing, would tie back to the initial scope.

7.3.2 User experience and usability of the framework

In my research, the framework implementation leveraged three-tier architecture, including the presentation layer. However, to be able to answer the defined research questions, the focus needed to be on the application and data tiers.

Successful adoption of any system requires that it is intuitive and efficient to use. A potential use case for the framework is in customer interactions, and well-thought usability is likely to improve customer perception of Nixu further. Thus, there is potential in research to improve the usability and user experience of the framework.

7.3.3 Industry-agnostic framework

TIBER-EU is designed for the financial sector. There are elements and definitions in TIBER-EU that are relevant for its target industry only, however, a concept of a structured process to execute red

teaming engagements is industry-agnostic. The researched standardized framework can, with a high likelihood, be evolved to be applicable to all industries or to have several industry-specific variations.

References

Accenture Security. (2018, February 13). *Cost of cyber crime study*. https://newsroom.accenture.com/news/cybercrime-costs-financial-services-sector-more-than-any-other-industry-with-breach-rate-tripling-over-past-five-years-according-to-report-from-accenture-and-ponemon-institute.htm

Baker, K. (2022, March 17). *What is cyber threat intelligence?* https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Beck, T., Demirgüç-Kunt, A., & Levine, R. (1999). *A New Database on Financial Development and Structure*. The World Bank. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.195.8454&rep=rep1&type=pdf

Benson, T., Pedersen, S., Tsalis, G., Futtrup, R., Dean, M., & Aschemann-Witzel, J. (2021). *Virtual Co-Creation: A Guide to Conducting Online Co-Creation Workshops*. https://doi.org/10.1177/16094069211053097

BetterValuation. (n.d.). *Triangulation*. https://www.betterevaluation.org/methods-approaches/methods/triangulation

Biscobing, J. (2019, September). *Entity Relationship Diagram (ERD)*. https://www.techtarget.com/searchdatamanagement/definition/entity-relationship-diagram-ERD

Breachlock. (2020, June 3). *Breachlock*. Top 3 Red Teaming Frameworks (TIBER,AASE,CBEST). https://www.breachlock.com/top-3-red-teaming-frameworks-tiberaasecbest/

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. US Department of Defense. https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Chauncey, W. (2013). *Credible Checklists and Quality Questionnaires*. Morgan Kaufmann.

Chawla, V. M. (2013, April 7). *ERD 'Crow's Foot' Relationship Symbols Cheat Sheet*. https://www.vivekmchawla.com/erd-crows-foot-relationship-symbols-cheat-sheet/

CircleID. (2019, June 6). *Threat Intelligence: Understanding Adversaries and Threats*. https://circleid.com/posts/20190606_threat_intelligence_understanding_adversaries_and_threats

Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime*, *27*(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008

Crowdstrike. (n.d.). *Crowdstrike Adversary Universe*. https://adversary.crowdstrike.com/

Crowdstrike. (2022). *2022 Global Threat Report*. https://go.crowdstrike.com/global-threat-report-2022.html

CubeCyber. (n.d.). *Types of Cyber Threat Actors and Their Motivations*. https://cubecyber.com/types-of-cyber-threat-actors-and-their-motivations/

Danmarks Nationalbank. (2020). *TIBER-DK General Implementation guide*. https://www.nationalbanken.dk/da/finansielstabilitet/fsor/Documents/TIBER%20implementeringsguide.pdf

Das, R. (2019, February 11). *Red teaming overview, assessment & methodology*. https://resources.infosecinstitute.com/topic/red-teaming-overview-assessment-methodology/

Dawson, C. (2009). *Introduction to Research Methods*. How To Content.

De Koning, J. I. J. C., Crul, M. R. M., & Wever, R. (2016, May). *Models of co-creation*. Fifth Service Design and Innovation conference, Copenhagen.

