Integrating NIS2 Requirements into a Collaboration Framework for Security Operations Centers

Avikarsha Mandal[1 *], Lasse Nitz[1, 2], and Mehdi Akbari Gurabi[1, 2]

[1]Fraunhofer FIT, Sankt Augustin, Germany
[2]RWTH Aachen University, Aachen, Germany
[*]Corresponding author: avikarsha.mandal@fit.fraunhofer.de.

Introduction

Security Operations Centers (SOCs) play a vital role in the security landscape by preparing for, detecting, and responding to cybersecurity threats and incidents in organizations. In light of evolving regulatory frameworks, however, SOCs face the challenge of maintaining fast and effective incident detection and response while ensuring compliance with increasingly complex EU regulatory frameworks such as NIS2, the Cyber Solidarity Act, and the GDPR. SOCs must maintain operational agility in incident handling while fulfilling legal mandates, ensuring that compliance is not merely a box-ticking exercise but also improves overall cyber hygiene across enterprises. At the same time, collaborative cybersecurity is crucial for building resilience against evolving cyberattacks, enabling secure threat intelligence sharing and coordinated incident response across sectors and borders. However, achieving this collaboration is increasingly challenging due to strict privacy, confidentiality, and data sovereignty requirements. According to a survey among Chief Information Security Officers conducted by the European Cyber Security Organisation (ECSO), medium- and small-sized companies have been impacted the most by integrating compliance requirements with technical security measures [1]. In relation to this work, the European project SAPPAN (H2020 833418) [2], as a previous initiative in this domain, proposed a reference architecture [3] for the exchange of cyber threat intelligence (CTI) and automation. However, the SAPPAN architecture lacked the compliance-level perspective in terms of auditability and traceability now required under NIS2. This work takes a first step toward bridging the gap between regulatory compliance and technical security in SOC collaboration, exploring how SOCs could achieve operational compliance within this framework.

Objective

For collaborative security operations in threat detection and response, the objective of this work is to guide practitioners in building a Compliance Orientation Layer (COL) leveraging the SAPPAN architecture [3]. This layer serves as the bridge that overlays and connects existing and advanced SOC functions, including detection, response, automation, and collaborative CTI sharing.

Methods

First, our methodology considers a gap analysis of the SAPPAN architecture from the NIS2 compliance perspective, followed by a mapping of identified gaps to technical components in the SAPPAN architecture. In this architecture, the key technical components most relevant for NIS2 compliance are as follows: an *automation engine*, a *case management system*, a *recommendation system*, a *data sanitization and transformation module*, and a *user dashboard*.
In line with Articles 20, 21, 23, 29, 30, 32 and 33 of Directive (EU) 2022/2555 (NIS2) [4], we identified the following key requirements that could be addressed or supported by integrating the COL into the SAPPAN architecture:

R1: Cybersecurity risk-management measures (Art. 21): Entities must implement relevant technical and organizational measures to manage cybersecurity risks. This includes establishing security policies, conducting systematic risk assessments, enforcing access control and secure configuration, ensuring network and service continuity, and man-

aging vulnerabilities. These measures must be continuously evaluated and updated to maintain an effective cybersecurity posture. **R2:** Timely and structured incident reporting (Art. 23): Entities must detect, classify, and report significant incidents to competent authorities in line with fixed notification timelines. **R3:** CTI sharing (Art. 29 and 30): Entities are encouraged to share CTI between each other and with relevant actors. However, due to the sensitive nature of the information, measures have to be taken to limit the exposure of shared information only to the degree necessary. **R4:** Accountability and Traceability (Art. 20, 32, and 33): Maintain audit logs and decision records linking detection, response, and reporting activities, with management oversight ensuring regulatory compliance. These can be shared with the auditing bodies when necessary.

Introducing the COL as a policy-driven control and evidence engine that interfaces with technical components of the SAPPAN architecture can aid human operators in monitoring the compliance process while also allowing to automatically aggregate the required information from the other components. This could, for example, be realized by mapping the regulatory requirements to technical measures and by allowing to keep track of which risk-management measures are in place. Additionally, automated workflows for structured reporting, privacy-preserving CTI sharing, and audit log generation could benefit from the aggregation capabilities of the COL.

Results

The SAPPAN architecture provides a basis for sharing CTI associated with different stages of the incident detection and response process. To extend this framework to consider the regulatory perspective, we propose to utilize the defined technical components to implement NIS2-mandated tasks in line with their purpose in the architecture. Additionally, the COL can be used to aid human operators in following NIS2-compliant processes and to coordinate the collection, archiving and transmission of data relevant for NIS2 compliance. This data can serve as means to demonstrate compliance of the organization with regulatory requirements by incorporating traceability and accountability into the incident detection and response process (**R4**). However, respective care has to be taken when implementing this component to ensure these properties. The integration of cybersecurity risk-management measures (**R1**) affects all technical components of the architecture, posing requirements on their realization. Further, exclusively organizational measures are outside the scope of the technical architecture. The COL can help in this regard by providing a list of common risk-management measures, by keeping track of which measures have been implemented in the organization, and when the measures have been last evaluated. Timely and structured incident reporting (**R2**) primarily affects the automation engine, case management system, and recommendation engine of the SAPPAN architecture. Requirements like reporting timelines need to be considered when modeling actions that should be automated or suggested to human operators. This may come with increased effort for adjusting old workflows and decision-making rule sets to comply with new requirements, but recent work showed how the structured reporting for NIS2 compliance can be automated [5]. The requirement of suitably dealing with personal and other sensitive information (**R3**) can be addressed by the data transformation and sanitization module in the existing architecture. As this module deals with both normalization and sanitization of data, national authorities may impose more specific requirements for sharing data with them in terms of formats and filtering rules.

Discussion

Requirements R2 and R3 can be realized by technical components of the SAPPAN architecture. Further, requirement R4 could be addressed by the integration of an additional component, the COL, which ideally is connected to the architecture's recommendation system and user dashboard to allow human operators to oversee the compliance status. Requirement R1, however, affects all technical components within as well as organizational measures outside the scope of the SAPPAN framework. Covering it hence requires additional means, most suitably by implementing technical standard frameworks like NIST CSF, ISO 27001, CIS Controls, or IEC 62443, depending on the domain [6]. It thus remains open which specific risk-management measures are sufficient for NIS2 compliance.

References

[1] European Cyber Security Organisation (ECSO), "White Paper: NIS2 Implementation: Challenges and Priorities," ECSO, Tech. Rep., Jan. 2025, accessed: 2025-10-27. [Online]. Available: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf

[2] Community Research and Development Information Service (CORDIS), "SAPPAN: Sharing and Automation for Privacy Preserving Attack Neutralization," https://cordis.europa.eu/project/id/833418.

[3] L. Nitz, M. Akbari Gurabi, M. Cermak, M. Zadnik, D. Karpuk, A. Drichel, S. Schäfer, B. Holmes, and A. Mandal, "On Collaboration and Automation in the Context of Threat Detection and Response with Privacy-Preserving Features," *Digital Threats*, vol. 6, no. 1, Feb. 2025. doi: 10.1145/3707651. [Online]. Available: https://doi.org/10.1145/3707651

[4] "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, 27 December 2022, p. 80–152, 2022, [2022] OJ L333/80. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[5] M. Akbari Gurabi, L. Nitz, A. Bregar, J. Popanda, C. Siemers, R. Matzutt, and A. Mandal, "Requirements for Playbook-Assisted Cyber Incident Response, Reporting and Automation," *Digital Threats*, vol. 5, no. 3, Sep. 2024. doi: 10.1145/3688810. [Online]. Available: https://doi.org/10.1145/3688810

[6] European Cyber Security Organisation (ECSO), "NIS2 Directive Transposition Tracker," https://ecs-org.eu/activities/nis2-directive-transposition-tracker/, 2025.