A service architecture for an enhanced Cyber Threat Intelligence capability[*]

Giuseppe Amato, Simone Ciccarone , Pasquale Digregorio
and Giuseppe Natalucci

Bank of Italy, Directorate General for Information Technology, IT Planning Directorate, CERTBI[†]
name.surname@bancaditalia.it

Abstract

Numerous organizations have setup their own Cyber Threat Intelligence (CTI) capabilities in recent years and are now increasingly boosting their maturity level in this field. At the same time, both the digital transformation and the steadily growing info-sharing networks have been making available a critical mass of data and information suitable for CTI analysis. On the other hand, most of cyber intelligence units are struggling in handling the large number of heterogeneous information sources and in managing effectively the overwhelming quantity and variety of collectable data. The need to consolidate and automate CTI processes become a priority at this stage in order to improve CTI operation effectiveness and sustainability. However, the area of CTI service processes definition and automation appears still quite immature. In order to help addressing this gap, this work proposes a real case of a CTI service architecture implementation, along with a possible approach to design an operational model to achieve an enhanced CTI capability level.

Keywords

cyber threat intelligence, CTI service architecture, CTI service components, information triage, intelligence case, technical investigation, security orchestration and automation

1. Introduction

Recently, a growing number of companies and governmental entities started programs for introducing a CTI capability in their own organizations in order to tackle more effectively the challenges related to the evolving cyber threat landscape. As an organization decides to enhance its CTI capability to a higher maturity level in order to produce actionable intelligence, it becomes necessary to improve its CTI management processes to make them scalable, measurable, repeatable and automatable. In this scenario an internal dedicated team, supported by a significant investment in competence, processes and technology, is replacing standalone specialists or fully outsourced services.

Many organizations are still in the process to tailor CTI methodology, initially inherited from military and national intelligence sectors [1], to their enterprise cyber security management model and specific business context.

The adoption of a CTI service architecture is an enabling factor for organizations that aim to reach the highest capability maturity level. The following classification schema [2] 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;

[†] Authors are listed in alphabetical order. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the Bank of Italy or their sub-units

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 analyzed and improvements to maximize the outcomes are selected;
6. **Innovating**: new CTI method and tooling are developed and deployed beyond the state of the art.

In this context, well-defined and automatable processes represent a key factor to achieve an Optimizing maturity level as it frees up resources for the high complex tasks of a fully proactive cyber intelligence service and pave the way to self-improvement behavior of the Innovating level. Most of the CTI units with not well-defined processes appear struggling in the CTI automation area as a consequence of relatively young age of commercial threat intelligence and lack of a standard process [3].

CTI tools have evolved from basic toolkits and techniques to highly advanced platforms that provide semi-automated workflows to manage huge volumes of data and information from multiple open and closed sources. Even the modern cyber attacker ecosystem is settling into a new level of business automation: an example could be the cyber-crime 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, considered among the major factors blocking the CTI effectiveness [3]. Moreover, tailored intelligence production requires a complete knowledge of the business and the assets to protect, which are often considered sensitive information and not to be shared with external entities.

Numerous CTI organizations are now reaching a sufficient level of maturity about technical capabilities and basic processes implementation [4]. The next step, in order to face increased complexity and interdependencies [5], would be to refine and consolidate the practices. In this phase, all CTI teams are encouraged to share their results and experience. The long-term goal is a standard CTI process, which could be beneficial for all CTI organizations both in terms of cost reduction, e.g. enabling the usage of standard orchestration tools, and better interoperability. A further implicit benefit should be the levelling of the capability of the CTI teams towards a standard reference, which enhances the effectiveness of the collaboration and info-sharing.

At the current state of the art, this work proposes the first case of a CTI service architecture design, along with a possible multi-step approach the make it effectively implementable and usable in a real environment. In the first step a context diagram, that identifies external entities and their relationships with the CTI service, is defined. The second step provides the high level architecture layout, structured in three layers: the Entity layer, the Information layer, where a deliverable taxonomy has been also defined, and the Service layer. In the third step, the Service layer is developed in details, identifying processes, structural capabilities, operational tasks and the interactions among them. At this point, each process can be implemented: this work proposes the definition of the Input Triage process workflow, using a simplified standard language derived from the Business Process Modeling Notation (BPMN) [6].

