



BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

A service architecture for an enhanced
Cyber Threat Intelligence capability and its value for the cyber
resilience of Financial Market Infrastructures

by Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio
and Giuseppe Natalucci



BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

A service architecture for an enhanced
Cyber Threat Intelligence capability and its value
for the cyber resilience of Financial Market Infrastructures

by Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio
and Giuseppe Natalucci

Number 43 – November 2023

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

*Printed copies can be requested from the Paolo Baffi Library:
richieste.pubblicazioni@bancaditalia.it.*

Editorial Board: STEFANO SIVIERO, LIVIO TORNETTA, GIUSEPPE ZINGRILLO, GUERINO ARDIZZI, PAOLO LIBRI, GIUSEPPE MARESCA, ONOFRIO PANZARINO, TIZIANA PIETRAFORTE, ANTONIO SPARACINO.

Secretariat: ALESSANDRA ROLLO.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

A SERVICE ARCHITECTURE FOR AN ENHANCED CYBER THREAT INTELLIGENCE CAPABILITY AND ITS VALUE FOR THE CYBER RESILIENCE OF FINANCIAL MARKET INFRASTRUCTURES

by Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio and Giuseppe Natalucci*

Abstract

In recent years, more and more organizations have been building up or enhancing their own Cyber Threat Intelligence (CTI) capability. Financial entities need to improve their own cyber resilience posture to face the ever-expanding range of money-driven or state sponsored threat actors aiming to undermine the stability of targeted countries by compromising their financial infrastructures. At the same time, the digital transformation process and steadily growing information sharing initiatives make a huge amount of data available for CTI analysis. International committees related to Financial Market Infrastructures (FMI), via commonly agreed policies or directives, and EU institutions, through normative initiatives, are firmly committed to improving the cybersecurity posture of FMIs. To this end, one of the main lines of action is to increase information sharing among financial entities. The large number of heterogeneous information sources and the overwhelming quantity and variety of available data could have negative impacts on the efficiency of CTI activities and compromise the effectiveness of defence capabilities. Therefore, the consolidation and automation of CTI processes must be prioritized in order to improve the effectiveness and sustainability of CTI operations. However, the definition and automation of CTI processes is still at a rather immature stage: for example, well-established and vendor-neutral best practices do not yet exist. The present paper proposes a framework, developed and adopted by the Computer Emergency Response Team of Banca d'Italia (CERTBI) that integrates a taxonomy and specific processes to develop an enhanced CTI capability.

JEL Classification: F50, O33, G20, L50, M15.

Keywords: CTI service architecture, CTI service components, information triage, intelligence case, technical investigation, security orchestration and automation.

Sintesi

Negli ultimi anni un numero sempre maggiore di organizzazioni sta implementando o potenziando le proprie capacità di *Cyber Threat Intelligence* (CTI) per fronteggiare le minacce *cyber*. In particolare, le entità finanziarie necessitano di contrastare una sempre più vasta gamma di *threat actors*, motivati da interessi economici o statuali, che mirano a indebolire la stabilità di un paese attraverso la compromissione delle sue infrastrutture finanziarie. Allo stesso tempo, la trasformazione digitale e la crescente diffusione di iniziative volte allo scambio volontario di informazioni sulle minacce *cyber* (*information sharing*) hanno generato un incremento del volume di dati e informazioni utilizzabili nell'ambito delle attività di CTI. Il miglioramento della postura di sicurezza *cyber* delle entità finanziarie, anche grazie a una più intensa condivisione di informazioni sulle minacce cibernetiche, costituisce un obiettivo primario dei comitati internazionali che

* Banca d'Italia, Directorate General for Information Technology, IT Planning Directorate, CERTBI Division. Authors are listed alphabetically.

regolamentano le infrastrutture dei mercati finanziari (*Financial Market Infrastructures, FMI*) ed è oggetto di specifiche iniziative normative da parte delle istituzioni europee. La numerosità delle sorgenti informative e la natura eterogenea dei dati da analizzare sono tuttavia fattori critici che, se non opportunamente gestiti, possono determinare impatti negativi sull'efficienza delle attività di CTI sino al punto di mettere a rischio l'efficacia delle connesse capacità difensive; è pertanto necessario adottare processi fortemente automatizzati al fine di aumentarne l'efficacia e di renderne sostenibile l'onere. Tuttavia, l'area di definizione e automazione dei processi di CTI appare ancora poco sviluppata, anche a causa della mancanza di *best practices* consolidate e indipendenti dalle specifiche soluzioni tecnologiche rese disponibili dai diversi *vendor*. Il lavoro propone un *framework* sviluppato dal *Computer Emergency Response Team* della Banca d'Italia (CERTBI) che integra aspetti tassonomici e specifici processi funzionali allo scopo di sviluppare avanzate capacità di CTI.

CONTENTS

1. Introduction	7
2. Cyber Threat Intelligence capability models	8
3. The value of an enhanced CTI capability for FMIs	10
4. The CTI capability development in Banca d'Italia	13
5. CTI service architecture	14
5.1 Architecture design	15
5.2 Entities layer	15
5.3 Information layer	16
5.4 Service layer	17
5.5 Service layer components	17
6. CTI service architecture processes implementation	19
6.1 Input triage	20
7. Conclusions and future development	24
8. References	26

1. Introduction

Digital transformation is associated with the onset of new cyber threat scenarios, as well as the constant evolution of cyber-attack techniques and procedures. Cyberspace¹ offers a tremendous opportunity to achieve political, military, economic and ideological goals to a wide-range of threat actors (state-sponsored, organized crime and hacktivists). Moreover, both the usage of tradecrafts available in the wild² and the outsourcing of malicious cyber activities³ significantly increased the number of adversaries for organizations to face. Despite the global focus on cybersecurity⁴ in recent years, significant improvements are still needed to thwart the continuously evolving cyber-attacks [1] as also confirmed by a double-digits yearly increase in cybersecurity investment forecast for the coming years [3].

The banking sector is one among the most affected by significant exposure to cyber threats in terms of incident costs [3]. In addition, cyber-attacks against Financial Market Infrastructures (FMIs) can pose a systemic risk for the financial stability by impairing the provision of critical economic functions and undermining confidence in the financial system [4]. The interconnectedness of the payment systems, their wide distribution across multiple countries and the intensive adoption of information technology are key factors that favour the speed and scale of cyber incident propagation. Moreover, financial sector represents a highly attractive target for threat actors⁵ looking for fast ways to monetize their malicious activities. Finally, cyber-attacks on FMIs can be performed with the intent of putting pressure on governments, since those are critical infrastructures to each State.

In this complex and fast evolving context, the adoption of an effective cyber resilience strategy is a key factor that allows an organization to continue to carry out its mission. It enables the capability of anticipating and adapting to cyber threats, as well as withstanding, containing and rapidly recovering from cyber incidents.

In order to achieve these objectives, adequate knowledge and solid understanding of the cyber threat landscape are crucial. Such needs can be satisfied by developing an appropriate situational awareness, namely the capability⁶ of an organization to achieve an understanding of the cyber threat environment within which it operates, the business implications of being in that environment and the adequacy of its cyber risk mitigation measures [5]. Situational awareness is a qualifying factor to facilitate decision making and the adoption of appropriate cyber risk mitigation strategies.

However, cyberspace differs from other domains: physical space and temporal dynamics are among distinctive factors to consider. First of all, cyberspace involves an enormous amalgamation of individual networks that provide relatively seamless communication of data [6], therefore threats against a specific network can be conveyed from anywhere else. Secondly, multiple temporal scales must be considered simultaneously. Cyber-attacks take place at “computational speed”, i.e. almost instantly, whereas their traces and effects can only be observed later. For this reason, it is hard to define a “situation” [7] in the cyberspace domain and a comprehensive situational awareness can be framed primarily through an effective Cyber Threat Intelligence (CTI) capability. This document addresses the above topics, firstly by defining the characteristics of an effective CTI capability, explaining why it contributes to enhance FMI cyber resilience and describing how Banca d’Italia has empowered its situational awareness in order to improve its cyber resilience. The second part introduces a framework, designed and adopted by

¹ Cyberspace is the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form [40].

² A tradecraft is a combination of methods, techniques and/or tools to be used in a cyber-attack. It is commonly referred to as being exploited “in the wild” when it is available through public sources such as websites, blog posts, forums, online cybercriminal databases or other platforms.

³ Cybercrime “as a service” (CaaS) is a criminal application of the ‘as-a-service’ business model that offers access to all manner of digital resources needed to commit cybercrimes, such as malicious software (malware), botnets (networks of computers infected with malware), hacking specialists, databases of stolen personal information, and other means.

⁴ With the term “cybersecurity” it is intended all the activities aiming to preserve the confidentiality, integrity and availability of information and/or information systems through the cyber medium. Note that the term “cyber resilience”, used in other parts of the text, has a broader meaning comprising also the ability of an organization to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents (definition adapted from [5]).

⁵ A threat actor is an individual, a group or an organization believed to be operating with malicious intent [5].

⁶ For the purpose of the document, as “capability” it is intended a combination of skills, resources, processes and systems bringing value to an organization’s business objective (adapted from [5]).

the Computer Emergency Response Team of Banca d'Italia (CERTBI), to build an enhanced cyber threat intelligence capability inside Banca d'Italia.

2. Cyber Threat Intelligence capability models

CTI aims at collecting and analysing heterogeneous data, coming from different internal and external information sources. Its main objective is to provide valuable knowledge to decision makers, also termed as “actionable intelligence” since it can be acted upon to address, prevent or mitigate a cyber threat. CTI is carried out by classifying, analysing and enriching collected relevant data and information in order to identify and assess cyber threats and threat-actor activities, as well as their possible motivations, capabilities, tactics, techniques and procedures (TTPs). Such produced intelligence helps an organization to assign a specific threat profile to its assets and to develop effective counter-actions.

Specifically, cyber threat intelligence can be broken down into three categories: technical/tactical, operational and strategic [8]. Tactical intelligence is focused on technical elements, and usually it is provided as Indicators of Compromise (IoCs)⁷, Common Vulnerabilities and Exposures (CVEs)⁸ and artefacts analysis. This can be used to tune operational defense capabilities, such as firewalls, intrusion-detection devices and response tools. Middle management typically consumes operational intelligence, that is focused on long-term cyber campaign analysis and TTPs employed by threat actors. Strategic intelligence provides elements on cyber threats that may affect organization business and, for this reason, is typically consumed by C-Level management.

A fundamental pillar to the CTI collection capability is information sharing, the process enabling the volunteer exchange of data and information related to cyber events or incidents among trusted peers or groups. Information sharing contributes to increased awareness on cyber threats, enhances the capacity to prevent threats from materializing into real incidents, and enables organizations to better contain the effects of cyber incidents [9]. This represents a relevant aspect to enhance the cyber resilience of involved parties, their specific sector and, potentially, the entire ecosystem.

