future internet

MDPI

Article

A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence

Alessandra de Melo e Silva [1], João José Costa Gondim [1,2], Robson de Oliveira Albuquerque [1,3] and Luis Javier García Villalba [3,*]

[1] Post Graduation in Electrical Engineering (PPEE), Department of Electrical Engineering, University of Brasília, Brasília 70910-900, Brazil; alessandra.melo@aluno.unb.br (A.d.M.e.S.); gondim@unb.br (J.J.C.G.); robson@redes.unb.br (R.d.O.A.)

[2] Department of Computer Science (CIC), University of Brasilia (UnB), Brasilia-DF 70910-900, Brazil

[3] Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM), Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid, Spain

* Correspondence: javiergv@fdi.ucm.es

Received: 18 May 2020; Accepted: 14 June 2020; Published: 23 June 2020

Abstract: The cyber security landscape is fundamentally changing over the past years. While technology is evolving and new sophisticated applications are being developed, a new threat scenario is emerging in alarming proportions. Sophisticated threats with multi-vectored, multi-staged and polymorphic characteristics are performing complex attacks, making the processes of detection and mitigation far more complicated. Thus, organizations were encouraged to change their traditional defense models and to use and to develop new systems with a proactive approach. Such changes are necessary because the old approaches are not effective anymore to detect advanced attacks. Also, the organizations are encouraged to develop the ability to respond to incidents in real-time using complex threat intelligence platforms. However, since the field is growing rapidly, today Cyber Threat Intelligence concept lacks a consistent definition and a heterogeneous market has emerged, including diverse systems and tools, with different capabilities and goals. This work aims to provide a comprehensive evaluation methodology of threat intelligence standards and cyber threat intelligence platforms. The proposed methodology is based on the selection of the most relevant candidates to establish the evaluation criteria. In addition, this work studies the Cyber Threat Intelligence ecosystem and Threat Intelligence standards and platforms existing in state-of-the-art.

Keywords: cyber security; cyber threat intelligence; threat intelligence platform; threat intelligence standard

1. Introduction

Over the last years, with the relevant increase in computational power and communication technologies, a new trend of diverse network devices and different technological systems emerged quickly and they are delivering a wider range of exploitable vulnerabilities [1]. Consequently, the number of cyber attacks and their costs have also increased [2]. Also, these new cyber exploits are more complex and targeted [3], generating sophisticated and improved attacks. Such facts indicate that the cybersecurity spectrum is fundamentally changing and becoming increasingly challenging.

The progressive evolution of the current cyber attacks arises from a cascade of new sophisticated applications that are being developed by attackers and security experts, and the more complex a system gets, the more insecure it becomes [4]. Another reason for the improvement of the attacks is the fact that these are being better planned and applied in a more specific way [5], which makes them more complex. Most of them are developed to not be detected by first level defenses, being able

to persist on the system [6]. Besides that, these new threats are in a constant process of modification and improvement, making their detection and defense more complicated [5]. The advances and modifications in the cyber attack ecosystem have encouraged changes in the traditional defense model and the search for more efficient and proactive methods [1,6].

Considering the presented scenario, the idea of Cyber Threat Intelligence (CTI) has been rapidly popularizing and is often posed as a new solution for applying effective security to enterprise [7]. Any valuable information that can be used to identify, characterize or assist in the response to cyber threats is commonly referred to as cyber threat information and the analysis of this type of information can produce intelligence to inform the user about threats to their system [8]. Within the limitations of the CTI approach, there is the heterogeneity of the data involved [9,10], and the massive amount of data for collection [11]. So, in order to effectively use the cyber threat information, mechanisms capable of consuming, analyzing, evaluating and classifying the information are highly needed [12].

