





# Structured Direction and Planning for Cyber Threat Intelligence in the Brazilian Financial System

Pedro Henrique Silva Gontijo <sup>\*†</sup>, Felipe Barreto de Oliveira <sup>†</sup>, Robson de Oliveira Albuquerque <sup>†‡</sup>,  
 João José Costa Gondim <sup>†</sup>  
 University of Brasilia - UnB<sup>†</sup>  
 Catholic University of Brasilia - UCB<sup>‡</sup>  
 Email: gontijo.unb@gmail.com<sup>\*†</sup>; felipe.oliveira@redes.unb.br<sup>†</sup>; robson@redes.unb.br<sup>†‡</sup>; gondim@unb.br<sup>†</sup>

**Abstract**—The increasing sophistication of cyber threats requires more structured and strategic threat intelligence planning, especially in Critical Infrastructures (CIs) such as the Brazilian Financial System (SFN). This paper presents a structured method for the Direction and Planning (DP) phase of Cyber Threat Intelligence (CTI). Inspired by classical intelligence doctrine, the methodology employs five integrated stages—Strategic Alignment, Threat Mapping, Priority Intelligence Requirements (PIRs), Requests for Information (RFIs), and Collection Plan—to transform organizational risk profiles into actionable requirements. Utilizing the OpenCTI platform in a conceptual case study, a baseline dataset of over 147,000 STIX domain objects was processed using the structured DP filter. This process reduced the volume to only 415 SFN-relevant objects, achieving approximately 99.7% reduction of the initial data. Results confirm that the proposed methodology significantly mitigates noise, provides methodological traceability, and generates intelligence aligned with SFN regulatory requirements. The main contribution is a replicable and adaptable model that comprehensively integrates all critical criteria for the secure operation of financial infrastructures.

**Keywords**—CTI; Critical Infrastructures; Brazilian Financial System; Direction and Planning; PIR.

## I. Introduction

Cyber attacks represent a critical threat to the integrity of Critical Infrastructures (CIs) [1], particularly the sensitive Brazilian National Financial System (SFN) [2]. Although Cyber Threat Intelligence (CTI) is essential for anticipating risks, its efficacy is hampered by methodological gaps in the initial Direction and Planning (DP) phase [3], [4], [5]. This negligence in defining strategic priorities leads to information overload, compromising relevance and actionability [6].

This work addresses this gap by proposing a structured, systematic, and replicable method for CTI Di-

rection and Planning phase, applied conceptually to the SFN. Inspired by classical intelligence doctrine [7], [8], [9], [10], [11], [12], the proposed five-stage process transforms high-level organizational risks into prioritized collection requirements, ensuring alignment with the risks faced by the SFN [13], [14].

The method was validated in the OpenCTI environment, where the structured Direction and Planning process significantly reduced informational noise from a large baseline dataset. The primary contribution of this work is a model that integrates a structured methodology for the DP phase, a quantitative focus on noise reduction and intelligence quality, and alignment with SFN regulatory mandates based on an Asset and Risk-Centric approach.

The rest of this work is organized as follows. Section II, reviews related works and identifies the methodological gap addressed by this study. Section III, presents the proposed five-stage methodology for the Direction and Planning phase of CTI. Section IV, describes a conceptual case study in the OpenCTI environment and presents the results of the structured noise reduction process. Section V discusses the findings, acknowledges limitations, and outlines directions for future work. Finally, Section VI concludes the study by summarizing its contributions and regulatory alignment.

## II. Related Work and Research Gap

The escalating frequency and sophistication of cyber threats necessitate highly relevant CTI, especially for CIs [1] such as the SFN [15], [16], [17], [2]. However, a significant methodological void persists in the upstream stages of the intelligence cycle, particularly the Direction and Planning phase. Initiatives often prioritize downstream activities (collection, analysis, dissem-

ination), resulting in an overwhelming volume of non-contextualized data that dilutes actionable intelligence [6], [5].

To delineate the unique contribution of this research, we evaluate key academic and regulatory works against six critical dimensions, summarized in Table I: Direction and Planning (DP), Structured Method (SM), Practical Application (PA), SFN Focus, Noise and Quality Focus (NQ Focus), and Asset and Risk-Centric Approach (AR Focus).

