Uncovering Critical Resources and Factors Influencing the Use of Threat Intelligence Sharing Platforms

Clemens Sauerwein
University of Innsbruck,
Innsbruck, Austria
Clemens.Sauerwein@uibk.ac.at

Christina Wenzl
University of Innsbruck,
Innsbruck, Austria
Christina.Wenzl@uibk.ac.at

Ruth Breu
University of Innsbruck,
Innsbruck, Austria
Ruth.Breu@uibk.ac.at

Abstract

Threat intelligence sharing is an effective security control to develop situational awareness of the rapidly growing number of new, increasingly sophisticated and targeted cyber threats. This collaborative practice involves the sharing of valuable data, information and knowledge about emerging threats, vulnerabilities and attack patterns between organisations and authorities to strengthen overall security. Although this is a promising solution, there has been limited research focused on understanding the critical resources and factors that influence the use of threat intelligence sharing platforms. To address this research gap, we conducted a systematic literature review by analysing 32 papers. In doing so, we identified 9 benefits and 14 challenges regarding the use of threat intelligence sharing platforms. Based on them we derived three critical resources and four influential factors on the use of threat intelligence sharing and discussed their relationships.

Keywords: Threat Intelligence Sharing, Critical Resources, Influencing Factors, Systematic Literature Review

1. Introduction

The increasing complexity, heterogeneity and global distribution of modern information systems, combined with the rising number of sophisticated cyber attacks, pose a serious threat to businesses (Lallie et al., 2021). Recent security incidents have shown that the spectrum of possible attacks steadily increases that the time frame for organizations to react shrinks constantly. Accordingly, appropriate security controls that enable a timely and targeted response to the threat landscape are required to ensure information security (Dandurand and Serrano, 2013). In this context, threat intelligence sharing across organisational boundaries with other companies and public authorities is a promising solution. In addition, threat intelligence sharing is mandated by standards (e.g. ISO27005:2022,...) and legislation (e.g. US Cybersecurity Information Sharing Act,...) as a mandatory security control in some industries (Yang et al., 2020). Accordingly, the collection, analysis and dissemination of cyber threat data, i.e. security-related information to support and manage information security in organisations (Chismon and Ruks, 2015), is widespread (Brown et al., 2015; Sauerwein et al., 2019). These platforms offer information sharing, information enrichment and analysis functions to obtain targeted and actionable threat intelligence (Dandurand and Serrano, 2013; Sauerwein et al., 2021).

Despite the fact that threat intelligence sharing is a promising solution, it is used at varying scales and levels of maturity across companies and organisations. Furthermore, a similar picture emerges in the characteristics and implementation of the individual platforms (Sauerwein et al., 2021). Accordingly, the critical factors for the organisational success of threat intelligence sharing platforms were investigated (Zibak and Simpson, 2019; Zibak et al., 2021). This resulted in a comprehensive model consisting of six interdependent constructs for determining the user satisfaction and net benefit of threat intelligence sharing platforms (Zibak et al., 2021). Among other constructs, the use was identified as a construct significantly affecting user satisfaction and net benefit. However, only its dependencies and relationships to other constructs and not the construct itself were examined in detail.

The aim of this paper is therefore to examine the construct of use in the context of threat intelligence sharing platforms in more detail and to identify concrete critical factors that influence it. In this way, the study will help to improve the effectiveness of the exchange and promote a deeper scientific understanding on the use of threat intelligence sharing platforms.

In order to accomplish this research goal, we conducted a systematic literature review (Kitchenham, 2004) to identify the benefits and challenges of the use of threat intelligence sharing platforms. In total 32

URI: https://hdl.handle.net/10125/106619
978-0-9981331-7-1

papers were investigated. Based on the literature review findings, we derived three critical resources and four factors influencing the use of threat intelligence sharing platforms. Finally, we also took a closer look at the relationships of these factors.

The remainder of this paper is structured as follows: Section 2 discusses related work in the context of threat intelligence sharing and associated platforms. Section 3 outlines the applied research methodology for conducting the systematic literature review. Section 4 presents the results of the literature review. Section 5 discusses the resources and factors that influence the use of threat intelligence sharing and the limitations of the research at hand. Last but not least, Section 6 concludes the paper and provides an outlook on future work.

2. Related Work

Over the course of ten years, extensive research has been conducted in the area of threat intelligence sharing, covering a wide range of topics. Various aspects such as the general possibilities and requirements, legal and regulatory considerations, standardisation efforts, platform implementation and organisational aspects have been investigated (Skopik et al., 2016).