Also for this reason, CTI effectiveness benefits from being performed by a single cyber intelligence organizational unit, with an intelligence-centric defensive approach. To such an extent, Computer Emergency Response Teams' (CERTs) role is crucial in centralizing cyber intelligence expertise, interacting with other business units and representing a single point of contact to cooperate – on the basis of mutual recognition and trust – with similar units operating in other organizations, within either public and private sector⁹. In fact, in order to incentivize the cyber threat intelligence exchange, information sharing takes place within trusted communities that protect the potentially sensitive nature of the shared information [10].

Recently, a growing number of companies and governmental entities started programs to introduce an enhanced CTI capability in their own organizations, in order to tackle more effectively the challenges related to the evolving cyber threat landscape. The need to enhance CTI capability has been already identified by European Systemic Risk Board (ESRB) as a relevant issue for financial entities in order to improve ability to collect, analyse, consume and share threat intelligence beyond the technical level [12]. In this scenario, a growing number of organizations with in-house CTI Capability are creating formal dedicated threat intelligence teams [11] with an increasing trend to seek for specific CTI professional skills.

Switching from consuming to (also) generating threat intelligence, tailored for the organization, is a key factor to step up the ability of improving CTI capability. However, the production of environmental-

⁷ Indicator of Compromise (IoC) is a digital evidence on a cyber-attack that is identified on organizational systems at host or network level (adapted from [40]). Indicators of Compromise give valuable information to investigate the event, prepare defenders for future attacks, and help prevent, detect and respond to similar attacks.

⁸ Common Vulnerabilities and Exposures (CVEs) are publicly known cybersecurity vulnerabilities provided as a list of entries, each containing a unique identification number, a description, and at least one public reference according to a common enumeration reference model (adapted from [40]).

⁹ CERTs and Computer Security Incident Response Teams (CSIRTs) are organizational units that usually provide three categories of services: reactive services (handle post incident reports from events related to threats or attacks such as compromised hosts, malware, vulnerabilities or others); proactive services (detect & prevent attacks before their effective impacts on production systems); security quality management services (review and improve the security posture of their organization). The information sharing and CTI activities fall in the proactive service category (<https://www.enisa.europa.eu/topics/csirt-cert-services>).

specific threat intelligence can only be effective by including, within the intelligence life cycle, the internal knowledge coming from intrusion analysis activities, the mastery of the organization's technical architectures and a deep understanding of business processes. In such a scenario, it is fundamental to identify the stakeholders' needs and translate them into intelligence requirements. These ones can be defined as any subjects that requires to fill information gaps about cyber threats. On the basis of intelligence requirements, it is possible to determine the type of threat intelligence to be generated, as well as its goals.

Furthermore, intelligence production needs to account for fundamental quality metrics [13] and, in order to be actionable, adhere to the following tenets [14]:

- **timeliness** - intelligence must be available when leadership requires it. Late intelligence is as useless as no intelligence. Timely intelligence enables leadership to anticipate events in the operational area. This enables leadership to time operations for maximum effectiveness and to avoid being surprised;
- **accuracy** - to be accurate, intelligence must be objective. It must be free from any political or other constraint and must not be distorted by pressure to conform with the positions held by higher levels of command. Intelligence products must not be shaped to conform to any perceptions of leadership's preferences. While intelligence is a factor in determining policy, policy must not determine intelligence;
- **usability** - intelligence must be tailored to the specific needs of leadership and provided in forms suitable for immediate comprehension. Leadership must be able to quickly apply intelligence to the task at hand. Providing useful intelligence requires the producers to understand the circumstances under which their products are used;
- **completeness** - complete intelligence answers leadership's questions about the adversary to the fullest degree possible. It also tells leadership what remains unknown. To be complete, intelligence must identify all the adversary's capabilities. It must inform leadership of the possible courses of action that are available to the adversary. When justified by the available evidence, intelligence must forecast future adversary actions and intentions;
- **relevance** - intelligence must be relevant to the planning and execution of the operation at hand. It must aid leadership in the accomplishment of the mission. Intelligence must contribute to leadership's understanding of the adversary. It must help leadership decide how to accomplish the assigned mission without being unduly hindered by the adversary.

As an organization decides to enhance its CTI capability to a higher maturity level and produce actionable intelligence, an improvement in its CTI management is necessary to achieve scalable, measurable, repeatable and automatable processes. In this scenario, the number of organizations that establish formal and dedicated cyber threat intelligence teams is growing [11] and consequently there are significant investments for acquiring specific competences and technology.

However, many organizations are still tailoring their CTI methodology [11], initially inherited from military and national intelligence sectors [15], to be fitted within their own enterprise cyber resilience security governance and the specific business context.

The following classification schema [16] can be used by organizations to assess their own CTI maturity level:

1. **Ad-Hoc** - some CTI tasks are initiated, but the activities are not yet organized and coordinated;
2. **Defined** - the business processes specific to CTI have been formalized and are running repeatedly;
3. **Aligned** - the CTI activities are starting to be integrated with the organization's processes;
4. **Controlled** - CTI activities are measured and correspondingly adapted to meet desired goals;
5. **Optimizing** - CTI processes are systematically analysed and improvements to maximize the outcomes are selected;
6. **Innovating** - new CTI methods and tooling are developed and deployed beyond the state of the art.

Numerous CTI organizations are currently reaching different levels of maturity through the implementation of technical capabilities and specific processes [2].

CTI tools have been evolving from rudimentary toolkits to highly advanced platforms, which provide semi-automated workflows to manage huge volumes of data and information from multiple open and closed sources. However, the modern ecosystem leveraged by threat actors is settling into a new level of business automation too: an example could be the cybercrime value-chain adoption of the “as-a-service” model. This scenario highlights the need to strike the unbalance between attackers and defenders, overcoming the defenders’ lack in dedicated processes and automation, which is considered among the major blocking factors to CTI effectiveness [15].

Well-defined and automatable processes represent a key factor to free up resources for the highly complex CTI tasks. Most of the CTI units with not well-defined processes appear struggling in the CTI automation area as a consequence of the relatively young age of commercial threat intelligence and the lack of a standard process [2] - [17].

The next step, in order to face increased complexity, is to refine and consolidate the practices [18]. The long-term goal is to run standard CTI processes, which could be beneficial for all organizations both in terms of cost reduction – e.g. enabling the usage of standard orchestration tools – and better interoperability. A further implicit benefit is the levelling of CTI teams’ capabilities towards a standard reference, which enhances the effectiveness of collaboration and information sharing.

Advanced technical capabilities, defined processes and automation represent invaluable factors to build an enhanced CTI capability, a pivotal element to reach at least an optimizing level of CTI maturity and to produce cyber intelligence tailored for fulfilling specific organization needs.

Although building an adequate CTI capability has become a well-known need, reference best practices don’t exist. In this respect, some models focus on the definition of common CTI concepts, principles and taxonomy [19] or define basic building blocks of generic CTI infrastructure [20]. Recent ones propose elements to address CTI information sharing [21].

CTI-like capabilities are often included in other security management processes, such as incident/information risk management, but usually with limited scope. Many open source and commercial threat intelligence platforms actually integrate a form of intelligence cases’ management capability, that is typically customised in proprietary and different ways by each platform [22]- [23].

Most of the issues related to the structuring a CTI high-level operational models, as practical and effective processes, are yet to be resolved [17]. Moreover, a reference standard model for inter-/intra-organization effective collaboration is still to be defined, as well as a common threat management workflow [2]- [22]. Furthermore, several examples of CTI infrastructure models and requirements [8] are available, although there is a demand for a common detailed definition of the related operational model and workflows.

A recent survey on the level of adoption of CTI [11], which has involved about 200 respondent organizations, half of them belonging to Banking and Finance or Government sector, revealed a relevant part of them is striving to develop an adequate CTI capability. The survey also highlighted a low usage of advanced tools, like CTI platforms, that could improve effectiveness of collecting information and disseminating intelligence. Finally, it points up the need of integrating CTI processes and tools.

3. The value of an enhanced CTI capability for FMIs

Organizations providing essential services are among those that can have the interest and resources to invest in establishing an enhanced CTI capability. Specifically, the systemic relevance of national critical infrastructures requires particular entities, identified as Digital Service Providers¹⁰ and Operators of Essential Services¹¹ according to the EU Directive “Network and Information Security” (NIS, recently replaced by NIS2) to increase their cyber resilience posture. In this context, CTI helps to identify the major threat scenarios [24] and to prioritize the proper countermeasures. CTI provides the possibility to select and prioritize the analysis of data subset that can actually affect an organization (e.g. related to specific threat actors).

¹⁰ A “digital service” is defined by the Directive (EU) 2015/1535 as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”. Nonetheless, in the context of the NIS, DSPs are limited to only three types of services: cloud, online marketplaces and search engines.

¹¹ Operators of Essential Services are public or private entities providing services “essential to the maintenance of critical societal and/or economic activities”. The following are sectors involved: energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, digital infrastructures.

Regarding the FMIs, a use case is represented by the early detection of external threats, useful to implement appropriate preventive controls and prepare an effective response. Specifically, a common signal of imminent cyber-threat is the presence of fake or compromised digital resources related to financial institutions (e.g. fake bank websites and social media profiles, stolen credit cards, mobile banking access credentials, etc.). It is a growing phenomenon associated to both financial fraud preparation and sophisticated state-sponsored campaigns against financial services or institutions. An enhanced CTI capability should be able to focus on the FMI related resources and promptly trigger the best counteractions in order to prevent the threat to realize (e.g. taking down the fictitious website, interdicting network access and providing advices to victims, involved financial entities and responsible security teams).

CTI is also pervasively used to provide up-to-date cyber threat scenarios that address threat led penetration testing, a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors [25]. Currently, mimicking an adversary behavior is one of the most valuable ways to verify cyber resilience posture. The test effectiveness thereby is directly correlated to the CTI capability to build an accurate profile of the malicious actors threatening financial entities. For example, in order to build an effective ransomware attack test scenario, CTI allows to provide knowledge about techniques leveraged by threat actor against the financial entities.

Moreover, CTI enables the design of effective security awareness campaigns based on current cyber threat evolution. As malicious actors evolve their techniques to swindle people, an advanced CTI capability should trigger and keep up ad-hoc security awareness programs to educate potential victims as soon as possible. For example, the financial sector has seen a growing trend in sophisticated scam techniques where threat actors have successfully used a combination of social engineering methods via emails, phone calls and IT systems vulnerabilities in order to illicitly operate on victims' banking accounts.

An advanced CTI capability in FMI shall therefore support a plethora of complex IT and organizational security needs.

In that regard, financial authorities recommend CTI capability enhancement being part of the cyber resilience strategy.

Namely, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) [26] indicate CTI as a key factor to drive the overarching components of a cyber resilience strategy. According to this principle, the European Central Bank (ECB), with the publication of the Cyber Resilience Oversight Expectations (CROE) [5], drives FMIs to set up their objectives based on the level of expectation they want to achieve (evolving, advancing or innovating). The CROE outlines five primary risk management categories¹² and three overarching components¹³ that should be addressed across an FMI's cyber resilience framework (see Figure 1).

