Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives

Clemens Sauerwein[1], Christian Sillaber[1], Andrea Mussmann[1,], and Ruth Breu[1]

[1] University of Innsbruck, Department of Computer Science, Innsbruck, Austria
{Clemens.Sauerwein,Christian.Sillaber,Andrea.Mussmann,Ruth.Breu}
@uibk.ac.at

Abstract. In the last couple of years, organizations have demonstrated an increased willingness to exchange information and knowledge regarding vulnerabilities, threats, incidents and mitigation strategies in order to collectively protect against today's sophisticated cyberattacks. As a reaction to this trend, software vendors started to create offerings that facilitate this exchange and appear under the umbrella term "Threat Intelligence Sharing Platforms". To which extent these platforms provide the needed means for exchange and information sharing remains unclear as they lack a common definition, innovation in this area is mostly driven by vendors and empirical research is rare. To close this gap, we examine the state-of-the-art software vendor landscape of these platforms, identify gaps and present arising research perspectives. Therefore, we conducted a systematic study of 22 threat intelligence sharing platforms and compared them. We derived eight key findings and discuss how existing gaps should be addressed by future research.

Keywords: Information Security, Threat Intelligence Sharing Platform, Information and Knowledge Sharing

1 Introduction

As information systems used in organizations today are characterized by continuously increased complexity, heterogeneity and interconnectedness, the number and complexity of security related incidents increases accordingly [1, 2]. Recent prominent security incidents have shown the growing spectrum of possible attacks and the immense business harm that result from these attacks, including a devastating loss of intellectual property, productivity, money and reputation [1, 3].

Therefore, the protection of an organization's infrastructure, vulnerability management, internal dissemination of cyber security information and security training have become key activities [4]. Beside these traditional countermeasures, there is an observable trend to increasingly exchange information and knowledge between trusted organizations to aid the management of vulnerabilities and threats and to mitigate incidents [5, 6]. To support these efforts, several standards (e.g. CybOX, STIX, or TAXII) have been developed to enable the automated exchange of threat intelligence [7, 8, 9, 10].

13th International Conference on Wirtschaftsinformatik,
February 12-15, 2017, St. Gallen, Switzerland

Sauerwein, C.; Sillaber, C.; Mussmann, A.; Breu, R. (2017): Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives, in Leimeister, J.M.;
Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017),
St. Gallen, S. 837-851

In 2013 Dandurand and Serrano introduced the concept of a threat intelligence sharing platform, whose requirements are to: (a) Facilitate information sharing,

(b) enable automation, and (c) facilitate the generation, refinement and vetting of data [11]. Today's threat intelligence sharing solutions more or less build on these requirements and several software vendors are offering products [12]. While there are already a variety of solutions on the market, the majority of publications investigate fundamental requirements and challenges for the development of threat intelligence sharing platforms [11, 13, 12, 14].

To which extent these platforms provide the needed means for threat intelligence sharing remains unclear since no scientific analysis of the state-of-the-art of threat intelligence sharing platforms exists and no empirical research has been conducted yet. To address this gap, we seek to answer the following research questions: (a) *What is the state-of-the-art of threat intelligence sharing platforms?* (b) *What are existing gaps in currently available threat intelligence sharing platforms?* and (c) *What are the implications for scientific research in this area?*

The goal of our research is therefore to provide a comprehensive analysis and comparison of the threat intelligence sharing platform market. Based on our findings we discuss the implications for scientific research and their significance.

To achieve this goal, we conducted a systematic study of 22 threat intelligence platforms, consisting of open and closed source products. We compared these solutions according to different dimensions, such as covered use cases, intelligence sharing functionalities and collaboration capabilities. Based on these results, we derived eight key findings and discuss their implications for scientific research.

Our research has shown that, although the interest in this domain has considerably increased over the past years, a common definition of threat intelligence sharing platforms is still missing. While STIX is the extensive de-facto standard for describing threat intelligence data, most platforms do not fully utilize its descriptive capabilities. This is illustrated by the fact that the majority of platforms primarily focus on the sharing of indicators of compromise.

The remainder of this paper is structured as follows. Section 2 provides related work regarding threat intelligence sharing platforms and related studies. Section 3 outlines the underlying research methodology and procedure carried out. Section 4 discusses the key findings. Section 5 discusses the results and implications for scientific research. Finally, Section 6 concludes the paper and provides outlook on future research.

2 Related Work

In the past, organizations used ad-hoc solutions such as email messages, phone calls, ticket systems, or face-to-face meetings to communicate security related information. Recently, a trend to form interconnected communities of exchange via associated platforms for the (semi-) automated exchange of security related threat intelligence can be observed [12]. Moreover, the exchange of security knowledge between experts across organizations presents a potential countermeasure to protect against today's sophisticated threat actors, as not every organization has the resources to develop an adequate information security program independently, and organizations can benefit from other organizations' experiences and knowledge [5, 15].