There has recently been an increase in empirical studies exploring certain organisational aspects. For example, these studies primarily focus on the integration of threat intelligence sharing platforms into information security management (Gschwandtner et al., 2018), exploring the pros and cons of threat intelligence sharing (Zibak and Simpson, 2019), as well as examining the data quality of shared threat intelligence (Sillaber et al., 2016; Zibak et al., 2022). Furthermore, several studies have explored criteria and characteristics for evaluating and selecting threat intelligence sharing platforms (Bauer et al., 2020; Borges Amaro et al., 2022; de Melo e Silva et al., 2020; Sauerwein et al., 2017, 2021). Additionally, a model has been developed to determine the maturity of threat intelligence sharing platforms (Sillaber et al., 2018).

Although the majority of the previously mentioned studies concentrate on the provider side of threat intelligence sharing platforms, only a few address the end-user perspective. These studies delve into topics such as user perceptions (Stojkovski et al., 2021) and user satisfaction with threat intelligence sharing platforms (Dannana et al., 2022; Zibak et al., 2021).

Previous research on threat intelligence sharing platforms has focused predominantly on the provider side, resulting in limited insights into the end-user perspective. Although a few studies have superficially examined the use of these platforms and their impact on user satisfaction and net benefits, a comprehensive understanding of the underlying factors is lacking. This paper addresses this research gap by uncovering critical resources and factors influencing the use of threat intelligence sharing platforms in depth.

3. Applied Research Methodology

In order to address the stated research objective (cf Section 1) we conducted a systematic literature review based on Kitchenham (2004) in the second half of 2022. In doing so, we carried out the following steps: *Definition of Search Strategy* (see Section 3.1), *Paper Selection* (see Section 3.2) and *Information Extraction* (see Section 3.3). In order to ensure the reproducibility and traceability of the applied research methodology, a review protocol was kept. It documented the search strategy, selection criteria, paper selection, quality assessment and information extraction.

3.1. Definition of Search Strategy

In order to obtain opportunities and challenges of threat intelligence sharing from scientific literature we derived the following search string: *(threat OR security) AND (intelligence OR information OR data) AND sharing AND (challenges OR barriers OR resources)*. The search term was applied to the title, keywords and abstracts of the publications contained in the following scientific databases: ACM Digital Library, AIS Electronic Library, Elsevier Science Direct, IEEE Xplorer, Springer Link, Taylor & Francis and Wiley. This initial search resulted in 348 scientific papers.

3.2. Paper Selection

In order to assess the relevance, timeliness and quality of the scientific papers identified, the results of the initial search were reviewed using inclusion and exclusion criteria. In doing so, we eliminated (i) all duplicates and (ii) excluded all papers that were published before 2007, (iii) were not available in full text and (iv) were written in languages other than English. By reading title, abstracts and keywords, as well as a cursory reading of the full texts of all papers, we (v) assessed their relevance to our research. Papers were selected that address the use, benefits, challenges, critical resources and factors of sharing threat intelligence or security information and their platforms. In addition, we have carried out quality assurance of the selected work based on the following three aspects: (vi) credibility of the findings, (vii) performance of addressing the research objective and (viii) extension of knowledge (Petticrew and Roberts,

2008). Finally, this selection procedure resulted in a set of 32 relevant papers (see Table 1 and Table 2).

3.3. Information Extraction

In order to extract relevant benefits and challenges related to threat intelligence sharing, we performed data extraction from the final set of 32 papers based on two concept matrices (Webster and Watson, 2002). In addition to the basic information about the paper (e.g. authors, year of publication,...), one concept matrix contained the identified benefits (see Table 1) and the other the identified challenges (see Table 2). In this context, it is worth mentioning that we took an iterative approach to define the categories of the concept matrices. This means that whenever we identified a new category in two papers during information extraction, we created a new category in the concept matrix. Based on the concept matrices (esp. Table 2) and the surveyed papers we derived critical resources and factors influencing the use of threat intelligence sharing platforms.

4. Results

Based on our systematic literature review, we identified 32 relevant papers. Based on them we identified 9 benefits (see Section 4.1) and 14 challenges (see Section 4.2) of threat intelligence sharing.

4.1. Benefits

As depicted in Table 1 the following nine benefits (B1 to B9) of the use of threat intelligence sharing platforms have been identified:

B1 - Improved operational reliability means higher detection accuracy, supported by faster identification, as well as longer up time and continuity of service, increasing the overall reliability of the system.