¹² The risk management categories are (i) governance, (ii) identification, (iii) protection, (iv) detection, and (v) response and recovery.

(i) Governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. (ii) Identification is the capability of an FMI to identify which of their operations and supporting information assets should, in order of priority, be protected against compromise (iii) Protection consists of effective security controls and system and process design that protect the confidentiality, integrity and availability of an FMI's assets and services. These measures should be proportionate to an FMI's threat landscape and systemic role in the financial system, and consistent with its risk tolerance. (iv) Detection is an FMI's ability to recognize signs of a potential cyber incident or detect that an actual breach has taken place. (v) Response and recovery are the FMI's arrangements enabling the resume of critical operations rapidly, safely and with accurate data in order to mitigate the potential systemic risks of failure and meet obligations.

¹³ The overarching components are the transversal elements of FMI's cyber resilience framework that should address such expectations. They are (i) testing, situational (ii) awareness, and (iii) learning and evolving.

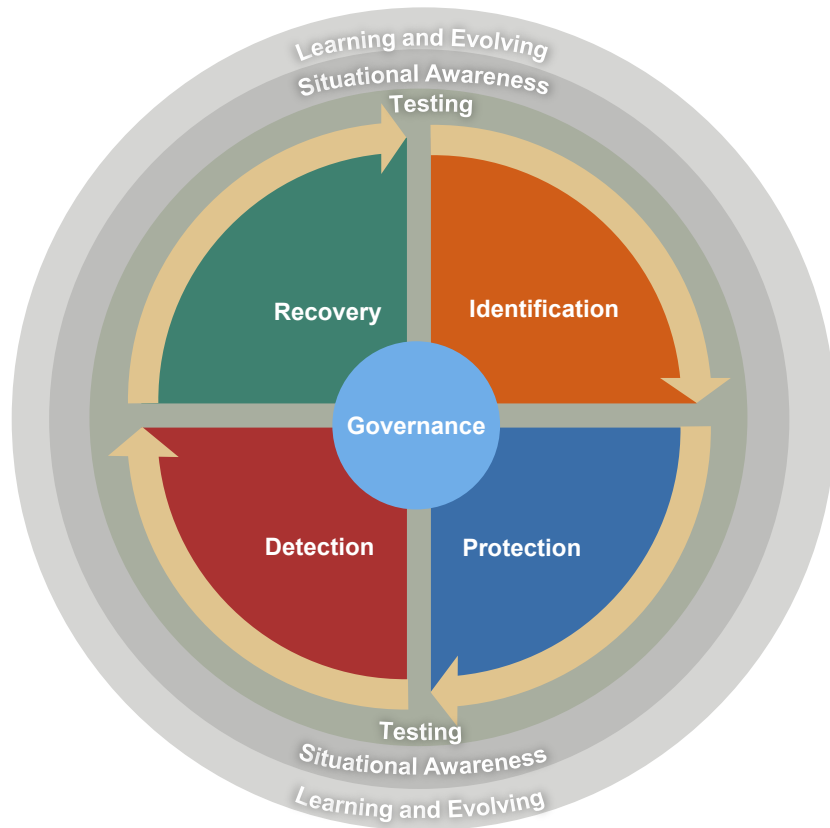


Figure 1: CROE risk categories and overarching components

In this context, cyber threat intelligence is mostly essential to address the situational awareness, namely the overarching component concerning the FMI capability to understand the surrounding cyber threat environment, the implications on its business and the adequacy of its cyber risk mitigation measures. Situational awareness can significantly advance FMI’s ability to pre-empt cyber events or to respond quickly and effectively to them. Moreover, it enables an FMI to validate its cyber resilience overall strategy and its effective implementation. Finally, building an enhanced CTI capability is a key factor to achieve and sustain the CROE requisites for the innovating level¹⁴. It is also worth mentioning the pivotal role that cyber threat intelligence plays in the security testing frameworks developed by the Bank of England (CBEST [20]) and by ECB (TIBER-EU [27]).

European Bank Authority (EBA), for its part, recommends the adoption of CTI to face the latest cyber threats and vulnerabilities and ensure business continuity [19].

Ultimately, the role CTI plays in the cyber resilience strategy is well known nowadays, in particular among FMIs. Indeed, Authorities set expectations on cyber threat intelligence capabilities of financial entities in order to strengthen the cyber resilience of the entity itself and the sector as a whole, also fostering the active participation in information sharing arrangements and collaboration with trusted stakeholders.

A noticeable example in the financial sector is the European Cyber Resilience Board Cyber Information and Intelligence Sharing Initiative (ECRB CIISI-EU)¹⁵, a multilateral cyber information and intelligence sharing initiative bringing together a community of public and private financial organizations.

¹⁴ CROE chapt. 2.8.2.1 CTI Learning and Evolving, Innovating level, item 13: The FMI should have capabilities in place to use multiple sources of intelligence, correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events to better understand the evolving threat landscape and proactively take the appropriate measures to improve its cyber resilience capabilities.

¹⁵ CIISI-EU was launched by the European Cyber Resilience Board (ECRB) for pan-European Financial Infrastructures, aiming to: raise cyber resilience awareness, catalyze joint initiatives, provide a place to share best practices and foster trust and collaboration. The CIISI community currently includes European financial infrastructures, central banks, critical service providers, European Union Agency for Cybersecurity (ENISA) and European Union Agency for Law Enforcement Cooperation.

Incentivizing the exchange of cyber threat information is also recommended by the Digital Operational Resilience Act (DORA)¹⁶, an EU Regulation where the improvement of information sharing is among the key factors to prevent cyber-attacks and reduce ICT threats to the financial system as a whole [10]. However, DORA does not recommend the adoption of any specific technological solution or process.

In this regard, the European Systemic Risk Board, as a primary step developing a pan-European systemic cyber incident coordination framework, recommends defining standard communication channels among financial authorities [4].

On the other hand, although authorities have defined requirements to fulfil, well-recognized reference frameworks and best practices are still lacking. Consequently, the level of CTI capability among FMI entities appear still jeopardized [11] while the ability to produce and consume high-quality and well-contextualized intelligence is fundamental to get the best benefit for the financial sector cyber resilience. The possibility to leverage on a shared model should be an enabling factor to achieve the goal: in particular, a common way of working organized into processes, structural capabilities and implementable operational tasks can facilitate the information sharing process.

4. The CTI capability development in Banca d'Italia

In order to face the rapid evolution of cyber threats and their continual rise in sophistication, Banca d'Italia has chosen to equip itself with an autonomous CTI capability and has promoted information sharing activities and collaborations with national and supranational qualified parties. So in 2017, the institutional CERT (CERTBI) was established, in line with the 2017-2019 strategic plan¹⁷, with the ultimate goal of concentrating in a single organizational unit all competencies needed to enable an effective production and to share information and intelligence on cyber threats with external counterparts. These activities complement IT security services provided by other units, increasing the Institution's preparedness to face cyber-attacks.

Currently, CERTBI carries out cyber intelligence activities for proactively countering cyber threats, producing actionable intelligence and disseminating it, in a timely and effective manner, to the Institute's internal and external stakeholders. As regards the activities to safeguard Banca d'Italia systems and services, it serves as institutional contact point for cooperation and cyber-threat information sharing initiatives with external qualified counterparts at national, EU and extra-EU levels, to face cyber threats according to the collective defense principle¹⁸. Moreover, CERTBI regularly takes part in cyber incident response exercises organized at national and international level to further strengthen collaboration with public and private sector counterparties. Finally, it promotes initiatives to increase its constituency¹⁹ security awareness, encouraging proper behaviors to prevent cyber incidents.

CERTBI has developed its own competencies to gain knowledge about cyber threat landscape and to provide situational awareness to various stakeholders, involved in the decision-making process at strategic, operational and tactical level, contributing towards increasing the Banca d'Italia digital operational resilience. To achieve this goal the following enabling-capabilities have been consolidated (see Figure 2):

- **Cooperation across national and supranational institutions:** the active involvement in a participatory security model realized by a joint collaboration on common cybersecurity issues. As main advantage, it allows leveraging on different competencies and knowledge basis and scale-up the Banca d'Italia capability to enhance its cyber resilience together with the inter-connected cyber ecosystem it relies on.
- **Information Sharing:** a constant exchanging of cyber-threat information with a growing number of high-qualified counterparts including both FMI entities and national institutions.

¹⁶ DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats [41].

¹⁷ https://www.bancaditalia.it/chi-siamo/organizzazione/Strategic-Plan-for-2017-2019.pdf?language_id=1

¹⁸ Collective defense uses information sharing and cooperation among defenders to counteract and rebalance the asymmetry that exists between cyber threats and an individual organization. In this way, the detection capability of one entity can improve the defense measures of another one.

¹⁹ Constituency: represents users that need to consume intelligence at strategic, operational or tactical level, including C-level executives, Corporate Security and Risk Management and -on need basis- specific Business Units. Security Operations are also included.

The extensive collection of information supports CERT ability to analyze the cyber threat landscape, timely produce actionable intelligence and provide it to the stakeholders.

- **Cyber Threat Intelligence:** the foundational capability to produce autonomously Cyber Threat Intelligence at technical, tactical, operational and strategic level in the context of an intelligence-led-cybersecurity paradigm.
- **Cyberspace Monitoring:** a continuous and proactive scrutiny of cyberspace looking after data and information related to potential threats. This activity enables the CERT capability to identify and trigger the execution of pre-emptive defense actions.

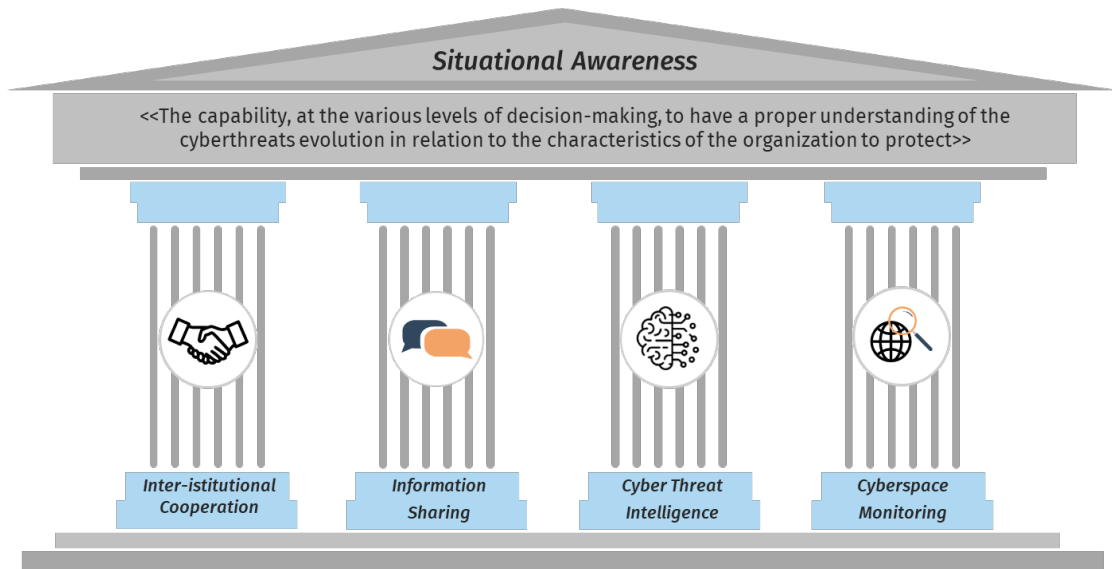


Figure 2: Situational Awareness and its enabling capabilities

To carry out its mission, CERTBI has embraced the “intelligence-driven” paradigm, with the objective to increase and consolidate its cyber intelligence capability.