The criterion Practical Application refers to the empirical execution of the methodology on a working Threat Intelligence Platform (TIP), differentiating it from purely theoretical models. As detailed in Section IV, our inclusion is based on the instantiation of the method in OpenCTI, enabling the generation of quantitative results, characterizing it as a conceptual case study.

### A. Comparative Analysis

Academic efforts commonly prioritize data remediation rather than prevention. This is observed in surveys like Tounsi & Rais [6], which confirm the information overload challenge, and in platforms like the Enriched Threat Intelligence Platform (ETIP) proposed by Faiella et al., which utilizes threat scoring for IoC quality improvement in the processing phase [18]. Similarly, quality-focused methodologies by Melo e Silva et al. and Silva et al. [4], [5] use the intelligence cycle to define data gaps, but concentrate on post-collection remediation and lack practical validation or regulatory SFN alignment.

Methodologies addressing program structure, such as the framework proposed by López & Awad [3], provide a Structured Method for establishing a Threat Intelligence Program, which is inherently Asset and Risk-Centric. Nevertheless, this work remains conceptual and lacks application testing against real data volumes in a regulated financial environment.

Operational and Regulatory models emphasize Practical Application and Asset and Risk-Centricity:

- *Frameworks for Testing:* Mechanisms like the UK’s CBEST [19] and the European DORA / TIBER-EU [20], [21] mandate Threat-Led Penetration Testing (TLPT). This approach requires DP to define targeted scenarios and TIBER-EU provides a Structured Method for the test execution itself, aimed at testing resilience against critical functions [19], [21]. However, they do not provide a methodology for continuous internal CTI program establishment aimed at massive noise reduction. The FS-ISAC [22] also operates on an SFN context, providing practical sharing mechanisms, but is not an SM

for DP. The same applies to CISA [23] guidance on CIs.

- *Brazilian SFN Regulations:* Res. CMN 4.893/2021 [14] and Res. BCB 85/2021 [13] demand explicit cyber security objectives and implementation plans. They require institutions to classify data by relevance and align policies with the risk profile. While practical, these are regulatory mandates defining the *what* and *why*, but they do not constitute a structured CTI methodology for DP nor offer mechanisms for data feed noise reduction.

The reviewed literature confirms a critical research gap: the lack of a comprehensive solution combining Structured Method for Direction and Planning with quantitative Noise Reduction and simultaneous alignment with the SFN regulatory context. This paper introduces a comprehensive solution that integrates all six dimensions, reducing a large initial dataset to a small, highly relevant subset. Table I summarizes how the reviewed works compare across the six critical dimensions introduced in this study.

Table I: Qualitative Comparison with Related Work

Reference	DP	SM	PA	SFN	NQ Focus	AR Focus
Tounsi & Rais (2018) [6]	×	×	×	×	✓	×
Faiella et al. (2019) [18]	×	×	✓	×	✓	×
Leszczyna & Wróbel (2019) [24]	×	×	✓	×	×	✓
Melo e Silva et. al. (2020) [4]	✓	×	×	×	✓	×
Silva et al. (2023) [5]	✓	✓	×	×	✓	×
López & Awad (2021) [3]	✓	✓	×	×	×	✓
FS-ISAC [22]	×	×	✓	✓	×	✓
CISA (USA) [23]	×	×	✓	×	×	✓
CBEST (BoE) [19]	✓	✓	✓	×	×	✓
DORA / TIBER-EU [20], [21]	✓	✓	✓	×	×	✓
Res. CMN 4.893 (2021) [14]	×	×	✓	✓	×	✓
Res. BCB 85 (2021) [13]	×	×	✓	✓	×	✓
<b>This Article</b>	✓	✓	✓	✓	✓	✓

### III. Proposed Methodology

The proposed method organizes a structured and replicable process for CTI Direction and Planning. The objective is to transform strategic direction into practical collection tasks, mitigating the informational noise problem identified in the literature [6]. This comprehensive methodology encompasses the Direction and Planning phase, serving as the foundational first step of the classical intelligence cycle (Direction and Planning, Collection, Analysis, and Dissemination) [7], [8], [9], [10], [11], [12], and ensuring continuous relevance and adaptation.

