The quest for the appropriate cyber-threat intelligence sharing platform[a]

Thanasis Chantzios[1], Paris Koloveas[1], Spiros Skiadopoulos[1], Nikos Kolokotronis[1], Christos Tryfonopoulos[1], Vasiliki-Georgia Bilali[2] and Dimitris Kavallieros[2]

[1]*Department of Informatics and Telecommunications, University of the Peloponnese, Tripolis, Greece*

[2]*KEMEA Center for Security Studies, Ministry of Citizen Protection, Athens, Greece*

{*tchantzios, pkoloveas, spiros, nkolok, trifon*}*@uop.gr,* {*g.bilali, d.kavallieros*}*@kemea-research.gr*

Keywords: Cyber-threat, Intelligence, Sharing

Abstract: Cyber-threat intelligence (CTI) is any information that can help an organization identify, assess, monitor, and respond to cyber-threats. It relates to all cyber components of an organization such as networks, computers, and other types of information technology. In the recent years, due to the major increase of cyber-threats, CTI sharing is becoming increasingly important both as a subject of research and as a concept of providing additional security to organizations. However, selecting the proper tools and platforms for CTI sharing, is a challenging task, that pertains to a variety of aspects. In this paper, we start by overviewing the CTI procedure (threat types, categories, sources and the general CTI life-cycle). Then, we present a set of seven high-level CTI plaftorm recommendations that can be used to evaluate a platform and subsequently we survey six state-of-the-art cyber-threat intelligence platforms. Finally, we compare and evaluate the six aforementioned platforms by means of the earlier proposed recommendations.

1 Introduction

Cyber-threat intelligence (CTI) is any information that can help an organization identify, assess, monitor, and respond to cyber-threats. Examples of such information include indicators (system artifacts or observables associated with an attack), security alerts, threat intelligence reports, as well as recommended security tool configurations.

Most organizations already produce an enormous amount of CTI in multiple forms and types (Dalziel, 2015). It is crucial for effective cyber-defense to share such intelligence and information. Specifically, CTI sharing provides increased awareness, improved security posture, knowledge maturing, and increased defensive agility.

In this paper, we evaluate the appropriateness of different vulnerability reporting frameworks for disseminating the identified cyber-threats across different organizations to promote awareness about emerging cyber-threats. Moreover, we investigate issues pertaining to the basic structure, the key elements (i.e., expressiveness, flexibility, extensibility, automation, structuring), and prominent strengths and weaknesses of the presented frameworks.

[a] This work was funded by EU's Horizon 2020 research and innovation program under grant agreement no. 786698 and reflects only the authors' view.

Our goal is to survey related tools and platforms, evaluate them and identify the most appropriate for cyber-threat intelligence sharing, similarly to the work carried out in (Farnham, 2013), in which the author surveys leading tools and standards for CTI systems. In a nutshell, this work:

- Overviews CTI sharing. Specifically, we illustrate the corresponding CTI types (indicators, tactics, alerts, etc.), review possible CTI sources, and detail the CTI processing and sharing cycle. Moreover, we discuss the benefits of CTI sharing and present the challenges of CTI sharing.
- Presents a set of seven high-level recommendations that may serve as requirements for a CTI sharing platform.
- Surveys six state-of-the-art CTI sharing platforms, namely MISP, GOSINT, OpenTPX, YETI, OpenTAXII and CIF.
- Compares and critically evaluates the six aforementioned sharing platforms.

This paper is structured as follows. Section 2 overviews CTI sharing focusing on threat information types, CTI categories, the CTI cycle and the CTI sharing requirements. Section 3 surveys six state-of-the-art CTI sharing platforms and Section 4 reviews and evaluate them. Conclusions are offered in Section 5.

2 CTI sharing overview

Over the decades, cyber-threats have grown, morphed and become more sophisticated. Adversaries may now use a vast set of tools and tactics in order to attack their victims. Their motivations range from intelligence collection to service destruction and from reputation acquirement to financial gain. Nowadays, understanding the attacker is an increasingly complicated and highly important task required for security assurance. The way to identify and understand an attacker as well as the use of that information to protect organizations and infrastructures is a fundamental concept behind cyber-threat intelligence. Threat intelligence is focused on the analysis of the capabilities, motivations, and the goals of an adversary; and CTI is focused on how these goals are achieved using the cyber domains (Deloitte, 2015).