Thus, new automated systems with the ability to consume a vast amount of data, provide sophisticated defense capabilities and respond to incidents in real-time are being developed and commonly referred to as Threat Intelligence (TI) platforms [13,14]. These platforms should include automatic processes of data transformation and intelligence production to ensure a more efficient, proactive and timely defense model [15]. Besides, due to the heterogeneity of the data inserted in the CTI context, considerable efforts have been made in order to standardize the data [13] and make it compatible among different systems[12]. The interoperability of the data is important to facilitate the automatic gathering and analysis of the data and the sharing of cyber threat intelligence [9].

However, since the field is growing rapidly [15], today CTI concept lacks a consistent definition [11,16] and a heterogeneous market of CTI platforms emerged. Diverse systems and tools, which accomplish different goals, are implemented as threat intelligence platforms [14]. Besides, capabilities, performance levels, and applicable use cases vary greatly among platforms an this is not always transparent to the user [14]. Therefore, it is notorious a research gap involving the analysis of CTI systems and tools available, in order to describe in detail their features and evaluate the quality of the information that can be produced and disseminated with them.

The goal of this research is to provide a methodology for the evaluation of the standards and platforms of Cyber Threat Intelligence. The research includes a review of the state-of-the-art regarding the cyber threat intelligence ecosystem and existing TI standards and platforms, by presenting the directions that the theme has been following in recent years and the TI initiatives that have been consolidated or have great potential to be consolidated in this area. To achieve that, first, a review of the existing CTI standards and platforms is made to identify potential and relevant research opportunities. Then, a selection strategy is proposed to define the most popular standards and platforms. The selected ones had their features and usability analyzed, in a practical way. Finally, they were evaluated based on holistic and comprehensive evaluation criteria.

Previous researches have focused on comparing a large number of platforms and apply little or trivial criteria in the evaluation process. Our work complements the related research work by summarizing a significant and comprehensive evaluation of TI standards and platforms simultaneously. It presents an adequate strategy for selecting relevant platforms and standards and an integrated methodology covering a wide range of aspects for the evaluation criteria. Finally, the results and discussion about the evaluation process provide a valuable overview of the CTI landscape.

The remainder of this paper is structured as follows. Section 2 brings an overview of related work and some definitions relevant to understanding the cyber threat intelligence landscape. Section 3 presents a methodology proposal for evaluating CTI standards and platforms. Sections 4 and 5 present the results of the evaluation. Section 6 gives a discussion. Finally, Section 7 concludes the paper.

2. Related Work and Definitions

In this section, a brief background on the CTI panorama is provided. Relevant related work to our research topic is presented along with some definitions and concepts.

Even though a lot of work has been done in the area of Cyber Threat Intelligence in recent years, most of it is not focused on analyzing and evaluating the state-of-the-art of TI standards and platforms. Besides, considering that this type of technology evolves at a rapid pace, some work and results can become out of date. To get a detailed picture of available work in the area and research gaps, a literature review was made.

Much work has been carried out into understanding and presenting the Cyber Threat Intelligence landscape. A survey [17] provides a broad description of the CTI topic and briefly mentions some platforms and standards. In Reference [18], the work is more focused on TI platforms and presents a general overview of the threat intelligence platforms landscape, including open source and commercial platforms. Other work [19] describes some selected open source threat intelligence platforms and standards but no evaluation is done. A recent survey [20] discourses about research opportunities regarding exchange standards and mentions, without any type of analysis, some of the most popular languages for CTI description and sharing, which are: Structured Threat Information eXpression (STIX), Trusted Automated Exchange of Intelligence Information (TAXII), Open Threat Partner Exchange (OpenTPX), Malware Attribute Enumeration and Characterization (MAEC), Incident Object Description Exchange Format (IODEF) e Vocabulary for Event Recording and Incident Sharing (VERIS).