B2 -Efficient and effective cyber threat detection and prevention involves improving security analytics and measures to reduce the likelihood of attackers exploiting the same vulnerability across multiple organisations. It also enables cyber security stakeholders to uncover attackers' motivations and tactics, techniques and procedures to take more effective countermeasures.

B3 - Increased organizational support for threat intelligence sharing provides the use of threat intelligence sharing platforms to automate processes, validate data and expand the scope of secure IT configurations, improving overall security and achieving essential security principles in IT infrastructures.

B4 - Improved situational awareness enables organisations to gain a comprehensive understanding of potential and ongoing incidents, the evolving threat landscape and the tactics, techniques and procedures used by threat actors. Through this comprehensive picture, organisations can improve their cyber situational awareness to better understand threats and more effectively anticipate future risks.

B5 - Improved security posture is achieved by leveraging collective knowledge and a deeper understanding of threats so that companies can build a stronger resistance to cyber attacks.

B6 - Positive impact on the overall organizational security strategy encompasses various benefits, such as enabling informed decision-making by business stakeholders, including executive boards, CISOs, CIOs, and CTOs. This knowledge empowers them to make intelligent investments, mitigate risks, enhance operational efficiency, and effectively preserve the organization's reputation.

B7 - Time savings are achieved by supporting threat intelligence sharing platforms due to automation, which enable more efficient use of IT resources and minimise delays caused by human factors

B8 - Cost savings result from minimising expenditure on cyber defence, as threat intelligence sharing platforms enable maximum discovery of vulnerabilities and threats at minimum cost. This means that the cost of investing in countermeasure development for cyber attacks is higher than investing in and using threat intelligence sharing platforms, making them a more cost-effective solution.

B9 - Improved collective learning plays a critical role in promoting the sharing of knowledge and expertise between organisations, effectively reducing the risk of cascading effects across entire systems, sectors or industries. This collaborative approach enables a proactive response to emerging threats and increases overall resilience by leveraging collective knowledge and experience.

4.2. Challenges

As depicted in Table 2 the following 14 challenges (C1 to C14) of the use of threat intelligence sharing platforms have been identified:

C1 - Quality Issues present a significant challenge in threat intelligence sharing, as users frequently encounter low-quality information, resulting in a lack of confidence regarding the accuracy of the shared data.

C2 - Technological Barriers arise from the complexity and limited interoperability of threat intelligence during collection and pre-processing, as well as the general procedural challenges of analysing the threat data overload in an automated manner.

Reference	B1	B2	B3	B4	B5	B6	B7	B8	B9
Alkalabi et al., 2021			x	x				x	x
Bauer et al., 2020									
Chantzios et al., 2019		x		x	x				
Garrido-Pelaz et al., 2016	x								
Kamhoua et al., 2015		x						x	x
Kolini and Janczewski, 2022	x				x				
Mavroeidis and Bromander, 2017		x			x				
Menges et al., 2021		x		x					
Mutemwa et al., 2017					x				
Rashid et al., 2021	x	x	x		x		x	x	
Skopik et al., 2016		x		x			x	x	
Stojkovski et al., 2021		x			x				x
Tosh et al., 2015		x						x	
Tounsi and Rais, 2018	x	x		x	x			x	x
Tounsi, 2019								x	
Vakilinia and Sengupta, 2017	x	x					x		
Wagner et al., 2019	x					x		x	
Wu et al., 2019		x		x	x				
Xie et al., 2020			x	x	x	x		x	
Zibak and Simpson, 2019				x	x	x			
Zibak et al., 2021			x						

Table 1. Concept Matrix - Mapping between identified papers and perceived benefits (B1 to B9)

C3 - Lack of Standardization hampers efficient threat intelligence sharing due to the utilization of inconsistent definitions, terminologies, and data formats.

C4 - Fear of Reputation Loss arises because companies fear that sharing threat intelligence could lead to negative publicity and damage their reputation because they fear regulatory sanctions, impact on market value and exploitation of the information by competitors for economic advantage.

C5 - Lack of Trust is a major barrier to effective threat intelligence sharing, as organisations are reluctant to share their information without a trusted environment.

C6 - Individual Decisions on whether to share threat intelligence or not act as an obstacle because they are influenced by factors such as personal instincts, the perceived importance of the incident and the perceived likelihood of successful prosecution.