In line with this objective, as people are the fundamental key asset, CTI team members are fostering to develop their expertise through highly specialized and professional training. Moreover, Banca d’Italia has launched a dedicated public competition in order to undertake the nowadays challenge to recruit high-profile cyber threat intelligence professionals.

Processes and technology are further fundamental components as they enable the collection and processing of a huge amount of data from heterogeneous sources, the correlation and the analysis of information and ultimately the production and dissemination of deliverables that effectively transfer knowledge to the intended recipients. To meet these requirements, CERTBI has developed its CTI service architecture and a set of integrated processes able to boost tasks standardization and automation: they have driven the setup of a technological solution for the security orchestration and automation capable of ensuring a high level of activities management and control, as well as achieving the introduction of advanced logics of automation inside CTI processes.

5. CTI service architecture

The approach used in this work to model CTI capability is inspired by the principles of Service-Oriented Architecture (SOA) methodology. It provides a set of guidelines and techniques in which business processes, information and enterprise assets can be effectively (re-)organized and (re-)deployed, to support and enable strategic plans and productivity levels that are required within competitive business environments [28].

As a driving principle, a business process can be broken down into a manageable hierarchy of fine-grained independent services, interacting together according to a customizable choreography. Each service can be implemented by a different application component as long as it keeps the same service interfaces and respect a set of general architecture constraints. These properties enable the possibilities

to use heterogeneous technologies, be able to replace one or more component without impacting the entire system and even re-use them in a different combination/choreography to realize another system. The combination of flexibility and high methodology maturity have been deemed strategic elements of choice for the support of a fast evolving activity like the CTI.

The underpinning concept that drives the design of a CTI service architecture is the identification and the modelling of all parties that can exchange data, information and intelligence. In other words, consumers of intelligence produced by the service, as well as other entities that collaborate to reach the goal, need to be defined. Operating under this assumption, boundaries between the service and its environment can be drawn, showing the entities and their interactions with it.

The first entity is the organization where the service is run, whose needs are to be satisfied. In addition, to accomplish its goals, the service exchanges data and information with external counterparts and deals with commercial CTI providers. Figure 3 shows the identified entities and their involved interactions.

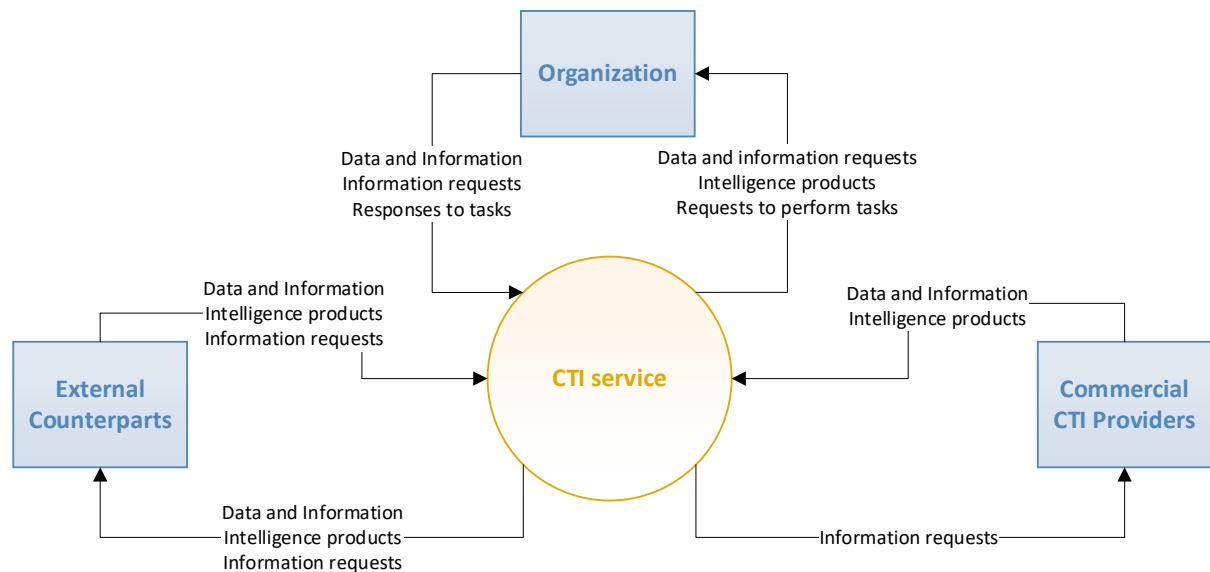


Figure 3: CTI service context diagram

In detail, the “data and information” flow depicted in above figure represent the exchange of raw data not yet fully analysed by CTI experts. “Intelligence products” are instead the outcome of analysis performed by the CTI service and tailored to the needs of the receiver at tactical, operational or strategical level. The “information requests” regards a specific information required to complete an intelligence investigations or needed by the organization in order to take informed actions. The “requests to perform tasks” typically identifies activities to be performed to fill an information gap.

5.1 Architecture design

The proposed service architecture is developed to cope with all phases of the intelligence life cycle (planning, collection, processing, analysis, production and dissemination of intelligence) [29]. As per Figure 3, it is made up of three layers: Entities layer, Information layer and Service layer. In each layer, three specific kinds of components are located: Entity, Information and Capability.

5.2 Entities layer

This layer includes all those parties that can provide/receive data, information and knowledge to/from the CTI service: Constituency, External Counterparts and Commercial CTI Providers.

Constituency represents the part of an organization that need to consume intelligence at strategic, operational or tactical level, including C-level executives, Corporate Security and Risk Management, as well as – depending on the organization structure – more specific Business Units. Security and

Operational units are included among them as well. Indeed, they are, at the same time, part of the constituency as primary consumer of tactical threat intelligence and the organisational unit aimed to produce a specific input (Alert) ingested by the service and to perform specific tasks in response to CTI service indications. Finally, the Constituency may proactively, or upon request, provide data and information to the CTI Service to accomplish its own goals.

External Counterparts are all the external organizations that are allowed to interact with the CTI service, in line with established agreements. Information sharing takes place with these entities. External counterparts can be summarized as follow:

- **peers** — organizations with whom one-to-one agreements are in place;
- **national institutions, bodies and agencies** — they represent domestic institutions, bodies and agencies (involved in law enforcement, defense and intelligence activities) that can provide CTI deliverables. This interaction is based on national information sharing agreement as well as on protocols to be followed in case of a national-scale cyber incident;
- **foreign and supranational institutions, bodies and agencies** — they can provide CTI deliverables representing non-national and non-commercial organizations which cooperation agreements are established with;
- **sharing communities** — they include formal/informal, sector/inter-sectorial, public/private groups aimed to share cyber threat data and information on a voluntary basis [30].

Vendors provide commercial CTI services, producing deliverables and fulfilling on-demand intelligence needs through “information requests”. Other than human-readable, they also provide Machine-Readable Threat Intelligence (MRTI) [31], that is a continuous flow of technical data (feeds), delivered in a structured notation, that can be (semi-)automatically ingested and processed by security tools and systems.

5.3 Information layer

The Information layer includes all the data, information and intelligence products that the CTI Service handles, as either input or output, towards entities: alerts, Request for Information (RFI) and deliverables.

An alert is raised when there is a piece of evidence related to a running or potential threat for the Constituency: it usually comes from the Security Operations Center (SOC), or it can be produced autonomously by a component of the CTI service.

A RFI is created when an information gap needs to be filled. Constituency or External Counterparts, as well as intelligence team members, may submit RFIs to generate intelligence collection efforts. RFIs are specific, time-sensitive, and not necessarily related to standing requirements or scheduled intelligence production (intelligence requirements). They may be either an input from Entities (Constituency or External Counterparts) or an output sent to them to enable CTI service to build intelligence regarding current or potential threats.

A deliverable is the CTI product used to effectively transfer information or knowledge related to one or more cyber threats. It can be either the output of the CTI service delivered to the Entities, or an input from them used by the CTI service to accomplish its goals. Deliverables can be disseminated either when pre-established conditions happen (periodically or triggered by specific events), or in reply to an RFI. On the basis of the expected consumer, the category of the intelligence to be transferred and its timing requirements, the following deliverables’ taxonomy is developed within this layer (main targets of deliverables are shown in parentheses):

- **Security Alert** — warning on imminent or ongoing cyber threats and associated short-term recommendations for prevention and/or mitigation (Constituency);
- **Security Advisory** — recommendation concerning preventive defense actions or workaround related to new relevant vulnerabilities or TTPs (Security and Operational staff);

- **Flash Report** — information regarding an imminent or ongoing threat to disseminate promptly to stakeholders in order to led them take effective decisions (internal/external decision makers);
- **Threat Bulletin** — analysis focused on a specific cyber event or cyber threat (internal/external decision makers);
- **Operational CTI Report** — operational periodic update about cyber threat landscape (Security and Operational managers);
- **Strategic CTI Report** — strategic periodic update about cyber threat landscape, with analysis of recent relevant cyber events and predictions (C-level executives).

5.4 Service layer

This layer includes all the capabilities of the CTI service (see Figure 4).

- **Input Interface** — the entry point for the incoming flows. It validates the source and categorizes the content of the input before invoking the appropriate process handling such input. In the same way, outgoing flows have a single exit point, the **Output Interface** component that triggers either the information delivery or the issuance of requests.
- **Internal CTI Production** — the production source for information and intelligence. It may require the Constituency to perform additional tasks, in order to fill information gaps at tactical and operational levels, through the **Reactive CTI Collection** component.
- **Proactive CTI Collection** — it monitors the cyberspace looking after data and information related to threats that could potentially affect the Constituency.
- **CTI Service Management** — it includes several structural capabilities needed to manage the service and its internal knowledge base, activities and resources.