Considering the existing limitations to fully implement CTI mechanisms as a model of defense, some work has been made to propose frameworks and platforms that could overcome these obstacles. An important limitation is the quality of CTI data produced and shared [4], that were addressed in many works with the use of machine learning techniques. To CTI be effective for defense models, it should be sensitive to the context which is applied [4,13]. Thereby, initiatives that uses machine learning techniques for predicting personalized and context-aware data, as the ones presented in References [21,22], could bring great advances to CTI by assisting in data enrichment processes. Also, as proposed in Reference [23], intrusion detection systems can benefit from artificial intelligence mechanisms, as machine learning, to build an intelligent data-driven system. Following this idea, in Reference [24] presents good prospects for the use of artificial intelligence in cyber security. The research discourses about the massive amount of threat data available and puts the powerful automation and data analysis capabilities of machine learning techniques as a solution to handle the volume of data. In Reference [25], using machine learning algorithms, a framework was developed to collect and analyze data and attribute threat incidents to their threat actors. Another work, Reference [26] proposed a threat intelligence platform with an architecture based on state-of-the-art systems like Malware Information Sharing Platform (MISP) and Collaborative Research into Threats (CRITs). The platform applies machine learning algorithms to analyze and classify email content and actively defends against social engineering. To increase the maliciousness estimation of threat indicators, Kazato et al. [27] uses a graph convolutional network based method. The method provided an improvement to the maliciousness estimation accuracy and reduced the time allocated to the analyses of indicators by human hands. Also in terms of improving the quality of threat indicators, in Reference [9] a novel method to automatically extract indicators and apply domain tags from social media is proposed. The method includes a convolutional neural network to recognize CTI domains and correctly classify threat data into these domains. The amount of related work that explores the use of artificial intelligence, manly machine learning techniques, in cyber security methods and frameworks shows the importance of its utilization and indicates some research opportunities.

Regarding another limitation, in Reference [8], the difficulty related to the lack of confidence from organizations in sharing sensitive CTI data is addressed. Chadwick, et al. [8] introduces a trust model among organizations combined with a data sharing and analysis framework allowing a confidential exchange of data. Irrespective of some limitations, the results presented show the achievement of expected results. Along the same lines, Riesco et al. [11] works to reduce the reluctance to share CTI data. The work provides an extensive list of the open challenges of existing solutions in information sharing, and propose a solution to cover all these challenges at the same time.

The solution uses a combination of STIX and Ethereum Blockchain to achieve its goal. Results presented showed an improvement in important points like identification of trusted sources, availability and economic cost, comparing to other solutions available. The approach presented in Reference [28] also works on the topic of sharing CTI data securely. The method not only provides trust levels among organizations, but it also combines the model of trust with encryption mechanisms for the data, bringing more confidence to the sharing process. In the same way, Wu et al. [29] proposes a framework for decentralized sharing of data using blockchain. The work considers the trust between participants, the trust of TI quality and the trust in the platforms, and uses encryption of data as one of the mechanisms to ensure confidentiality. Thus, it is notorious that the use of encryption systems like the ones presented in Reference [30,31] could bring improvements to CTI processes. Even though encrypt CTI data before sharing it could improve the confidence from organizations in exchanging their sensitive data, the majority of the TI standards use common formats, like JSON and XML, to provide threat data, relying the security on the transport mechanism used. Since most standards follow this perspective, TI platforms available usually also do not support encrypted data as import or export formats. However, considering the benefits that the combination of encryption systems and CTI platforms could bring, this should be considered a productive research gap.

In another perspective of analysis and comparison, some research was made regarding CTI standards taxonomies and ontologies. The work presented in Reference [32] aimed to analyze different CTI exchange ontologies. A layered model is proposed and two sharing protocols, together with their respective transport protocols (STIX/TAXII and IODEF/RID), are examined using the model. The work provides a great overview of the analyzed protocols, presenting a detailed schema of each one and leaving research opportunities about the topic. In Reference [33], taxonomies, sharing standards and ontologies relevant to CTI scope are evaluated. These topics are analyzed based on data and concepts defined by two different CTI models presented, relationships with other taxonomies and ontologies and description provided by its documentation and source files. The sharing standards evaluated were STIX, MAEC and OpenIOC, however, they were not the main topic of discussion since the focus of the work stood out on the ontologies subject. Reference [34] focuses on semantic ontologies for sharing standards. In this work, STIX and IODEF were mapped into RDF/OWL ontologies and the mappings were analyzed providing an overview of their characteristics and showing differences and similarities between the standards.

