Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Towards an Evaluation Framework for Threat Intelligence Sharing Platforms

Sara Bauer
University of Innsbruck
sara.bauer@uibk.ac.at

Daniel Fischer
Technische Universität Ilmenau
daniel.fischer@tu-ilmenau.de

Clemens Sauerwein
University of Innsbruck
clemens.sauerwein@uibk.ac.at

Simon Latzel
Technische Universität Ilmenau
simon.latzel@tu-ilmenau.de

Dirk Stelzer
Technische Universität Ilmenau
dirk.stelzer@tu-ilmenau.de

Ruth Breu
University of Innsbruck
ruth.breu@uibk.ac.at

Abstract

Threat intelligence sharing is an important countermeasure against the increasing number of security threats to which companies and governments are exposed. Its objective is the cross-organizational exchange of information about actual and potential threats. In recent years, a heterogeneous market of threat intelligence sharing platforms (TISPs) has emerged. These platforms are inter-organizational systems that support collaborative collection, aggregation, analysis and dissemination of threat-related information. Organizations that consider using TISPs are often faced with the challenge of selecting suitable platforms. To facilitate the evaluation of TISPs, we present a framework for analyzing and comparing relevant TISPs. Our framework provides a set of 25 functional and non-functional criteria that support potential users in selecting suitable platforms. We demonstrate the applicability of our evaluation framework by assessing three platforms: MISP, OTX and ThreatQ. We describe common features and differences between the three platforms.

1. Introduction

The adequate protection of information and communication systems against threats constitutes a major challenge for companies and governments. Not only have attacks become more frequent (e.g. by opportunistic malware), but they have also become more targeted and complex (e.g. advanced persistent threats) [1, 2]. The impact of these attacks on business activities can be catastrophic and cause immense damage. Companies and public authorities are well advised to implement countermeasures against these threats. This requires, besides other activities, gathering and evaluating information about potential threats. Such threat-related information is also referred to as threat intelligence (TI). We refer to TI as any evidence-based knowledge, information or data about existing or emerging threats that can be used for mitigation and prevention [1]. Currently, most organizations carry out the gathering and evaluation of TI individually, with little to no cross-organizational exchange of information. However, cross-organizational exchange of TI is an important measure towards effective and efficient threat detection and response [3].

To enhance cross-organizational communication relating to TI, the concept of threat intelligence sharing (TIS) has emerged. It denotes the exchange of information about actual and potential threats across companies and public authorities [4–6]. A more systematic and automated TIS improves the information level of all parties involved [1]. Furthermore, TIS enables organizations to collaboratively use their IT security resources more efficiently. This helps to reduce IT security costs [3, 7]. In recent years, a heterogeneous market of so-called threat intelligence sharing platforms (TISPs) has emerged. These platforms are inter-organizational systems that enable companies and public authorities to collaboratively collect, aggregate, analyze and share threat-related information [8]. TISPs have become a useful tool helping organizations to share TI more effectively. However, performance levels and capabilities vary greatly between platforms. Although several market overviews and comparisons of TISPs have been published, most of them are either incomplete or not sufficiently transparent or are outdated [1, 9]. Organizations which consider using a TISP often face the challenge of choosing a suitable platform that meets their needs. Up to now, there is no framework to adequately support the evaluation and selection of TISPs.

The objective of this paper is to present a framework for analyzing and comparing TISPs and to demonstrate

URI: https://hdl.handle.net/10125/63978
978-0-9981331-3-3

its applicability. We address the following research question: What are essential criteria to describe, evaluate and compare TISPs?

To determine essential evaluation criteria for TISPs we conducted a systematic literature review based on both Webster & Watson [10] and Kitchenham [11]. Since the topic of TIS has only emerged in the last decade, we considered papers published between 2008 and 2018. Using the results of the literature review, we developed a framework for analyzing and comparing TISPs. Finally, we demonstrated the applicability of the framework by analyzing three exemplary TISPs. We followed the design research approach proposed by [12].

The paper is structured as follows: Section 2 discusses related work. In section 3, we outline the underlying research methodology to develop the framework for evaluating TISPs. In section 4 we demonstrate the applicability of the framework by evaluating three TISPs and we describe salient similarities and differences between these platforms. In section 5 we discuss the limitations of the research at hand. Section 6 concludes the paper and provides an outlook on future work.

2. Related Work

Research in the field of TIS can be classified in five categories: *opportunities and challenges*, *legal and regulatory aspects*, *standardization efforts*, *aspects of organizational integration of TIS* and *implementation of TISPs* [7].

Based on the concept of TIS described by [8], several researchers focus on *opportunities and challenges* of TIS. They describe sharing scenarios, discuss advantages and disadvantages of TIS and present requirements for effective and efficient TIS [1,4,13–15]. Other scholars focus on *legal and regulatory* aspects of TIS [16, 17]. Several *standardization efforts* facilitate the structured exchange of TI [5, 18–20]. Researchers provide comprehensive overviews of these standards [7, 18, 21] and analyze how they overlap or differ [22–25]. [26] introduces a taxonomy to evaluate and assess TIS standards. Several studies focus on *aspects of organizational integration* of TI and its impact on organizational processes and decisions [27–30]. Based on the standardization efforts and the concept described by [8], several researchers, governmental institutions and cyber security solution providers started with the *implementation of TISPs* [8, 14, 31–34]. These platforms provide functions for collecting, aggregating and analyzing TI that can be disseminated to other organizations via the platforms. [1, 9] provide an initial overview and comparison of commercial and open source platforms with a focus on customers' demands.

