Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***CTI-Balanced***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***Threat Classification in Cyber Threat Intelligence Sharing***

Table of Contents

Threat Classification in Cyber Threat Intelligence Sharing

Prepared for CTI-Balanced reporting to the Innovation Agency

1. Purpose and scope

This report describes the scientific study conducted to investigate the application of cyber threat classification in cyber threat intelligence sharing, in line with the cybersecurity legal regulation and best practices.

The results of the study have been submitted for publication in IEEE Access journal. Paper title: “A Unified Ontological Framework for Integrated Regulatory Compliance and Cybersecurity Requirements in Critical Infrastructure”.

2. Cyber threat classification

Various models and frameworks have been proposed to support threat analysis, modelling, risk assessment, and classification of cyber threats, including MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [1], Microsoft STRIDE framework [2], Damage, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD) [3], and NIST SP 800-154 [4], among others.

MITRE ATT&CK is the predominant framework, widely adopted across sectors such as government, academia, and industry, including critical infrastructure [5]. It enables the mapping of adversarial tactics, techniques, and procedures (TTPs) and enhances the systematic detection and analysis of cyber threats, particularly advanced persistent threats (APTs).

The MITRE ATT&CK framework is organized into three primary technology domains - Enterprise, Mobile, and Industrial Control Systems (ICS), which involve different tactics and techniques, representing the adversarial behaviours relevant to each domain [1]. It includes 94 techniques, grouped into several categories: initial access, execution, persistence, privilege escalation, evasion, discovery, lateral movement, collection, command and control, and inhibit response function. These techniques can be linked together to create an attack chain, which can be used to characterize cyberattacks.

Furthermore, the MITRE ATT&CK framework can be mapped to the NIST CSF to facilitate cybersecurity risk management in an organization. In [6], the authors proposed the Cyber Threat Dictionary (CTD), which links MITRE ATT&CK and NIST CSF and can be used to identify security gaps, map them to ATT&CK techniques, develop mitigation and detection techniques, prioritize vulnerabilities, and develop appropriate prevention solutions.

3. Cyber Threat Intelligence (CTI) sharing

There are three main types of Cyber Threat Intelligence (CTI) – strategic, tactical and operational [7]. Strategic CTI is of high-level, which can provide organisations with an overview of the threat landscape;

tactical CTI is aimed at technical audiences and focuses on indicators of compromise; operational CTI provides an overview of how different threat actors plan and execute their attacks and operations.

Janosek claims that the EU's approach to CTI sharing is built upon a triad of key regulations – NIS2 mandates a standard level of cybersecurity across critical sectors and facilitates voluntary threat information exchange, while DORA provides a more specific framework to ensure the operational continuity of the financial industry [8]. These frameworks operate under the strict data privacy requirements of the GDPR, which governs the lawful processing of any CTI that contains personal data.

Art. 29 of NIS2 directive establishes that EU Member States shall ensure that entities (in the scope of NIS2 and not) should be able to exchange on a voluntary basis relevant cybersecurity information [9]. Such sharing should aim to prevent, detect, etc. incidents and mitigate their impacts as well as enhance the level of cybersecurity, and should be done through arrangements which respect potentially sensitive nature of the information shared. According to NIS2, ENISA shall provide assistance for such information sharing.

The information sharing arrangements are also foreseen in Art. 45 of DORA [10]. DORA establishes that financial entities may exchange cyber threat information and intelligence among themselves. Such information sharing should aim to enhance the digital information resilience of financial entities, take place within trusted communities of financial entities, and be implemented through information-sharing arrangements that respect business confidentiality, protect personal data in accordance with the GDPR, and comply with competition policy. In other words, while DORA specifies which specific constraints should be taken into account (business confidentiality, data protection, competition), it can be assumed that at least the same approach should be taken under NIS2 considering the reference to 'potentially sensitive nature of information'.

In their paper Rajamäki et al. also focus on the GDPR's implications to CTI exchanges [7]. The authors establish that 'to conduct a CTI exchange involving GDPR-protected data, it is only legal in case data is necessary and the legal groundwork for sharing can be labelled as a legitimate interest.' They also claim that CTI sharing projects are recommended to prepare a data protection impact assessment (Art. 35 of the GDPR) and that CTI exchanges should anonymize identifiable data. As related to the GDPR, Janosek claims that CTI sharing should be structured to reduce or avoid the inclusion of personal data [8]. The suggested examples include, e.g., that reports can pseudonymize user identifiers by hashing emails or hostnames or by aggregating event details; instead of raw log lines detailing specific IPs, user identifiers, or exact timestamps, CTI reports might summarize activity per hour. Furthermore, MITRE ATT&CK threat classification can be considered as a ground-truth for CTI sharing among organizations.