2. Related Works

Few examples have been found in literature about detailed definition of CTI operational processes. Most paper focused on the definition of common CTI concept, principles and taxonomy [7] or on building blocks of a CTI infrastructure [8]. Many of recent papers address the crucial problem of CTI organization interoperability and info-sharing [9].

A kind of CTI capability is often included in some other security management processes like 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 but, typically, this is custom, proprietary and different on each platform [10] [11].

The Forum of Incident Response and Security Teams [12] proposes, for management of operational threat intelligence, the adoption of the F3EAD cycle (Find, Fix, Finish, Exploit, Analyse and Disseminate), an intelligence cycle commonly used within western military doctrines. The CBEST framework [13] includes a high-level implementation guide of threat intelligence phase but it is specific to red teaming activities purposes, as well as the TIBER-EU guidance [14] to produce target threat intelligence report.

Most of the issues related to the translation of CTI high-level operational models to practical and effective process are yet to be resolved [15]. Moreover, a reference standard model for inter/intra organization effective collaboration is still to be defined as well as a common threat management workflow [4] [10]. Also in the financial sector, several examples of CTI infrastructure model and requirements [16] are available, although there is a demand for a common detailed definition of the related operational model and workflows.

3. CTI service architecture

For an organization, making the switch from consuming to (also) generating threat intelligence is a key factor to enhance the chance to fully satisfy its own intelligence needs. The production of environmental-specific threat intelligence can be effective only by including in the intelligence life cycle the internal knowledge coming from the intrusion analysis activities, the mastery of organization’s technical architectures and the understanding of businesses processes. In this scenario, it is fundamental to identify the audience’s needs and translate them in intelligence requirements.

These ones can be defined as any subjects upon which there is a need for collecting data or producing intelligence to fill information gaps in organizational knowledge or in understanding the threat actors’ operational environment. On the base of requirements, is possible to determine the type of threat intelligence to generate and its goals. Furthermore, the intelligence production needs to take into account fundamental standards to measure its quality [17]. For this reason, an intelligence product should adhere to the following tenets: it should be available when consumer needs it (timeliness), based on the rational judgment of available information (accuracy), tailored to the specific needs of consumer and provided in forms suitable for immediate comprehension (usability).

In addition, it should answer questions to the fullest possible degree, specifying what remains unknown (completeness) and, finally, it should aid consumer in the accomplishment of its mission (relevance).

The intelligence production can be broken down in three categories: technical/tactical, operational and strategic [16]. Tactical intelligence is focused on technical information, and it is provided in IoCs (Indicators of Compromise), CVEs (common vulnerabilities and exposures), forensic evidences and technical descriptions. This may form part of the operational defense capabilities of an organization, as firewalls, detection technology and response capabilities are updated in near real time in response to changes in known indicators. Middle management typically consumes operational intelligence that is focused on the technical and context analysis. It deals with information related to Tools, Tactics, Techniques and Procedures (TTP’s) employed by an actor. Strategic intelligence is high-level information consumed by those that control the strategy of an organization, typically executive teams or management. The focus of this product is on aspects of a threat that may affect business decisions.

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, it is necessary to define consumers of the intelligence produced by the service and other entities that can collaborate to reach the goal. Operating under this assumption, it is possible to define boundaries between the service and its environment, showing the entities and their interactions with it.

The first party is the organization where the service is run, whose needs to be satisfied. In addition, to accomplish its goals, the service exchanges data and information with external counterparts and deals with commercial CTI providers. In the Figure 1, the identified parties and the involved interactions are reported.