Cyber-threat information is any kind of information that could help an organization protect itself against any threat and detect the activities of an adversary. There are many types of threat information that may include:

Indicators. These are observables or technical artifacts suggesting that an attack is going to happen or that a compromise of the system has already occurred. Indicators can be used in a system to protect it against any potential threats. Examples of indicators include the IP address of a suspicious command, a distrustful DNS domain name, a URL that references suspicious content, a file hash using a malicious executable, or text code of a malicious email message.

Tactics, techniques, and procedures (TTPs). These elements are used to describe the behavior of an adversary. Specifically, *tactics* are descriptions of behavior, *techniques* are descriptions of tactics and *procedures* are detailed descriptions in the context of a technique. TTPs describe the willingness of an adversary to use a specific attacking tool, a malware variant, an exploit or a delivery mechanism (e.g., phishing).

Security alerts. Also known as *advisories*, security alerts are brief and human-readable notifications regarding vulnerabilities, exploits or security issues.

Threat intelligence reports. These include documents that describe TTPs, types of systems, adversaries and target information, as well as any other information related to cyber-threats that provide enhanced awareness to an organization.

Tool configurations. These include recommendations for the installation and the use of mechanisms in order to collect, process, exchange and analyze CTI. Tool configuration information may consist of instructions on how to customize and use intrusion detection signatures, web filter configuration files, or firewall rules.

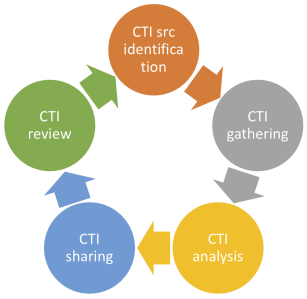

Figure 1: The CTI life-cycle

CTI sources can be categorized into three different categories: internal, community, and external (Friedman and Bouchard, 2015), and are briefly explained below:

Internal sources. In this group of sources, CTI is collected from an intra-organization level. This may include reported information from security tools like intrusion prevention systems (IPS), firewalls, host security systems (anti-virus), etc. In addition, a significant internal source of CTI derives from computer forensic analysis, which provides information about application settings, running processes, services used, system events, and so on, and could indicate adversarial behavior as well.

Community sources. These include CTI shared via a trusted relationship with multiple members having shared interests. This can be an informal group with member organizations that are in the same industry sector or that have other common interests. The information sharing and analysis centers are such an example (ENISA, 2018). They are non-profit organizations providing a central resource for gathering CTI and allowing two-way sharing between the private and the public sector.

External sources. This group contains CTI gathered outside of an organization. External sources may be distinguished into there categories. (a) *Public* that are provided freely and are based on volunteered data. (b) *Private* that require paid subscription and offer guaranties for data quality and credibility. (c) *Unindexed* that include sites accessible only from the deep or the dark web (e.g., chatrooms, pastebins, forums, marketplaces)

The CTI cycle, illustrated in Figure 1, is the process of generating and evaluating CTI. The first step of this process is CTI *source identification* (or *direction*). It pertains to the identification of threat information that needs to be collected from monitoring devices, feeds, and security repositories to support decision-making and raise cyber-security awareness.

The next step, CTI *gathering*, is the collection of the necessary data from the identified sources, along

with the tools for extracting a wide variety of information, like tactical information (infrastructure, malware, and exploits) and strategic information (revealing attackers' goals). This process requires a series of steps starting from the collection of relevant IP addresses. Moreover, it is not a one-time action, but, it should be performed in a continuous manner. The main goal at this stage is to collect as much information as possible and allow correlations and further analysis.

The third step is CTI *analysis* and is built upon the information that has being collected; it includes both automated and human means of analysis.

The fourth step is CTI *sharing* to the relevant stakeholders, i.e., the entities that can utilize the generated intelligence, in a form that they find to be appropriate, useful, and in many cases actionable. This makes sharing highly-dependent on the audience (e.g., tactical, operational, and strategic level).