Several researchers identified challenges and requirements for threat intelligence sharing platforms [11, 13, 12, 14]. In addition, several standardization efforts have been made to facilitate cyber security data sharing in a standardized manner, e.g. Open Incident of Compromise(OpenIOC), Cyber Observable eXpression (CybOX), Structured Threat Information eXpression (STIX), Incident Object Description Exchange Format (IODEF) or Trusted Automated eXchange of Indicator Information (TAXII) [8, 9, 10]. Moreover these standards form more or less the basis for today's threat intelligence sharing platforms. In order to select the right standard for a particular use case Burger et al. provide an agnostic framework in which standards can be evaluated and assessed [16].

Only a few studies and descriptions of existing threat intelligence sharing platforms can be identified. In [17] the SANS Institute gives an overview of a small selection of open source threat intelligence platforms, including the Collective Intelligence Framework (CIF), Collaborative Research into Threats (CRITs), MANTIS Cyber-Intelligence Management Framework, Malware Information Sharing Platform (MISP), and Soltra Edge, and conclude that the market for threat intelligence sharing is still developing. Brown et al. discuss the community requirements and expectations of an all-encompassing threat intelligence management platform based on studies on a few threat intelligence sharing platforms [12]. These contributions take into consideration only a subset of available threat intelligence sharing platforms without providing a comprehensive analysis of the state-of-the-art. Several tool and vendor studies loosely related to threat intelligence sharing in organizations can be found, e.g. on software vendors in the area of Governance, Risk & Compliance (GRC) management software [18], cloud providers [19] and the security software market [20].

Moreover, as part of our research methodology we use a multivocal literature review [21]. Only few systematic literature reviews using this methodology can be found in information systems research [22, 23, 24]. As outlined by Garousi et al., multivocal literature reviews can be valuable in closing the gap between academic research and practice [25].

To the best of our knowledge, no prior research has been conducted on threat intelligence sharing platforms in order to provide a comprehensive analysis of existing software solutions and research perspectives that could guide research and industry.

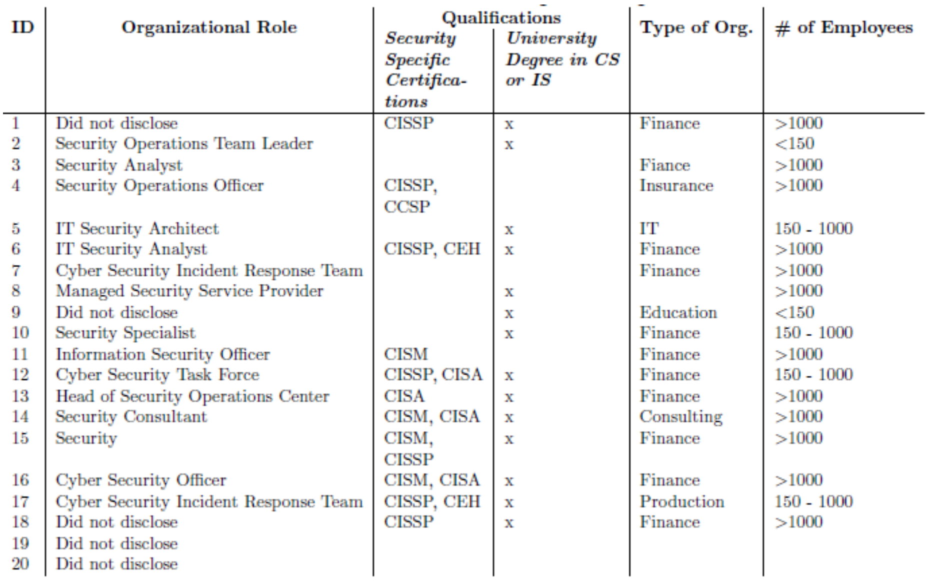
3 Research Methodology

Our research is based on an exploratory study carried out in close collaboration with a security expert group developing a nation-wide threat intelligence sharing community in a German-speaking country. It consisted of two parts and was conducted between May 2016 and July 2016. At first two workshops with the community were held to form the basis of our subsequent multivocal literature review on threat intelligence sharing platforms in industrial and academic context. In order to guarantee reproducibility of the applied research methodology, a research protocol was developed, including workshops transcripts, search term definitions, search results, platform selections, data extractions and platform classifications.

3.1 Workshops

Two focus group discussions [26] with respectively ten security experts from industry being members of the aforementioned security expert group were conducted. Table 1 gives an overview of the participants, their organizational roles, qualifications, type and size of their organizations. The findings from the first round were evaluated and refined in the second round. The primary goal of these two workshops was to get an understanding what the participants recognize as threat intelligence sharing platform and to compile a list of platforms they either use or consider for usage at their organization.