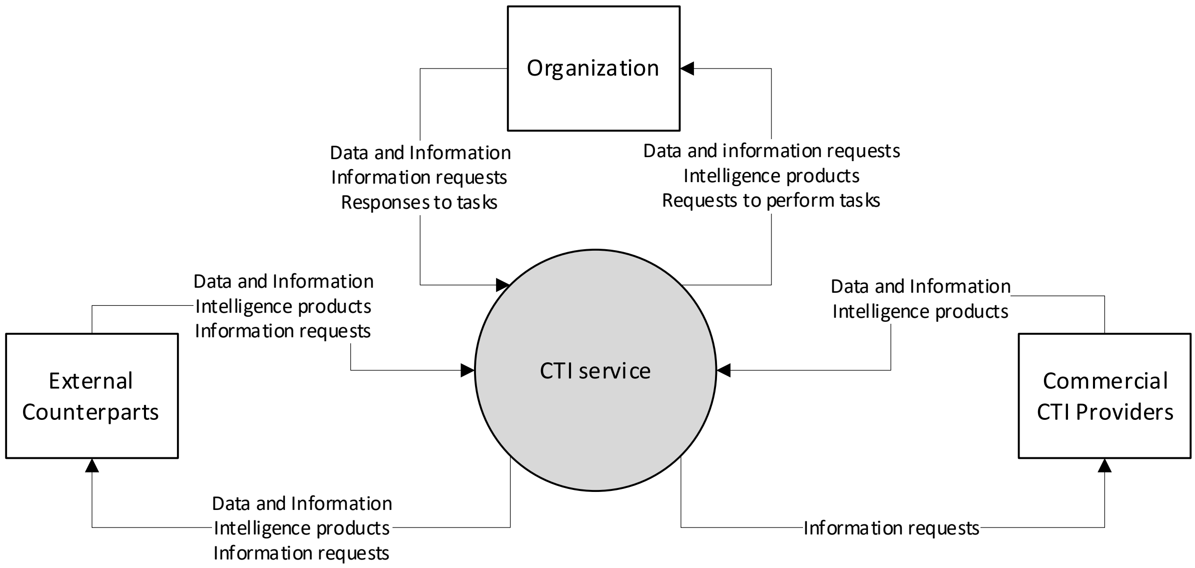

Figure 1: CTI service context diagram

3.1. Architecture design

The proposed service architecture is developed to cope all phases of the intelligence life cycle (planning, collection, processing, analysis, production and dissemination of intelligence). As in Figure 2, it is made up of three layers: Entities layer, Information layer and Service layer. In each layer, three specific kind of components take place: Entity, Information and Capability.

3.1.1. Entity layer

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

Constituency represents users that require to consume intelligence at strategic, operational or tactical level; they include C-Levels management, Corporate Security and Risk Management functions as well as, depending on the organization structure, specific Business Units. Security Operations are included among them too, and specifically they are the primary consumer of tactical threat intelligence and, at the same time, the producer of a specific input (Alert) ingested by the service. Finally, Constituency may proactively, or upon request, provide data and information to the CTI Service to accomplish its goals.

External Counterparts are all the external organizations that are allowed to interact with the CTI service in line with agreements established. 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 national institutions, bodies and agencies involved law enforcements, defence 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 security incident;
- **foreign and supranational institutions, bodies and agencies**: they represent non-national and non-commercial organizations with which cooperation agreements are established;

- **sharing communities**: they include formal/informal, sectorial/inter-sectorial, public/private groups aimed to share cyber threat data and information on voluntary basis [18].

Commercial CTI Providers make available commercial CTI services, providing deliverables and intelligence on-demand through Request for Information (RFI). Beside human-readable, they provide machine-readable threat intelligence (MRTI) [19]: 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.

3.1.2. Information layer

The Information layer includes all the data, information and intelligence products that the CTI Service handles as input or output towards entities: alert, RFI and deliverable.

An Alert is raised when there is an evidence related to a running or potential threat for the Constituency: it may come from the Security Operations Center or it can be produced autonomously by a component of CTI service.

A Request For Information (or RFI) is forged when there is the need to fill an information gap. 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). It may be either an input from Entities (Constituency or External Counterparts) or an output sent towards them in order to allow the CTI service to build intelligence around running or potential threats.