Department of Defense. (2003). *The Role and Status of DoD Red Teaming Activities*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Washington, D.C. 20301-3140. https://irp.fas.org/agency/dod/dsb/redteam.pdf

European Central Bank. (2018). *How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

European Central Bank. (2020a). *Guidance for Target Threat Intelligence Report*. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf

European Central Bank. (2020b). *TIBER-EU Scope Specification Template*. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Scoping_specification_template_July_2020.pdf

European Central Bank. (2022). *What is TIBER-EU?* https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

European Commission. (n.d.). *Bank recovery and resolution*. https://finance.ec.europa.eu/banking-and-banking-union/banking-regulation/bank-recovery-and-resolution_en

European Union. (n.d.). *Single Resolution Board*. https://www.srb.europa.eu/en

Finlands Bank. (n.d.). *TIBER-FI Implementation guideline—Procedures*. https://www.suomenpankki.fi/en/money-and-payments/tiber-fi-implementation-guideline/procedures/

Finnish Transport and Communications Agency National Cyber Security Centre. (2021). *Information security in 2020, Annual report of the National Cyber Security Centre Finland*. https://www.traficom.fi/sites/default/files/media/publication/TRAFICOM_Tietoturvan-vuosi-2020_EN_210608_WEB%20%281%29.pdf

Fox, J. (2021, August 31). *How Pentesting Differs from Ethical Hacking*. https://www.cobalt.io/blog/how-pentesting-differs-from-ethical-hacking

Godyla, N., & Hickey, M. (2021, June 10). *How purple teams can embrace hacker culture to improve security*. https://www.microsoft.com/security/blog/2021/06/10/how-purple-teams-can-embrace-hacker-culture-to-improve-security

Gourley, B. (2018, March 19). *Security Intelligence at the Strategic, Operational and Tactical Levels*. https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/

Haber, M. J. (2017, May 17). *What is the Difference Between a Threat Actor, Hacker and Attacker?* https://www.beyondtrust.com/blog/entry/difference-between-a-threat-actor-hacker-attacker

IBM Cloud Education. (2020, October 28). *Three-Tier Architecture*. https://www.ibm.com/cloud/learn/three-tier-architecture

IBM Security. (2022). *X-Force Threat Intelligence Index 2022*. https://www.ibm.com/downloads/cas/ADLMYLAZ

InfoSecurity. (2020, November 13). *The 4 Types of Threat Intelligence Vendors*. https://www.realinfosec.net/hot-cybersecurity-news/the-4-types-of-threat-intelligence-vendors/

Institute for Security and Open Methodologies. (2010). *The Open Source Security Testing Methodology Manual*. https://www.isecom.org/OSSTMM.3.pdf

Institute of Development Studies. (n.d.). *Participatory Methods*. Participatory Action Research. https://www.participatorymethods.org/glossary/participatory-action-research

Juneja, P. (n.d.). *Data Collection Plan*. https://www.managementstudyguide.com/data-collection-plan.htm

Kellermann, T., & Young, B. (2019). *Modern Bank Heists: The Bank Robbery Shifts to Cyberspace*. https://www.bankinfosecurity.com/whitepapers/modern-bank-heists-bank-robbery-shifts-to-cyberspace-w-5874

Larson, R., & Larson, E. (2009, October 13). *Top five causes of scope creep ... And what to do about them*. PMI Global Congress 2009, North America, Orlando, FL. https://www.pmi.org/learning/library/top-five-causes-scope-creep-6675

Liska, A. (n.d.). *Threat Intelligence in Practice*. https://www.oreilly.com/library/view/threat-intelligence-in/9781492049302/ch01.html

Mandiant. (n.d.). *Advanced Persistent Threats (APTs)*. https://www.mandiant.com/resources/apt-groups

Morgan, S. (2022, January 19). *2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*. https://cybersecurityventures.com/cybersecurity-almanac-2022/

Mortensen, D. H. (2020). *How to Do a Thematic Analysis of User Interviews*. https://www.interaction-design.org/literature/article/how-to-do-a-thematic-analysis-of-user-interviews

Müller, E., Sarjakivi, P., & Storm, M. (2022). *Future developments in cybersecurity—2022 and beyond*. https://www.nixu.com/whitepaper/future-developments-cybersecurity-2022-and-beyond

Narang, M. (2023, February 9). *Ethical Hacking vs Penetration Testing—Discover the Differences!* https://www.knowledgehut.com/blog/security/ethical-hacking-vs-penetration-testing

National Institute of Standards and Technology. (n.d.-a). *Red Team*. Retrieved 30 April 2022, from https://csrc.nist.gov/glossary/term/red_team

National Institute of Standards and Technology. (n.d.-b). *Red Team/Blue Team Approach*. https://csrc.nist.gov/glossary/term/red_team_blue_team_approach

National Institute of Standards and Technology. (n.d.-c). *White Team*. https://csrc.nist.gov/glossary/term/white_team

Ola, O. (2019, May 21). *The Tier of Threat Actors – Cheatsheet*. https://itblogr.com/tier-of-threat-actors-cheatsheet/