Table 1. Overview Workshop Participants



ID	Organizational Role	Qualifications		Type of Org.	# of Employees
		Security Specific Certifications	*University Degree in CS or IS*		
1	Did not disclose	CISSP	x	Finance	>1000
2	Security Operations Team Leader		x		<150
3	Security Analyst			Fiance	>1000
4	Security Operations Officer	CISSP, CCSP		Insurance	>1000
5	IT Security Architect		x	IT	150 - 1000
6	IT Security Analyst	CISSP, CEH	x	Finance	>1000
7	Cyber Security Incident Response Team			Finance	>1000
8	Managed Security Service Provider		x		>1000
9	Did not disclose		x	Education	<150
10	Security Specialist		x	Finance	150 - 1000
11	Information Security Officer	CISM		Finance	>1000
12	Cyber Security Task Force	CISSP, CISA	x	Finance	150 - 1000
13	Head of Security Operations Center	CISA	x	Finance	>1000
14	Security Consultant	CISM, CISA	x	Consulting	>1000
15	Security	CISM, CISSP	x	Finance	>1000
16	Cyber Security Officer	CISM, CISA	x	Finance	>1000
17	Cyber Security Incident Response Team	CISSP, CEH	x	Production	150 - 1000
18	Did not disclose	CISSP	x	Finance	>1000
19	Did not disclose				
20	Did not disclose				

The workshops were held in parallel after the participants were instructed by two researchers. The aim of these parallel workshops was to limit bias from other participants and to get more comprehensive results. The researchers asked questions during the discussions to clarify participant’s statements. Each workshop was recorded and then transcribed. Finally, qualitative summaries were produced [27] from the discussions in order to derive keywords and a common understanding for the subsequent multivocal literature review. In addition, a comprehensive list of threat intelligence sharing platforms used by participants was compiled to evaluate the results of the systematic search.

3.2 Multivocal Literature Review

Secondly, we conducted a multivocal literature review (MLR) to identify relevant threat intelligence sharing platforms used in research and practice through a systematic analysis of academic literature and grey literature (e.g. blogs, white papers, webpages) [21, 25]. Moreover, a MLR closes the gap between research and practice [28] and provide a more comprehensive picture on the state-of-the-art of a particular research field [25]. According to that there are no systematic guidelines for conducting MLRs in computer science [25], we oriented us on [23] which conducted a MLR in information system research. In doing so, we derived the following three research steps:

Search Strategy: At first we conducted a systematic search where we used the following academic search engines as well as ordinary web search engines: ACM Digital Library, Cite Seer, ScienceDirect, Google Scholar, IEEE Digital Library, Springer, Scopus, Taylor&Francis and Wiley, Google and Bing. According due that there isn't a common definition and consistent description for the approach of exchanging threat intelligence we derived the following keywords from the discussions during the two workshops: *(Cyber Security OR Threat) AND (Intelligence OR Information OR Data) AND Sharing (Platform OR Tool)* We used these keywords for our search where we tried to identify threat intelligence sharing platforms through analysis of the titles and reading the abstracts of the obtained academic and grey literature. In doing so, we obtained a list of 31 threat intelligence sharing platforms with corresponding references including academic literature as well as grey literature (e.g. white papers, vendor specific web pages). We compared the resulting list of threat intelligence sharing platforms with the list of platforms compiled by the participants of the workshops and with commercial market studies carried out by Gartner [29] and Forrester [30]. The comparison resulted in an unchanged list of 31 threat intelligence sharing platforms for further investigations.

Inclusion and Exclusion: Based on the list of 31 threat intelligence sharing platforms we collected for each platform as many artifacts as possible. These artifacts included websites, white papers, discussions on blogs/forums, technical reports, scientific papers and tool demos. According to that there are apparent issues of reliability and validity associated with grey literature [23] we ranked the quality of the artifacts with respect to the trustworthiness and reliability of the sources. Based on the compiled list of platforms with corresponding references, we applied the following selection procedure: Based on reading of the identified artifacts, we excluded tools that either do not enable the sharing of threat intelligence or do not address organizational cyber security (such as general purpose wikis). We included tools, when the evaluated quality of artifacts was adequate (e.g. websites provided more than a couple of buzzwords), they were published since 2010, and dealing with (cyber security-) threat intelligence sharing. This procedure resulted in a final set of 22 threat intelligence sharing platforms for further analysis.

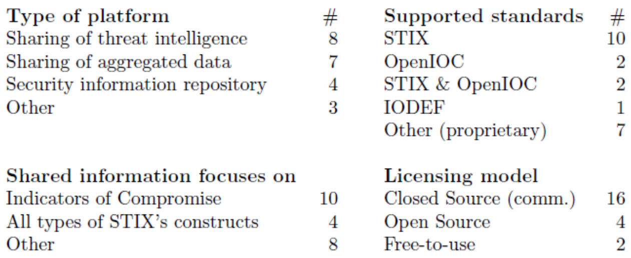
Classification of platforms: Finally, we analyzed these 22 platforms. At first, we assessed the platforms' web pages and studied the provided documentations. Secondly, if there was a free or trial-version available, the software was tested locally. Since this was not possible for every threat intelligence sharing platform, we also analyzed all product videos that were available. During our gradual approach we analyzed every platform according to the following perspectives: Licensing model, use cases, supported standards, supported threat intelligence constructs, shared information/threat intelligence, sharing functionalities, collaboration capabilities, integration capabilities, analysis, deployment, and provided user interfaces.