A Deliverable is the CTI product used to transfer effectively information or knowledge related to one or more cyber threats. It can be 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 when pre-established conditions happens (periodically or triggered by specific events) or in reply to an RFI. Depending on the expected consumer, the category of the intelligence to be transferred and its timing requirements, the following taxonomy has been developed:

- **Security Alert**: artefact used to provide to the Constituency warnings about imminent or on going cyber threats and suggesting short-term recommended course of actions;

- **Security Advisory**: artefact used to inform Constituency's IT operations teams about new vulnerabilities or threat actors' TTPs that can be exploited against the Constituency assets and to propose preventive defensive actions;

- **Flash Reporting**: unstructured intelligence product used to inform Constituency's or External Counterparts' middle management decision makers on a specific threats. It includes recommendations on preventive or reactive actions;

- **Threat Bulletin**: structured intelligence product focused on a specific cyber threat, a particular threat actor or a recent offensive cyber operation;

- **Periodic CTI Report**: structured intelligence product used to provide to decision makers a periodic update of the cyber threat landscape, analysis of the recent relevant events along with cyber threats trends and predictions;

- **Executive Brief**: unstructured intelligence product used to inform Constituency's C-level on a specific imminent or on-going threat.

3.1.3. Service layer

This layer includes all the capabilities composing the CTI service.

Input Interface component is the entry point for the incoming flows. It validates the source and categorizes the content of the input before invoking the appropriate process to handle it. In the same way, outgoing flows have a single exit point, the Output Interface component that triggers the action to deliver the information or to make requests.

Internal CTI Production is where information and intelligence are produced: it can require constituency to perform tasks, in order to fill information gaps at tactical and operational level, through Reactive CTI Collection component.

Proactive CTI Collection monitors the cyberspace looking after data and information related to threats that could potentially affect the Constituency.

CTI Service Management represents the component that groups several structural capabilities needed to manage the service and its internal knowledge base, activities and resources.

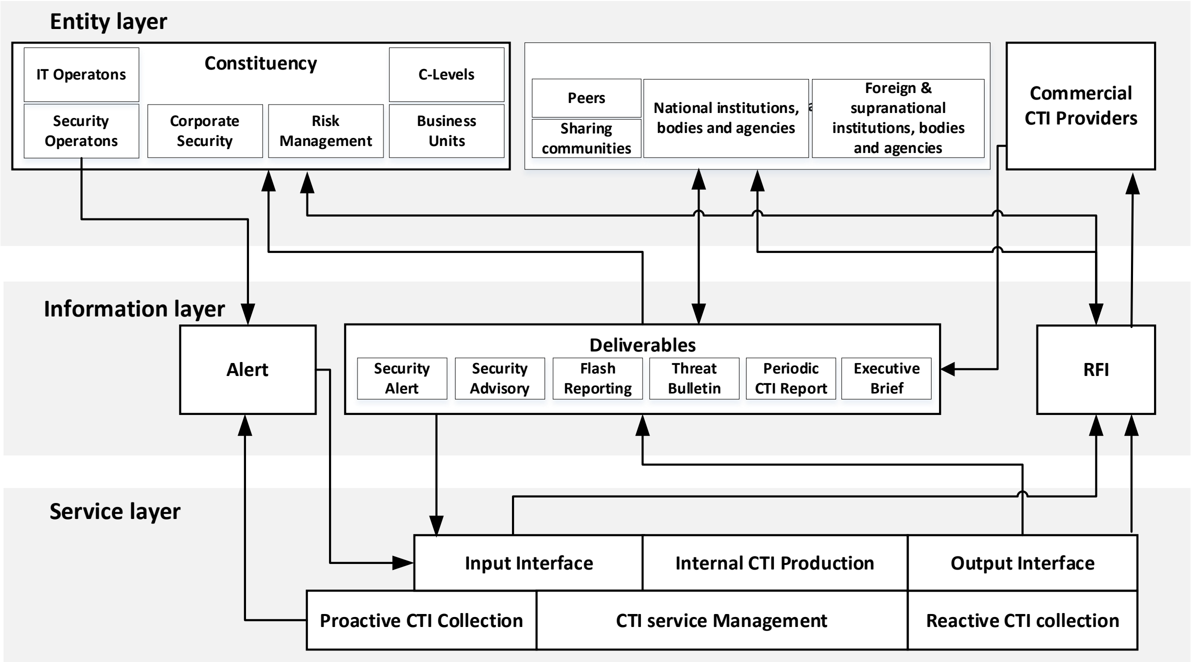

Figure 2: Service architecture

3.2. 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 operations teams.