The strategy, partly inspired by openly available industry guidelines such as the Red Hat Developing PIRs

and the Feedly PIR Blueprint [25] [26], is structured into five integrated stages: (i) Strategic Alignment; (ii) Threat Mapping; (iii) Definition of Priority Intelligence Requirements (PIRs); (iv) Formulation of Requests for Information (RFIs); and (v) Development of the Collection Plan. The integration and sequential flow of these five stages are visually represented in Figure 1, demonstrating traceability from high-level strategic objectives to concrete tactical collection tasks.

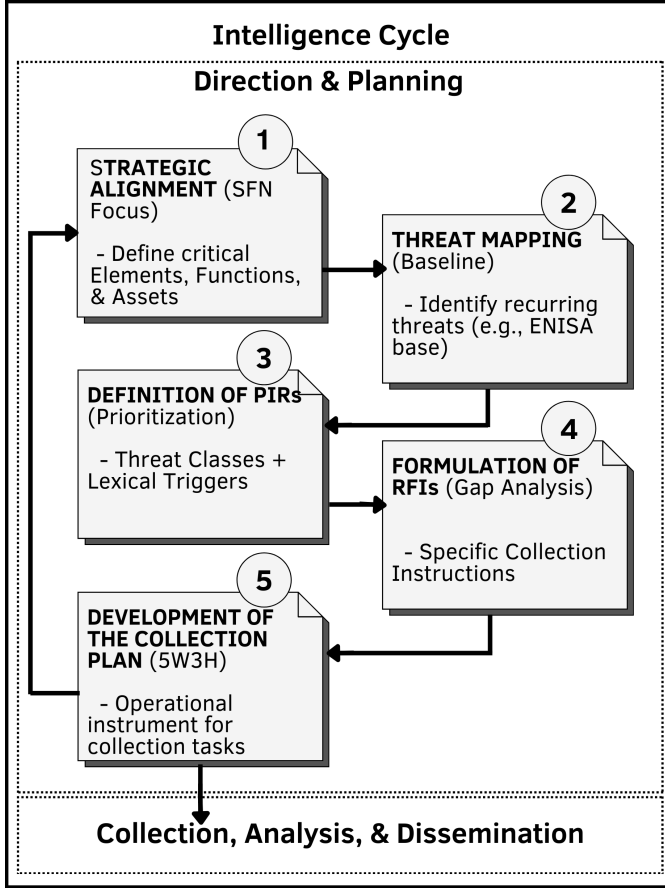


Figure 1: Proposed Structured Methodology for CTI Direction and Planning.

#### A. Strategic Alignment

Stage 1 defines the scope of the intelligence program by linking CTI activities directly to the organization's critical assets and business functions. This ensures CTI priorities are aligned with risk management policies, fulfilling mandates such as the establishment of metrics and indicators of effectiveness required by the SFN [13], [14].

#### B. Threat Mapping

Threat Mapping identifies and classifies adversarial activities relevant to the organization's scope defined

in Stage 1. It correlates the identified critical assets with relevant threat classes, creating a prioritized taxonomy of threats (Table II), which serves as the foundation for defining lexical filters in the later stages of the methodology.

#### C. Definition of PIRs

PIRs convert high-level threats and risks identified in Stage 2 into specific intelligence questions that require an answer from the CTI function. By nature, PIRs are strategic, ensuring that all collection efforts are focused on critical knowledge gaps. This process is crucial for preventing the indiscriminate collection of generic threat data, which is the main source of informational noise [6].