Olsen, X. (2022). *Enterprise Purple Teaming: An Exploratory Qualitative Study* [Doctor of Science, Marymount University]. https://www.proquest.com/docview/2658836337

Orchilles, J. (2022, March 24). *Cyber Kill Chain, MITRE ATT&CK, and Purple Team*. https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/

Penetration Testing Execution Standard. (2014, August 16). *PTES pre-engagement*. http://www.pentest-standard.org/index.php/Pre-engagement

Redlegg. (2020, April 2). *7 Types of Cyber Threat Actors and Their Damage*. https://www.redlegg.com/blog/cyber-threat-actor-types

Roberts, A. (2021). *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers*. Apress. https://doi.org/10.1007/978-1-4842-7220-6_1

Routin, D., Thoores, S., & Rossier, S. (2022). *Purple Team Strategies*. Packt.

Saarainen, V. (2021). *Red Teaming: Regulatory and non-regulatory frameworks used in adversarial simulations*. https://urn.fi/URN:NBN:fi:amk-2021053112749

Single Resolution Board. (2017). *Critical Functions: SRB Approach*. https://www.srb.europa.eu/system/files/media/document/critical_functions_final.pdf

Song, I.-Y., Evans, M., & Park, E. K. (1995). A Comparative Analysis of Entity-Relationship Diagrams. *Journal of Computer and Software Engineering*, *Vol. 3*(No.4).

Steffens, T. (2020). *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Springer. https://doi.org/10.1007/978-3-662-61313-9

Strom, D. (2021, September 7). *MITRE ATT&CK framework: Understanding attack methods*. https://www.csoonline.com/article/3267691/mitre-att-and-ck-framework-understanding-attack-methods.html

Synopsys, Inc. (2022). *Red Teaming*. https://www.synopsys.com/glossary/what-is-red-teaming.html

Szajnfarber, Z., & Gralla, E. (2017). *Qualitative Methods for Engineering Systems: Why we need them and how to use them*. https://cecas.clemson.edu/cedar/wp-content/uploads/2016/07/Szajnfarber-and-Gralla-2017-DRAFT-for-class.pdf

TechTarget. (2021, April). *What is red teaming?* https://www.techtarget.com/whatis/definition/red-teaming

The European Union Agency for Cybersecurity. (n.d.). *ENISA Threat Landscape through the years*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

The European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

The MITRE Corporation. (n.d.-a). *MITRE ATT&CK*. https://attack.mitre.org/

The MITRE Corporation. (n.d.-b). *MITRE ATT&CK Groups*. https://attack.mitre.org/groups/

The MITRE Corporation. (2020). *MITRE ATT&CK: APT29 Techniques Mapped to Mitigations and Data Sources*. https://attack.mitre.org/docs/attack_roadmap_2020_october.pdf

University of Jyväskylä. (2012, February 29). *Observations*. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/data-collection/observations

Verizon. (2020, May 19). *Money makes the cyber-crime world go round—Verizon Business 2020 Data Breach Investigations Report*. https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

Verizon. (2022). *Financial Services Data Security Breaches*. https://www.verizon.com/business/resources/reports/dbir/2022/financial-services-data-breaches/

World Economic Forum. (2015). *The Future of Financial Services*. https://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

Zenko, M. (2015). *Red Team: How to Succeed by Thinking Like the Enemy*. Basic Books.

Appendices

Appendix 1. As-Is Analysis Interview Questions

The interview questions are categorized to base questions, TIBER-EU questions, and specific questions for red teaming and threat intelligence depending on expertise of the interviewee.

Base Questions

#	Question
B1	What is your role at Nixu?
B2	Have you been part of TIBER-EU engagements?
B3	If yes, which parts of the TIBER-EU process have you been part of? - Preparation phase: engagement and scoping - Preparation phase: TI/RT services procurement - Testing phase: threat intelligence - Testing phase: red teaming - Closure Phase: remediation planning - Closure phase: result sharing

TIBER-EU Questions

#	Question
Q1	TIBER-EU states: "The preparation phase is mandatory for each implementation of the TIBER-EU framework". Please elaborate based on your experience how well the process is followed?
Q2	Why is it so, and what are the consequences for Nixu and the Entity?
Q3	During the engagement and scoping phase, how clear scope definition is given for the suppliers?
Q4	TIBER-EU process states the scenario development is done during the testing phase based on the (draft) targeted threat intelligence. Please elaborate if this reflects the reality of TIBER-EU procurement and engagements.