C7 - Situational Unawareness resulting from organizations operating in isolation and lacking awareness of ongoing cyber incidents, can impede the sharing of threat intelligence.

C8 - Lack of Competences among security employees in gathering and analyzing threat intelligence serves as an additional challenge to threat intelligence sharing.

C9 - Closure of Information resulting from organizations' concerns of being targeted and potential exploitation of their threat information and vulnerabilities by hackers, can hinder effective threat intelligence sharing.

C10 - Competition presents a challenge to threat intelligence sharing, as organizations are cautious about potential misuse of shared TI by competitors to gain advantage, exacerbated by the presence of free riders who solely consume information without active participation.

C11 - Financial Barriers arise from technology costs and budgetary constraints that make it difficult for proponents to justify and invest in threat intelligence sharing, as there is no immediate return on investment.

C12 - Missing Incentives, such as the desired return on investment and other motivating factors, hinders the adoption and active utilization of threat intelligence sharing by organizations.

C13 - Privacy Concerns related to sensitive information such as personal data and corporate secrets hinder the sharing of threat intelligence as well as the inadvertent classification of certain threat intelligence as private, which limits its use and dissemination.

C14 - Legal Regulations create uncertainty and discourage companies from engaging in threat intelligence sharing because concerns about potential data breaches, liabilities and fines go unanswered.

Reference	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14
Abu et al., 2018	x	x											x	
Al-Ibrahim et al., 2017	x				x				x	x				
Alkalabi et al., 2021	x							x		x	x		x	x
Brilingaitė et al., 2022		x			x			x				x		x
Bromander et al., 2021								x					x	
Chantzios et al., 2019		x			x									
Daniel et al., 2020		x	x			x					x		x	x
Du et al., 2020	x				x	x					x		x	x
Ehrensperger et al., 2021									x	x				
Garrido-Pelaz et al., 2016										x			x	
Guarascio et al., 2022	x		x										x	
Kamhoua et al., 2015				x										
Kolini et al., 2022	x		x	x				x		x	x		x	x
Mattila, 2020		x												
Mavroeidis et al., 2017			x											
Menges et al., 2021													x	x
Mohaisen et al., 2017				x					x	x			x	
Motlhabi et al., 2022		x												
Mutemwa et al., 2017							x	x						
Rashid et al., 2021				x					x		x		x	
Skopik et al., 2016	x	x		x										
Stojkovski et al., 2021		x	x						x	x				x
Tosh et al., 2015					x						x			x
Tounsi et al., 2018	x			x	x	x	x				x		x	x
Vakilinia et al., 2017										x				
Wagner et al., 2019				x				x	x	x		x	x	
Wu et al., 2019				x	x					x			x	
Xie et al., 2020				x	x								x	
Zibak et al., 2019	x		x					x		x	x		x	x

Table 2. Concept Matrix - Mapping between identified papers and challenges (C1 to C14)

5. Critical Resources and Factors Influencing

Based on the described results (cf Section 4) we derived seven factors influencing the use of threat intelligence sharing platforms. In the following Section we discuss the identified factors (cf Section 5.1 to 5.7), their relationships (cf Section 5.8) and the limitations of our study (cf Section 5.9).

5.1. R1 - Technical Resources

In order to overcome technological challenges (cf C2) the integration of a platform into an organization and the incorporation of technological features are essential technical resources. Without these resources, the platform's functionalities cannot be accessed. Specific conditions outlined by Chantzios et al. (2019) include enabling information sharing, ensuring expressiveness and scalability, supporting both human and machine readability, storing information sources, and enabling filtering and alerting.

5.2. R2 - Financial Resources

Financial resources play a vital role in the proper implementation of threat intelligence sharing. Investing in security infrastructure and trained security personnel is crucial for an effective deployment of threat intelligence sharing platform. Without the necessary financial investment, neither technical resources nor human resources can be adequately allocated. Accordingly, it requires a variety of financial resources so that these do not represent a barrier (cf 11) (Mavroeidis and Bromander, 2017; Zibak and Simpson, 2018).

5.3. R3 - Human Resources

Human resources, in the context of threat intelligence sharing platforms, primarily encompass the expertise and skill level of personnel, as well as their tacit knowledge. The Tacit knowledge, which resides within the expertise of analysts, is difficult to capture and automate. Consequently, the involvement of experts is crucial for effectively working with threat intelligence sharing platforms and overcoming the lack of competences (cf C8) while analyzing results and ensuring their proper handling (Mavroeidis and Bromander, 2017; Skopik et al., 2016; Wagner et al., 2019).