Some similar research interested in the evaluation or comparison of standards or platforms were conducted. One of the first works on this subject [35], introduces 8 different exchange formats: Common Intrusion Detection Framework (CIDF), IODEF, Common Announcement Interchange Format (CAIF), Intrusion Detection Message Exchange Format (IDMEF), Abuse Reporting Format (ARF), Common Event Expression (CEE), Extended Abuse Reporting Format (X-ARF) and Syslog. These formats are evaluated based on an evaluation methodology proposed that consists of 10 different criteria such as interoperability, confidentiality and practical application. The evaluation provides a significant methodology and good results but some important formats, that are currently relevant, have not been addressed showing that some results are out of date. In Reference [36], the complete CTI panorama is considered and some CTI standards are presented. Besides that, a good evaluation of some open source threat intelligence tools is done in order to compare them with the tool proposed in the work. In Reference [16] the classification and analysis of 23 threat intelligence platforms are made based on the licensing model, supported standards, type of platform and type of information shared. The result of the analysis presents some interesting facts about the CTI panorama, like the finding that most of the threat intelligence platforms are closed source, the description of STIX as the de-facto standard for describing threat intelligence and the discovery that most platforms prioritizes sharing over analyzing the information. However, the results are consolidated in eight key findings, which does not allow an in-depth understanding of the features and operation of the platforms. In Reference [37] a satisfactory comparative analysis of some important incident reporting formats, including different versions, is performed revealing strengths, weaknesses and additional information of the formats.

In Reference [12], in order to explore the existing interoperability challenges when using specific sharing solutions, Rantos et al. [12] analyse semantic, syntactic and technical aspects of the most prominent standards considered by the work. Thus, some characteristics including type of data and supporting sources were described and can be used as a base for future research in the area.

A recent work [13] provides a comparative analysis of cyber threat intelligence sources, formats and languages. Several CTI sources are presented and examined, and based on the results of the examination together with literature research, some CTI standards were selected for further analysis. Many criteria and features were considered in the comparison, providing a great and detailed description of the capabilities of some relevant CTI standards. Some specific CTI standards are analyzed in the work, like STIX and MISP, but some common formats like CSV and RSS are also included in the comparison, which differs from the standards selected in this paper that were designed specifically to represent threat intelligence data. With a similar goal to this work, Bauer et al. [14] presents a framework capable of analyzing and comparing threat intelligence sharing platforms. Based on a systematic literature review, 40 different publications that contained characteristics or requirements for Threat Intelligence Sharing Platforms (TISPs) were studied. Therewith, 62 essential evaluation criteria were determined and divided into six main categories that were used by the proposed framework to evaluate the platforms. The work mentions that the framework was applied to ten different TISPs, but only three of them had the results described. The results revealed interesting information about the described platforms, including some similarities and differences. However, for limitation issues, only a small set of platforms were considered.

Most of the research and work developed in the field focus on comparing a large number of platforms or standards and does not provide a critical analysis. On the other hand, few works present great evaluation or comparison but only of a few platforms or standards. Besides, some works focus efforts on TI initiatives that have not been consolidated in the area or are out of date. So, to the best of our knowledge, no prior research has been conducted that simultaneously analyzes and evaluates standards and platforms relevant for the TI scenario, based on a methodology that covers a wide range of criteria for the evaluation.

Some fundamental concepts must be presented to facilitate the understanding of the methodology adopted and results obtained. These definitions will be presented as following.

2.1. New Threat Landscape

The great evolution of computing in recent years largely stems from the appearance of multiple and heterogeneous devices [38] that can interact with other objects and applications over the internet [39]. However, the heterogeneity and interconnectedness of these devices lead to a significant increase in the number of security attacks [40] and the threat environment is expanding in alarming proportions. This growth comes together with more complex attack scenarios and sophisticated threats. Nowadays, adversary behavior is more focused on the target and it considers multi-staged attacks that aim to persist on the host or system and cause ongoing damage [41]. Most of these attacks do not generate noise or substantial changes in the environment, making it harder to detect.