4. Methodology and integrated ontological framework

An ontology-driven methodology has been developed to enable the formal integration and operationalization of regulatory compliance and cybersecurity requirements. The approach is grounded in semantic web technologies and proceeds through four main stages: knowledge acquisition, ontological modelling, semantic formalization, and instance-based validation.

The methodology adopts a four-domain integration approach, systematically identifying knowledge sources across:

(A) cybersecurity risk management frameworks (e.g., NIST CSF 2.0);
(B) regulatory frameworks (e.g., GDPR, NIS2, AI Act);
(C) technical standards (e.g., IEC 62443-3-3); and
(D) threat intelligence models (e.g., MITRE ATT&CK for ICS).

As illustrated in Figure 1, these sources were selected to synthesize both organizational and technical dimensions of cybersecurity compliance. Key concepts and relationships were extracted and harmonized into a unified conceptual structure, with particular attention to linking regulatory obligations to operational cybersecurity constructs.

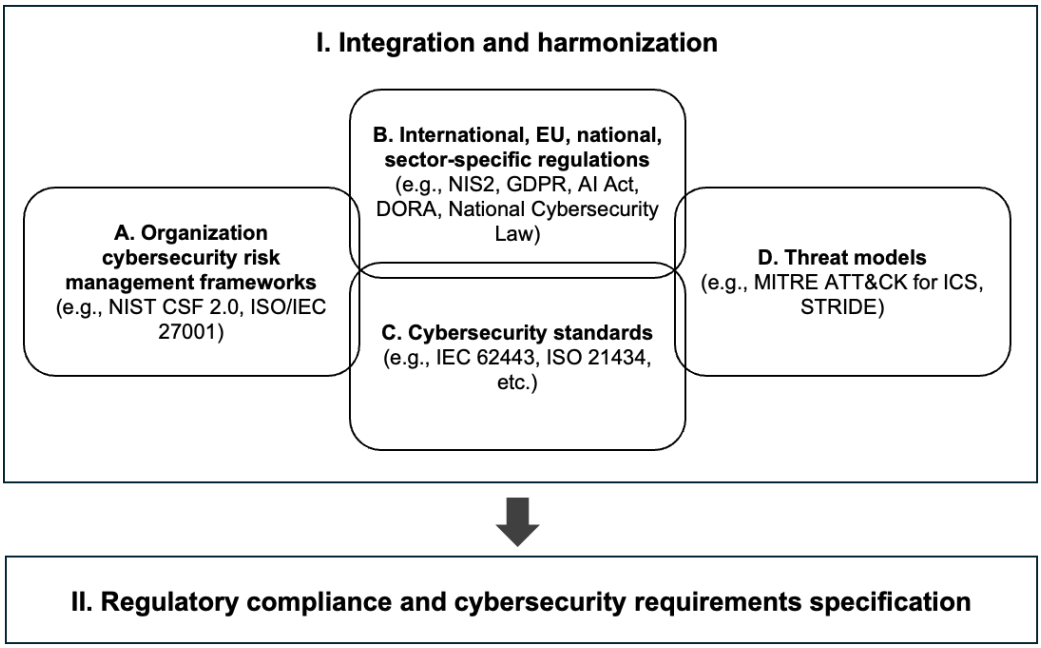

Figure 1. Ontological framework scope. Here, the integration of four domains is depicted: organizational cybersecurity risk management frameworks, regulations, cybersecurity standards, and threat models. These work together in support of regulatory compliance and the specification of cybersecurity requirements.

Based on the proposed methodology, an integrated ontological framework has been developed, that bridges the gap between high-level regulatory compliance and low-level cybersecurity engineering in critical infrastructure. Unlike existing approaches that treat regulations, technical standards, and threat models in isolation, the proposed framework provides a unified semantic representation that links legal obligations (e.g., NIS2, GDPR, AI Act), organisational cybersecurity processes (NIST CSF 2.0), technical controls (IEC 62443), and adversarial behaviours (MITRE ATT&CK for ICS). By establishing a unified semantic model, the framework provides traceable, machine-interpretable links between legal obligations, operational controls, and specific adversarial behaviours, thereby supporting compliance-by-design and threat-informed requirements specification within a single coherent model.