5.4. F1 - Perceived Trust

Perceived trust is a fundamental requirement in the context of threat intelligence sharing, as shared threat intelligence is often sensitive information that requires a trusted environment for effective sharing (Tounsi, 2019). Moreover, a lack of trust (cf C5) could be a major barrier for threat intelligence sharing. In this context trust can be categorised into different groups, including trust between participants, trust in the platform and trust in the quality of information (Tounsi, 2019; Wu et al., 2019).

Trust between participants depends on factors such as the nature and sensitivity of threat intelligence and the purpose of its exchange. Given the sensitivity of threat data, it is usually only shared with highly trusted partners. Furthermore, trust within sharing communities can be compromised if some members feel they are contributing too little by merely consuming others' data. This underlines the importance of building mutual trust for reliable and effective information sharing (Tounsi, 2019; Wu et al., 2019). Moreover, the trust between participants play a major role to overcome the fear of reputation loss (cf C4) among others in competition (C10) and closure of information (cf C9).

Trust in the platform relates to the concept of IT security trust. Various mechanisms are used to ensure the confidentiality and integrity of data, such as strict access control, encryption of data at rest and in transit, and VPNs. Trust in the platform also contributes to overall trust between participants, especially within sharing communities, as the platform's security mechanisms directly support community participation policies (Wu et al., 2019). Therefore, these mechanisms and trust in the platform are important to build trust between participants to overcome the challenges mentioned above (cf C4, C9 and C10).

Finally, trust in the quality of threat intelligence (TI) is of paramount importance. The quality of TI is determined by factors such as accuracy, actionability, interoperability, provenance, relevance, reliability and timeliness (Zibak et al., 2022). With the rapidly growing amount of threat data, confidence in the reliability of information quality is critical to effectively process incoming data and make informed decisions about which TI data, data sources or communities to work with (Wu et al., 2019).

5.5. F2 - Level of Cooperation

For effective threat intelligence sharing, cooperation between sharing partners is crucial. This requires the active participation and commitment of all stakeholders to create a mutually beneficial environment and avoid free riders who only consume without contributing to the TIS effort. In sharing communities, reciprocity is an important incentive (cf 12) that promotes effective collaboration and thus ensures the effectiveness of threat intelligence sharing (Alkalabi et al., 2021; Garrido-Pelaz et al., 2016; Kolini and Janczewski, 2022). Accordingly, a high degree of cooperation is required to overcome challenges such as individual decisions (cf C6) or situational unawareness (cf c7).

5.6. F3 - Degree of Standardization

The use of standards is repeatedly highlighted in the literature as another crucial prerequisite (cf C3) for effective threat intelligence sharing. Mavroeidis and Bromander (2017) emphasise the need for a knowledge base for threat information and a robust vocabulary for representing this knowledge. To achieve this, it is proposed to use subjective logic as a modelling approach for threat information and to develop a suitable model for sharing between the parties involved. To achieve this, the adoption of predefined standards and ontologies is recommended. These standards ensure the interoperability of different intelligence cycle functions and facilitate the effective use of threat intelligence sharing platforms (de Melo e Silva et al., 2020; Mavroeidis and Bromander, 2017; Mutemwa et al., 2017). In addition, both technical (cf C2) and regulatory hurdles (cf C13 and C14) can be removed to some extent.

5.7. F4 - Information Quality

For effective threat intelligence sharing, confidence in the quality of threat intelligence is essential and of great importance (cf C1) (Zibak et al., 2021, 2022). distinguishes between content quality and system

quality. Content quality can be improved through the efforts of information producers and platform specific quality assurance features. System quality can be improved through the implementation of the functionalities of the intelligence cycle (Sauerwein et al., 2021). Ensuring high quality in both content and system aspects can provide contextual and actionable threat intelligence that ensures a proactive and predictive response to cyber attacks (Mutemwa et al., 2017).

5.8. Relationship of Factors

The relationship between financial, human, and technical resources regarding the use of threat intelligence sharing platforms is illustrated in Figure 1. These resources serve as fundamental prerequisites for the effective utilization of threat intelligence sharing platforms.

The adequate provision of technological resources and their integration into an organisation's infrastructure are crucial for the efficient use of threat intelligence sharing and the promotion of information sharing (Chantzios et al., 2019; Skopik et al., 2016; Zibak et al., 2021). Inadequate technological integration is a barrier to the adoption of threat intelligence sharing.