However, the aforementioned comparisons of TISPs lack a common evaluation framework and systematic approach to describe, evaluate and compare TISPs. Moreover, related work focuses only on a subset of existing platforms. To the best of our knowledge, no comprehensive framework for evaluating TISPs has been published so far.

3. Development of Evaluation Framework

The aim of this contribution is the development of a framework to evaluate TISPs. Therefore, we conducted a systematic literature review (see section 3.1). Based on the results of our literature review, we propose criteria and subcriteria for analyzing and comparing TISPs and categorize them in our framework (see section 3.2).

3.1. Systematic Literature Review

The objective of the literature review was to identify and analyze publications that describe characteristics or requirements for TISPs. The literature review, carried out between April and September 2018, is based on the methodologies proposed by [35] and [10]. We applied the following procedure: *definition of search strategy and initial search*, *paper selection* and *criteria extraction*. To ensure reproducibility of the research methodology, a review protocol was developed. It includes the search strategy, search terms, selection criteria, selection procedure, quality assessment and data extraction. The complete literature review process is shown in Figure 1.

Definition of Search Strategy and Initial Search. To get an overview of TIS and TISP, we analyzed eight publications [1, 4, 7–9, 15, 16, 33]. We then defined the following two search strings for our database search: *[((cyber threat AND (intelligence OR information OR knowledge)) OR (cyber security AND (information OR data))) AND (sharing OR exchange)]* and *[((cyber threat AND (intelligence OR information OR knowledge)) OR (cyber security AND (information OR data))) AND (platform OR service OR tool OR system)]*. The reason for the first search string is to identify all studies related to TIS. The second search string is used to identify all publications mentioning TISPs. For a comprehensive literature search we used the databases ACM Digital Library, AIS Electronic Library, EBSCOhost, ELSEVIER ScienceDirect, IEEE Xplorer Digital Library, GoogleScholar, Microsoft Academic Search, Semantic Scholar, Springer Link, Taylor & Francis Online, Web of Science and Wiley Online Library. Depending on the database, we searched for both search strings in the titles, abstracts, keywords and, if applicable, in the full texts. Only papers published between 2008 and 2018 were considered. Our initial search yielded 1,492 papers in total.

Paper Selection. We eliminated all duplicates and excluded all papers that (i) were not available in full text, (ii) had not been peer-reviewed or (iii) are gray or white papers. By analyzing the title, abstracts and keywords of all papers, we assessed their relevance for answering our research question (see section 1). We did not consider papers that do not provide answers to this question. This selection procedure resulted in a set of 67 papers. In a subsequent step, four authors of this paper classified each of the 67 papers as either relevant or not relevant. Relevance in this context means that a paper provides description criteria or requirements for TIS or TISPs. The classifications of all four authors were merged and compared. If all four authors classified a paper as not relevant, we excluded it from the set of papers. The result was a set of 46 relevant papers. They were included in the review.

Criteria Extraction. For structuring and analyzing the 46 papers, we defined a concept matrix. The concept matrix consists of the following categories: description criteria for TISPs, functional and non-functional requirements for TISPs, names of TISPs, description of TISPs, comparison of TISPs, discussion of strengths and weaknesses of TISPs and standards. We split the set of 46 papers into three subsets. Three of the authors received one particular subset, while a fourth author was assigned to the full list of papers. This technique guaranteed that each paper was evaluated by at least two researchers. We then excluded six further papers as they contained no or only subjectively evaluable criteria or requirements, e.g. usability of platforms. From the 40 remaining papers, we extracted a total of 62 criteria.

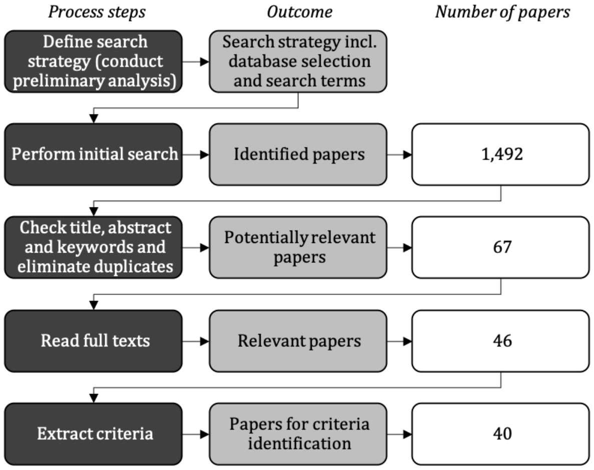
Process steps
Outcome
Number of papers
Define search strategy (conduct preliminary analysis)
Search strategy incl. database selection and search terms
Perform initial search
Identified papers
1,492
Check title, abstract and keywords and eliminate duplicates
Potentially relevant papers
67
Read full texts
Relevant papers
46
Extract criteria
Papers for criteria identification
40

Figure 1. Systematic literature review process.