Table II: PIR Taxonomy by Threat Class and Lexical Triggers

PIR	Threat Class	Keywords
PIR-1	DDoS	ddos; denial of service
PIR-2	Data-related threats (exposure/leak)	data leak; data exposure; data loss; exposed data; database dump
PIR-3	Social Engineering	phishing; smishing; vishing; social engineering; pretexting
PIR-4	Fraud	fraud; scam; account takeover; atm skimming; carding; chargeback
PIR-5	Ransomware	ransomware
PIR-6	Malware (general)	malware; trojan; infostealer; loader; botnet; backdoor
PIR-7	Supply Chain / Third-Party Attacks	supply chain; third-party; dependency attack; software supply chain
PIR-8	Intrusion	initial access; webshell; living off the land; lateral movement; persistence
PIR-9	Web and Mobile App Threats	sql injection; xss; csrf; deserialization; rce; web attack
PIR-10	Emerging / Transversal	ai; llm; deepfake; quantum; blockchain; crypto assets/currency; defi

#### D. Formulation of RFIs

RFIs operationalize the PIRs by defining specific technical and operational details required for collection. RFIs specify the required time constraints, reporting standards (e.g., STIX [18]), and dissemination needs. This ensures collected data meets the core intelligence attributes of relevance and timeliness.

#### E. Development of the Collection Plan

The final stage translates the approved RFIs into explicit directives for technical collection, exploitation, and reporting. This plan specifies the collection assets

(feeds, sensors, OSINT tools), ensuring a multidisciplinary approach [8]. The Collection Plan mandates the application of lexical filters (keywords derived from PIRs) to contextualize raw data, directly contributing to quantitative noise reduction.

To ensure clarity and completeness, this structured approach utilizes the widely recognized 5W3H methodology [27]. This framework is employed across various disciplines to obtain a complete description and contextualization of a topic, adopted here to ensure comprehensive definition of operational parameters for CTI collection efforts. The adaptation of the 5W3H framework for the Collection Plan is detailed in Table III.

Table III: 5W3H Method for the Collection Plan

Element	Application in Collection Plan
What	Defines the specific threats or data to be collected (e.g., indicators, TTPs).
Why	Describes the motivation or required impact (e.g., risk mitigation, PIR fulfillment).
Where	Specifies the source of collection (e.g., OSINT feeds, commercial platforms).
How	Describes the format in which the CTI product will be shared.
When	Specifies time frames, frequency of collection, and reporting deadlines.
Who	Specifies the stakeholders who will receive the disseminated CTI.
How Much	Refers to the cost or allocation of resources (e.g., budget, tool usage).
How Long	Description of the required duration for the collection effort or validity of the intelligence.

This structured approach, exemplified in Figure 2, provides clear guidance on resource allocation and ensures full alignment between the CTI function and the SFN’s critical asset protection needs.

#### IV. Conceptual Case Study and Results

This section details the conceptual case study conducted to validate the structured Direction and Planning methodology proposed in this work. The primary goal was to demonstrate the method’s capacity for quantitative noise reduction and alignment with the SFN’s specific context.

##### A. Study Setup and Data Baseline

The methodological validation was conducted using the OpenCTI platform, a TIP chosen for its robust capabilities in managing CTI knowledge and enabling a holistic approach. A custom rule-based classification engine was implemented within the platform to support the process.

The ingestion process relied on specific connectors to build the data baseline:

- *AlienVault/OTX*: Used for collecting broad OSINT and general indicators.

- *MITRE ATT&CK*: Used for categorizing TTPs (Tactics, Techniques, and Procedures), facilitating Threat Mapping and tactical alignment.

The resulting baseline dataset, collected in August 2025, exceeded 147,000 STIX Domain Objects (SDOs), comprising 3,675 Reports, 964 Intrusion Sets, 3,513 Malware, 137,773 Indicators, and 1,596 Attack Patterns. This initial dataset contained generalized data not filtered for the financial sector.

##### B. Threat Context and PIRs Taxonomy

The definition of the 10 PIR families was based on Strategic Alignment (Stage 1) and Threat Mapping (Stage 2). Threat Mapping was grounded in the analysis of multiple threat intelligence reports relevant to the financial sector [28], [29], [30], [31], [32]. Among them, the ENISA Threat Landscape – Finance Sector [32] was used as a primary reference, as it synthesizes and consolidates the key threats identified across these sources, as illustrated in (Figure 3).