Similarly, the availability of qualified personnel with their expertise and tacit knowledge as a vital human resource is essential for the successful use of threat intelligence sharing platforms (Mavroeidis and Bromander, 2017; Tounsi and Rais, 2018; Wagner et al., 2019).

Financial resources play a crucial role not only in facilitating the use of threat intelligence sharing platforms but also in influencing the availability and effectiveness of technological and human resources. They are essential for the proper technological implementation of threat intelligence sharing platforms within the organization's infrastructure and for ensuring the training of competent security personnel. (Menges et al., 2021; Zibak and Simpson, 2018).

Human resources play a significant role in influencing technical resources, as they are crucial for the implementation of TISP, along with financial resources (Mattila, 2020).

Furthermore, as illustrated in Figure 1, the use of threat intelligence sharing platforms is influenced by four interconnected factors (F1 to F4).

Perceived Trust is not only essential for effective sharing of sensitive data but also impacts the level of cooperation among partners, where mutual trust enhances the exchange of threat intelligence (Tounsi, 2019; Tounsi and Rais, 2018). Trust, in turn, is influenced by technological resources and information quality, as the integration of technical features and high-quality platform content increases trust in threat intelligence sharing platforms (Alkalabi et al., 2021; Wu et al., 2019).

The level of cooperation is affected by perceived trust, technological resources, and the degree of standardization, as the integration of threat intelligence sharing platforms into organizations and the adoption of standardized models promote effective collaboration between partners (Brilingaitė et al., 2022; Zibak and Simpson, 2019).

Last but not least, the degree of standardization standards, such as the use of standardized models to represent threat intelligence and appropriate sharing models, fosters cooperation and elevates the level of cooperation among sharing partners (Mavroeidis and Bromander, 2017; Zibak and Simpson, 2019).

The use of threat intelligence sharing platforms is influenced by the aforementioned resources (R1 to R3) and factors (F1 to F4), which address the identified challenges (C1 to C14). It is crucial to effectively utilize threat intelligence sharing platforms in order to harness their full potential benefits (B1 to B9).

5.9. Limitations

The research at hand might be limited by a (i) *selection bias of relevant papers*, (ii) *strong focus on research papers* and (iii) *incorrect classification and extraction*. In order to counteract (i) we based our research methodology and selection criteria on well established research methodologies (Kitchenham, 2004; Webster and Watson, 2002). Moreover, to enhance the validity of the search strategy and minimize the risk of overlooking relevant papers, iterative development of search strings and validation by a second person were conducted. In addition, the final paper selection was also reviewed by a second person. (ii) could only be addressed to a limited extent. Since we did not consider grey literature in our systematic literature review. Nevertheless, the identified papers contain empirical research from practice. Accordingly, the practice perspective was also taken into account to a certain extent. In our future work, we would also like to explore the practice perspective in more detail through surveys and expert discussion. Last but not least, to mitigate (ii), we implemented a cross-validation approach where each contributor was assigned a subset of papers that intersected with another contributor's set, enabling early detection and limitation of classification discrepancies through re-classification. However, it is important to acknowledge that some classification uncertainties may still persist.