Different components can interact in two ways: by information flows and by operational flows. Information flows carries 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 3 and described in the following.

Input interface is composed by the Input Triage and the Incoming RFI handling processes. The Input Triage process, described in detail in chapter 5, analyzes incoming deliverables, alerts and RFIs in order to prioritize them and provide information needed to determine resulting actions; in case of deliverables and alerts, the decision to send them directly towards the output interface or trigger Internal CTI Production component is taken.

Input RFIs, instead, are preliminary checked and routed to the devoted CTI 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 the information to be shared or requested to Entities: mapping the content to the intended recipients and identifying the right procedures to send/request the information (i.e. through which communication channel and with which level of confidentiality and shareability to 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 analyzing a threat among the internal or external perimeters or by setting up a specific investigation environment. A technical investigator can escalate and ask to open an Intelligence Case if needed.

An Intelligence Case analyzes a potential or running cyber threat in order to determine the appropriate defensive or preventive courses of action and strategies at organizational level 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 that has the responsibility to coordinate all the activities and interactions needed to solve the case. If needed an Intelligence Case can trigger one or more Technical Investigations.

Reactive CTI Collection is used by Internal CTI Production to dispatch requests to operations teams of its organization: Technical Investigation process can start tasks to be requested to Security Operations teams or to IT Operations teams. Intelligence Case process can open task to be dispatched to Cyber Intelligence Operations that performs active research and collection of information (in or through the cyberspace) when specific know-how 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.