CTI *review* (also referred to as CTI *feedback*), which is the last step in the above process, constitutes the key to the continuous improvement of the generated intelligence.

Threat information sharing provides access to threat information that in a different case might be unavailable to an organization. There is a plethora of benefits in sharing CTI that include:

Increased situational awareness. Using shared resources enhances security by leveraging the capabilities (e.g., knowledge, experience) of partners in a proactive way.

Improved security posture. It has become easier for organizations to identify affected systems, implement measures for protection, enhance their detection methods and recover from attacks.

Knowledge maturing. This process increases the value of information by enriching existing indicators and developing knowledge of adversary TTPs that are associated with a specific incident, threat, or threat campaign.

Increased defensive agility. Threat adversaries continuously adapt their TTPs and try to evade detection, security controls, and exploit new vulnerabilities. In order to reduce the probability of successful attacks, organizations are often informed about changing TTPs and usually detect and respond to threats rapidly.

Sharing threat intelligence information has numerous benefits; still it also raises several challenges that relate to the production and consumption of threat information that have to be addressed. In the following, we outline some important challenges; see also (NIST, 2016) for a thorough discussion of the topic.

Establishing trust. Trust relationships create the basics for information sharing, but their maintenance requires significant effort. To achieve that, all members participating in such relationships, should be provided with a common mechanism that is capable of preserving and continuously monitoring a trust model for the community.

Achieving interoperability and automation. The use of standardized data formats is an important building block for interoperability because it allows organizations and repositories to easily exchange threat information in a standardized way. However, an organization might require significant time and resources to adopt to new data formats.

Securing sensitive information. Publishing sensitive information such as controlled unclassified data and personally identifiable information may result in violating sharing agreements, and loss of reputation, or even financial loss. Organizations should implement policies and technical controls that disallow the disclosure of sensitive data.

Enabling information sharing. All organizations that are willing to publish and consume threat intelligence information need related tools and well-trained personnel. Typically, tools are responsible for information sharing (intelligence publication and consumption) while personnel focus on analysis, decision and action making.

The above is an indicative list of CTI sharing challenges and it is by no means complete. Several other issues need to be resolved. For instance, how to access external sources and incorporate actionable CTI, how to estimate the quality of the received CTI and how to provide CTI, how to comply with policies or requirements pertaining to privacy and the limitation of attribution should also be addressed (Brown et al., 2015; NIST, 2016).

We conclude this section by presenting recommendations of CTI sharing aspects by relying on a set of high-level requirements, and by considering the findings of desk research on the current situation on CTI sharing (Dandurand and Serrano, 2013; Sauerwein et al., 2017).

Requirement 1: The sharing mechanism must allow CTI sharing between the platform and different stakeholders (like service providers and certified authorities).

Requirement 2: The sharing mechanism must allow CTI sharing between the platform and the end-users' devices.

Requirement 3: The sharing mechanism and platform should be expressible, flexible, and scalable.

Requirement 4: The sharing mechanism (and platform) should allow information to be both human and machine readable and facilitate automation.

Requirement 5: The sharing platform should allow storing information about the source of CTI.

Requirement 6: The sharing platform should support information filtering and alerting.

Requirement 7: The sharing platform should be open source.

3 CTI sharing platforms

The complexity of modern infrastructures leads to a cyber-threat landscape of growing sophistication and complexity, where cyber-security incidents occur with increasing frequency. This fact necessitates efficient and automated tools for analyzing and sharing heterogeneous CTI related to the present systems' configurations, attacker's threats and tactics, indicators of ongoing incidents, and so on, in order to build proper and effective defensive capabilities. Given the numerous architectures, products and systems being used as sources of data for information sharing systems, standardized and structured CTI representations are required to allow a satisfying level of interoperability across the various stakeholders.

As highlighted in several works (Hernandez-Ardieta et al., 2013; Skopik, 2018) considerable efforts have been put during the last decade to standardize the data formats and exchange protocols related to CTI. The initiative led by MITRE, referred to as making security measurable (MSM)[1], constitutes the most prominent such effort along with the more recent initiatives of ENISA towards improving cyber-threat information sharing among the Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), Law Enforcement Agencies (LEAs), and other relevant stakeholders (ENISA, 2013; ENISA, 2015; ENISA, 2016). An overview of existing efforts is presented in Figure 2, where standards are classified into different areas. As we can see there is a wide variability in the areas covered by the standards that include: configuration guidance, vulnerability alerts, treat alerts, risk/attack indicators and so on. Furthermore, some of these standards, define how CTI should be outlined, on the matter of which information is useful and should be encompassed by the CTI sharing paradigm. For example, STIX (Structured Threat Information eXpression) belongs in three vulnerability areas (namely threat alerts, risk/attack indicators, and incident reports), since it encapsulates information about attack patterns, courses of action, vulnerabilities, reports, and more (OASIS-Open, 2018).

[1] https://msm.mitre.org

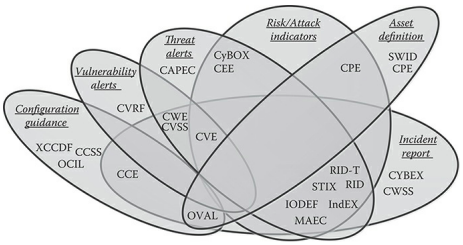

Figure 2: Different vulnerability areas covered by existing standards (Skopik, 2018)

The need of assessment, detection and gathering cyber-threat information escalated over the years; this is also demonstrated by the ENISA threat landscape report of 2017 (ENISA, 2017). Specifically, the survey of ENISA indicates that 9 cyber-threats out of the top 15 had an increased trend factor in 2016, whereas in the 2017, 11 cyber-threats' trend had been increased. That translates to a 13% increase of cyber-threats in one year. To address the increasing CTI needs, the formats and languages discussed in the beginning of this section, were realized into functional platforms. In the sequel, we outline six platforms and tools (namely MISP, GOSINT, OpenTPX, YETI, OpenTAXII, and CIF) that implement the aforementioned frameworks and language platforms for CTI sharing, also used by ENISA.

The malware information sharing platform (MISP). One of the most widespread CTI sharing platforms is Malware Information Sharing Platform (MISP) (Wagner et al., 2016). MISP is an open source threat intelligence and open standard for threat information sharing platform, which detects, stores and shares technical and non-technical information about malware samples, incidents, attackers and intelligence (MISP-Community, 2019). Specifically, MISP provides a User Interface (UI), which enables users to create, search or share events amongst other MISP users or communities. Furthermore, all CTI stored in the MISP database can be accessed through an API, which allows for data exporting in a wide variety of formats, such as XML, JSON, OpenIOC, STIX, and more.

Additionally, MISP has an automatic correlation mechanism that is able to identify relationships between attributes, objects and indicators from malware correlation engines. Moreover, MISP stores data in a structured format, provides extensive support of cyber-security indicators for different vertical sectors, and supports CTI sharing for both human and machine applications. More details about MISP functionalities are described in https://github.com/MISP/MISP.

Intelligence vocabularies (MISP galaxy) can be bundled with existing threat adversaries, malware

and ransomware or linked to events from MITRE ATT&CK[2], which is a publicly available knowledge base, that contains adversary tactics and techniques based on real observations. Communities can leverage MITRE ATT&CK, in order to develop specific threat models and methodologies for Tactics, Techniques and Procedures (TTPs).

Finally, MISP provides a flexible free text import tool to facilitate the integration of unstructured reports into MISP and an adjustable taxonomy to classify and tag events according to the users' own classification schemes and taxonomies.

The open source intelligence gathering and processing framework (GOSINT) GOSINT is another popular open source platform, developed by Cisco CSIRT, and it focuses on intelligence gathering and processing. It collects, processes and exports IoCs; in this way it controls the data inclusion process in the platform and enriches it with high-quality metadata. GOSINT aggregates, validates, and sanitizes indicators for consumption by other tools including MISP and CRITs[3], or directly into log management systems and SIEMs, while also supporting STIX, TAXII (Trusted Automated eXchange of Intelligence Information) and VERIS (Vocabulary for Event Recording and Incident Sharing) formats used in the CTI sharing paradigm.

Other than the aforementioned formats, GOSINT also supports Incident Object Description Exchange Format (IODEF) and Intrusion Detection Message Exchange Format (IDMEF), and it allows forensic experts to gather structured and unstructured data from incidents occurring at third parties. Thus, it may also act as a powerful aggregator of IoCs before they are passed to another analysis platform or a SIEM. Furthermore, GOSINT supports several actions to provide additional context to indicators in the preprocessing phase. Such actions may include the identification of IoCs with systems like Cisco Umbrella[4]. The information returned from these services may help analysts judge the value of the indicator, as well as tag the indicator with additional context that might be used later in the analysis pipeline.

The GOSINT framework is written in Go with a JavaScript frontend. The main drawbacks of the GOSINT platform are mainly related to package management. Specifically, package managers of GOSINT provide out-of-date versions of the software, and hence they should be tested to ensure compatibility. Furthermore, packages' names are differentiated, with regard to the package managers or OS release repository at hand.

Open threat partner exchange (OpenTPX). OpenTPX[5] is a JSON-based data model repository platform that enables registering and sharing incident information. It supports several well-known protocols including HTTP, SMTP, FTP, and so on, and it was created to build highly scalable machine-readable threat intelligence, analysis and network security products that exchange data at large volumes and at high speed. Moreover, OpenTPX defines a comprehensive model for describing cyber-threats, and also provides mechanisms to convey network topology information, network ownership, network segmentation, threat metadata, threat intelligence and mitigation actions. Furthermore, aspects of data available in the STIX format (e.g., indicators), have direct mapping to OpenTPX. Finally, it uses the threat score conceptual model (LookingGlass, 2015), which aims to describe, in a comprehensive manner, the score of the security landscape.

Your everyday threat intelligence (YETI). YETI is an open source, distributed, machine and analyst-friendly threat intelligence repository[6]. YETI is a platform meant to organize observables, IoCs, TTPs, and threat intelligence in a single, unified repository. Moreover, YETI automatically enriches observables (e.g., by resolving domains and geolocating IPs) on behalf of the user and provides a bootstrap-based user interface for humans and an API-based for machines so that to facilitate communication and interoperability with other CTI tools[7].

Trusted automated exchange of indicator information (OpenTAXII). The OpenTAXII platform[8] is an upgraded form of TAXII services. Its architecture follows the TAXII specifications with functional units for the TAXII transfer unit, the TAXII message handler, and other back-end services. OpenTAXII is a robust Python implementation of TAXII services that delivers a rich feature set. It offers extendable persistence and authentication layers (both via a dedicated API) and provides a collection of threat specifications. Additionally, it provides an appropriate set of services and message exchange functionality to facilitate CTI sharing between parties. Some other characteristics of OpenTAXII include customizable APIs, authentication and flexible logging. Furthermore, it automatically handles the data of the frameworks, provides machine-readable threat intelligence, and combines network security operations data with threat intelligence, analysis and scoring of data in an optimized

[2] https://attack.mitre.org
[3] https://crits.github.io
[4] https://umbrella.cisco.com
[5] https://opentpx.org/
[6] https://yeti-platform.github.io/
[7] http://gosint.readthedocs.io/en/latest/
[8] http://www.opentaxii.org/en/stable/

manner.

Collective intelligence frameworks (CIF). CIF[9] is a CTI management system and one of the platforms of choice of ENISA for CTI sharing (ENISA, 2017). CIF helps users to parse, normalize, store, post-process, query, share and produce CTI data, while allowing them to combine known malicious threat information from many sources and utilize that information for identification (incident response), detection (Intrusion Detection System) and mitigation (null route). It also supports an automated form of the most common types of threat intelligence such as IP addresses and URLs that are observed to be related to malicious activity. The CIF framework aggregates various data-observations from different sources. When a user queries for CTI data, the system returns a series of chronologically ordered messages; users are then able to make decisions by examining the returned results (e.g., series of observations about a particular adversary) in a way similar to examining an email threat. The CIF server consists of a few different modules including: CIF-smrt, CIF-worker, CIF-starman, CIF-router and ElasticSearch.

The CIF-smrt module has two primary capabilities: (a) to fetch files using http(s) and (b) to parse files using built-in parsers for regular expressions, JSON, XML, RSS, HTML and plain text files.

Finally, the CIF-worker module helps CIF extract additional intelligence from collected threat data, the CIF-starman module offers an HTTP API environment, the CIF-router module provides the broker mechanism between the client and web framework, while the ElasticSearch module is a data warehouse for storing (meta)data for intrusions.

4 CTI platforms evaluation

An observed outcome reached out from the characteristics of the six referred platforms, is the utilization of the same threat intelligence framework, namely STIX; notice that STIX and TAXII are currently two of the most used sources in the threat intelligence platforms.

We will now review the benefits and the drawbacks of the six CTI sharing platforms we have considered in Section 3. For convenience, our findings are summarized in Figure 3. In the following, we present the highlights of each platform.

MISP platform is fully organized and the range of individuals that could utilize it could be developers or even simple users, providing material for stand-alone sharing. It is very flexible, expandable and automated. The information in the database can be extended by external sources while its functionality can be extended by integrating with third-party tools. MISP is both human and machine readable, making correlations between observables and attributes possible, which is an exceptional characteristic consisted by series of data models created by MISP community.

GOSINT has an organized repository, a managing system and exporting data functionalities. It can also be extended by external sources (URL, TEXT, ADHOC). It has a community that applies research that automatically identifies similar, or identical, indicators of malicious behavior. Finally, GOSIT is both human and machine readable.

OpenTPX has an organized repository, is very flexible, extensible and provides automation support. It also offers enhancements of data capabilities by allowing extensions to threat observables descriptions. It provides a comprehensive threat-scoring framework that allows security analysts, threat researchers, network security operations and incident responders to make relevant threat mitigation decisions straightforwardly.

YETI platform has an organized repository, is very flexible, extensible and provides automation support. It is both human and machine readable. YETI's goal, is to turn it into a self-sustainable project, where not only the core developers but the whole community helps out. To this end, the communication between community partners is centralized and is based on GitHub.

OpenTAXII has an organized repository and managing system, and can also mimic already known cases and threats. It is flexible and extendable since it is providing machine-readable threat intelligence, possibility of layer extension, source intelligent extension and APIs extension. It also provides automation support.

CIF has an organized repository and managing system. It also offers data exporting facilities. It provides combination of malicious threats and utilize that information for identification (incident response), detection (IDS) and mitigation (null route). CIF can be extended by indicators of malicious behavior. It also provides automation support. Finally, it is both human and machine readable.

Based on the above discussion, we proceed to map in a simple manner the extent to which properties of Requirements 3, 4 and 5 are being met by the candidate platforms. Requirement 7 is not considered since all tools are open source. Score values are analyzed in the following table:

[9] https://github.com/csirtgadgets/massive-octo-spice/wiki/The-CIF-Book

Platform	MISP	GOSINT	OpenTPX	YETI	OpenTAXII	CIF
Organized repository	MISP GALAXY (support of big objects and complex data), taxonomies, MITRE ATT&CK	Taxonomies, alert data, intrusions	Network topology information, network ownership, network segmentation, threat metadata, threat intelligence, mitigation actions, network security products	XML feeds, JSON feeds, taxonomies	References, data and metadata of threats, mitigation actions	CIF intelligence vocabularies (CIF-feeds), Combination of malicious threats
Organized community	Gitter community	GOSINT community (chatting)	Threat scoring framework	YETI GitHub Community	-	-
Helpful documentation	Draft documents and training material	Draft documents, lexicons, artifacts	-	MISP instances	-	-
Creativity	Already applied and suggested data models, opportunity to make your own models	-	Comprehensive model of threat associated, tools of optimizing threats	-	-	-
Added tools	Free text import tool	-	-	-	-	-
Additional benefits	Organized GitHub, complete online documentation	-	-	-	-	-
Drawbacks	-	Not providing updates. Package managers may name packages differently	It is not human readable only machine	Does not provide tools for creation of incident attack. Does not make correlations between observable and attributes	Does not provide tools for creation of incident attacks	Only observed threats (such as IPs)

Figure 3: CTI platform comparison

Platforms	MISP	GOSINT	OpenTPX	YETI	OpenTAXII	CIF
Interoperable	2	2	1	1	2	1
Expressiveness	2	1	2	1	1	1
Flexibility	2	1	2	2	1	1
Extensibility	2	2	1	1	2	1
Automation	2	2	2	2	2	2
Human/machine readable	2	2	-	2	1	2
Overall score	12	10	-	9	9	8

Table 1: Overall scoring of the referred platforms

Score	Explanation
-	not supported
1	supported to a satisfying level
2	supported to a high level

As shown in Table 1 all platforms support a number of requirements from those presented in Section 3, to a different extend as depicted in their score.

From the above comparison, it is evident that MISP and GOSINT are taking the lead in platforms' race, when compared to the rest of the platforms.

5 Conclusions

This paper presented an overview of CTI sharing. Initially, we have illustrated the corresponding threat information types (indicators, tactics, alerts, etc.), reviewed possible CTI sources, and detailed the CTI processing and sharing cycle. Then, we have discussed the benefits and presented the challenges of CTI sharing. Moreover, we have presented a set of seven high-level recommendations for a CTI sharing platform that can be used for evaluation. Subsequently, we have surveyed six state-of-the-art CTI sharing platforms (MISP, GOSINT, OpenTPX, YETI, OpenTAXII and CIF) and compared and evaluated them, using the suggested recommendations.

REFERENCES

Brown, S., Gommers, J., and Serrano, O. S. (2015). From cyber security information sharing to threat management. In *WISCS 2015*, pages 43–49.

Dalziel, H. (2015). *How to Define and Build an Effective Cyber Threat Intelligence Capability*. Elsevier.

Dandurand, L. and Serrano, O. S. (2013). Towards improved cyber security information sharing. In *CyCon 2013*, pages 1–16.

Deloitte (2015). Building an informed community: New cyber-threat landscape makes sharing intelligence imperative. Online. Accessed: 3 Mar. 2019.

ENISA (2013). Detect, share, protect: Solutions for improving threat data exchange among certs. Online. Accessed: 26 Feb. 2019.

ENISA (2015). Information sharing and common taxonomies between csirts and law enforcement. Online. Accessed: 26 Feb. 2019.

ENISA (2016). Report on cyber security information sharing in the energy sector. Online. Accessed: 26 Feb. 2019.

ENISA (2017). Enisa threat landscape report 2017 - 15 top cyber-threats and trends. Online. Accessed: 27 Feb. 2019.

ENISA (2018). Information sharing and analysis centres (isacs): Cooperative models. Online. Accessed: 25 Feb. 2019.

Farnham, G. (2013). Tools and standards for cyber threat intelligence projects. SANS Institute Information Security Reading Room.

Friedman, J. and Bouchard, M. (2015). *Definitive Guide to Cyber Threat Intelligence*. CyberEdge.

Hernandez-Ardieta, J., Tapiador, J., and Suarez-Tangil, G. (2013). Information sharing models for cooperative cyber defense. In *CyCon 2013*, pages 63–90.

LookingGlass (2015). Opentpx v2.2. Online. Accessed: 3 Mar. 2019.

MISP-Community (2019). Misp user guide: A threat sharing platform. Online. Accessed: 2 Mar. 2019.

NIST (2016). Guide to Cyber Threat Information Sharing. *Special Publication*, 800(150).

OASIS-Open (2018). Introduction to stix. Online. Accessed: 2 Mar. 2019.

Sauerwein, C., Sillaber, C., Mussmann, A., and Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In *WI 2017*.

Skopik, F. (2018). Collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks at national level. *CRC Press*.

Wagner, C., Dulaunoy, A., Wagener, G., and Iklody, A. (2016). MISP: the design and implementation of a collaborative threat intelligence sharing platform. In *WISCS 2016*, pages 49–56.