Q5	Would you say the following statements are *true*, *partially true*, or *false*: - During the procurement phase Nixu is typically given a clear scope or set of requirements for the engagement? - During the procurement phase Nixu typically has a good understanding of the target characteristics relevant to plan and scope a TIBER-EU engagement? - An engagement scope proposed/delivered is often dependent on who from Nixu is part of the procurement phase?
Q6	Please elaborate how does Nixu define the scope for a TIBER-EU engagement?
Q7	What are the key improvement areas of TIBER-EU engagement scoping phase? For Nixu? For the Entity?
Q8	When scoping an engagement, what are the attributes and characteristics used to define the engagement scope?
Q9	Would you agree the following Entity characters have significance in defining the scope and scenarios for an Entity? - Industry presence (including providing other than banking services) - Geographical presence - Number of employees - Revenue - Recent mergers or acquisitions - Ownership structure - Employee presence in social media - Company media presence - Outsourced services - Digital vs. physical presence - Recent major incidents - Use of certain technology - Experience in TIBER-EU vs. executing first time - Business relationships and interconnections to other companies and industries Which characteristics would you add?
Q10	Please elaborate local jurisdiction impact on the scope and execution?
Q11	When the scope and scenarios have been decided to be relevant for an Entity, do you have / does Nixu have the scenario definitions in place?
Q12	In which format the definitions exist?
Q13	What are the key improvement areas for the scenario definitions: for Nixu people?
Q14	What are the key improvement areas for the scenario definitions: for an Entity and communication between Nixu and an Entity?

Q15	TIBER-EU refers a lot to risk management. How is risk management planned and communicated during the preparation phase?

Red Teaming Questions

#	Question
RT1	TIBER-EU Services Procurement Guidelines –document states: *RT providers should have robust methodologies in place to conduct the most advanced and innovative forms of red team testing. The RT provider should aspire to conduct the highest-level tests, such that they can mimic a nation state actor and demonstrate sophistication, agility, use of advanced techniques and perseverance to match the level of defense of an entity. The RT provider should have processes in place to be able to clearly explain its methodologies, how they evolve and how they result in effective and high-quality red team tests.* What are the strengths and improvement areas for Nixu?

Threat Intelligence Questions

#	Question
TI1	TIBER-EU Services Procurement Guidelines –document states: *TI providers should have robust methodologies in place to develop their threat intelligence and reconnaissance. The TI provider should be able to clearly explain its methodologies, how they evolve and how they result in effective and high-quality outputs for red team tests.* What are the strengths and improvement areas for Nixu?

Appendix 2. Survey Questions

The questions sent to the stakeholders after the second co-creation workshop.

#	Question and Options for the Answers
Q1	I think our company would benefit using a structured framework in TIBER engagements • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree
Q2	I think it is possible to design a framework that can be applied in real-life TIBER engagements • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree
Q3	I think the concept implemented in the Thesis provides valuable insights in how a structured framework could work • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree
Q4	I think the concept implemented in the Thesis provides a starting point for the actual implementation of the structured framework • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree

#	Question and Options for the Answers
Q5	I think the structured framework could be used across industries, not only for TIBER EU • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree
Q6	I think the framework implemented for the Thesis is good enough to test out the concept in a real engagement (possible bugs ironed out) • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree
Q7	I think we have the data in place to populate the objects needed for a structured framework (e.g. scenarios, groups, critical functions and so forth) • Strongly Agree • Agree • Neither Agree or Disagree • Disagree • Strongly Disagree
Q8	I think the key benefits of a common framework for TIBER engagements are • There are no benefits • Brings organization closer together • Facilitates information sharing and understanding • Harmonizes processes and ways of working • Improves quality of customer engagements • Improves profitability of customer engagements • Improves communication with customers • Improves our company's credibility in TIBER engagements • Makes my work more efficient • Makes my colleagues' work more efficient • Other (please describe, can be several)

#	Question and Options for the Answers
Q9	I think the next steps should be • We should not proceed with this • Our company needs to establish an implementation initiative to have production ready framework in place • Our company needs to establish a rollout initiative to deploy the framework in use • Our company needs to adapt processes to use the framework efficiently • Our company needs to increase resources to use the framework efficiently • Our company needs to adapt our existing resource availability to use the framework efficiently • Our company needs new technologies to deploy and use the framework efficiently • Other (please describe)