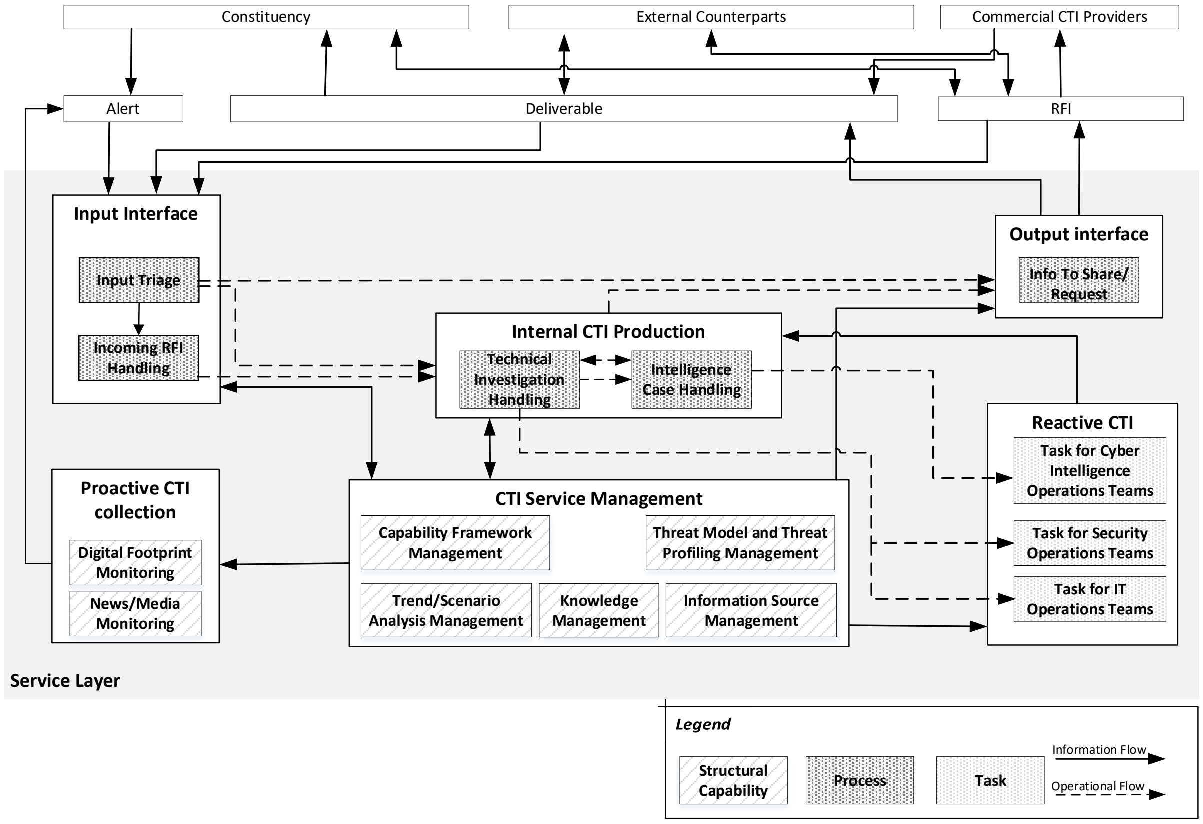

Figure 3: Service layer components

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 manage an information source repository containing their attributes (reliability score, agreements and obligations, allowed and expected information, etc.);
- **Capability Framework Management**, which is responsible for the CTI service architecture review and maintenance and for the provisioning and allocation of resources needed to perform processes and to reach the 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 organization's threat models and threat actors' profiles.

3.3. Input triage process

Organizations with higher CTI maturity level require a formal, holistic, transparent, and repeatable process for evaluating data sources and input information [20]. This process must balance the need to empower the information collection capabilities with the available information processing resources, by filtering, prioritizing and validating the information that are relevant to protect the Constituency.

Input information has to be assessed, at first in terms of source identification and input data compliance. Afterwards, a qualitative and quantitative evaluation is performed to define the information relevancy and to calculate a priority score (valorization); nevertheless, alerts from Security Operations can be considered a pre-validated inputs, that are immediately forwarded to the valorization phase.

As shown in Figure 4, 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. In case the input includes a RFI, the CTI Incoming RFI Management process is invoked (2.a): input is evaluated, classified, and eventually replied, depending on the evaluation outcomes. CTI Incoming RFI Management triggers further processes with the purpose to produce the requested information with the format and timing agreed with the sender. On the other hand, if the input is an information, it is stored in the knowledge repository (2.b), and it is evaluated against its relevancy (3). Finally, in case of Alert, input is automatically considered as relevant and it is sent directly to the step (4).

An information is considered as "relevant" when it satisfies one or more collection intelligence requirements: these ones can be identified by considering the available Threat Model and evaluating the proximity to the Constituency of the potential threat related to the information handled, referred as Threat Proximity (TP). This indicator measures the "distance" between the entities affected by the event and the Constituency. As precondition, it is needed to define a custom metric, for example based on criteria related to involved business sectors, geographical location and the level of connection to the organization's supply chain.

Relevant information is then valorized (4) by the use of several scoring frameworks, with the purpose to determine the more appropriate handling actions: at this step the information stored in the Knowledge Management repository is enriched with the vector {AS, TS, PS}, where each value is defined below:

- **Admiralty Scoring (AS)**: it uses the Admiralty Code [20] [21] to score the input information credibility and the information source reliability. Each piece of evidence according to the expected reliability of the source in providing accurate information on this occasion (rated from A to F) and the likely validity of the claim (rated from 1 to 6).

- **Threat Scoring (TS)**: it represents how much the threat is worrisome. Its calculation considers both the Threat Level (a score related to the Threat Actor, provided by the capability Threat Model and Profiling Management) and the confidence on the threat truthfulness.
- **Priority Scoring (PS)**: it classifies the threat by the priority it has to be dealt with. It is calculated by considering Threat Score and Threat Proximity.

Finally, the information confidentiality is classified according to national law, internal policy and the Traffic Light Protocol (TLP) [22]. Once the information is dissected, analyzed and valorized, the appropriate process (5.a, 5.b or 5.c) is triggered:

(5.a) invoke the Info To Share/Request process to share the received information with the Constituency or the 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 details: a) check for unwanted disclosures in the deliverable, alert or RFI to submit; b) package them in the appropriate format for the intended recipients; c) deliver them and redirect any feedbacks received by the recipients to the appropriate service component.