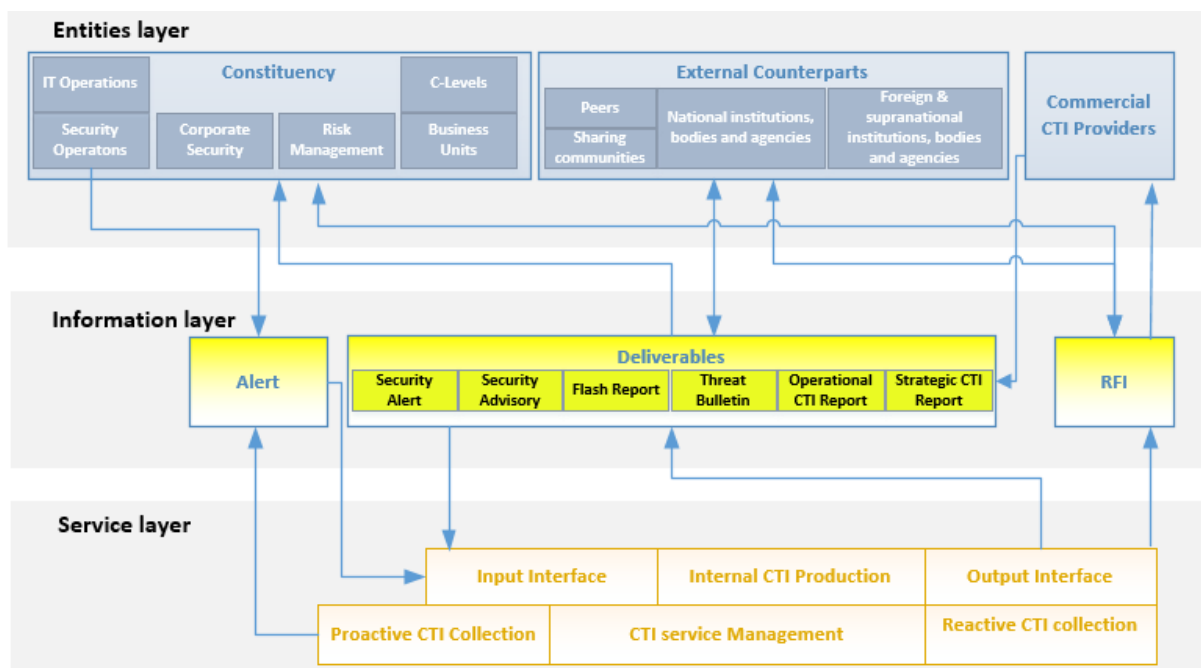


Figure 4: Service architecture

5.5 Service layer components

Service layer components are containers used to group homogeneous entities such as structural capabilities (consisting of activities that run continuously, independently from the service inputs), processes or tasks for specific operational units.

Interaction between different components can be two-fold: by information flows and by operational flows. Information flows carry any element included in the Information layer. Operational flows are

instead a command path leading to capability or process invocation. Service layer components are shown in Figure 5 and described below.

The Input interface is composed of the Input Triage and the Incoming RFI handling processes. The **Input Triage** process, described in detail in the following paragraph, analyses incoming deliverables, alerts and RFIs, in order to prioritize them and provide the information needed to determine resulting actions. In case of deliverables and alerts, a decision is required to either send them directly towards the output interface or trigger the Internal CTI Production component.

Input RFIs, instead, are preliminarily checked and routed to the devoted **Incoming RFI handling** process, where the opportunity to reply to the request – with a given priority – or provide a feedback to the requestor, is evaluated. When the decision to reply is taken, the process triggers the internal CTI production component in order to create the needed knowledge.

The Output interface relies on the **Information To Share/Request** process to evaluate information to be shared or requested to Entities: this is performed by mapping the content to the intended recipients and identifying the right procedures to send/request the information (i.e. selecting which communication channels, sharing/re-sharing capabilities and classification/confidentiality levels are to be adopted with third parties).

The Internal CTI Production component contains the core CTI operational processes: Technical Investigation handling and Intelligence Case handling.

A **Technical Investigation** provides technical/tactical information deliverables by analysing a threat among the internal and external perimeters, or by setting up a specific investigation environment. A technical investigator can escalate and, if needed, ask for an Intelligence Case to be opened.

An **Intelligence Case** analyses a potential or running cyber threat in order to determine the appropriate defensive or preventative actions and strategies against the threat. The Intelligence Case can be used to build knowledge in order to reduce the uncertainty about relevant cyberspace phenomena. Each Intelligence Case is assigned to a case officer who is responsible for the overall activities' coordination and interactions towards case resolution. If needed, an Intelligence Case can trigger one or several Technical Investigations.

Reactive CTI Collection is used by Internal CTI Production to dispatch requests to Operations teams within the organization: Technical Investigation process can initiate a request to perform task to either Security Operations or IT Operations. Intelligence Case process can start tasks to be dispatched to Cyber Intelligence Operations, which performs active research and collection of information (in or through the cyberspace), when specific knowledge on threat actors tactics and procedures are needed.

Proactive CTI Collection is composed by Digital Footprint Monitoring and News/Media Monitoring, which routinely scan the cyberspace searching for, respectively, CTI data/information and news/media sources related to potential threats affecting the Constituency.

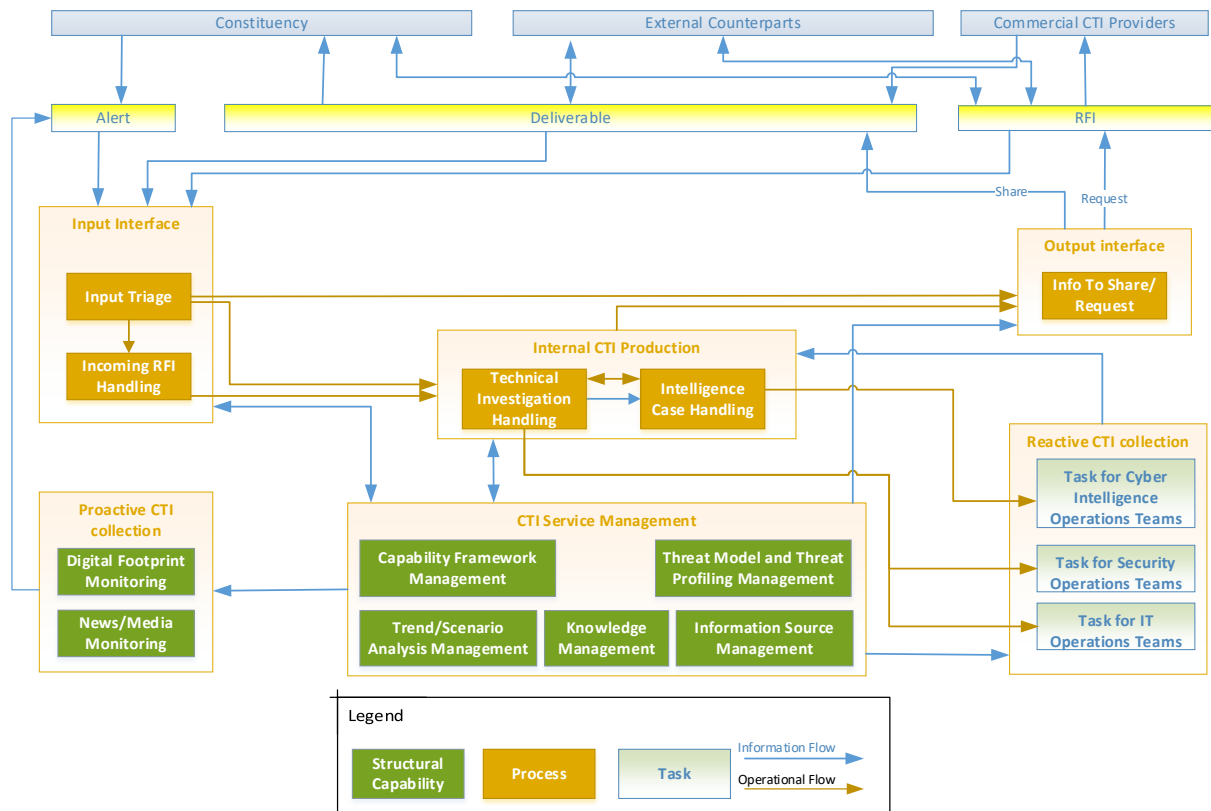


Figure 5: Service layer components

Finally, the CTI management is made up of the followings sub-components:

- **Knowledge Management**, which handles data, information, knowledge and intelligence collected as part of the CTI service, and includes a repository to store and retrieve them;
- **Information Source Management**, which handles the relationship with Entities and manages an information source repository containing attributes on such entities (reliability score, agreements and obligations, allowed and expected information, etc.);
- **Capability Framework Management**, which is responsible for the CTI service architecture's review and maintenance, as well as the provisioning and allocation of resources required to enact processes and to accomplish set goals;
- **Trend/Scenario Analysis Management**, which leverages on the Knowledge Management repository to perform descriptive and predictive analysis on potential or imminent threats;
- **Threat Model and Threat Profiling Management**, which produces and maintains the organization's threat models and threat actors' profiles.

6. CTI service architecture processes implementation

The model described above, in line with SOA business processes decomposition principle, defines all the elements of the CTI service architecture and its main operational and information flows. In the subsequent steps, the model is translated in an actual operational service framework. In particular, the implementation of the model pivots around the transformation of the five CTI processes to executable workflows which coordinate the CTI team activities integrated with CTI structural capabilities and ancillary tasks execution in order to consume, produce and disseminate data and intelligence. The implementation keeps a high degree of technology agnosticism, allowing for reusability in other contexts. It aligns with the common requirement for organizations with a higher CTI maturity level to provide a formal, holistic, transparent and repeatable process [32].

Among the five implemented CTI processes, the following paragraph aims to provide more details about the implementation of the Input Triage, which is the primary beneficiary of the enhanced workflow definition and automation. This process is executed for all data and information fed into CTI services from various threat intelligence sources, including internal, external, counterpart, or commercial sources.

6.1 Input triage

This process must balance the need to empower the information collection capabilities with the available information processing resources by filtering, prioritizing and validating relevant information for the protection of the Constituency.

Input information has to be assessed, at first, in terms of source identification and input data compliance. Afterwards, qualitative and quantitative evaluations are performed to define the information relevancy and to calculate a priority score (i.e. valorisation phase). Nevertheless, alerts from Security Operations can be considered as pre-validated inputs and thus are immediately forwarded to the valorisation phase.

As shown in Figure 6, the Input Triage process starts (1) with the source identification and the input data compliance checks in terms of source authorization, reliability score, predefined agreements, used communication channels, expected information type and format.

During the following step, information is dissected. If the input includes a RFI, the Incoming RFI Management process is invoked: (2.a) input is evaluated, classified, and eventually replied, depending on the evaluation outcomes. Incoming RFI Management triggers further processes aimed at producing the requested information with format and timing pre-agreed with the sender. On the other hand, if the input is a piece of information, it is stored in the knowledge repository (2.b), and it is evaluated against its relevancy (3). Finally, in case of Alert, the input is automatically considered as relevant and it is sent directly to step (4).