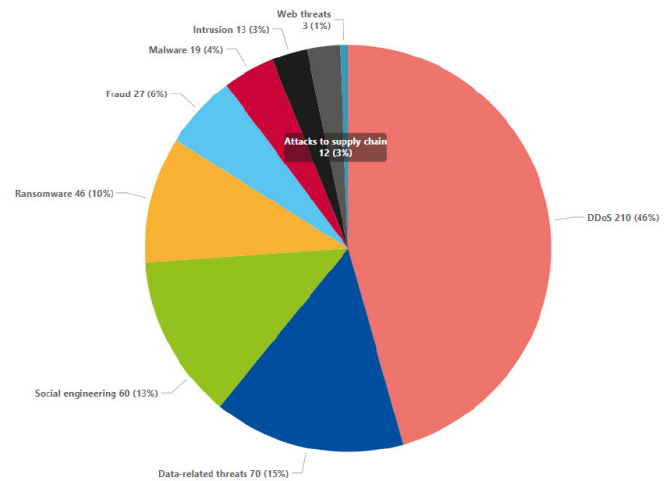


Figure 3: Observed threats in the European financial sector 2023–2024 [32].

The resulting Taxonomy of PIRs (Table II), whose keywords were derived using a Large Language Model (LLM) based on the analysis of these referenced reports, served as the basis for the lexical filters applied during the Direction and Planning phase.

##### C. Results of Informational Noise Reduction

The core methodological phase, DP, was operationalized through a two-step filtering mechanism based on lexical triggers derived from the taxonomy of PIRs. This pipeline applied contextual labels and progressively split the dataset to isolate SFN-relevant threats.

The two-tier filtration process was defined as:



Table IV: STIX Object Reduction and Informational Density

Class	Base (n)	SFN (n)	Retention vs Base
Reports	3,675	17	0.5%
Intrusion Sets	964	3	0.3%
Malware	3,513	16	0.5%
Indicators	137,773	350	0.3%
Attack Patterns	1,596	29	1.8%

#### D. Methodological Traceability

The final output of the Direction and Planning phase is the Collection Plan. This plan guarantees methodological traceability by mapping the PIRs to specific operational parameters, typically utilizing the 5W3H method [27] adapted for the CTI context.

An illustrative example of the Collection Plan structured in 5W3H (Figure 2) demonstrates how strategic PIRs are translated into actionable directives through the 5W3H framework, ensuring traceability and contextual relevance for SFN-specific threats.

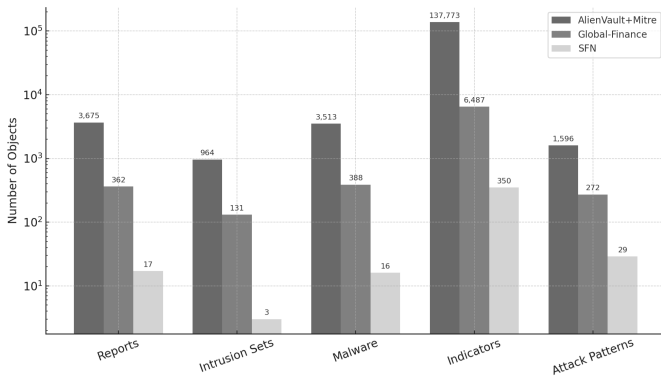


Figure 5: Filtering Impact per STIX Object Class.

### V. Discussion, Limitations and Future Work

#### A. Discussion

The results validate the proposed approach as an effective solution to the upstream gap in the CTI cycle. Unlike prior work focused on post-collection enrichment or deduplication [18], [5], the method demonstrates that early-stage filtering at the Direction and Planning phase yields greater efficiency. By translating broad requirements into structured PIRs and RFIs, it prevents the indiscriminate collection of irrelevant data and optimizes subsequent analysis [6].

Grounded in classical intelligence doctrine [7], [8], [9], [10], [11], [12], the methodology ensures full traceability from strategic priorities to tactical needs, reinforcing the Asset and Risk-Centric approach essential for CIs [1], [33]. At the same time, it aligns with SFN regulations [13], [14], including Art. 21, II of Res. BCB

n° 85/2021, by linking PIRs directly to critical business functions and enabling metrics and indicators to reflect operational effectiveness against institutional risks.

While purely lexical filtering inherently risks missing entirely novel TTPs or zero-day vulnerabilities not yet mapped to PIR keywords, this risk is mitigated by the cyclical and adaptive nature of the proposed methodology. Strategic Alignment necessitates continuous threat mapping, ensuring PIRs and corresponding filters are regularly revised based on emerging adversary tactics, thus maintaining continuous relevance.