(5.b) start a Technical Investigation, to provide tactical information deliverables by analyzing a threat among the internal or external perimeters or by setting up a specific investigation environment.

(5.c) open an Intelligence Case, to analyzes a potential or running cyber threat in order to determine the appropriate defensive or preventive courses of action and strategies at organizational level against the threat; the Intelligence Case can be used to build knowledge in order to reduce the uncertainty about relevant cyberspace phenomena.

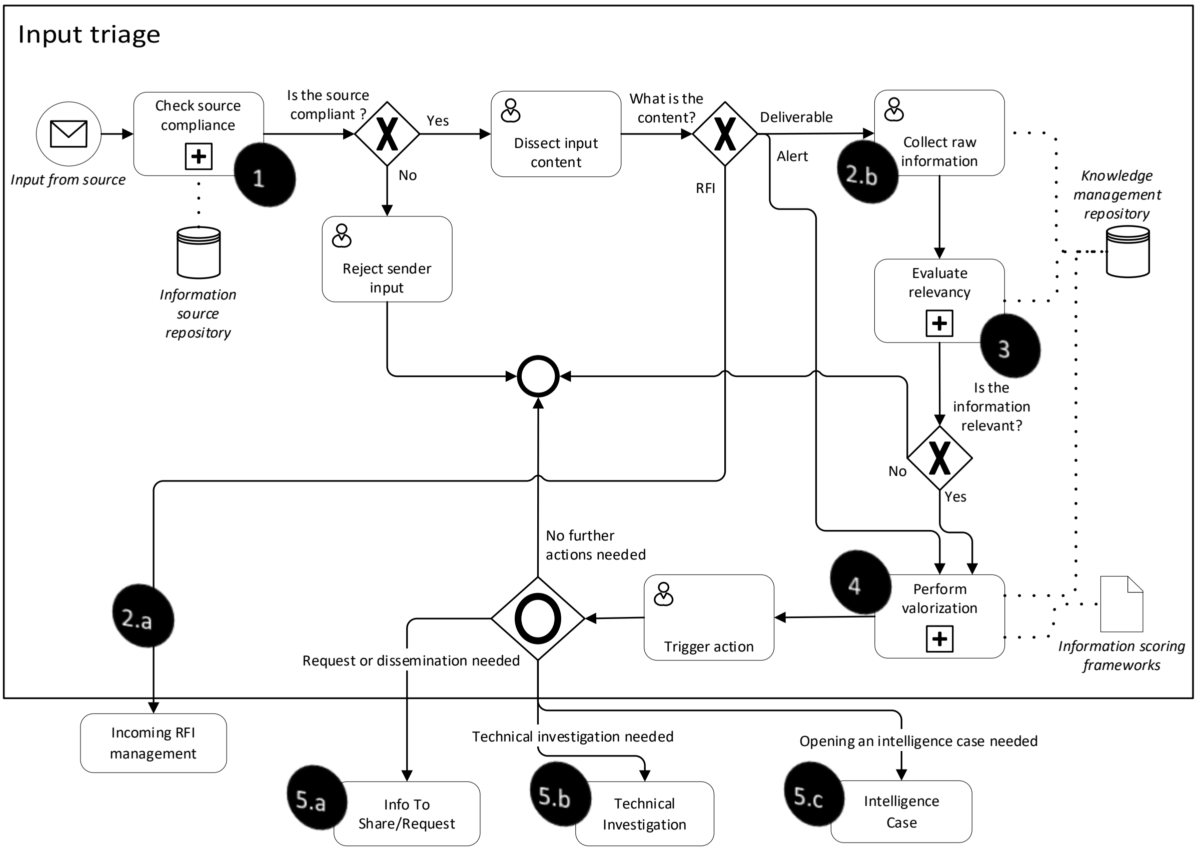

Figure 4: Input triage

4. Conclusions

An enhanced cyber threat intelligence capability represents a game changer for organizations to empower the effectiveness of their own cyber defense, but it also increases the complexity of their cyber security 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 evolve their CTI capabilities and interoperate to face cyber-attacks that are evolving and becoming more sophisticated, widespread and undetected.