5. Application of the proposed framework to support CTI sharing among critical infrastructure organizations

The application of the framework to CTI sharing demonstrates its versatility beyond the ICS domain. The ontology formally maps the inherent regulatory tension between NIS2 Article 29, which encourages broad information exchange, and GDPR Article 5, which mandates data protection principles including data minimization. By linking the CTI platform to both requirements, the framework provides compliance analysts with a structured tool to navigate these conflicting mandates during Data Protection Impact Assessments (DPIAs). Within the ontology, the NIS2 Directive and the General Data Protection Regulation (GDPR) are instantiated as Regulation entities. NIS2 gives rise to an incident reporting requirement (*imposesRequirement*), while GDPR similarly imposes data minimization and data breach reporting requirements. Together, these requirements form the basis for subsequent semantic propagation across the framework.

The incident reporting requirement is mapped to the “Respond” function of the NIST Cybersecurity Framework (CSF) 2.0 (*mapsToFunction*), situating it within an established cybersecurity governance

structure. In parallel, the data minimization requirement is applied to a CTI sharing platform (*appliesTo*), reflecting constraints on the handling and dissemination of sensitive threat information.

The CTI sharing platform is further linked to the process of threat intelligence sharing, which is associated with a critical infrastructure organization. This establishes a chain connecting regulatory obligations to organizational participation in information-sharing activities. The platform is also contextualized within this CTI scenario, representing its deployment in an operational scenario.

Using SPARQL queries over the instantiated knowledge graph, these relationships can be retrieved as a coherent traceability structure linking regulations, requirements, functions, platforms, processes, and organizational entities.

Figure 2 presents a representative instance-level traceability chain for a CTI sharing environment. This example focuses on the propagation of regulatory requirements across governance, platform, and organizational layers within an information-sharing context.

The figure, derived from instantiated RDF data and retrieved via SPARQL queries in the Stardog environment, illustrates how requirements imposed by regulatory frameworks are mapped to cybersecurity functions and applied to operational platforms and processes.

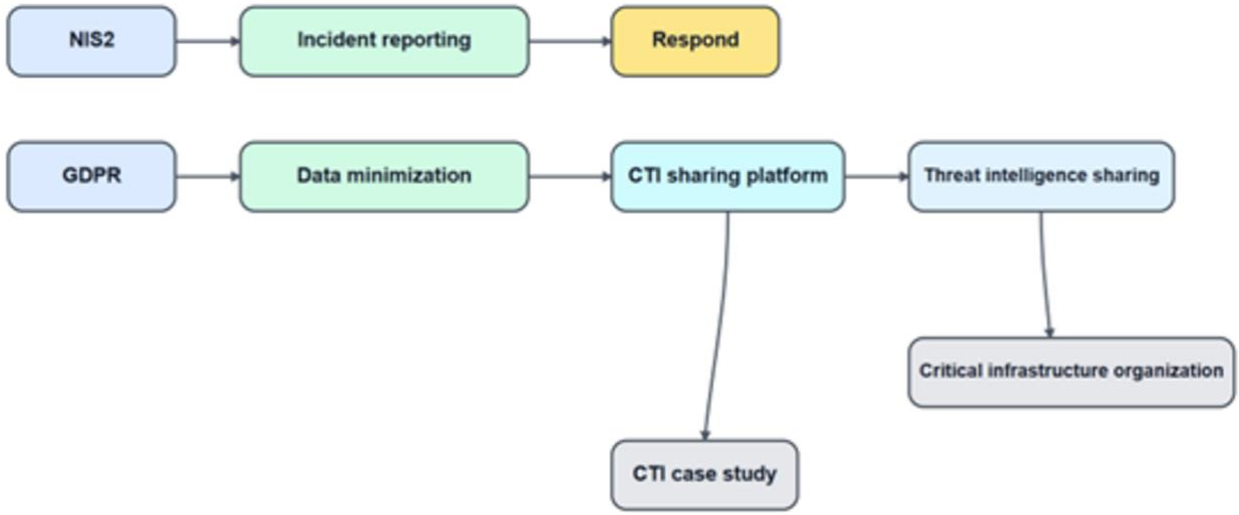

Figure 2. Integrated regulatory compliance and cybersecurity framework: CTI-sharing traceability chain.

Figure 2 presents an instance-level traceability chain for a CTI sharing scenario. The NIS2 Directive and GDPR are instantiated as regulatory sources that impose requirements (*imposesRequirement*), namely incident reporting and data minimization. The incident reporting requirement is aligned with the “Respond” function of the NIST Cybersecurity Framework (*mapsToFunction*), while the data minimization requirement is applied to a CTI sharing platform (*appliesTo*).