#### B. Limitations and Future Work

The primary limitation of this study is the conceptual case study’s lack of integration into a real operational environment, despite its application to real and representative data from the financial threat landscape.

Additionally, the dataset was derived primarily from AlienVault/OTX and MITRE ATT&CK, chosen for their suitability for controlled validation. In real-world deployments, financial institutions often ingest a broader mix of proprietary and contextual feeds, which may alter noise ratios but not the methodology’s structural applicability.

Future work will focus on three areas: (i) *Live Deployment within SFN Institutions*: Transitioning from controlled conceptual application to live deployment within an SFN organization, to assess the methodology’s operational performance, filtering latency, integration complexity, and resource demands. This will also support alignment with PNCiber objectives and sector resilience goals [17]; (ii) *Metrics Integration*: Expanding the evaluation framework to include both traditional metrics (e.g., precision, recall, F1-score) and CTI-specific indicators such as Actionability Score—the proportion of intelligence used in decision-making—and Time-to-Detect—the reduction in detection delay due to targeted collection; (iii) *Cross-Sector Adaptability*: Evaluating the replicability of the structured method across other Brazilian CIs, aligned with the objectives of the PNSIC [15] and the National Strategy for Critical Infrastructure Security [16], which encourage cooperation and best practice dissemination [15].

### VI. Conclusion

This article presented a structured and replicable methodology for Cyber Threat Intelligence Direction and Planning, tailored to the Brazilian National Financial System regulatory context. Grounded in classical intelligence doctrine, the proposed five-stage process establishes a clear and logical path from strategic objectives to prioritized collection tasks.

The conceptual application in the OpenCTI environment demonstrated the methodology's capacity for quantitative Noise and Quality Focus, significantly reducing data irrelevance while enhancing contextual relevance for operational decision-making. These results confirm that early-stage structured planning can transform high-volume generic data into targeted, actionable intelligence, while maintaining alignment with institutional risk profiles and regulatory mandates.

By addressing a critical upstream gap in the intelligence cycle, the methodology contributes to more effective CTI programs and supports the resilience of financial institutions against increasingly sophisticated cyber threats.