In order to address these needs, this work proposes a vendor-agnostic service model not affected by technical bias. The service architecture has been developed using a top-down approach to define specific processes, structural capabilities and operational tasks. Each process has been developed in order to be smoothly translated in an automated workflow: as proof of this, a practical implementation of the input triage process has been developed and described using a standard business process modeling notation. This approach makes the service architecture ready to be implemented in a security orchestration and automation (SOA) enabled threat intelligence platform.

The integrated, fully defined and automatable processes presented in this work could contribute in aligning the CTI activities towards a standard reference, enhancing the effectiveness of the collaboration and info-sharing. Moreover, it aims to be beneficial to a leveled quality of the threat intelligence generated to feed Red Team testing operations, empowering their effectiveness and ensuring a level playing field among the involved entities.

5. References

[1] Joint Chiefs of Staff (CJCS) of US Armed Forces, Cyberspace Operations - Joint Publication 3-12, 2018.

[2] M. Luchs and C. Doerr, "Measuring Your Cyber Threat Intelligence Maturity," Hasso Plattner Institut and Delft University of Technology.

[3] R. M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," Febbraio 2020. URL: https://www.sans.org/reading-room/whitepapers/threats/paper/39395.

[4] ENISA - The European Union Agency for Cybersecurity, "ENISA Threat Landscape 2020 - Cyber threat intelligence overview," 20 October 2020. URL: https://www.enisa.europa.eu/publications/cyberthreatintelligenceoverview/at_download/fullReport.

[5] B. Shin and 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, Volume 92, May 2020.

[6] URL: https://www.omg.org/spec/BPMN/

[7] F. Menges and G. Pernul, "Unifying Cyber Threat Intelligence," in International Conference on Trust and Privacy in Digital Business, 2019.

[8] Bank of England, "CBEST Intelligence-Led Testing - Understanding Cyber Threat Intelligence Operations," 2016. URL: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf.

[9] T. D. Wagner, K. Mahbub, E. Palomar and A. Abdullah, "Cyber threat intelligence sharing: Survey and research directions," in Computers & Security Volume 87, 2019.

[10] ENISA - The European Union Agency for Cybersecurity, "Exploring the opportunities and limitations of current Threat Intelligence Platforms," 26 March 2018. URL: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms/at_download/fullReport.

[11] S. Brown, J. Gommers and 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.

[12] FIRST - Forum of Incident Response and Security Teams, "Method and Methodology". URL: https://www.first.org/global/sigs/cti/curriculum/methods-methodology.

[13] Bank of England, "CBEST Threat Intelligence-Led Assessments: Implementation Guide". URL: https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide.

[14] European Central Bank, "TIBER-EU Guidance for Target Threat Intelligence Report," July 2020. URL: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.

[15] K. Oosthoek and C. Doerr, "Cyber Threat Intelligence: A Product Without a Process?". International Journal of Intelligence and CounterIntelligence.

[16] P. Digregorio and B. Giannetto, "Development of Cyber Threat Intelligence apparatus in a central bank," Ottobre 2019. URL: https://www.bancaditalia.it/pubblicazioni/qef/2019-0517/QEF_517_19.pdf.

[17] W. S. Brei, "Getting Intelligence Right: The Power of Logical Procedure," Joint Military Intelligence College - Occasional Paper Number Two, Washington DC, 1996.

[18] NIST, "NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing," 2016. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

[19] A. Ramsdale, S. Shiaeles and N. Kolokotronis, "A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages," Electronics, Volume 9, 2020.

[20] J. Ettinger, "Cyber IntelligenceTradecraft Report - The State of Cyber Intelligence Practices in the United States," Carnegie Mellon University, 2019.

[21] J. M. Hanson, "The Admiralty Code: A Cognitive Tool for Self-Directed Learning," International Journal of Learning, Teaching and Educational Research, vol. 14, no. 1, pp. 97-115, 2015.

[22] FIRST - Forum of Incident Response and Security Teams, "Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance - Version 1.0". URL: https://www.first.org/tlp/docs/tlp-v1.pdf.