The inclusion of data minimization is critical here because CTI often contains information that could identify a natural person, such as IP addresses, hostnames, and metadata which, therefore, is considered personal data. While NIS2 Article 29 encourages the broad exchange of cybersecurity information to enhance collective resilience, GDPR Article 5 mandates that the processing of such personal data be limited to what is strictly necessary. By mapping this requirement directly to the CTI sharing platform node, the framework enables compliance analysts to verify that the platform’s technical architecture supports the privacy-preserving measures during inter-organizational exchange.

The platform is linked to the process of threat intelligence sharing, which is associated with a critical infrastructure organization, representing the operational context in which information exchange occurs. The platform is further situated within a CTI case study, illustrating its deployment in a concrete scenario.

Together, these relationships demonstrate how regulatory obligations are propagated across governance, platform, processing, and organizational layers.

The application of the framework to CTI sharing illustrates its ability to make inherent regulatory tensions formally navigable. Specifically, it captures the conflict between NIS2 Article 29, which encourages broad, voluntary information exchange, and GDPR Article 5, which mandates that personal data be limited to what is strictly necessary. By linking the CTI platform to both requirements simultaneously, the framework enables compliance analysts to identify which constraints apply to a given operational context, thereby directly supporting the preparation of Data Protection Impact Assessments (DPIAs) as recommended by Rajamäki et al. (2024) [7] and mandated under GDPR Article 35. Furthermore, as B. Al-Sada (2025) notes [5], the MITRE ATT&CK framework is an increasingly standard vocabulary for CTI exchange, and our proposed ontology provides the formal semantic foundation for sharing intelligence while maintaining strict traceability to the regulatory constraints governing such activities.

6. Conclusion

As part of our research, an integrated ontological framework has been developed, which bridges the persistent gap between regulatory compliance and cybersecurity engineering in critical infrastructure environments. By formally unifying the selected EU regulatory instruments (NIS2, GDPR, the AI Act, and the CRA), organizational cybersecurity risk management (NIST CSF 2.0), sector-specific technical standards (IEC 62443-3-3), and threat classification (MITRE ATT&CK for ICS) within a single RDF/OWL ontology, the framework enables machine-interpretable traceability from legal obligations to concrete mitigations, a capability that no individual standard provides in isolation.

Furthermore, the framework has been successfully applied for CTI sharing using MITRE ATT&CK for ICS threat classification matrix, as demonstrated in Section 5. In future, we are planning to extend the framework to incorporate MITRE ATT&CK Enterprise and Mobile matrices to enable the modelling of cross-domain attack paths that reflect realistic adversarial campaigns targeting critical infrastructure through IT/OT convergence points.

7. References

[1] MITRE Corporation, "MITRE ATT&CK for ICS," [Online]. Available: https://attack.mitre.org/matrices/ics/

[2] A. Shostack, Threat Modeling: Designing for Security. Indianapolis, USA: Wiley, 2014.

[3] H. Michael, D. LeBlanc, Writing secure code. Washington, USA: Microsoft Press, 2003.

[4] National Institute of Standards and Technology, “Guide to Data-Centric System Threat Modeling,” NIST SP 800-154, Mar. 2016. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/154/ipd

[5] B. Al-Sada, A. Sadighian, and G. Oligeri, “MITRE ATT&CK: State of the Art and Way Forward,” ACM Comput. Surv., vol. 57, no. 1, pp. 1–37, Jan. 2025, doi: 10.1145/3687300

[6] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 2020, pp. 106-112, doi: 10.1109/RWS50334.2020.9241271

[7] J. Rajamäki et al., “Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals,” WSEAS Transactions on Computers, vol. 23, pp. 1–11, Apr. 2024, doi: 10.37394/23205.2024.23.1

[8] D. Janosek, “Toward a Global Framework for Cyber Threat Intelligence Sharing,” CDR, vol. 10, no. 2, pp. 99–114, Dec. 2025, doi: 10.55682/cdr/sgyw-5r5p.

[9] European Parliament and Council of the European Union, “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive),” Official Journal of the European Union, L 333, Dec. 27, 2022, pp. 80–152. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[10] European Parliament and Council of the European Union, “Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011,” Official Journal of the European Union, L 333, Dec. 27, 2022, pp. 1–79. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Finansuoja Europos Sąjunga
NextGenerationEU
Mykolo Romerio universitetas
NAUJOS KARTOS LIETUVA

Editor
<<Main Editor>>

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)

Disclaimer