Some of these new generation threats are denominated Advanced Persistent Threats (APTs). They perform a sophisticated type of attack characterized by establishing a persistent foothold into the target and stay undetected for a long period of time [5]. Also, there are polymorphic threats with the capability of constant modification, making the detection a complex task. Additionally, other type of threat largely exploited is the zero-day vulnerabilities. Since they explore unknown vulnerabilities of software, it is easy to stay undetected for long periods until the flaw is discovered and patched [4].

2.2. Threat Intelligence

The term intelligence has the most diverse definitions. This can be explained due to the fact that intelligence is a concept strongly dependent on the context it is inserted. A generalized definition of

the term was presented in Reference [42] and considered widely applicable. It describes intelligence as the process of transforming topics from the completely unknown stage until reaching a state of complete understanding. In order to achieve this goal, random and generic data must be filtered in a minor and relevant data set based on the context intended, which are then processed and transformed into information.

In this sense, the information, when analyzed and contextualized, becomes intelligence [7]. Considering such assumptions, a generic intelligence production process is commonly composed of three main stages: collection of data, processing the data to transform into information and analysis of the information to produce intelligence.

The intelligence concept can be divided into different strands, where actionable intelligence is one of them. So, for intelligence to be considered actionable, it must meet the requirements of being timely, accurate and relevant [43].

Following this perspective, threat intelligence should satisfy these characteristics to provide assistance in developing efficient mechanisms to respond to threats, which is commonly defined as a type of actionable intelligence. Thereby, in addition to the generic intelligence production flow aforementioned, the stages of deploying and disseminating the intelligence are also contemplated as essential to the generation process of threat intelligence. So, in the context of this work, the intelligence process flow is composed of five main stages, as presented in Figure 1:

1. **Collection**: This step refers to the gathering of data, which are simple indicators or facts.
2. **Processing**: works on combining the data aiming to answer specific questions and provide information.
3. **Analysis**: evaluates data and information together helps to uncover patterns and to produce actionable intelligence. With the intelligence produced, it is possible to
4. **Deploy**: it by making decisions to utilize the intelligence.
4. **Dissemination**: Expand it by sharing the intelligence with interested parts.

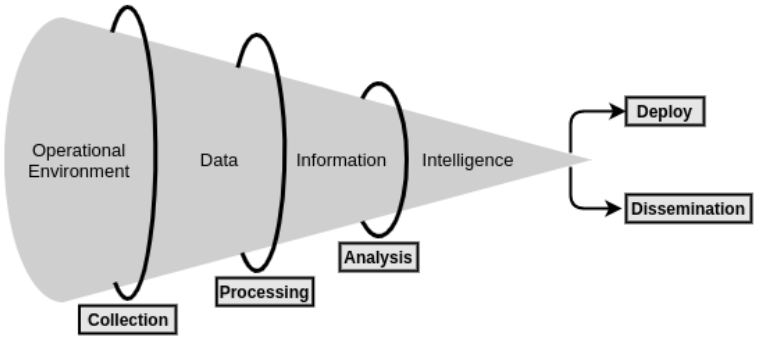

Figure 1. Threat Intelligence Production Process Flow.

2.3. Cyber Threat Intelligence

Within the spectrum of threat intelligence is the concept of Cyber Threat Intelligence (CTI), a relatively new approach that has become highly encompassing and used to define different types of services offered. It can be considered an actionable intelligence generated based on evidence of mechanisms, indicators, implications and context concerning threats or incidents in the cyber domain. It provides knowledge about adversaries and methods that can assist in the decision making process of responding to threats [43].