4 Study Results and Key Findings

The applied methodology, described in the previous Section identified the following 22 threat intelligence sharing platforms: Accenture Cyber Intelligence Platform, Anomali ThreatStream, Anubis Networks Cyberfeed, BrightPoint Security Sentinel, Collaborative Research into Threats (CRITs), Comilion, Facebook Threat Exchange, Falcon Intelligence Crowdstrike, MANTIS Cyber Threat Intelligence Management Framework, Malware Information Sharing Platform (MISP), McAfee Threat Intelligence Exchange, Microsoft Interflow, Open Threat Exchange (OTX), Soltra Edge, HP ThreatCentral, ThreatCloud IntelliStore, ThreatConnect, ThreatQ, ThreatTrack ThreatIQ, Eclectic IQ, IBM X-Force Exchange, Collective Intelligence Framework (CIF).

The classification and analysis of the identified platforms resulted in eight key findings. They are described in this chapter and examples are given. A summary of the tool classification is also provided in Table 2.

Table 2. Overview analysed tools



Type of platform	#	**Supported standards**	#
Sharing of threat intelligence	8	STIX	10
Sharing of aggregated data	7	OpenIOC	2
Security information repository	4	STIX & OpenIOC	2
Other	3	IODEF	1
		Other (proprietary)	7
Shared information focuses on		**Licensing model**	
Indicators of Compromise	10	Closed Source (comm.)	16
All types of STIX's constructs	4	Open Source	4
Other	8	Free-to-use	2

4.1 Key Finding 1: There is no common definition of threat intelligence sharing platforms

Beside the standards for describing (e.g. STIX) and sharing (e.g. TAXII) of threat intelligence, research and practice have not yet developed a comprehensive definition and common understanding of what constitutes a threat intelligence sharing platform. Therefore, different types of platforms were identified:

Eight of the identified platforms focus on the sharing of threat intelligence between organizations. While they aggregate information from the users participating in the platform, seven platforms only share only data (and not intelligence in its strictest sense) that is automatically aggregated from various available paid and open information security data sources (cf. Open Source Intelligence). One of the identified platforms provides a hybrid form of a threat intelligence sharing platform, where data from multiple data sources is combined with the threat intelligence provided by participating users. Moreover, there are four tools which only consist of a central repository which provides context specific security information (e.g. information about malware). The two remaining platforms focus on the sharing of technical data (e.g. SNORT rules) between security applications.

Due to this heterogeneity and diversity of threat intelligence platforms, prospective end users are challenged with the selection of a platform for their particular use case.

4.2 Key Finding 2: STIX is the de-facto standard for describing threat intelligence

The landscape of standards available to describe threat intelligence is rather small compared to the number of sharing platforms available. Our analysis showed that most threat intelligence sharing platforms rely on standards such as OpenIOC, STIX, and IODEF. More than two-thirds of the analyzed platforms provide direct import and export capabilities supporting the standards mentioned above. In detail, ten platforms rely on STIX, two on OpenIOC, two on both of them, and one platform on IODEF. For example, the Open Threat Exchange (OTX) platform provides STIX as well as OpenIOC import and export functionalities.

We found that STIX is the most commonly used standard and can be considered as the de-facto standard for describing threat intelligence. It builds upon the CybOX, CAPEC, MAEC and CVRF standards, and provides a unifying architecture tying together a diverse set of cyber threat information [31]. The STIX architecture consists of eight core cyber threat concepts as independent and reusable constructs and takes their interrelationship into account. The eight constructs describing Cyber Observables (e.g. IP addresses, file names, hashes), Indicators, Incidents, Adversary Tactics Techniques and Procedures (including attack patterns, kill chains, etc.), Exploit Targets (e.g. vulnerabilities, weaknesses), Courses of Action (e.g., incident response, mitigation strategies), Cyber Attack Campaigns, and Cyber Threat Actors. These constructs can be - at least partially - found in all analyzed platforms.

Moreover, these constructs can be used to provide meaningful inputs to information security processes like prevention, detection, or response. For example, valuable inputs for response processes are shared Course of Actions with corresponding Incident descriptions.

4.3 Key Finding 3: Platforms primarily focus on sharing of indicators of compromise

The observed platforms primarily focus on the sharing of indicators of com- promise, e.g. the Open Threat Exchange (OTX) platform. Indicator of compromise include information that enable the identification of potentially malicious activities. For example, indicators of compromise are malicious IP addresses, anomalous user activities, descriptions of malicious files, etc. While the OpenIOC standard is primarily designed to share them, the analyzed platforms use the STIX's Observable and

Indicator constructs to describe them. Although the STIX standard is rather expressive (cf. Key Finding 2), the majority of platforms use the two aforementioned STIX constructs.