3.2. Structure and Content of Framework

The considerable amount of extracted criteria necessitated the introduction of apt aggregation and categorization. To enhance the comprehensiveness of the evaluation framework, the criteria were sub-categorized. The resulting hierarchical construction ensures a conceptually sensible grouping apt for vertical and horizontal expandability. [36] suggests a framework for the evaluation and selection of software packages and software systems. According to this framework, we distinguished between two categories, namely functional and non-functional criteria. The framework is shown in Table 1 and outlines all criteria (italicized), subcriteria (in square brackets) and corresponding references (last column).

In our context, FUNCTIONAL CRITERIA characterize the functions of a TISP. We distinguished phases of TIS and cross-phase support.

Phases of TIS. We partitioned the TIS process into four distinct phases: *Collection, Aggregation, Analysis* and *Dissemination of TI*. These phases were derived from current TIS process models and TIS activities as described in the literature. [9], for instance, extracts the phases of data collection, analysis and distribution from the Intelligence Lifecycle Model; these three phases are also mentioned by [9, 23, 38]. By contrast, [40] considers aggregation a predominant TIS phase, as do [7, 27, 37, 40, 40, 44]. [37] mentions all four TIS process phases.

All phases share two common subcriteria: (i) *Available Functions* details which functions a platform provides to support a phase. Note that the retrieved functions are stored in a list without any prioritization (for exemplary functions, see Section 4). (ii) *Degree of Automation* describes whether the functions work in a fully-automated, semi-automated or manual manner. For example, functions within *Collection of TI* [27, 39–42] can retrieve threat-related information semi-automatically or functions within *Analysis of TI* can perform risk analysis fully-automatically.

Analysis of TI [1, 2, 7, 9, 15, 39, 40, 44, 46, 47] is further structured by the subcriteria *Visualization* and *Rating/Prioritization*. The former expresses whether analysis results can be displayed visually. The latter expresses options to rate or to prioritize TI to demonstrate its relevance [6, 8, 14, 15, 38, 45, 47].

Dissemination of TI is further described by *Dissemination Mechanism* and *Real-Time Capacity*. The subcriterion *Dissemination Mechanism* denotes if a push or pull approach is used to distribute incoming TI [4, 7, 9, 20, 23, 26, 33]. In this context, push means that the originator of TI disseminates the information,

Table 1. Mapping of categories, subcategories, criteria and subcriteria to the literature.

	FUNCTIONAL CRITERIA	
Phases of TIS	*Collection of TI* [Available Functions, Degree of Automation]	[9, 16, 23, 27, 37–42]
	Aggregation of TI [Available Functions, Degree of Automation]	[2, 7, 27, 37, 43, 44]
	Analysis of TI [Available Functions, Degree of Automation, Visualization, Rating/Prioritization]	[1, 2, 6–9, 14, 15, 23, 37–40, 44–47]
	Dissemination of TI [Available Functions, Degree of Automation, Dissemination Mechanism, Real-Time Capacity]	[4, 7, 9, 15, 16, 20, 23, 26, 29, 33, 37, 38, 48]
Cross-Phase Support	*Information Security* [Available Functions]	[5, 9, 13, 15, 33, 34, 47, 49]
	Data Privacy [Available Functions, Supported Countries/Federations]	[7, 9, 13, 15, 16, 47]
	Data Quality [Available Functions]	[1, 2, 4–8, 13, 14, 16, 27, 29, 49]
	Trust [Available Functions]	[2, 5, 6, 9, 13, 15, 16, 27, 29, 33, 47, 49, 50]
	Import & Export [Available Functions, Supported Import and Export Standards]	[1, 9, 13, 14, 38]
	Collaboration [Available Functions, Anonymity Levels, Exchange Channels]	[1, 2, 6–9, 13, 15, 29, 33, 39, 49, 51, 52]
	Reporting [Available Functions, Filtering, Form]	[1, 2, 9, 14, 26, 27, 29, 38, 39, 44, 46, 51]
	Additional Functions	
	NON-FUNCTIONAL CRITERIA	
Architecture & Interfaces	*Type of Platform*	[1, 7, 24, 41]
	Architecture	[4, 9, 16, 20, 24, 26, 37]
	APIs [Type of APIs, Supported IT Systems]	[1, 7, 14, 44]
	User Interface [Type, Languages]	[7–9, 33, 39, 42]
Content & Standardization	*Data Origin* [Number of Internal and External Sources, Type of External Data Sources]	[4, 7, 15, 16, 38, 43, 48, 53]
	Threat Intelligence [Content Type, Content Form, Content Language]	[1, 2, 6, 7, 9, 19, 37, 41]
	Standardization [Description Standards, Exchange Protocols, Standard Extensions]	[1, 2, 4, 5, 7–9, 13–16, 19, 20, 22, 23, 26, 27, 33, 34, 40–48, 50, 51, 53, 54]
Provider & Users	*Provider* [Sector, Location, Organization Size, Role]	[5, 6, 23, 37, 48, 50–52]
	Users [Sector, Location, Organization Size, Number of Users, Number of Active Users]	[5, 7, 29, 33, 39, 50, 52]
Usage Fees, License & Distribution	*Usage Fees* [Non-Recurring, Recurring]	[1, 4, 5, 9, 23, 52]
	License	[1, 4, 9, 23, 52]
	Geographical Focus	[5, 7, 41, 51, 54]
	Sectoral Focus	[5, 39, 48, 54]

while pull means that the platform user launches the dissemination. *Real-Time Capacity* details if TI can be shared in real time [7, 15, 16, 29, 37, 38, 47, 48].