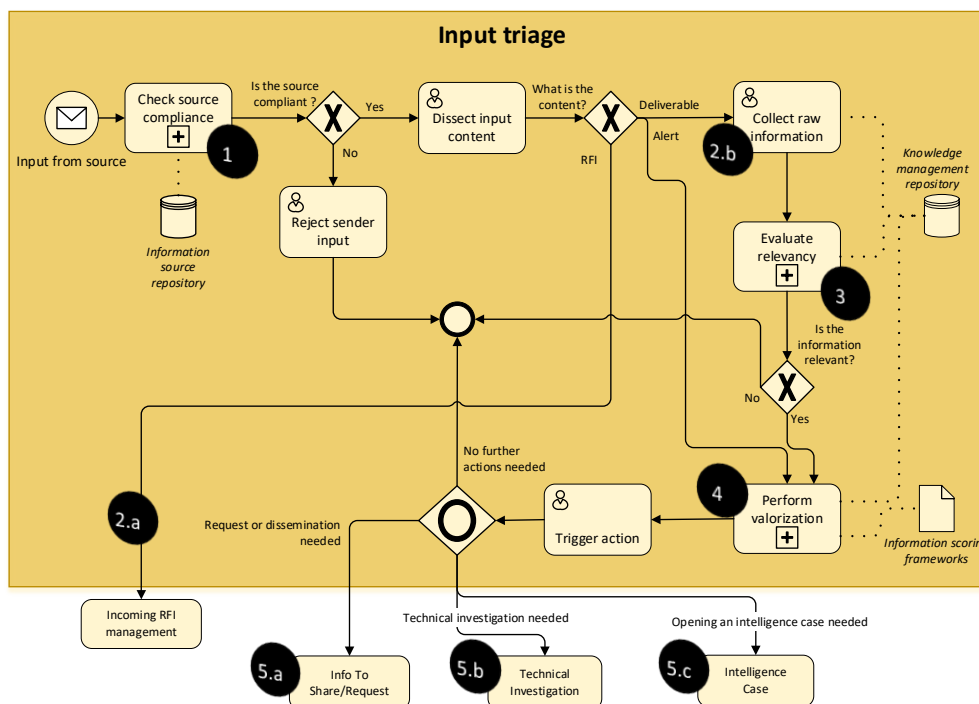


Figure 6: Input triage

A piece of information is considered as “relevant” when it satisfies one or more collection intelligence requirements. They can be identified by considering the available threat model and by evaluating the potential threat’s proximity to Constituency, referred to as Threat Proximity (TP). This indicator measures the distance between the entities impacted or potentially affected by the event and the Constituency. As a precondition, custom metrics need to be defined: they can be based, for example,

on criteria related to the involved business sectors, the geographical location and the level of connection with the organization’s supply chain.

Relevant information is then valorised (4) by the use of multiple scoring frameworks, with the purpose of determining the most appropriate handling. More in detail, at this step, information stored in the Knowledge Management repository is enriched with the vector {AS, TS, PS} defined below:

- **Admiralty Score (AS)** - based on Admiralty Code, the score represents the confidence level applicable to the information [32] [33]. Specifically, it measures the input information credibility and the information source reliability. The Code prompts the requestor to rate each piece of evidence according to:
 - a. the expected source reliability in providing accurate information on this occasion, rated from “A” to “F”. The judgment is primarily based on the source type and reputation, e.g. the highest “A” rating may label trusted private- or public-sector entities; the intermediate “C2” rating may label news published by proper respectable medium; the lowest “F” rating may label a brand new, not yet assessed source. The other rating factor is the level of competence attributed to the source: a specialized cyber threat intelligence center is likely more reliable than a generic administration department.
 - b. the validity likelihood of the claim, rated from 1 to 6. The rating accounts for how the claim compares with other verified evidence (e.g. whether it contradicts the evidence or not), and how well it fits with existing theories/explanations (e.g. whether it is consistent with international regulations or it can be actually feasible within a given context and timeframe).

Reliability of the source		Validity likelihood of the claim	
A	Completely reliable	1	Completely credible
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usual reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

Table 1: Admiralty Score-values scale definition

For a more convenient usage, Admiralty Score (AS) can be mapped to a unique credibility indicator, the **Confidence Range (CR)**, adapting specific criteria [33]. With this method, from AS scores is possible to derive a scale of CR values with the level of granularity deemed most appropriate for the organization needs. For the purpose of the document, it is reported a simplified mapping example where the confidence range span among three values: “0: Not Credible”; “0,5: Uncertain/to further investigate”; “1: Credible”.

VALIDITY LIKELIHOOD	SOURCE RELIABILITY						CONFIDENCE RANGE	
	A1	B1	C1	D1	E1	F1	■ 1: Credible	■ 0.5: Uncertain/ to further investigate
	A2	B2	C2	D2	E2	F2		
	A3	B3	C3	D3	E3	F3		
	A4	B4	C4	D4	E4	F4	■ 0: Not credible	
	A5	B5	C5	D5	E5	F5		
	A6	B6	C6	D6	E6	F6		

Table 2: Mapping Admiralty Score to the Confidence Range

- **Threat Score (TS)** - the indicator measures the danger of the threat. Its calculation takes in account the Confidence Range and the Threat Level.

The **Threat Level (TL)** is a score resulting by the combination of threat actor offensive capability (e.g. level of its financial and people resources), its hostile intent (e.g. geopolitical or financial gain interests) and attack opportunities against the target (e.g. possible vulnerability to leverage on). For example, in the context of financial services, an elevated threat level may be assigned to a threat actor that is: i) categorized as state-sponsored, i.e. it can count on vast resources provided by the sponsoring state (high offensive capability); ii) historically targeting financial entities for political or economic reasons (clear hostile intent); iii) able to leverage software vulnerabilities (relevant attack opportunities). The value of Threat Level can be calculated adopting various criteria: for the purpose of this document, an example is shown in the Table 3:

Threat level	Description
High (1)	Sophisticated targeted attack
Medium (2)	Unsophisticated targeted attack
Low (3)	Non-targeted attack

Table 3: Threat levels example

The value of Threat Score can be calculated adopting various criteria: for the purpose of this document, an example is shown in the Table 4:

		CONFIDENCE RANGE			THREAT SCORE	
		Credible	Uncertain	Not credible		
THREAT LEVEL	High					1
	Medium					2
	Low					3
						4
						5

Table 4: Threat Score

- **Priority Score (PS)** – it is the synthetical indicator, calculated on the basis of Threat Score and Threat Proximity, that can be used to prioritize the information to manage and the cyber threat prevention or mitigation initiatives.

Threat Proximity (TP) measures the potential threat target's proximity to the Constituency on the basis of selected parameters characterizing the organization business and IT assets. TP common evaluation parameters are the potential geographical, political, economic, interdependencies the organization has with the threatened entities, e.g. in relation to its supply-chain. As example, a simplified TP proximity scale is reported in the following table:

Threat Proximity	Description
1	Constituency
2	Organization partners or suppliers
3	Organization in the same sector or with other specific interdependencies
4	Others

Table 5: Threat Proximity Scale

Priority Score can either be calculated by a mathematical formula or by a complex mapping functions, possibly considering organization-specific adjustment parameters to tune it against false positives. For the purpose of the document, a simplified example of PS calculation is reported in the Table 6.

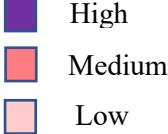
		Threat Proximity				Priority Score
		1	2	3	4	
Threat Score	1	High	High	High	Medium	
	2	High	High	Medium	Low	
	3	High	Medium	Medium	Low	
	4	Medium	Medium	Low	Low	
	5	Medium	Low	Low	Low	

Table 6: Priority Score identification matrix

Finally, the information confidentiality is classified according to national law, internal policies and the Traffic Light Protocol (TLP) [34]. Once the information is dissected, analysed, valorised and classified, the appropriate process (**5.a**, **5.b** or **5.c**) is triggered:

- (**5.a**) Invocation of the Info To Share/Request process to share the received information with Constituency and/or External Counterparts, when appropriate (e.g. for detecting and preventing the threat described in the information) or to demand more data, information or intelligence (RFI) from Entities. In detail: a) check for unwanted disclosures in the submitting deliverable, alert or RFI; b) package in the appropriate format the sanitized deliverable, alert or RFI to deliver them to the intended recipients; c) redirect any feedback received by the recipients to the appropriate service components.
- (**5.b**) Start of a Technical Investigation, to provide tactical information deliverable by analysing a threat among the internal and/or external perimeter, or by setting a specific investigation environment up.
- (**5.c**) Open an Intelligence Case, to analyse a potential or current cyber threat in order to determine the appropriate defensive or preventative counter-actions and strategies. The Intelligence Case may also be used to build knowledge in order to reduce uncertainty about relevant cyberspace phenomena.

7. Conclusions and future development

An enhanced CTI capability represents a game changer for FMIs to empower the effectiveness of their own cyber defense, but it also increases the complexity of their cybersecurity operations' management.

Furthermore, the demand for an overarching service architecture and well-defined common processes is becoming increasingly relevant as more public and private entities improve their CTI capabilities and collaborate to face cyber-attacks that are constantly evolving and becoming increasingly more sophisticated, widespread and undetected.

In recent years, financial authorities and regulation entities have promoted many initiatives to enhance the cyber resilience of the financial ecosystem.

Notably, the development of an advanced CTI capability is a key element required by CROE in order to achieve a higher level of expectations (the "innovating" level) in the area of threat prevention and proactive defense against cyber-attacks.

However, even though the widespread awareness about the main role CTI plays in the cyber resilience of the entire financial sector, there is a lack of processes and methodologies capable to support the development of an enhanced CTI capability.

Furthermore, insufficient information sharing and cooperation on cyber threat intelligence at the strategic, operational and tactical level prevent organizations from adequately assessing, monitoring, defending against and responding to cyber threats.

In order to address those needs, a vendor-agnostic service model, not affected by any technical bias, is proposed. Specifically, this document describes, omitting sensitive details, the CTI service architecture that currently supports cyber threat intelligence activities carried out by Computer Emergency Response Team of Banca d'Italia (CERTBI). Its adoption has enhanced the autonomous CTI capability of the Institute and has empowered its cyber situational awareness. As main benefit, CERTBI has increased its effectiveness in providing situational awareness to the decision-makers at strategic, operational and tactical levels, contributing towards the enhancement of the Banca d'Italia cybersecurity posture and digital operational resilience.

The service architecture has been designed using a top-down approach, defining specific processes, structural capabilities and operational tasks. Each process has been developed in order to be smoothly translated into an automated workflow: a practical input triage implementation process has been described using a structured notation. Such an approach provides the service architecture model and the processes to be implemented in a threat intelligence platform supporting orchestration and automation functionalities.

The adoption of a service architecture provides a set of advantages. It is extremely useful to fasten daily routine tasks: it removes repetitive actions burden from CTI team and unlocks time and resources for higher added value activities. In addition, automated workflows provide guidance to the CTI analysts, keeping them disciplined in following required steps and facilitating task execution through integration with intelligence tools and services: as a result, CTI team's efficiency increases.

Moreover, the implementation of the architecture allows to measure the effectiveness of CTI activities and, consequently, to collect metrics useful for improving performance. Finally, CTI analysts coordination is made easier, a particularly important aspect when the CTI team or part of it works remotely.