To the CTI be applied correctly and have effective results, it is necessary to establish a process flow for its production [1]. First, it is important to understand the needs of the users of the intelligence being developed and the context in which it is inserted [44], thus the requirements are important to be defined properly.

Once the requirements for the CTI are defined, start the data collection stage. It is known that data and information without treatment and context are not considered intelligence, but these are the basic materials for its production. Then, some mechanisms consume this information and perform the processing and analysis to generate structured information and find patterns. The treated information can be integrated with other defense mechanisms and then used to perform and develop methods of defense and threat mitigation [43].

Finally, as organizations lack the ability to understand the cyber threat landscape holistically, the stage of sharing and disseminating threat information between organizations is of utmost importance [41].

2.4. Threat Intelligence Standards

A crucial aspect of the entire threat intelligence process is the format of the shared data. First, for an adequate and automated processing of the collected data, it is important that they are formatted in a structured model and outlined in a common language. In addition, the establishment of standards provides a prior definition about the type of information will be shared and the density of that information [37]. As a result, a variety of initiatives have emerged with the aim of standardizing the information collected, consumed and disseminated within the CTI ecosystem [34].

2.5. Threat Intelligence Platforms

The establishment of a new threat landscape encouraged the change of traditional defense models. New systems with proactive action and capabilities of real-time response to incidents are being developed and commonly referred to as Threat Intelligence Platforms (TIPs) [34]. They are specialized software systems that implement the processes of collection, processing, analyzing, producing, deploying and integrate internal and external threat intelligence. The main goal of this type of platform is to serve as an assistant to decision makers related to incident response [18].

3. Proposed Evaluation Methodology

In this section, the approach proposed to evaluate CTI standards and platforms is described. First, a method is developed to restrict and define which standards and platforms will be analyzed. Then, the criteria for evaluation are introduced and explained.

3.1. Selection Strategy

The threat intelligence scenario is very extensive and includes a wide range of systems, platforms, tools, standards and formats. In order to perform an accurate evaluation, it is necessary to define a strategy of inclusion and exclusion to select some of them. Thereby, in this work, we focus on the most popular and open source standards and platforms.

A literature review was conducted aiming to obtain a complete overview of the CTI panorama. Some web research engines were used in this task, including Google Scholar, IEEE Digital Library, Springer and ScienceDirect. The following terms were merged to find suitable results: (Threat Intelligence OR Cyber Threat Intelligence) AND (platform OR tools OR standards). The searching process resulted in a large number of works and some of them were filtered based on their relevance to the topic and number of citations.

For the filtering methods applied to the searching process, a considerable amount of initiatives of TI standards and platforms were collected. Thus, to reduce the number of results found, based on brief readings of the official web sites and documentation, standards or platforms that were not able to address two or more stages from the threat intelligence process flow, presented in Figure 1, were excluded and not considered for the selection process.

Then, in order to select for evaluation the most relevant standards and platforms in the TI field, the results found with the searching process were described in terms of popularity and license model:

- **Popularity criteria**: In the context of this work, the popularity was estimated according to the number of times the standard or platform was mentioned in reliable works and sources, combined with collected statistics about the percentage of utilization among organizations.
- **License model criteria**: The type of license was analyzed aiming to limit the work to standards or platforms available to all interested communities by including only free or open source solutions and initiatives.

Finally, based on the criteria aforementioned, a minor data set of standards and platforms, composed with the most popular ones and those with permissive licenses or free versions, were chosen for evaluation.

3.2. Evaluation Criteria

In order to define the criteria for evaluating TI standards and platforms, two main aspects were taken into consideration. First, we analyzed the applicability in different use cases by defining a holistic architecture model. Then, some general evaluation criteria were inferred of the intelligence process flow.

3.2.1. Data Model Architecture

In terms of architecture, to define the applicability in different use cases, four main entities were used to represent the *cyber* threat intelligence scenario in a generic manner. In this approach, those entities indirectly derives from the 5W3H (what, who, why, when, where, how, how much and how long) method, which aims to answer the questions presented in Table 1. This is a generic method, applied in different areas, with the main objective of clarifying a topic in its completeness.