Cross-Phase Support. In this subcategory we summarized functions which encompass more than one phase (or even span over the whole TIS process). All criteria listed in this subcategory are expanded by the subcriterion *Available Functions*.

Information Security denotes whether the platform provides functions or measures to protect confidentiality, integrity and availability of information and services provided by the TISP [5, 9, 13, 15, 22, 33, 47, 49], e.g. encryption mechanisms to guarantee the integrity and confidentiality of TI.

Data Privacy and *Data Quality* cover functions enforcing a platform's data privacy and data quality rules. Lacking privacy may prevent users from accepting TISPs [7, 9, 13, 15, 16, 47]. As data privacy regulations may vary between countries, the subcriterion *Supported Countries/Federations* was added. *Data Quality* specifies the usage of control mechanisms to ensure a certain degree of data quality provided by the platform [1, 2, 4–8, 13, 14, 27, 29, 49].

Considering the vast increase in available TI, more attention should be paid to estimate its potential validity. Building on the aforementioned reluctance of users to accept TI, we introduced the criterion *Trust*. Examples for functions are reputation mechanisms or mechanisms for creating an Information Exchange Policy [13].

Focusing on integration aspects, *Import & Export* describes the functions for importing and exporting content provided by the platform [1, 9, 13, 14, 38].

Standards supported by the platform are of particular importance here.

Collaboration between platform users is an essential feature of TISPs [8, 9, 29]. It denotes functions supporting cooperation of platform participants. This criterion is further structured by *Anonymity Levels* and *Exchange Channels*. The former subcriterion describes how users can participate in collaboration processes supported by the platform, i.e. anonymously, using a pseudonym or publicly [6, 9, 49–51]. The latter denotes whether the platform provides options to collaborate privately, publicly or in communities [1, 7–9, 13, 15, 33, 52].

Reporting covers the provision of reporting mechanisms, such as the generation of reports for information security risk management, e.g. according to the ISO/IEC 27001 standard [55]. The subcriteria *Filtering* and *Form* indicate options to customize reports with filtering options or selecting between a visual or textual format. To list any further salient functions, we introduced the criterion *Additional Functions*.

We divided NON-FUNCTIONAL CRITERIA into four subcategories, namely *Architecture & Interfaces*, *Content & Standardization*, *Provider & Users* and *Usage Fees, License & Distribution*.

Architecture & Interfaces. This subcategory characterizes the platform's architecture and interfaces. We distinguished four criteria: *Type of Platform*, *Architecture*, *APIs* and *User Interface*. *Type of Platform* describes two types of TISP instances: operational platforms and software to build a platform [1, 7, 24, 41]. The former enables users to utilize a fully-fledged platform, including TIS services and an existing community. The latter offers users a software solution upon which a platform and corresponding functionalities can be built.

Architecture specifies the architectural concept upon which the platform is based. This criterion was partially derived from [20], mentioning three exchange models for TIS [20]: (i) Client-Server (ii) Peer-to-Peer (iii) Hub and Spoke [4, 9, 24, 26, 37].

APIs describes interfaces to integrate the platform into an organization's IT infrastructure, detailed in subcriteria *Type of APIs* and *Supported IT Systems* [1, 7, 14, 44]. The former describes all APIs offered by the platform. The latter lists IT systems, e.g. risk and vulnerability management systems or incident management systems, which can be integrated into the platform.

User Interface is described in more detail using *Type* and *Languages* [7–9, 33, 39, 42]. The subcriterion *Type* specifies if the platform provides a graphical user interface (GUI) or a command line. The subcriterion *Languages* lists all languages in which the user interface is available [7].

Content & Standardization. This subcategory details the content provided and the standards used by the platform. *Data Origin* describes the sources of data used to produce TI. [53] distinguishes internal, public and commercial data sources, [48] differentiates between internal, public and community sources. Similarly, [4] distinguishes internal, external and community sources. [43] and [15] synthesize the aforementioned categories into internal and external data sources. We used the subcriteria *Number of Internal Sources* and *Number of External Sources* [4, 15, 16, 43]. Internal sources provide data that are generated directly by the platform provider or platform users. External sources provide data that are generated from third parties [38]. [7] further differentiate external data sources into public or commercial data feeds. We followed this distinction and introduced the subcriterion *Type of External Sources*.

Threat Intelligence is subdivided into three subcriteria: *Content Type*, *Content Form* and *Content Language*. First, *Content Type* specifies the objects described by the platforms [1, 2, 7, 9, 19, 37]. Object types may range from Indicators of Compromise (IoC), represented by an IP address, to fully fledged attack scenarios called Tactics, Techniques and Procedures (TTP). Second, *Content Form* describes whether TI is available in a structured format (e.g. via specified data structures) or in an unstructured (e.g. textual) form [6]. Third, *Content Language* denotes the languages in which TI is expressed.

Standardization details which standards and protocols are supported by the platform. Note that almost all papers we evaluated in detail discuss the use of standards relating to TISPs. We used the subcriteria *Description Standards*, *Exchange Protocols* and *Standard Extensions*. The first two subcriteria specify which description standards and exchange protocols the platform supports, e.g. Structured Threat Information eXchange (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII) [19, 20, 56]. *Standard Extensions* indicates whether the platform has published extensions to standards [53].