## References

- [1] O. Osliaik, A. Saracino, F. Martinelli, and P. Mori, "Cyber threat intelligence for critical infrastructure security," in *Concurrency and Computation Practice and Experience*, vol. 35, no. 7759, 2023.
- [2] Banco Central do Brasil. (2025) Sistema Financeiro Nacional. Accessed: 2025-09-21. [Online]. Available: <https://www.bcb.gov.br/estabilidadefinanceira/sfn>
- [3] E. M. Lopez and A. I. Awad, "A framework to establish a threat intelligence program," Master's thesis, Luleå University of Technology, 2021.
- [4] A. de Melo e Silva, R. de Oliveira Albuquerque, J. J. C. Gondim, and L. J. G. Villalba, "A methodology to evaluate standards and platforms within cyber threat intelligence," *Future Internet*, 2020.
- [5] R. de Oliveira Silva, R. de Oliveira Albuquerque, and J. J. C. Gondim, "Methodology to improve the quality of cyber threat intelligence production through open source platforms," in *International Conference on Computer Science, Electronics and Industrial Engineering (CSEI)*, 2022, pp. 86–98.
- [6] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, 2018.
- [7] United States Department of the Army, *Collection Management and Synchronization Planning*, Department of the Army, Washington, DC, 1994, accessed: 2025-04-25. [Online]. Available: <https://irp.fas.org/doddir/army/fm34-2/Appd.htm>
- [8] Department of Defense, "Joint publication 2-0: Joint intelligence," Joint Chiefs of Staff, Tech. Rep., 2013.
- [9] NATO. (2016) Allied joint doctrine for intelligence procedures ajp-2.1.
- [10] Joint Chiefs of Staff, "Joint doctrine for intelligence support to operations," United States Department of Defense, Tech. Rep., 1995.
- [11] U.S. Marine Corps, "Mcpw 2-2: Magtf intelligence collection," U.S. Marine Corps, Tech. Rep., 2004.
- [12] UK Ministry of Defence, "Joint doctrine publication 2-00: Intelligence, counter-intelligence and security support to joint operations," UK MoD, Tech. Rep., 2023.
- [13] Banco Central do Brasil. (2021) Resolução BCB nº 85 de 8/4/2021.
- [14] Conselho Monetário Nacional. (2021) RESOLUÇÃO CMN Nº 4.893, DE 26 DE FEVEREIRO DE 2021.
- [15] Presidência da República. (2018) Decreto nº 9.573, 2018-11-22: Política nacional de segurança de infraestruturas críticas.
- [16] —. (2020) Decreto nº 10.569, 2020-12-09: Estratégia nacional de segurança de infraestruturas críticas.
- [17] —. (2023) Decreto nº 11.856, 2023-12-26: Política nacional de cibersegurança.
- [18] M. Faiella, G. G. Granadillo, I. Medeiros, R. Azevedo, and S. G. Zarzosa, "Enriching threat intelligence platforms capabilities," in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, (ICETE)*, 2019, pp. 37–48.
- [19] Bank of England. (2014) Cbest threat intelligence-led assessments. Accessed: 2025-05-12. [Online]. Available: <https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide>
- [20] Official Journal of the European Union. (2022) Digital operational resilience act. Accessed: 2025-05-12. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR>
- [21] European Central Bank. (2024) Adopting tiber-eu will help fulfil dora requirements. Accessed: 2025-05-12. [Online]. Available: <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.miptopical240926.en.pdf>
- [22] FS-ISAC. (2025) Financial Services Information Sharing and Analysis Center. [Online]. Available: <https://www.fsisac.com/>
- [23] CISA, "Critical infrastructure sectors," accessed: 2025-05-12. [Online]. Available: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>
- [24] R. Leszczyna and M. R. Wróbel, "Threat intelligence platform for the energy sector," *Softw. Pract. Exp.*, vol. 49, no. 8, pp. 1225–1254, 2019.
- [25] Red Hat. (2023) Developing Priority Intelligence Requirements. Accessed: 2025-05-12. [Online]. Available: <https://github.com/redhat-infosec/priority-intelligence-requirements-dev>
- [26] Feedly, "Feedly PIR Blueprint," <https://docs.google.com/spreadsheets/d/1kexL5XQJxkH2isejsLu5LzqOj9eFCpq-/edit?gid=789249930>, 2023, accessed: 2025-09-25.
- [27] Sloan and M. C., "Aristotle's as the original locus for the septem circumstantiae," *Classical Philology*, vol. 105, no. 3, pp. 236–251, 2010.
- [28] Board of Governors of the Federal Reserve System, "Cybersecurity and financial system resilience report," 07 2024. [Online]. Available: <https://www.federalreserve.gov/publications/files/cybersecurity-report-202407.pdf>
- [29] Office of the Comptroller of the Currency, "Cybersecurity and financial system resilience report," 07 2025. [Online]. Available: <https://www OCC.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/files/pub-2025-cybersecurity-report.pdf>
- [30] FS-ISAC, "Navigating cyber 2025: Annual threat review and predictions," 2025. [Online]. Available: <https://www.fsisac.com/navigatingcyber2025>
- [31] NFCERT, "Cyber threat landscape for the nordic financial sector," 03 2025. [Online]. Available: [https://communication.nfcert.org/hubfs/CTL Reports/2025%20TLP\\_CLEAR%20NFCERT%20Cyber%20Threat%20Landscape%20%28CTL%29%20Report%20v1.0.pdf](https://communication.nfcert.org/hubfs/CTL Reports/2025%20TLP_CLEAR%20NFCERT%20Cyber%20Threat%20Landscape%20%28CTL%29%20Report%20v1.0.pdf)
- [32] ENISA, "Threat landscape: Finance sector," 02 2025. [Online]. Available: [https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024\\_Final.pdf](https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf)
- [33] H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sánchez, and U. M. Ismail, "Modelling language for cyber security incident handling for critical infrastructures," *Comput. Secur.*, vol. 128, p. 103139, 2023.