4.4 Key Finding 4: The Majority of platforms is closed source

There are six free- to-use threat intelligence sharing platforms available on the market, whereof four are open source tools released under the GNU General Public License, including the Malware Information Sharing Platform (MISP), Collective Intelligence Frame- work (CIF), Collaborative Research Into Threats (CRITs) and MANTIS Cyber- Intelligence Management Framework. The Open Threat Exchange (OTX) and Soltra Edge platform are free-to-use but were not released under an open source license. The remaining 16 are closed source.

4.5 Key Finding 5: Most platforms focus on data collection instead of analysis

The “intelligence” provided by the majority of threat intelligence sharing platforms does not constitute “intelligence” in the traditional sense. In the context of information security “intelligence” is the product of the intelligence lifecycle model, which includes several activities like planning, data collection, analysis and, dissemination [32, 33].

However, we found that the majority of tools primarily focuses on data collection and more or less neglects the other activities of the intelligence lifecycle. Therefore, most currently available threat intelligence platforms resemble data warehouses more than “real” intelligence sharing platforms.

Moreover, they provide limited analysis and visualization capabilities and lag behind comparable knowledge sharing platforms and data mining solutions from other domains. This is insofar surprising as the value of these platforms is constrained by the user’s ability to interpret, absorb, enhance and react to the provided information [34]. Moreover, only a few platforms provide interfaces for third party tools that would enable further analysis of the received threat information.

Threat intelligence sharing platforms currently provide basic analysis capabilities, such as browsing, attribute based filtering and searching of information. Additionally, only a small fraction of platforms implement pivot functionalities which enable the visualization of relationships between the threat intelligence constructs.

4.6 Key Finding 6: Trust issues between users and platform providers are mostly neglected

Our research showed that there are two possible perspectives on trust: the organization, which uses such a platform, towards the provider and vice-versa. Since organizations may share private or sensitive information it is necessary to establish a trust-bond between organizations and the provider of said threat intelligence sharing platform. Moreover, the provider or other organizations must be able to trust the information provided by a particular organization. This means that users of a threat intelligence sharing platform must be careful when dealing with intelligence provided by the platform. In addition, the access to these platforms must be restricted in order to avoid any unauthorized access. For example, the shared intelligence might be of potential interest to attackers.

In order to overcome these trust and access control issues, threat intelligence sharing platforms must provide control mechanisms to specify what information is shared, how much of it and with whom. In addition, access control plays an important role to these platform, since these platforms might be of potential interest to attackers.

Accordingly, six platforms provide trust modelling functionalities, like forming trusted and closed communities, peer-to-peer connections, anonymization of shared threat intelligence, or policies for maximum control of privacy and security. However, they are mostly limited to group-based access control and ranking mechanisms.

Moreover, this topic gained traction in research as well. For example, Steinberger et al. present a trust model that determines trust ratings for security events [35]. Murdoch and Leaver discuss the barriers to participate in a threat intelligence sharing platform caused by the conflict between the need for anonymity versus the need to trust the shared information [36]. In [37] the authors introduce privacy principles for sharing cyber security data that can reduce the risk of data exposure and help to manage trust.

4.7 Key Finding 7: Academic and commercial interest in threat intelligence sharing increases

In November 2011, the OpenIOC standard was released and laid the foundation for threat intelligence sharing. Between 2010 and 2012 only little attention was drawn to threat intelligence sharing in research and practice. In 2013 Dandurand and Serrano introduced the first concept of a threat intelligence management platform with associated requirements [11]. Between 2013 and 2014 the comprehensive STIX and TAXII standards were released. Since then, the number of publications and vendors providing threat intelligence sharing platforms has grown remarkably. For example, the total amount of publications in 2015 was more than threefold compared to 2014. As the market for threat intelligence sharing platforms is relatively new and still developing [17], it can be expected that the number of platforms and scientific publications will continue to grow in the near future.

4.8 Key Finding 8: Many manual tasks make the user the bottleneck

Threat intelligence sharing platforms provide limited automated data integration capabilities. Therefore, a lot of manual user interaction for sharing and acquiring valuable intelligence is necessary. Moreover, the success of a threat intelligence platform depends on the willingness of users to share intelligence which is limited by the organizations’ availability of free resources and the employee’s motivation to actively participate. As most platforms lack automated means of intelligence gathering, and more importantly, automatic sanitation of sensitive intelligence, these activities still require manual effort. Beside classical file importing functionalities, most threat intelligence sharing platforms lack convenient user interfaces for quickly adding new data records and require many user interactions to achieve the desired goal.

5 Discussion and Research Implications

In this section we provide a discussion on the limitations of this exploratory study and a discussion on the results and their implications for research.

5.1 Limitations

Our exploratory study might be limited by certain threats to validity. Limitations that have to be acknowledged and accounted for are an (i) incomplete list of threat intelligence sharing platforms, (ii) wrong definition of key words and inclusion/exclusion criteria, (iii) wrong classification and analysis of platforms, and (iv) incomplete or biased descriptions of platforms.