Provider & Users. This subcategory describes the parties involved in the provision and usage of the TISP. *Provider* and *Users* both share the subcriteria *Sector*, *Location* and *Organization Size*. The subcriterion *Sector* describes the industrial sector of the provider [5, 6, 23, 48, 51, 52]. Sectors are described following the International Standard Industrial Classification (ISIC), which differentiates between 21 distinct categories [57].

Location details the country in which the provider resides. *Organization Size* describes the size of the provider (small, medium or large organization) [58]. *Provider* is further specified by the subcriterion *Role*. It details if the provider uses the platform or if he acts as an intermediary [37, 50]. *Users* are described with similar subcriteria: *Sector* [7, 33, 39, 50], *Location* [52] and *Organization Size*. Additionally we used the subcriteria *Number of Users* and *Number of Active Users* [5,29,33,50]. An active user is a user who regularly uses the platform.

Usage Fees, License & Distribution. The last subcategory covers several business aspects of a TISP. *Usage Fees* describes fees charged for the use of the platform. It may be detailed into *Non-Recurring* and *Recurring* fees [1, 4, 5, 9, 23, 52]. *License* describes if the platform's source code is publicly available (open source) or if it is a proprietary software (closed source). *Geographical Focus* specifies the platform's geographical focus (regional, national, international, global) [5, 7, 41, 51, 54]. *Sectoral Focus* describes whether the platform targets a specific industrial sector or has a multi-sector focus [5, 39, 48, 54].

4. Demonstration of Evaluation Framework

As part of our literature review (see section 3.1) and an extensive web search, we identified 35 TISPs. We excluded platforms from our study for which we could not find detailed information.We applied the evaluation framework to a total of ten TISPs, three of which will be described in section 4.1. For reasons of brevity, the platforms will be presented in a succinct manner to highlight similarities and salient differences (see section 4.2).

4.1. Selected Platforms

MISP. The Malware Information Sharing Platform (MISP) is an open source platform funded by the European Union and the Computer Incident Response Center Luxembourg (CIRCL) [33, 59]. All four phases of the threat intelligence sharing process are supported by the platform: Collection of TI is enabled by the import of feeds and the option to produce TI for platform users. Aggregation of TI is achieved by using several functions (e.g. Fuzzy hashing or CIDR block matching). TI analysis can be conducted in groups and can yield visual results. Automated pull and push methods are provided to disseminate the resulting TI (e.g. in form of STIX or other textual formats). Information security measures are enforced according to ISO 27000, whereas data privacy measures are implemented according to the General Data Protection Regulation [60]. Collaboration can be supported either pseudonymously or publicly, with trust groups as a further means to team up. The supported import standard is Open Indicators of Compromise (OpenIOC), whereas both OpenIOC and STIX are listed as export standards. Interestingly, no details on data quality or reporting mechanisms are published on the platform. It is possible to equip the platform with various additional functions with the help of expansion modules. We classified MISP as an operational platform; however, it is also available as a software to build a platform. MISP provides an API for integrating the platform into security systems (e.g. into the intrusion detection systems Snort or Suricata) and a web-based user interface (English only). The content provided by MISP originates from internal sources created by platform users and 55 further public feeds (external sources). TI is provided in the form of IoC available both in structured (STIX and OpenIOC) and unstructured formats (English only). Various modules are available for exchanging TI, one of which supports the exchange protocol TAXII. No information about standard extensions is provided. The platform provider CIRCL uses the platform as part of its internal IT security management. Using the platform is free of charge and the platform's source code is publicly available. The platform does not belong to any sector. Users currently include 800 organizations worldwide.

OTX. Labeled the "world's largest open threat intelligence community" [61], Open Threat Exchange (OTX) is run by AT&T Cybersecurity, a subsidiary of AT&T Communications with headquarters located in the US. The platform supports three phases of the TI sharing process: The collection of TI occurs (either manually or in a semi-automated manner) via so called pulses which contain entries on TI. Various functions for TI aggregation are mentioned on the platform, however, no insights into concrete functions are given. By contrast, analysis procedures are outsourced to AT&T Cybersecurity TI experts who test, evaluate and reprocess the provided TI. Subsequent distribution occurs through the OTX DirectConnect API either in an automated push manner or a manual pull manner. Both mechanisms support information sharing in real time. Information security measures are enforced by taking "reasonable precautions", whereas data privacy is ensured by a privacy policy that is in conformity with the legal regulations of numerous countries (including the US, EU and several other European countries). Collaboration can happen anonymously or publicly either within forums or comment sections. Trust can, among other measures, be built by voting pulses up and down. This influences the reputation of pulse producers.

STIX serves both as the supported import and export standard. OpenIOC is also listed as supported export standard. Data quality functions are not described in detail, however, the provider states that means to ensure data quality are implemented internally. OTX provides means to report on TI events on a dashboard. We classified OTX as an operational platform. OTX provides an API (called DirectConnect) for integrating the platform into existing systems. The provider lists 29 supported IT systems. OTX offers a graphical user interface (English only). Little to no information is provided about the origin of the data sources. The provider states that in addition to the internal TI, selected public feeds and commercial data sources are included. OTX also uses honeypots that are operated by the provider as data sources. TI is provided in both structured and unstructured form, ranging from Common Vulnerability Exposures (CVE) and IoC to high-level summary reports about threats. STIX is listed as a description standard, whereas TAXII is used as an exchange protocol. AT&T Cybersecurity uses the platform for its own Unified Security Management. OTX is part of the information and communications sector. Currently, over 100,000 individuals and 7,000 organizations are registered as users. Given that the platform is open source, neither usage nor license fees are charged. The platform offers its services worldwide and has a cross-sector orientation.