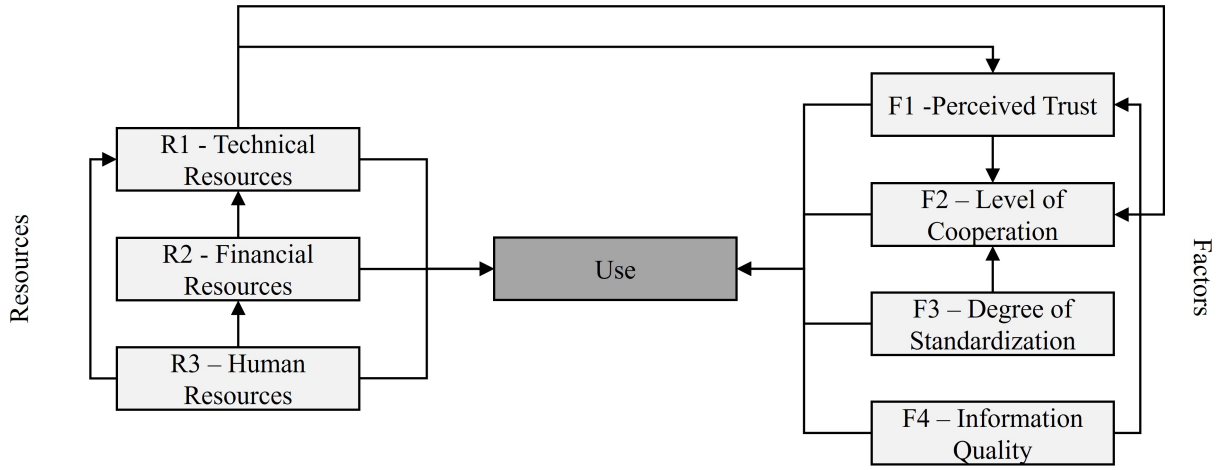

Figure 1. Relationships between resources and factors and their influence on the use

6. Conclusion & Outlook

In this paper we identified critical resources and factors influencing the use of threat intelligence sharing platforms. Therefore, we conducted a systematic literature review and examined 32 papers on the benefits, challenges and derivable influencing factors regarding the use of threat intelligence sharing platforms. We identified 9 benefits and 14 challenges in terms of operational, organisational, economic and policy issues. In order to overcome these challenges and achieve the benefits it pointed out that human, financial and technical resources play a major role. In addition, factors such as perceived trust, the degree of cooperation, the degree of standardisation and the quality of information should be fulfilled at a high level. This allows the benefits of threat intelligence sharing to be realised and ensures effective and efficient use of threat intelligence sharing platforms. In future work, we aim to delve deeper into our findings, particularly the relationship between the identified resources and factors. This will be accomplished through empirical research conducted with end users and platform providers, adopting a practitioner perspective.

References

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371–379.

Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Beyond free riding: Quality of indicators for assessing participation in information sharing for threat intelligence. *arXiv preprint arXiv:1702.00552*.

Alkalabi, W., Simpson, L., & Morarji, H. (2021). Barriers and incentives to cybersecurity threat information sharing in developing countries: A case study of saudi arabia. *2021 Australasian Computer Science Week Multiconference*, 1–8.

Bauer, S., Fischer, D., Sauerwein, C., Latzel, S., Stelzer, D., & Breu, R. (2020). Towards an evaluation framework for threat intelligence sharing platforms. *HICSS*, 1–10.

Borges Amaro, L. J., Percilio Azevedo, B. W., Lopes de Mendonca, F. L., Giozza, W. F., Albuquerque, R. d. O., & Garcia Villalba, L. J. (2022). Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. *Applied Sciences*, *12*(3), 1205.

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of cybersecurity*, *8*(1), 1–9.

Bromander, S., Swimmer, M., Muller, L. P., Jøsang, A., Eian, M., Skjøtskift, G., & Borg, F. (2021). Investigating sharing of cyber threat intelligence and proposing a new data model for enabling automation in knowledge representation and exchange. *Digital Threats: Research and Practice (DTRAP)*, *3*(1), 1–22.

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*, 43–49.

Chantzios, T., Koloveas, P., Skiadopoulos, S., Kolokotronis, N., Tryfonopoulos, C., Bilali, V.-G., & Kavallieros, D. (2019). The quest for the appropriate cyber-threat intelligence sharing platform. *DATA*, 369–376.

Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating. *MWR InfoSecurity Ltd*, *3*(2), 36–42.

Dandurand, L., & Serrano, O. S. (2013). Towards improved cyber security information sharing. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1–16.

Dannana, S., Prabakaran, T., Rajasekaran, A. S., Kumareshan, N., Shadrach, S. F. D., & Kalyanchakravarthi, P. (2022). A novel system model for managing cyber threat intelligence. *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, 1–5.

de Melo e Silva, A., Costa Gondim, J. J., de Oliveira Albuquerque, R., & Garcia Villalba, L. J. (2020). A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, *12*(6), 108.

Du, L., Fan, Y., Zhang, L., Wang, L., & Sun, T. (2020). A summary of the development of cyber security threat intelligence sharing. *International Journal of Digital Crime and Forensics (IJDCF)*, *12*(4), 54–67.

Ehrensperger, R., Sauerwein, C., & Breu, R. (2021). Toward a maturity model for digital business ecosystems from an it perspective. *2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)*, 11–20.

Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). Shall we collaborate? a model to analyse the benefits of information sharing. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 15–24.

Gschwandtner, M., Demetz, L., Gander, M., & Maier, R. (2018). Integrating threat intelligence to enhance an organization's information security management. *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 1–8.