In order to counteract (i), we evaluated the list of identified platforms with the results of our stakeholder workshops and commercial market studies on threat intelligence sharing platforms. However, there might be the possibility of non-identifiable tools if they were released after our cutoff day (after July 2016) or there is not any public information available about them.

There might be the possibility of type (ii) limitations. In order to avoid them the keywords and inclusion/exclusion criteria were developed based on expert opinions collected during our workshops with the stakeholders.

To inhibit (iii), we have chosen a type of cross-validation approach in which each contributor to this research was given a subset of platforms to analyze and classify that intersected with another contributor's set. Hence, classification discrepancies were discovered and limited through re-classification and analysis. Finally, to overcome (iv), we tried to use more than one information source to classify and analyze a platform.

5.2 Discussion of results and implications for research

Our comprehensive exploratory study pointed out that there is an increasing interest in threat intelligence sharing in research and practice, i.e. the number of publications that apply to his research and number of platforms increased over the last three years. Moreover, it seems that there is a different focus in research and practice since several publications discuss the principles of threat intelligence sharing although there are already a variety of solutions on the market. This might be traced back to a missing common understanding of what threat intelligence sharing is about, due to the diversity of threat intelligence sharing platforms. Hence, one of the biggest gaps is the lack of a common definition and characterization of threat intelligence sharing platforms.

Aware of the possible limitations of the research at hand, the following implications for research, based on the eight key findings, can be derived:

Since key finding 1 and 5 showed that software vendors have a different understanding on threat intelligence sharing, it is necessary to develop a standardized definition and characterization of threat intelligence sharing platforms. In this context it might be beneficial to adopt the wide spread intelligence life cycle model, including planning, collection, analysis, and dissemination activities, to the threat intelligence sharing domain in order to generate intelligence. Thereby, it might be necessary to investigate and define how the different activities within the model can be addressed by a threat intelligence sharing platform. Moreover, these standardization efforts might pave the way for a prospective threat intelligence sharing platform which provides “real” intelligence instead of data warehousing and limited data analysis capabilities. Additionally, organizations might benefit from a common understanding as well, since it might simplify the selection of an appropriate threat intelligence platform.

Key finding 2 showed that three standards are used to facilitate the description of threat intelligence of which STIX is the most used. We believe that it is becoming the de-facto standard in the field. STIX is a detailed and extensive standard consisting of eight constructs which enable the description of a broad range of security related information and their relationships. While the number of standards and available exchange formats is limited at the moment, a trend towards use case specific description formats can be observed (e.g. internal sharing vs sharing across the organizational boundaries).

According to key finding 3 the majority of tools only share indicators of compromise which can be described by two constructs of the STIX standard. Based on this observation the following two implications can be derived: (a) Standards for describing threat intelligence are too generic and powerful, or (b) only the low hanging fruits, namely indicators of compromise, are shared at the moment. In order to get deeper insights on this issue, empirical research on the expected, needed and shared information within a threat intelligence sharing platform is needed.

One argument for using a threat intelligence sharing platform is resource reduction through sharing security knowledge and information. However, as outlined in key finding 5, the majority of tools are rather data-warehouses than intelligence sharing platforms. Consequently, organizations must often evaluate the received information which might result in a lot of additional work. In order to address this issue, research in this area should focus on moving away from mere security data sharing towards knowledge and ultimately intelligence sharing.

As key finding 5 showed that threat intelligence sharing platforms suffer from deficient analysis and visualization functionalities and key finding 8 showed that the submission of new threat intelligence is hindered by limited input options, existing platforms and their user interfaces should be scientifically evaluated to identify potential weaknesses and requirements. In doing so, empirical studies on the required functionalities and visualization options of threat intelligence sharing platforms should be conducted.

Key finding 6 showed that trust plays a paramount role in the context of threat intelligence sharing platforms. To some extent threat intelligence platforms already provide preliminary functionalities to establish trust between the collaborators. In order to support the ongoing research and provide a generally accepted model to guarantee trust, empirical research on the sharing behavior of users and their expectations on data privacy and security is needed.

Key finding 7 showed that there is an increasing interest of threat intelligence sharing in research and practice. Additionally, key finding 4 states that the majority of platforms are closed source. Accordingly, there might be a lack of open threat intelligence platforms and open data sets for scientific research, e.g. to conduct empirical studies.

In order to address this gap it might be necessary that research collaborates with industry. Furthermore, such collaborations imply new research questions resulting from arising problems in practice, and provide potential for future research.

In order to address key finding 8 it is necessary to conduct empirical research on how to motivate users and organization to share information on a threat intelligence sharing platform. For example, it might be necessary to develop and evaluate incentive mechanisms to foster the collaboration within threat intelligence sharing platforms.

Our objective is to explore potential research opportunities by pointing to research questions that (1) investigate threat intelligence as an artifact; (2) see threat intelligence data within an ecosystem of competing and complementary frameworks and standards; or (3) evaluate the usage of threat intelligence in organizations.