CTI service architecture has been designed to be technologically agnostic to avoid lock-in risks and vendor polarization. This is undeniably a strong suit, but its implementation could require a significant effort.

In addition, the CTI service architecture is subject to continuous improvements and optimizations based on experience gathered during its application in daily activities. With this approach, an increased level of automation is expected, especially on routine tasks, in order to improve the effectiveness of CTI analysts' efforts in core areas.

However, this work could stimulate debates among information sharing and trusted group entities peers discussion, raise the awareness on their level of maturity in producing effective CTI and let them identify gaps to address. Bridging the gaps, e.g. with the adoption of similar service oriented approaches for CTI capability, would increase the effectiveness of the information sharing by levelling-up the

ability to consume and produce intelligence, hence improving the cyber resilience of the whole ecosystem.

The integrated, fully defined and automatable processes described in the present paper can contribute to align CTI activities towards a common model, enhancing the effectiveness of collaboration and information sharing. Moreover, it aims to be advantageous for the quality metrics' perspective of the produced threat intelligence, to feed further threat led penetration testing, empowering their effectiveness and ensuring a level-playing field among the involved entities.

A more effective information sharing among financial entities would ease the application of DORA regulation, which is expected to increase the number of involved organizations and the amount of cyber related information exchanged between them. To a greater extent, a similar benefit is foreseen for critical infrastructures going to apply the NIS2 directive where an improvement of the information sharing is strongly recommended. Another example could be the TIBER-EU framework where a CTI service could help to produce organization targeted threat intelligence needed to design threat scenarios.

As a consequence, the proposed CTI service architecture could be a case study also for FMIs and may stimulate a beneficial collaboration among financial entities.

8. References

- [1] G. Research, «How to Respond to the 2022 Cyberthreat Landscape,» 2022. [Online]. Available: <https://www.gartner.com/en/documents/4013107>.
- [2] ENISA - The European Union Agency for Cybersecurity, «ENISA Threat Landscape 2020 - Cyber threat intelligence overview,» 20 October 2020. [Online]. Available: https://www.enisa.europa.eu/publications/cyberthreatintelligenceoverview/at_download/fullReport.
- [3] ENISA - The European Union Agency for Cybersecurity, «NIS Investment 2022,» November 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/nis-investments-2022/@@download/fullReport>.
- [4] European Systemic Risk Board (ESRB), «Mitigating systemic cyber risk,» 2022. [Online]. Available: <https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemicCyberRisk.220127~b6655fa027.en.pdf>.
- [5] ECB - European Central Bank, «CROE-Cyber Resilience Oversight Expectations,» [Online]. Available: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.
- [6] Opte Project, [Online]. Available: <https://www.opte.org/>.
- [7] S. Varga, J. Brynielsson e U. Franke, «Cyber-threat perception and risk management in the swedish financial sector,» *Computers & Security*, 2021.
- [8] P. Digregorio e B. Giannetto, «Development of Cyber Threat Intelligence apparatus in a central bank,» October 2019. [Online]. Available: https://www.bancaditalia.it/pubblicazioni/qef/2019-0517/QEF_517_19.pdf.
- [9] European Parliament and Council, «(NIS2) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union,» 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555>.
- [10] European Commission, «Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector,» 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1680779154997>.
- [11] R. Brown e P. Stirparo, «SANS 2022 Cyber Threat Intelligence Survey,» 2022.
- [12] European Systemic Risk Board (ESRB), «Systemic cyber risk,» 2020. [Online]. Available: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.
- [13] W. S. Brei, «Getting Intelligence Right: The Power of Logical Procedure,» Joint Military Intelligence College - Occasional Paper Number Two, Washington DC, 1996.
- [14] K. Sherman, *The Theory of Intelligence*, CIA Books, 1968.
- [15] Joint Chiefs of Staff (CJCS) of US Armed Forces, «Cyberspace Operations,» pp. 3-12, 2018.
- [16] M. Luchs e C. Doerr, «Measuring Your Cyber Threat Intelligence Maturity, a 5-minute introduction,» Hasso Lattner Institut.
- [17] K. Oosthoek e C. Doerr, «Cyber Threat Intelligence: A Product Without a Process?,» *International Journal of Intelligence and CounterIntelligence*.

- [18] B. Shin e P. B. Lowry, «A review and theoretical explanation of the ‘Cyberthreat-Intelligence (CTI) capability’ that needs to be fostered in information security practitioners and how this can be accomplished,» *Computers & Security*, vol. 92.
- [19] European Banking Authority (EBA), «Final Report on Guidelines on ICT and security risk management,» 2019. [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.
- [20] BoE - Bank of England, «CBEST Intelligence-Led Testing - Understanding Cyber Threat Intelligence Operations,» 2016. [Online]. Available: <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligenc>.
- [21] T. D. Wagner, K. Mahbub, E. Palomar e A. Abdullah, «Cyber threat intelligence sharing: Survey and research directions,» *Computers & Security*, vol. 87, 2019.
- [22] ENISA - The European Union Agency for Cybersecurity, «Exploring the opportunities and limitations of current Threat Intelligence Platforms,» March 2018. [Online]. Available: <https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-c>.
- [23] S. Brown, J. Gommers e O. Serrano, «From Cyber Security Information Sharing to Threat Management,» in *Computer Science, Engineering Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 2015.
- [24] ENISA, «Threat Landscape 2022,,» November 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport>.
- [25] G7, «G-7 FUNDAMENTAL ELEMENTS FOR THREAT-LED PENETRATION TESTING,» 2018. [Online]. Available: https://www.bancaditalia.it/media/notizie/2018/G7-FE-Threat-Led-Penetration-Testing.pdf?language_id=1.
- [26] BIS - Bank for International Settlements, «Guidance on cyber resilience for financial market infrastructures,» [Online]. Available: <https://www.bis.org/cpmi/publ/d146.pdf>.
- [27] ECB - European Central Bank, «TIBER-EU Guidance for Target Threat Intelligence Report,» July 2020. [Online]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.
- [28] M. Papazoglou e W. V. Den, «Service-oriented design and development methodology,» vol. 2(4), 2006.
- [29] M. Phythian, in *Understanding the Intelligence Cycle*, Routledge, 2013.
- [30] NIST- National Institute of Standards and Technology, «Special Publication 800-150 Guide to Cyber Threat Information Sharing,» 2016. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.
- [31] A. Ramsdale, S. Shiaeles e N. Kolokotronis, «A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages,» *Electronics*, vol. 9, 2020.
- [32] J. Ettinger, *Cyber Intelligence Tradecraft Report - The State of Cyber Intelligence Practices in the United States*, Carnegie Mellon University, 2019.
- [33] J. Hanson, «The Admiralty Code: A Cognitive Tool for Self-Directed Learning,» *International Journal of Learning, Teaching and Educational Research*, vol. 14, n. 1, pp. 97-115, 2015.
- [34] FIRST - Forum of Incident Response and Security Teams, «Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance - Version 1.0,» [Online]. Available: <https://www.first.org/ttp/docs/ttp-v1.pdf>.

- [35] G. Pernul e F. Menges, «Unifying Cyber Threat Intelligence,» in *International Conference on Trust and Privacy in Digital Business*, 2019.
- [36] R. M. Lee, «2020 SANS Cyber Threat Intelligence (CTI) Survey,» Febbraio 2020. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/threats/paper/39395..>
- [37] FIRST - Forum of Incident Response and Security Team, «Method and Methodology,» [Online]. Available: <https://www.first.org/global/sigs/cti/curriculum/methods-methodology>.
- [38] BoE - Bank of England, «CBEST Threat Intelligence-Led Assessments: Implementation Guide,» [Online]. Available: <https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide>.
- [39] J. E. a. N. Jenkinson, «Cyber risk is the new threat to financial stability,» International Monetary Found, 7 Dicembre 2020. [Online]. Available: <https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/>.
- [40] Computer Security Resource Center (CSRC) of National Institute of Standard and Technology (NIST), «Glossary,» [Online]. Available: <https://csrc.nist.gov/glossary>.
- [41] European Council, «Digital finance: Council adopts Digital Operational Resilience Act,» 2022. [Online]. Available: <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/>.

8. References

- [1] G. Research, «How to Respond to the 2022 Cyberthreat Landscape,» 2022. [Online]. Available: <https://www.gartner.com/en/documents/4013107>.
- [2] ENISA - The European Union Agency for Cybersecurity, «ENISA Threat Landscape 2020 - Cyber threat intelligence overview,» 20 October 2020. [Online]. Available: https://www.enisa.europa.eu/publications/cyberthreatintelligenceoverview/at_download/fullReport.
- [3] ENISA - The European Union Agency for Cybersecurity, «NIS Investment 2022,» November 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/nis-investments-2022/@@download/fullReport>.
- [4] European Systemic Risk Board (ESRB), «Mitigating systemic cyber risk,» 2022. [Online]. Available: <https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemicCyberRisk.220127~b6655fa027.en.pdf>.
- [5] ECB - European Central Bank, «CROE-Cyber Resilience Oversight Expectations,» [Online]. Available: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf.
- [6] Opte Project, [Online]. Available: <https://www.opte.org/>.
- [7] S. Varga, J. Brynielsson e U. Franke, «Cyber-threat perception and risk management in the swedish financial sector,» *Computers & Security*, 2021.
- [8] P. Digregorio e B. Giannetto, «Development of Cyber Threat Intelligence apparatus in a central bank,» October 2019. [Online]. Available: https://www.bancaditalia.it/pubblicazioni/qef/2019-0517/QEF_517_19.pdf.
- [9] European Parliament and Council, «(NIS2) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union,» 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555>.
- [10] European Commission, «Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector,» 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1680779154997>.
- [11] R. Brown e P. Stirparo, «SANS 2022 Cyber Threat Intelligence Survey,» 2022.
- [12] European Systemic Risk Board (ESRB), «Systemic cyber risk,» 2020. [Online]. Available: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.
- [13] W. S. Brei, «Getting Intelligence Right: The Power of Logical Procedure,» Joint Military Intelligence College - Occasional Paper Number Two, Washington DC, 1996.
- [14] K. Sherman, *The Theory of Intelligence*, CIA Books, 1968.
- [15] Joint Chiefs of Staff (CJCS) of US Armed Forces, «Cyberspace Operations,» pp. 3-12, 2018.
- [16] M. Luchs e C. Doerr, «Measuring Your Cyber Threat Intelligence Maturity, a 5-minute introduction,» Hasso Lattner Institut.
- [17] K. Oosthoek e C. Doerr, «Cyber Threat Intelligence: A Product Without a Process?,» *International Journal of Intelligence and CounterIntelligence*.