Guarascio, M., Cassavia, N., Pisani, F. S., & Manco, G. (2022). Boosting cyber-threat intelligence via collaborative intrusion detection. *Future Generation Computer Systems*, *135*, 30–43.

Kamhoua, C., Martin, A., Tosh, D. K., Kwiat, K. A., Heitzenrater, C., & Sengupta, S. (2015). Cyber-threats information sharing in cloud computing: A game theoretic approach. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 382–389.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(2004), 1–26.

Kolini, F., & Janczewski, L. J. (2022). Exploring incentives and challenges for cybersecurity intelligence sharing (cis) across organizations: A systematic review. *Communications of the Association for Information Systems*, *50*(1), 2.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, 102248.

Mattila, T. (2020). Integration of arctic node threat intelligence sharing platform with suricata.

Mavroeidis, V., & Bromander, S. (2017). Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *2017 European Intelligence and Security Informatics Conference (EISIC)*, 91–98.

Menges, F., Putz, B., & Pernul, G. (2021). Dealer: Decentralized incentives for threat intelligence reporting and exchange. *International Journal of Information Security*, *20*(5), 741–761.

Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). Rethinking information sharing for threat intelligence. *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*, 1–7.

Motlhabi, M., Pantsi, P., Mangoale, B., Netshiya, R., & Chishiri, S. (2022). Context-aware cyber threat intelligence exchange platform. *International Conference on Cyber Warfare and Security*, *17*(1), 201–210.

Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017). Developing a cyber threat intelligence sharing platform for south african organisations. *2017 Conference on Information Communication Technology and Society (ICTAS)*, 1–6.

Petticrew, M., & Roberts, H. (2008). *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons.

Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity

information sharing ecosystem. *Future Generation Computer Systems*, *124*, 436–466.

Sauerwein, C., Fischer, D., Rubsamen, M., Rosenberger, G., Stelzer, D., & Breu, R. (2021). From threat data to actionable intelligence: An exploratory analysis of the intelligence cycle implementation in cyber threat intelligence sharing platforms. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–9.

Sauerwein, C., Pekaric, I., Felderer, M., & Breu, R. (2019). An analysis and classification of public information security data sources used in research and practice. *Computers & security*, *82*, 140–155.

Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. *Proceedings of Wirtschaftsinformatik 2017*, 837–851.

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data quality challenges and future research directions in threat intelligence sharing practice. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 65–70.

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2018). Towards a maturity model for inter-organizational cyber threat intelligence sharing: A case study of stakeholder's expectations and willingness to share. *Proceedings of Multikonferenz Wirtschaftsinformatik (MKWI 2018)*, 6–9.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

Stojkovski, B., Lenzini, G., Koenig, V., & Rivas, S. (2021). What's in a cyber threat intelligence sharing platform? a mixed-methods user experience investigation of misp. *Annual Computer Security Applications Conference*, 385–398.

Tosh, D. K., Sengupta, S., Mukhopadhyay, S., Kamhoua, C. A., & Kwiat, K. A. (2015). Game theoretic modeling to enforce security information sharing among firms. *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 7–12.

Tounsi, W. (2019). What is cyber threat intelligence and how is it evolving? *Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT*, 1–49.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security*, *72*, 212–233.

Vakilinia, I., & Sengupta, S. (2017). A coalitional game theory approach for cybersecurity information sharing. *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, 237–242.

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

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii–xxiii.

Wu, Y., Qiao, Y., Ye, Y., & Lee, B. (2019). Towards improved trust in threat intelligence sharing using blockchain and trusted computing. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 474–481.

Xie, W., Yu, X., Zhang, Y., & Wang, H. (2020). An improved shapley value benefit distribution mechanism in cooperative game of cyber threat intelligence sharing. *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 810–815.

Yang, A., Kwon, Y. J., & Lee, S.-Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, *120*(9), 1777–1794.

Zibak, A., Sauerwein, C., & Simpson, A. (2021). A success model for cyber threat intelligence management platforms. *Computers & Security*, *111*, 102466.

Zibak, A., Sauerwein, C., & Simpson, A. C. (2022). Threat intelligence quality dimensions for research and practice. *Digital Threats: Research and Practice*, *3*(4), 1–22.

Zibak, A., & Simpson, A. (2018). Can we evaluate the impact of cyber security information sharing? *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–2.

Zibak, A., & Simpson, A. (2019). Cyber threat information sharing: Perceived benefits and barriers. *Proceedings of the 14th international conference on availability, reliability and security*, 1–9.