Threat intelligence as an artifact: There is a clear need to investigate the foundations, design, applicability, and internal consistency (or lack thereof) in threat intelligence sharing formats and standards. For example, the dominating STIX standard includes many significant artifacts that can be used to describe different aspects of cyber threats (e.g. Indicators of Compromise, Techniques-Tactics & Procedures). However, the success of this expressiveness is not yet clear. Furthermore, little is known about the quality requirements for threat intelligence data artifacts [38]. Questions include: (1) *How can the expressiveness of threat intelligence exchange formats be compared?* (2) *Which concepts of threat intelligence formats are superficial?*

Threat intelligence ecosystem: The core principle of the design of most standards for threat intelligence exchange is to align systematically with cognate standards and formats. These include specialized formats (e.g. IOC, CybOX) as well as formats of higher abstraction (e.g. STIX, TAXII). Understanding how threat intelligence analysis operates in an ecosystem of competing and collaborating standards and frameworks is important. Questions include: *(3) How can organizations manage the integration of different threat intelligence data sources?* (4) *How can organizations decide on which data sources to include?* (5) *How can organizations identify missing data sources?* (6) *Are fewer but complex formats better than many, diversified formats?*

Threat intelligence in use: Little is known on the actual value provided to organizations that participate in threat intelligence sharing platform. There is no academic research about the value proposition of threat intelligence sharing platforms. Questions include: (7) *How can an organization evaluate the impact of threat intelligence sharing platforms?* (8) *How is threat intelligence disseminated within organizations?* (9) *What is the impact of threat intelligence sharing on organizational decision making processes?* (10) *How can organizations be motivated to participate in threat intelligence sharing platforms?* (11) *How can trust be established in threat intelligence sharing platforms?* (12) *How can stakeholders be incentivized to participate in threat intelligence sharing platforms?* (13) *Which visualization and query options are required by organizational stakeholders?* (14) *Which impact do different levels of participation have in threat intelligence sharing platforms?*

6 Conclusion

In this paper we presented an exploratory study on software vendors of threat intelligence sharing platforms and derived future research perspectives. Therefore, we conducted two workshops and a Multivocal Literature Review, including academic and grey literature. It identified a list of 22 threat intelligence sharing platforms used in research and practice. With respect to our research questions we briefly analyzed them and elicited eight key findings. For example, our key findings identified that there is an increasing interest towards threat intelligence sharing, research and practice lacks a consistent definition of threat intelligence sharing, and current threat intelligence sharing is comparable to data warehousing and doesn't provide "real" intelligence. Based on the key findings, we discussed several implications for future research focusing on the creation of a common understanding of threat intelligence sharing and the improvement of current practice. Our future work will focus on empirical research in order to provide a common definition and characterization of threat intelligence sharing platforms for research and practice.

Acknowledgment

This work was partially supported by the Austrian Federal Ministry of Science, Research and Economics (BMWFW), FFG Project 855383 SALSA (ICT of the Future).

References

1. Marinos, L., Belmonte, A., Rekleitis, E.: ENISA Threat Landscape 2015. Technical Report, ENISA - The European Union Agency for Network and Information Security (2016)
2. Miller, A., Horne, R., and Porter, C.: 2015 information security breaches survey. Technical Report, PWC- PrisewaterhouseCoopers (2015)
3. PWC: The Global State of Information Security Survey 2016. Technical Report, PWC-PrisewaterhouseCoopers (2016)
4. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 757–778 (2010)
5. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. J. Information Management & Computer Security 22, 410–430 (2014)
6. Fransen, F., Smulders, A., Kerkdijk, R.: Cyber security information exchange to gain insight into the effects of cyber threats and incidents. J. e & i Elektrotechnik und Informationstechnik 132, 106–112 (2015)
7. Kert, M., Lopez, J., Evangelos, M., Preneel, B.: State-of-the-Art of Secure ICT Landscape. Technical Report, ENISA - NIS Platform - Working Group 3 (2014)
8. Kampanakis, P.: Security automation and threat information-sharing options. J. IEEE Security & Privacy. 12, 42–51 (2014)
9. Steinberger, J., Sperotto, A., Golling, M., and Baier, H.: How to exchange security events? overview and evaluation of formats and protocols. In: IEEE International Symposium on Integrated Network Management (IM), pp. 261–269. IEEE, Los Almitos (2015)