ThreatQ. Developed and maintained by the US-based company ThreatQuotient Inc., ThreatQ is described as an ”open and extensible threat intelligence platform that accelerates security operations through streamlined threat operations and management” [62]. The platform supports all four phases of the TI process, but discloses only few details of the supported functions. The collection process encompasses the import of information provided by internal and external sources. Aggregation is achieved by functions that enable automatic combination, normalization and contextualization of threat data. Several analysis functions are listed, including the analysis of phishing attacks and adversary tracking. Distribution is enabled by automated push methods (i.e. sending specific actions, rules or signatures to network and end point security solutions). Information security measures are enforced according to ”appropriate technical and physical safeguard measures”. However, they are not described in detail. Data privacy is guaranteed according to an US-based privacy policy, which is also mentioned as a means to build trust. The supported import standards are STIX and OpenIOC, whereas only STIX is listed as an export standard. Collaboration is facilitated by the formation of cross-organizational teams. We could not discern any details on data quality functions and reporting mechanisms. ThreatQ offers a Software Development Kit (SDK) for customizing and extending the platform’s functionalities. We classified ThreatQ as an operational platform which provides an API and standard interfaces to be connected to existing security systems as well as ticketing systems. The platform also offers a graphical user interface (English only). Besides utilizing an internal TI data source, ThreatQ uses over 100 public and 49 commercial data sources. The TI content type is STIX as are the resulting artifacts; it thus includes both structured and unstructured contents (English only). Description standards encompass STIX and OpenIOC. TAXII is mentioned as an exchange protocol. We could neither identify the number of users nor details about the platform’s role (except that it is located in the information and communications sector). Platform users pay an annual fee. ThreatQ aims at customers worldwide. It has no industrial sector focus.

4.2. Similarities and Differences of the Platforms

The investigation of the three TISPs revealed some interesting similarities. We observed that all platforms intensively support the collection, aggregation and dissemination of TI; however, this is not the case for the analysis of TI. All platforms offer functions for enhancing information security, data privacy, collaboration, trust and import & export of TI. Moreover, all provide one or more APIs for integrating the platform into an organization’s IT infrastructure. All three platforms offer a graphical user interface. All platforms not only rely on internal data sources, but process a wide range of external data sources. Another common feature is that all platforms mainly use the following three standards: STIX, TAXII and OpenIOC. Interestingly, all three providers use their own platform as an element of their internal IT security management, i.e. they are not only intermediaries but benefit from the TI generated by their customers. Last, all providers make their platform available worldwide and have no industry sector focus.

We have discerned significant differences between the TISPs described in section 4.1, both on a functional as well as on a non-functional level. While the general support of the phases of TIS between platforms is similar, their functional scope in the individual phases differs considerably. ThreatQ, for example, offers substantially more sophisticated aggregation functions than the two other platforms. This significantly influences the later analysis of TI. The three platforms have two fundamentally different approaches for analyzing TI. OTX, for example, outsources measures to analyze TI to designated specialists, i.e. analysis functions are not processed by the platform. This means that standard functions for analyzing TI are missing on the platform. In contrast, MISP and ThreatQ take a different approach: TI is analyzed on the platforms and can be collaboratively examined by platform users or in user groups to yield vital results. These different approaches entail that the resulting TI which is to be distributed varies considerably in both content and expressiveness. There are also substantial differences in cross-phase functions, especially relating to data quality and reporting functions. Reporting is supported by non-customizable dashboards or individual threat reports. Only OTX offers more comprehensive reporting functions which also allow individualization, as well as various textual and visual reports. OTX is the only platform that states that it takes internal measures to ensure data quality.

Analyzing non-functional criteria also revealed a wide range of differences. Although all three platforms are operational platforms, MISP is also offered as software for building individual platforms. The number of external data sources used to generate TI is another significant difference between the three platforms. ThreatQ, for example, uses more than three times as many external data sources as MISP does. There are also salient differences in the content provided by the platforms. MISP focuses primarily on IoC, whereas ThreatQ and OTX provide information about Tactics, Techniques and Procedures (TTP) and high-level summary reports about threats (so-called tactical, operational and strategic TI [3]). There are also significant differences in the number of platform users: whereas OTX has 7,000 participating organizations, MISP only has 800.

5. Limitations

The research at hand might be limited by a *selection and classification bias of relevant publications*. In order to counteract this, we ensured that at least two authors selected and classified each paper. Moreover, the framework might be limited by an *incomplete list of evaluation criteria* since we only considered academic literature. Given that our approach relies solely on academic sources, it partially includes a practical perspective, as some of the papers based their results on empirical investigations (e.g. [27]). Still, the application of the evaluation framework showed that it seems to cover the majority of relevant criteria of a TISP. In this context, it is worth mentioning that the research at hand might be limited by the *small subset of TISPs we considered for the application of the framework*. This limitation can be justified by space limitations and our intention to primarily demonstrate the applicability of the framework. Thereby, we tried to select a representative set of platforms, namely an open source TISP, the largest publicly available TISP and a commercial TISP. Since we had full access to each TISP we comprehensively analyzed and evaluated these three TISPs. Furthermore, we had to extract information from provider websites and technical reports, which again could have biased our research.