Table 1. Description of the 5W3H method.

Question	Description
What	Directly describes the topic being addressed
Where	Specifies geographic references about the topic
When	Specifies relevant time frames to the topic like date and time
Who	Associates the topic with an entity capable of executing it
Why	Describes possible motivations for the occurrence of the topic
How	Describes the main characteristics and mechanisms of the topic
How much	Refers to the costs and impacts generated by the topic
How long	Description of the topic's effectiveness in terms of time

The method was used for representation because, since it consists of an effective mechanism to obtain the complete description of a topic, it facilitates any necessary decision making about the subject addressed. Thus, within the threat intelligence ecosystem, the method can be used not only to identify and characterize threats and incidents. When correlating data from indicators and the information generated with the questions raised by the 5W3W method, it is simpler to implement effective mechanisms for detecting and mitigating threats.

First, *what* is used to directly define the topic that is being analyzed. In the cyber threat intelligence context, it can be usually summarized by the terms threats and incidents, which cover since evidences and probable attacks to real malicious occurrences. For an adequate definition, these terms should be accompanied by other information like the type of threat or incident and the context it is inserted. After defined, the topic can be characterized using *where*, *when* and *how*. *Where* can refer to the geographic location it started and parts of the path it took until it reaches the target. *When* provides a time frame, specifying date and time of occurrence. *How* is used to describe the way the threat or

incident took place and the tactics and techniques applied. It is important to say that the granularity of the information describing these entities is variable depending on the use case.

Another essential point is to associate the threat or incident with its threat actor, which can be described by *who* and *why*. *Who* can be an organization or an individual that is responsible for the threat or incident. *Why* is important to better characterize the threat actor by understanding the motivations behind the event.

Some detailed characteristics of the threat or incident can be discovered using *how long* and *how much*. *How long* indicates the effective durability of the threat or incident if no action is taken. *How much* is used to measure the intensity of the attack and analyze its damage capacity and defense cost. The information gathered with the *how long* and *how much* statements, together with all the characteristics described with the *how* statement, can also be used to analyze and measure the capacity of action of the threat actor.

Further, using the correlation between all the information raised about the threat, incident or threat actor using the 5W3H method, it is very likely that actionable intelligence was produced and it is possible to use it to define mechanisms for defense and specify some courses of action.

Based on the exposed, the four main entities used to delineate a holistic representation of the cyber threat intelligence scenario are threat, incident, threat actor and defense. To illustrate the context that these entities are inserted and the relationships between them, a diagram is shown in Figure 2.