10. Martin, R.A.: Making security measurable and manageable. In: IEEE Military Communications Conference, pp. 1–9. IEEE, Los Almitos (2008)
11. Dandurand, L., Serrano, O.: Towards improved cyber security information sharing. In: 5th International Conference on Cyber Conflict (CyCon), pp. 1–16. IEEE, Los Almitos (2013)
12. Brown, S., Gommers, J., Serrano, O.: From Cyber Security Information Sharing to Threat Management. In: 2nd ACM Workshop on Information Sharing and Collaborative Security, pp. 43–49. ACM, New York (2015)
13. Serrano, O., Dandurand, L., Brown, S.: On the design of a cyber security data sharing system. In: ACM Workshop on Information Sharing and Collaborative Security, pp. 61–69. ACM, New York (2014)
14. Appala, S., Cam-Winget, N., McGrew, D., Verma, J.: An Actionable Threat Intelligence system using a Publish-Subscribe communications model. In: 2nd ACM Workshop on Information Sharing and Collaborative Security. ACM, New York (2015)
15. Ernest Chang, S., Lin, C.-S.: Exploring organizational culture for information security management. J. Industrial Management & Data Systems 107, 438–458 (2007)
16. Burger, E. W., Goodman, M. D., Kampanakis P., Zhu, K.A.: Taxonomy model for cyber threat intelligence information exchange technologies. In: ACM Workshop on Information Sharing & Collaborative Security, pp. 51–60. ACM, New York (2014)
17. Poputa-Clean, P.: Automated Defense - Using Threat Intelligence to Augment Security. Technical Report, SANS Institute InfoSec (2015)
18. Racz, N., Weippl, E., Seufert, A.: Governance, risk & compliance (GRC) software-an exploratory study of software vendor and market research perspectives. In: 44th Hawaii International Conference on Information Sciences (HICSS), pp. 1–10. IEEE, Los Almitos (2011)
19. Repschlaeger, J.: Transparency in cloud business: Cluster analysis of software as a service characteristics. In: International Conference on Grid and Pervasive Computing, pp. 1–10. Springer, Berlin Heidelberg (2013)
20. Dey, D., Lahiri, A., Zhang, G.: Quality Competition and Market Segmentation in the Security Software Market. Mis Quarterly 38, 589–606 (2014)
21. Ogawa, R. T., Malen, B.: Towards rigor in reviews of multivocal literatures: Applying the exploratory case study method. J. Review of Educational Research. 61/3, 265–286, (1991)
22. Ampatzoglou, A., Chatzigeorgiou, A., Avgeriou, P.: The financial aspect of managing technical debt: A systematic literature review. J. Information and Software Technology. 64, 52–73 (2015)
23. Tom, E., Aurum, A., Vidgen, R.: An exploration of technical debt. Journal of Systems and Software. 86/6, 1498–1516 (2013)
24. Sulayman, M., Mendes, E.: A systematic literature review of software process improvement in small and medium web companies. In: International Conference on Advanced Software Engineering and Its Applications, pp. 1-8. Springer (2009)
25. Garousi, V., Felderer, M., Mantyla, M.V.: The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature. In.: 20th International Conference on Evaluation and Assessment in Software Engineering, p. 26. ACM, New York (2016)
26. Wilkinson, S.: 10 focus group reseach. J. Qualitative research: Theory, method and practice, p. 177 (2004)
27. Mayring P., Gläser-Zikuda, M.: Die Praxis der Qualitativen Inhaltsanalyse. Beltz, Weinheim, (2008)

28. Elmore, R.F.: Comment on towards rigor in reviews of multivocal literatures: Applying the exploratory case study method. J. Review of Educational Research. 61, no. 3, pp. 293–297 (1991)
29. McMilian, R., Pratap, K.: Market Guide for Security Threat Intelligence Services. Technical Report, Gartner (2014)
30. Holland, R., Balauras, S., Blackborow, J.: The State of the Cyberthreat Intelligence Market. Technical Report, Forrester (2015)
31. Barnum, S.: Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX™). Technical Report, MITRE Cooperation (2012)
32. Gill, P., Phythian, M.: Intelligence in an insecure world. Polity, Cambridge (2006)
33. Heuer, R.J.: Psychology of intelligence analysis. Technical Report, CIA (1999)
34. Sander, T., Hailpern, J.: Ux aspects of threat information sharing platforms: An examination & lessons learned using personas. In: 2nd ACM Workshop on Information Sharing and Collaborative Security, pp. 51-59. ACM, New York (2015)
35. Steinberger J., Kuhnert, B., Sperotto, A., Baier, H., Pras, A.: In whom do we trust-sharing security events. In: International Conference on Autonomous Infrastructure, Management and Security, pp. 111-124. Springer, Berlin (2016)
36. Murdoch, S., Leaver, N.: Anonymity vs. trust in cybersecurity collaboration. In: 2nd ACM Workshop on Information Sharing and Collaborative Security, pp. 27-29, ACM, New York (2015)
37. Fisk, G., Ardi, C., Pickett, N., Heidemann, J., Fisk, M., Papadopoulos, C.: Privacy principles for sharing cyber security data. In: IEEE Security and Privacy Workshops (SPW), pp.193-197, IEEE, Los Almitos (2015)
38. Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Data quality challenges and future research directions in threat intelligence sharing practice. In: 3rd ACM Workshop on Information Sharing and Collaborative Security, pp.65-70 ACM, New York (2016)