6. Conclusion

In this paper we introduced an evaluation framework to analyze and compare current TISPs, which is of potential interest to both research and practice. It provides a basis for a common understanding of TISPs and thus supports the description, analysis and evaluation of these platforms. We developed the evaluation framework based on requirements and characteristics of TISPs derived from a set of 40 papers. To identify these papers, we conducted a literature review in which an initial set of 1,492 papers was analyzed. We demonstrated the applicability of the evaluation framework by analyzing three representative TISPs, including (i) MISP, (ii) OTX and (iii) ThreatQ. Our demonstration of the evaluation framework showed that the evaluation criteria and subcriteria specified in the framework allow a detailed description and comparison of TISPs. Commonalities, but also many differences between the three platforms could be presented comprehensively and systematically. Future work includes a comprehensive evaluation of the framework according to [12]. In doing so, we plan to conduct case studies with organizations selecting TISPs and ask experts to assess the completeness and applicability of the framework. By conflating academic and industry-based resources, the framework will become more balanced and robust. Moreover, our future work will focus on a comprehensive evaluation of all available TISPs, together with establishing a weighting of criteria and functions within the framework. The latter will add valuable granularity to our framework, and will render it more expressive.

References

[1] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018.

[2] G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, M. Carolan, D. Conroy, K. Boettinger, M. Gall, G. Brost, C. Ponchel, *et al.*, “A collaborative cyber incident

management system for european interconnected critical infrastructures," *Journal of Information Security and Applications*, vol. 34, pp. 166–182, 2017.

[3] D. Chismon and M. Ruks, "Threat intelligence: Collecting, analysing, evaluating," *MWR InfoSecurity Ltd*, 2015.

[4] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence–issue and challenges," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, pp. 371–379, 2018.

[5] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," *NIST special publication*, vol. 800, p. 150, 2016.

[6] A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, and L. Njilla, "Rethinking information sharing for threat intelligence," in *Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies*, p. 6, ACM, 2017.

[7] F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *computers & security*, vol. 60, pp. 154–176, 2016.

[8] L. Dandurand and O. S. Serrano, "Towards improved cyber security information sharing," in *Cyber Conflict (CyCon), 2013 5th International Conference on*, pp. 1–16, IEEE, 2013.

[9] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives," in *Towards Thought Leadership in Digital Transformation: 13. Internationale Tagung Wirtschaftsinformatik, WI 2017, St.Gallen, Switzerland, February 12-15, 2017.*, 2017.

[10] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*, pp. xiii–xxiii, 2002.

[11] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[12] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[13] O. Serrano, L. Dandurand, and S. Brown, "On the design of a cyber security data sharing system," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, pp. 61–69, ACM, 2014.

[14] S. Brown, J. Gommers, and O. Serrano, "From cyber security information sharing to threat management," in *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*, pp. 43–49, ACM, 2015.

[15] W. Zhao and G. White, "A collaborative information sharing framework for community cyber security," in *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pp. 457–462, IEEE, 2012.

[16] A. Schwartz, S. C. Shah, M. H. MacKenzie, S. Thomas, T. S. Potashnik, and B. Law, "Automatic threat sharing: How companies can best ensure liability protection when sharing cyber threat information with other companies or organizations," *U. Mich. JL Reform*, vol. 50, p. 887, 2016.

[17] A. Nolan, *Cybersecurity and information sharing: Legal challenges and solutions*. Congressional Research Service, 2015.

[18] R. A. Martin, "Making security measurable and manageable," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pp. 1–9, IEEE, 2008.

[19] S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (stix)," *MITRE Corporation*, vol. 11, pp. 1–22, 2012.

[20] J. Connolly, M. Davidson, and C. Schmidt, "The trusted automated exchange of indicator information (taxii)," *The MITRE Corporation*, 2014.

[21] J. Steinberger, A. Sperotto, M. Golling, and H. Baier, "How to exchange security events? overview and evaluation of formats and protocols," in *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pp. 261–269, IEEE, 2015.

[22] E. Asgarli and E. Burger, "Semantic ontologies for cyber threat sharing standards," in *Technologies for Homeland Security (HST), 2016 IEEE Symposium on*, pp. 1–6, IEEE, 2016.

[23] P. Kampanakis, "Security automation and threat information-sharing options," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 42–51, 2014.

[24] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," *Proceedings of the IEEE*, 2017.

[25] F. Menges and G. Pernul, "A comparative analysis of incident reporting formats," *Computers & Security*, vol. 73, pp. 87–101, 2018.

[26] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, pp. 51–60, ACM, 2014.

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

[28] C. Sauerwein, C. Sillaber, and R. Breu, "Shadow cyber threat intelligence and its use in information security and risk management processes," in *Multikonferenz Wirtschaftsinformatik 2018*, pp. 1333–1344, 2018.

[29] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, "Towards a maturity model for inter-organizational cyber threat intelligence sharing: A case study of stakeholders' expectations and willingness to share," in *Multikonferenz Wirtschaftsinformatik 2018*, pp. 1409–1420, 2018.

[30] M. Gschwandtner, L. Demetz, M. Gander, and R. Maier, "Integrating threat intelligence to enhance an organization's information security management," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, p. 37, ACM, 2018.