- [18] B. Shin e P. B. Lowry, «A review and theoretical explanation of the ‘Cyberthreat-Intelligence (CTI) capability’ that needs to be fostered in information security practitioners and how this can be accomplished,» *Computers & Security*, vol. 92.
- [19] European Banking Authority (EBA), «Final Report on Guidelines on ICT and security risk management,» 2019. [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.
- [20] BoE - Bank of England, «CBEST Intelligence-Led Testing - Understanding Cyber Threat Intelligence Operations,» 2016. [Online]. Available: <https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligenc>.
- [21] T. D. Wagner, K. Mahbub, E. Palomar e A. Abdullah, «Cyber threat intelligence sharing: Survey and research directions,» *Computers & Security*, vol. 87, 2019.
- [22] ENISA - The European Union Agency for Cybersecurity, «Exploring the opportunities and limitations of current Threat Intelligence Platforms,» March 2018. [Online]. Available: <https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-c>.
- [23] S. Brown, J. Gommers e O. Serrano, «From Cyber Security Information Sharing to Threat Management,» in *Computer Science, Engineering Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 2015.
- [24] ENISA, «Threat Landscape 2022,,» November 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport>.
- [25] G7, «G-7 FUNDAMENTAL ELEMENTS FOR THREAT-LED PENETRATION TESTING,» 2018. [Online]. Available: https://www.bancaditalia.it/media/notizie/2018/G7-FE-Threat-Led-Penetration-Testing.pdf?language_id=1.
- [26] BIS - Bank for International Settlements, «Guidance on cyber resilience for financial market infrastructures,» [Online]. Available: <https://www.bis.org/cpmi/publ/d146.pdf>.
- [27] ECB - European Central Bank, «TIBER-EU Guidance for Target Threat Intelligence Report,» July 2020. [Online]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.
- [28] M. Papazoglou e W. V. Den, «Service-oriented design and development methodology,» vol. 2(4), 2006.
- [29] M. Phythian, in *Understanding the Intelligence Cycle*, Routledge, 2013.
- [30] NIST- National Institute of Standards and Technology, «Special Publication 800-150 Guide to Cyber Threat Information Sharing,» 2016. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.
- [31] A. Ramsdale, S. Shiaeles e N. Kolokotronis, «A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages,» *Electronics*, vol. 9, 2020.
- [32] J. Ettinger, *Cyber Intelligence Tradecraft Report - The State of Cyber Intelligence Practices in the United States*, Carnegie Mellon University, 2019.
- [33] J. Hanson, «The Admiralty Code: A Cognitive Tool for Self-Directed Learning,» *International Journal of Learning, Teaching and Educational Research*, vol. 14, n. 1, pp. 97-115, 2015.
- [34] FIRST - Forum of Incident Response and Security Teams, «Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance - Version 1.0,» [Online]. Available: <https://www.first.org/ttp/docs/ttp-v1.pdf>.

- [35] G. Pernul e F. Menges, «Unifying Cyber Threat Intelligence,» in *International Conference on Trust and Privacy in Digital Business*, 2019.
- [36] R. M. Lee, «2020 SANS Cyber Threat Intelligence (CTI) Survey,» Febbraio 2020. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/threats/paper/39395..>
- [37] FIRST - Forum of Incident Response and Security Team, «Method and Methodology,» [Online]. Available: <https://www.first.org/global/sigs/cti/curriculum/methods-methodology>.
- [38] BoE - Bank of England, «CBEST Threat Intelligence-Led Assessments: Implementation Guide,» [Online]. Available: <https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide>.
- [39] J. E. a. N. Jenkinson, «Cyber risk is the new threat to financial stability,» International Monetary Found, 7 Dicembre 2020. [Online]. Available: <https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/>.
- [40] Computer Security Resource Center (CSRC) of National Institute of Standard and Technology (NIST), «Glossary,» [Online]. Available: <https://csrc.nist.gov/glossary>.
- [41] European Council, «Digital finance: Council adopts Digital Operational Resilience Act,» 2022. [Online]. Available: <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/>.

PAPERS PUBLISHED IN THE 'MARKETS, INFRASTRUCTURES, PAYMENT SYSTEMS' SERIES

- n. 1 TIPS - TARGET Instant Payment Settlement – The Pan-European Infrastructure for the Settlement of Instant Payments, *by Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi and Giovanni M. Sabelli* (INSTITUTIONAL ISSUES)
- n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *by Mauro Arcese, Domenico Di Giulio and Vitangelo Lasorella* (RESEARCH PAPERS)
- n. 3 Green Bonds: the Sovereign Issuers' Perspective, *by Raffaele Doronzo, Vittorio Siracusa and Stefano Antonelli* (RESEARCH PAPERS)
- n. 4 T2S - TARGET2-Securities – The pan-European platform for the settlement of securities in central bank money, *by Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci and Diego Toma* (INSTITUTIONAL ISSUES)
- n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *by Pietro Tiberi* (RESEARCH PAPERS)
- n. 6 Proposal for a common categorisation of IT incidents, *by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (INSTITUTIONAL ISSUES)
- n. 7 Inside the black box: tools for understanding cash circulation, *by Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene and Massimo Valentini* (RESEARCH PAPERS)
- n. 8 The impact of the pandemic on the use of payment instruments in Italy, *by Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini and Giorgia Rocco* (RESEARCH PAPERS) (in Italian)
- n. 9 TARGET2 – The European system for large-value payments settlement, *by Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina and Massimo Valentini* (INSTITUTIONAL ISSUES) (in Italian)
- n. 10 A digital euro: a contribution to the discussion on technical design choices, *by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi and Alessia Vita* (INSTITUTIONAL ISSUES)
- n. 11 From SMP to PEPP: a further look at the risk endogeneity of the Central Bank, *by Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo and Antonio Scalia* (RESEARCH PAPERS)
- n. 12 TLTROs and collateral availability in Italy, *by Annino Agnes, Paola Antilici and Gianluca Mosconi* (RESEARCH PAPERS) (in Italian)
- n. 13 Overview of central banks' in-house credit assessment systems in the euro area, *by Laura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi and Stephan Sauer* (INSTITUTIONAL ISSUES)

- n. 14 The strategic allocation and sustainability of central banks' investment, *by Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez and Giovanni Secondin* (RESEARCH PAPERS) (in Italian)
- n. 15 Climate and environmental risks: measuring the exposure of investments, *by Ivan Faiella, Enrico Bernardini, Johnny Di Giampaolo, Marco Fruzzetti, Simone Letta, Raffaele Loffredo and Davide Nasti* (RESEARCH PAPERS)
- n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, *by Massimiliano Renzetti, Fabrizio Dinacci and Ann Börestam* (RESEARCH PAPERS)
- n. 17 What's ahead for euro money market benchmarks?, *by Daniela Della Gatta* (INSTITUTIONAL ISSUES) (in Italian)
- n. 18 Cyber resilience per la continuità di servizio del sistema finanziario, *by Boris Giannetto and Antonino Fazio* (INSTITUTIONAL ISSUES) (in Italian)
- n. 19 Cross-Currency Settlement of Instant Payments in a Cross-Platform Context: a Proof of Concept, *by Massimiliano Renzetti, Andrea Dimartina, Riccardo Mancini, Giovanni Sabelli, Francesco Di Stasio, Carlo Palmers, Faisal Alhijawi, Erol Kaya, Christophe Piccarelle, Stuart Butler, Jwallant Vasani, Giancarlo Esposito, Alberto Tiberino and Manfredi Caracausi* (RESEARCH PAPERS)
- n. 20 Flash crashes on sovereign bond markets – EU evidence, *by Antoine Bouveret, Martin Haferkorn, Gaetano Marseglia and Onofrio Panzarino* (RESEARCH PAPERS)
- n. 21 Report on the payment attitudes of consumers in Italy: results from ECB surveys, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco* (INSTITUTIONAL ISSUES)
- n. 22 When financial innovation and sustainable finance meet: Sustainability-Linked Bonds, *by Paola Antilici, Gianluca Mosconi and Luigi Russo* (INSTITUTIONAL ISSUES) (in Italian)
- n. 23 Business models and pricing strategies in the market for ATM withdrawals, *by Guerino Ardizzi and Massimiliano Cologgi* (RESEARCH PAPERS)
- n. 24 Press news and social media in credit risk assessment: the experience of Banca d'Italia's In-house Credit Assessment System, *by Giulio Gariano and Gianluca Viggiano* (RESEARCH PAPERS)
- n. 25 The bonfire of banknotes, *by Michele Manna* (RESEARCH PAPERS)
- n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *by Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli and Ciro Oliviero* (RESEARCH PAPERS)
- n. 27 Statistical and forecasting use of electronic payment transactions: collaboration between Bank of Italy and Istat, *by Guerino Ardizzi and Alessandra Righi* (INSTITUTIONAL ISSUES) (in Italian)
- n. 28 TIPS: a zero-downtime platform powered by automation, *by Gianluca Caricato, Marco Capotosto, Silvio Orsini and Pietro Tiberi* (RESEARCH PAPERS)

- n. 29 TARGET2 analytical tools for regulatory compliance, *by Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini and Stefano Vespucci* (INSTITUTIONAL ISSUES)
- n. 30 The security of retail payment instruments: evidence from supervisory data, *by Massimiliano Cologgi* (RESEARCH PAPERS)
- n. 31 Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices, *by Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti and Benedetto Andrea De Vendictis* (INSTITUTIONAL ISSUES) (in Italian)
- n. 32 Banks' liquidity transformation rate: determinants and impact on lending, *by Raffaele Lenzi, Stefano Nobili, Filippo Perazzoli and Rosario Romeo* (RESEARCH PAPERS)
- n. 33 Investor behavior under market stress: evidence from the Italian sovereign bond market, *by Onofrio Panzarino* (RESEARCH PAPERS)
- n. 34 Siamese neural networks for detecting banknote printing defects, *by Katia Boria, Andrea Luciani, Sabina Marchetti and Marco Viticoli* (RESEARCH PAPERS) (in Italian)
- n. 35 Quantum safe payment systems, *by Elena Buccioli and Pietro Tiberi*
- n. 36 Investigating the determinants of corporate bond credit spreads in the euro area, *by Simone Letta and Pasquale Mirante*
- n. 37 Smart Derivative Contracts in DatalogMTL, *by Andrea Colombo, Luigi Bellomarini, Stefano Ceri and Eleonora Laurenza*
- n. 38 Making it through the (crypto) winter: facts, figures and policy issues, *by Guerino Ardizzi, Marco Bevilacqua, Emanuela Cerrato and Alberto Di Iorio*
- n. 39 The Emissions Trading System of the European Union (EU ETS), *by Mauro Bufano, Fabio Capasso, Johnny Di Giampaolo and Nicola Pellegrini* (in Italian)
- n. 40 Banknote migration and the estimation of circulation in euro area countries: the italian case, *by Claudio Doria, Gianluca Maddaloni, Giuseppina Marocchi, Ferdinando Sasso, Luca Serrai and Simonetta Zappa* (in Italian)
- n. 41 Assessing credit risk sensitivity to climate and energy shocks, *by Stefano Di Virgilio, Ivan Faiella, Alessandro Mistretta and Simone Narizzano*
- n. 42 Report on the payment attitudes of consumers in italy: results from the ecb space 2022 survey, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco*