MISP Management Models for Effective Threat Intelligence in Cybersecurity

Saku-Lassi Eljaala, Meri Laine, Nella Okko, Edward Pacil and Jyri Rajamäki
Laurea University of Applied Sciences

saku-lassi.eljaala@student.laurea.fi
meri.laine@student.laurea.fi
nella.okko@student.laurea.fi
edward.paci@student.laurea.fi
jyri.rajamaki@laurea.fi

Abstract: Studies conducted in the context of the DYNAMO Horizon Europe project reveal that a significant proportion of regional cyber threat intelligence (CTI) data is still shared through manual methods such as email and chat. While these systems are generally viewed positively, they are also understood to be prone to delays and inaccuracies. The interest in utilizing the Malware Information Sharing Platform (MISP) is rising, yet its implementation is still nascent. Effective integration of MISP into cybersecurity operations hinges on selecting an appropriate governance model. This paper evaluates four models—Centralized, Decentralized, Hybrid, and Federated—to understand their advantages, limitations, and suitability for diverse organizational needs. As cyber threats grow in complexity, organizations increasingly rely on collaborative tools like MISP, requiring robust management frameworks to ensure efficient threat intelligence sharing. This study involves a systematic review of literature and desk research of materials produced during the DYNAMO project to analyse different governance models in terms of their alignment with MISP's objectives, operational needs, and organizational structures. The study's main conclusion is that no single governance model fits all scenarios. Centralized models ensure compliance and consistency, making them ideal for small or regulated environments. Decentralized models offer flexibility for organizations with varied local demands but risk fragmentation. Hybrid and Federated models balance centralized control with local autonomy, providing scalability and resilience for large or complex organizations. Among these, the hybrid model stands out for its ability to dynamically address cybersecurity threats while maintaining cohesive governance. However, successful MISP integration also depends on user engagement, clear protocols, and adaptability to evolving needs. This study provides actionable insights to optimize MISP governance, enhancing collaboration, compliance, and cybersecurity resilience. The study also highlights the importance of ongoing training, clear procedures, and active user participation to maximize MISP's benefits. These insights help organizations build resilience and stay adaptable to evolving cybersecurity challenges.

Keywords: MISPiIntegration, Cybersecurity governance models, Centralized and decentralized management, Hybrid and federated structures, Cyber resilience

1. Introduction

As the volume of threat data continues to grow, automating Cyber Threat Intelligence (CTI) sharing is becoming increasingly essential (Haque & Krishnan, 2021; Wagner et al., 2019). Traditional manual methods, such as email and chat, are inefficient and lead to delays and information overload (Kampanakis, 2014). However, a significant proportion of regional CTI data is still shared through manual methods (Henttonen & Rajamäki, 2024). Despite the acknowledged importance of automated CTI sharing (Wagner et al., 2019; Haque & Krishnan, 2021), challenges remain in ensuring data accuracy and the sophistication of algorithms, which are necessary to avoid false positives or missed threats (Wagner, 2019). Additionally, concerns regarding privacy legislation are substantial (Schwartz et al., 2016; Sullivan & Burger, 2017).

Next-generation cybersecurity operations rely on collaborative tools to enhance threat intelligence. Among these tools, the Malware Information Sharing Platform (MISP) has emerged as a valuable resource for managing and sharing threat intelligence data. With proper integration of MISP, it is possible to enhance security and improve data sharing, so when it comes to determining the efficiency and scalability of the integration, management models have an important role. This study focuses on four different management models: centralized, decentralized, hybrid and federated models, which each have their own distinct features. Because of the unique characteristics of the models and the diverse needs of the organizations, it is unlikely that one model would fit every situation.

This paper aims to determine the advantages and disadvantages of each of the four management models in the context of MISP integration. This research is necessary given the growing importance of threat intelligence sharing when fighting cyber threats.

2. Method

The research methodology is meticulously designed to thoroughly investigate the governance models pertinent to the integration of the MISP. A systematic approach is employed, involving the review of scientific articles and the conduction of desk research to build a comprehensive understanding of key concepts associated with MISP and its governance frameworks.

The initial step in this methodology involves an extensive review of scientific literature related to MISP and governance models. This literature review facilitates the gathering of insights from various studies, theories, and frameworks proposed in the field. By analysing these articles, prevailing trends, challenges, and opportunities within the realm of information sharing and cybersecurity governance can be identified.

In conjunction with the literature review, desk research is conducted to deepen the understanding of key concepts related to governance models. This involves synthesizing information from various sources, including academic articles, industry reports, and case studies. By doing so, the definitions, characteristics, and implications of the different governance models—Centralized, Decentralized, Hybrid, and Federated—as they pertain to MISP integration are clarified.

From this review and analysis, conclusions are drawn regarding the most suitable governance model for integrating MISP. This process involves critically evaluating the strengths and weaknesses of each model in relation to MISP's objectives.

3. MISP Governance Models

Selecting the right management model for MISP integration is critical to the operational success and cybersecurity resilience of organizations. Assessing the benefits and drawbacks of each selected governance model (Centralized, Decentralized, Hybrid, Federated) it might be possible to bring insight to derive best practices for model selection and MISP integration. Though our hypothesis is that there will not be a one-size-fits-all model; each governance structure offers unique advantages that align differently depending on the organization.

Centralized governance is a top-down model where decision-making and policy-setting are controlled by a single authority (Ciner, 2018). It ensures consistent policies, improves system interoperability, and enhances data trust, making it effective for organizations with strict compliance needs (Atlan, 2024). However, it can lead to bureaucracy, reduced flexibility, and limited team ownership, potentially causing decentralized workarounds and security risks.

Decentralized governance distributes control across teams, allowing policies to be tailored to localized needs (Ciner, 2018). It offers flexibility, supports adaptable governance practices, and fosters team ownership and accountability. However, it may result in policy inconsistencies, data silos, and reduced interoperability. Large organizations often face challenges with cohesion and may eventually adopt hybrid structures to address these issues (Atlan, 2024).

The hybrid model combines centralized and decentralized governance elements. Conforming hybrids separate conflicting logics; while dissenting hybrids blend multiple objectives to create unique structures (Mair et al., 2015). This approach offers flexibility, balancing governance requirements with operational agility. However, managing the complexity of dual logic can pose alignment challenges. Clear structures are essential to prevent conflicts between governance and operational units.

The federated model balances central governance with localized autonomy. A central team establishes overarching policies, while individual domains handle governance tailored to their specific needs (Altamimi et al., 2023). This model enhances decision-making by combining central control with local flexibility, making it well-suited for managing crises with both agility and oversight. However, maintaining this balance requires ongoing adjustments, which can demand significant resources.

We initially reached out to 12 organizations meeting specific criteria: operating in Finland's energy, healthcare, or logistics/transport sectors, ranking among the country's largest in their respective fields, headquartered in Finland, and identified by the Finnish National Emergency Supply Agency as critical for national supply security. Eventually, representatives from six organizations agreed to participate in interviews. Please refer to Table 1 for a summary of the informants and their organizations. Following our commitment to confidentiality, we maintain the anonymity of the interviewees and their organizations.

4. Governance Model Selection

The findings emphasize that governance models must align with an organization's structure, operational needs, and strategic objectives, particularly in the context of integrating collaborative platforms like MISP. No single governance model is universally optimal, but each offers unique benefits depending on organizational needs. Centralized models are well-suited for environments requiring strict compliance and uniformity, such as government applications. Small organizations can also benefit from centralized governance, as a single lead can unify business understanding with operational demands, ensuring clarity and efficiency in managing MISP's data-sharing capabilities (Firigan, 2024).

Decentralized models, on the other hand, excel in organizations that require flexibility to meet localized needs, such as geographically dispersed teams or sectors with varying operational demands. By empowering local units to address specific challenges, decentralized governance enhances adaptability while ensuring alignment with overall organizational goals. This model can be useful in MISP implementations where regional autonomy in data sharing and analysis is critical (Firigan, 2024).

ederated and hybrid governance models provide the most flexibility for large, complex organizations implementing MISP. Federated models have proven effective in industries like banking, where centralized policies ensure security and compliance while enabling localized autonomy for adaptive responses. For MISP, federated models can streamline collaboration across departments or regions while maintaining central oversight. Hybrid models extend this versatility by combining centralized policy control with decentralized execution. In a MISP context, this enables consistent data governance across the organization while allowing units to customize practices for specific cybersecurity needs. This balance enhances collaboration, ensures compliance, and strengthens resilience by facilitating quick responses to emerging threats while maintaining a cohesive framework (Digital Data Design Institute, 2024; Firigan, 2024).

Rajamäki, Feyesa, and Nepal (2024) emphasize the Diverse Governance Model for Cyber Information Sharing as particularly applicable to platforms like MISP. This model supports multi-organization collaboration while ensuring legal and ethical compliance, making it highly adaptive in addressing cybersecurity complexities.

Governance model selection for MISP integration should reflect organizational scale, structure, and needs. Centralized models work well for smaller or tightly regulated environments, while federated and hybrid models better serve larger organizations requiring a balance of oversight and local autonomy. Hybrid governance, in particular, fosters collaboration, compliance, and resilience, enabling MISP users to respond dynamically to evolving threats while maintaining consistency and collaboration across teams (Atlan, 2024).

5. Discussion

The study features the need to fit governance models to organizational structures and goals for effective MISP integration. Centralized governance offers simplicity and compliance but can be too rigid for dynamic cybersecurity environments. Decentralized models promote adaptability but may lead to fragmentation and inefficiencies without proper coordination. Hybrid and federated models, which combine centralized oversight with localized autonomy, are promising solutions for balancing complex operational demands with standardized threat intelligence sharing.

The findings imply that the hybrid model is particularly effective. It balances collaboration and control, ensuring compliance while allowing units to address their unique challenges. This side well with MISP's collaborative nature, which thrives on data sharing and decentralized analysis but requires central governance for data accuracy and security. However, the hybrid model also faces challenges in maintaining alignment between centralized policies and decentralized execution, requiring clear protocols and consistent communication.

One aspect to consider is the scalability of governance models and their adaptability to long-term organizational changes. Hybrid models, while inherently flexible, may require periodic reviews and structural adjustments to remain effective as organizations grow, diversify, or face evolving cybersecurity challenges. Ensuring scalability involves not only maintaining alignment but also anticipating shifts in operational demands and resource allocation.

This also underlines the role of human factors, such as training and collaboration, in maximizing MISP's potential. Regardless of the governance model, successful MISP integration depends on user engagement and effective workflows. Organizations must prioritize these elements to fully leverage MISP's capabilities. The

findings encourage a subtle approach to governance model selection, with the need for adaptability in meeting evolving cybersecurity challenges.

6. Conclusion

The study underscores the significance of governance models in the integration of the Malware Information Sharing Platform (MISP) into cybersecurity operations. The findings suggest that no single model is universally applicable; the selection is contingent upon the organizational structure, operational requirements, and strategic objectives. Centralized models are optimal for small or compliance-oriented entities, as they ensure data consistency and control. Conversely, decentralized models are suitable for organizations requiring flexibility, particularly those with dispersed teams or diverse local needs.

Hybrid and federated models are particularly valuable for large, complex organizations. These models bring together centralized oversight and localized flexibility, strengthening resilience and encouraging effective threat intelligence sharing. The hybrid model offers a balanced approach that allows organizations to respond dynamically to cybersecurity threats while maintaining a unified governance structure.

The study hopes to provide practical guidance for selecting and tailoring governance models to optimize MISP integration. It provides feasible support to improve collaboration, ensure compliance, and streamline cybersecurity operations. The study also highlights the importance of ongoing training, clear procedures, and active user participation to maximize MISP's benefits. These insights help organizations build resilience and stay adaptable in the face of evolving cybersecurity challenges.

Acknowledgements

Acknowledgment is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

Altamimi, H., Liu, Q. and Jimenez, B. 2023, 170–185. Not Too Much, Not Too Little: Centralization, Decentralization, and Organizational Change. Journal of Public Administration Research and Theory. Advance access publication 16 March 2022. https://doi.org/10.1093/jopart/muac016

Atlan.com. 2024 accessed 9.10.2024 Data Governance Models: Centralized, Decentralized, Federated (atlan.com)

Borges, E. 2024. MISP: The Open Source Threat Sharing Intelligence Platform. Posted: 15th May 2024.Recordedfuture.com 2024. Accessed 9.10.2024

Çiner, C.U. (2018). Centralization and Decentralization. In: Farazmand, A. (eds) Global Encyclopedia of Public Administration, Public Policy, and Governance. Springer, Cham. https://doi.org/10.1007/978-3-319-20928-9_2451, pp. 692–697.

From Data to AI: Maximizing Organizational Value Through Effective Operating Models. Digital Data Design Institute at Harvard. Accessed 2.11.2024 https://d3.harvard.edu/from-data-to-ai-maximizing-organizational-value-through-effective-operating-models/

Haque, M.F. and Krishnan, R. (2021). Toward automated cyber defense with secure sharing of structured cyber threat intelligence. Information Systems Frontiers 23, pp. 883–896. Available at https://doi.org/10.1007/s10796-020-10103-7

Henttonen, K., and Rajamäki, J. (2024, June). CTI Sharing Practices and MISP Adoption in Finland's Critical Infrastructure Protection. In European Conference on Cyber Warfare and Security (Vol. 23, No. 1).

Horsely, C. and Postolovski, T. 2024. Cosive.com. Accessed 9.10.2024. https://www.cosive.com/blog/7-misp-best-practices-lessons-from-effective-threat-intel-teams https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/misp

Jong, J.and Faerman, S.R. (2021). Centralization and Decentralization: Balancing Organizational and Employee Expectations. In: Farazmand, A. (eds) Global Encyclopedia of Public Administration, Public Policy, and Governance. Springer, Cham. https://doi.org/10.1007/978-3-319-31816-5_4179-1 (pp 1-6.)

Kampanakis, P. (2014). Security automation and threat information-sharing options. Security & Privacy, IEEE, 12(5), pp. 42-51.

Mair, J., Mayer, J., and Lutz, E. (2015). Navigating Institutional Plurality: Organizational Governance in Hybrid Organizations. Organization Studies, 36(6), 713-739. https://doi-org.nelli.laurea.fi/10.1177/0170840615580007

MISP Project.org. Accessed 9.10.2024. https://www.misp-project.org/misp-training/handout/1.2-misp-integration_handout.pdf

Firigan, G. 2024. Data governance operating models exposed. LightsOnData. Accessed 2.11.2024 https://www.lightsondata.com/data-governance-operating-models-exposed/

Rajamäki, J. Feyesa, A. & Nepal, A. 2024. E- EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector. Proceedings of the 23rd European Conference on Cyber Warfare and Security. Academic Papers Vol. 23 No. 1 (2024). Accessed 4.11.2024 https://papers.academic-conferences.org/index.php/eccws/article/view/2073/2183.21.6.2024.

Sullivan, C. and Burger, E. (2017). In the public interest: The privacy implications of international business-to-business sharing of cyber-threat intelligence. Computer Law & Security Review, 33(1), 14–29. ISSN 0267-3649. [Online] Available at: https://doi.org/10.1016/j.clsr.2016.11.015

Schwartz, A., Shah, S. C., MacKenzie, M. H., Thomas, S., Potashnik, T. S., and Law, B. (2016). Automatic threat sharing: how companies can best ensure liability protection when sharing cyber threat information with other companies or organizations. U. Mich. JL Reform, 50, 887.

Wagner, T.D., Mahbub, K., Palomar, E. and Abdallah, A.E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.