[31] E. V. D. Heuvel and G. K. Baltink, "Coordination and cooperation in cyber network defense: the dutch efforts to prevent and respond," *Best Practices in Computer Network Defense: Incident Detection and Response*, vol. 35, p. 121, 2014.

[32] M. A. Alhawamdeh, "Developing a conceptual national information sharing security framework to combat cybercrimes in jordan," in *Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on*, pp. 344–350, IEEE, 2017.

[33] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 49–56, ACM, 2016.

[34] S. Appala, N. Cam-Winget, D. McGrew, and J. Verma, "An actionable threat intelligence system using a publish-subscribe communications model," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pp. 61–70, ACM, 2015.

[35] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1–26, 2004.

[36] A. S. Jadhav and R. M. Sonar, "Framework for evaluation and selection of the software packages: A hybrid knowledge based system approach," *Journal of Systems and Software*, vol. 84, no. 8, pp. 1394–1407, 2011.

[37] A. Modi, Z. Sun, A. Panwar, T. Khairnar, Z. Zhao, A. Doupé, G.-J. Ahn, and P. Black, "Towards automated threat intelligence fusion," in *Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on*, pp. 408–416, IEEE, 2016.

[38] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Computers & Security*, vol. 67, pp. 35–58, 2017.

[39] T. Sander and J. Hailpern, "Ux aspects of threat information sharing platforms: An examination & lessons learned using personas," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pp. 51–59, ACM, 2015.

[40] G. Settanni, Y. Shovgenya, F. Skopik, R. Graf, M. Wurzenberger, and R. Fiedler, "Acquiring cyber threat intelligence through security information correlation," in *Cybernetics (CYBCONF), 2017 3rd IEEE International Conference on*, pp. 1–7, IEEE, 2017.

[41] R. Lewis, P. Louvieris, P. Abbott, N. Clewley, and K. Jones, "Cybersecurity information sharing: a framework for sustainable information security management in uk sme supply chains," 2014.

[42] G. Lodi, L. Aniello, G. A. Di Luna, and R. Baldoni, "An event-based platform for collaborative threats detection and monitoring," *Information Systems*, vol. 39, pp. 175–195, 2014.

[43] M. Bromiley, "Threat intelligence: What it is, and how to use it effectively," *SANS Institute InfoSec Reading Room*, 2016.

[44] D. Shackleford, "Who's using cyberthreat intelligence and how," *SANS Institute*, 2015.

[45] J. L. Hernandez-Ardieta, J. E. Tapiador, and G. Suarez-Tangil, "Information sharing models for cooperative cyber defence," in *CyCon*, pp. 1–28, 2013.

[46] H. Gascon, B. Grobauer, T. Schreck, L. Rist, D. Arp, and K. Rieck, "Mining attributed graphs for threat intelligence," in *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, pp. 15–22, ACM, 2017.

[47] Y. Zhao, B. Lang, and M. Liu, "Ontology-based unified model for heterogeneous threat intelligence integration and sharing," in *Anti-counterfeiting, Security, and Identification (ASID), 2017 11th IEEE International Conference on*, pp. 11–15, IEEE, 2017.

[48] S. E. Jasper, "Us cyber threat intelligence sharing frameworks," *International Journal of Intelligence and CounterIntelligence*, vol. 30, no. 1, pp. 53–65, 2017.

[49] S. Murdoch and N. Leaver, "Anonymity vs. trust in cyber-security collaboration," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pp. 27–29, ACM, 2015.

[50] S. Laube and R. Böhme, "Strategic aspects of cyber risk information sharing," *ACM Computing Surveys (CSUR)*, vol. 50, no. 5, p. 77, 2017.

[51] A. L. Joyce, N. Evans, E. A. Tanzman, and D. Israeli, "International cyber incident repository system: Information sharing on a global scale," in *Cyber Conflict (CyCon US), International Conference on*, pp. 1–6, IEEE, 2016.

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

[53] F. Fransen, A. Smulders, and R. Kerkdijk, "Cyber security information exchange to gain insight into the effects of cyber threats and incidents," *e & i Elektrotechnik und Informationstechnik*, vol. 132, no. 2, pp. 106–112, 2015.

[54] J. C. Haass, G.-J. Ahn, and F. Grimmelmann, "Actra: A case study for threat information sharing," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pp. 23–26, ACM, 2015.

[55] ISO/IEC, "ISO/IEC 27001:2005: Information technology, security techniques, information security management systems, requirements," 2005.

[56] OASIS. https://www.oasis-open.org/committees/cti. Last accessed 6-7-2019.

[57] UnitedNations, "United nations statistic division: International standard industrial classi- fication of all economic activities (isic) revision 4." https://unstats.un.org/unsd/classifications/Family/Detail/27. Last accessed 6-7-2019.

[58] OECD. https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm. Last accessed 6-7-2019.

[59] MISP-Project. https://www.misp-project.org/. Last accessed 6-7-2019.

[60] EUR-Lex, "Regulation (eu) 2016/679 of the european parliament and of the council." https://eur-lex.europa.eu/eli/reg/2016/679/oj. Last accessed 6-7-2019.

[61] AT&T-Cybersecurity. https://www.alienvault.com/open-threat-exchange. Last accessed 6-7-2019.

[62] ThreatQuotient. https://www.threatq.com/threat-intelligence-platform/. Last accessed 6-7-2019.