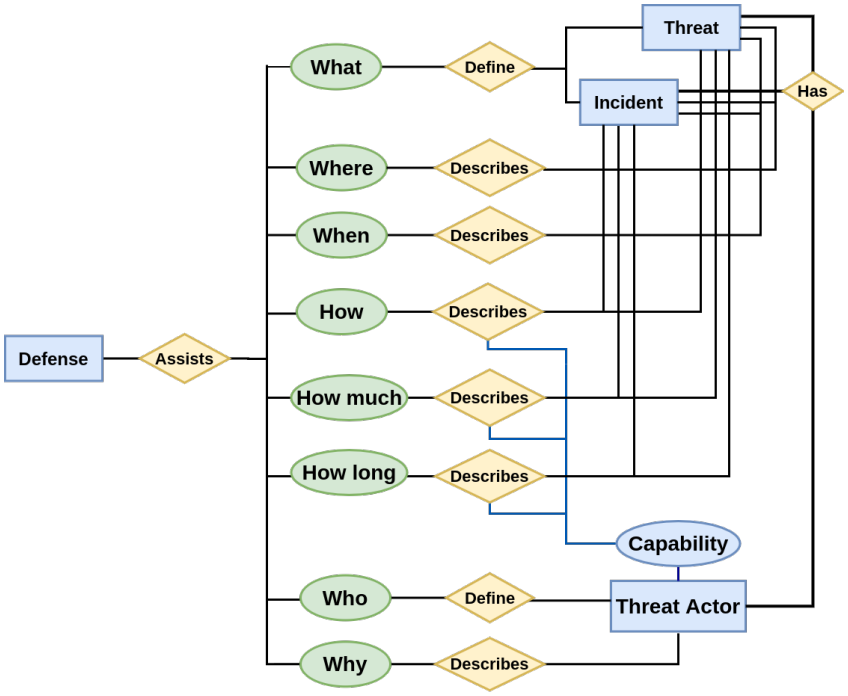

Figure 2. Main entities relationship diagram.

3.2.2. Intelligence Process

In order to be able to evaluate general criteria, essential features to achieve a complete threat intelligence process were delineated including some criteria proposed in References [35,37]. Considering the threat intelligence flow presented in Section 2.2, for the collection stage, it is important to provide the data in a common format to facilitate the process of gathering it. Next, to process and normalize the data, a structured format and machine readability are essential. Also, low overhead produces a more efficient processing. The analysis step requires an unambiguous data model to perform correlations and classify the information, besides relationship mechanisms to represent those correlations. With the analyzed information accessible, interoperability between formats, systems and platforms is necessary so the actionable intelligence can be deployed correctly and automatically. Later,

to disseminate intelligence and information, along with some above mentioned aspects, it is relevant to have a specific transport mechanism and good practical use in the community.

3.2.3. Additional

When referring to the TI platforms, considering that ease of use and flexibility for the implementation of new features are relevant aspects, some additional criteria were applied. Thus, the quantity and quality of the documentation and the permissions declared in their licenses were evaluated.

Based on the above, all evaluation criteria for TI standards and platforms have been defined. Tables 2 and 3 summarize the whole criteria explained in this section.

Table 2. Evaluation criteria for Cyber Threat Intelligence (CTI) standards.

Data Model Architecture	
Holistic Architecture	Threat
	Incident
	Threat Actor
	Defense
Intelligence Process	
Collection	Common formatting
Processing	Structured format
	Low overhead
	Machine readability
Analysis	Unambiguous data model
	Relationship mechanisms
Deploy	Interoperability
Dissemination	Transport mechanism
	Practical application

Table 3. Evaluation criteria for CTI platforms.

Data Model Architecture	
Holistic Architecture	Use case applicability
5W3H method	Answering capability
Intelligence Process	
Collection	Import formats
	Automatic gathering
Processing	Export format
	Graphic visualization
Analysis	Correlation
	Classification
Deploy	Integration with security systems
Dissemination	Sharing method
Additional	
Usability	Documentation
	License model

4. Standards Evaluation Results

First step to evaluate, the standards are selected based on the strategy described in Section 3.1. Furthermore, the results of the evaluation are based on the evaluation criteria proposed in Section 3.2.

After gathering the most suitable results from the searching process of TI standards, some relevant initiatives were found. In References [33,36] some projects that aim to standardize threat intelligence data are mentioned, such as STIX, TAXII, CybOX, OpenIOC, CAPEC, MAEC and ATT&CK, being STIX considered the most used one.

In Reference [37] other standards are mentioned such as VERIS, STATL, ARF and X-ARF and some of them are evaluated. Other works [16,19] only mentions the standards considered as consolidated, which are: OpenIOC, CybOX, STIX, TAXII e IODEF. A survey [45] presents in statistical terms the most used patterns, which are: STIX, OpenIOC, CybOX e IODEF. In Reference [32] a comparison between IODEF/RID and STIX/TAXII, considered as the most popular standards. Finally, some recent works [9,12] present standards that are considered prominent nowadays.

Since all the standards found are released for community use, the popularity was the key criteria for selecting them. Considering the results obtained with the literature research, complemented with the review of the official web sites and documentation of most standards, the standards were ranked in terms of popularity and the results are presented in Table 4.

Table 4. Threat Intelligence (TI) standards described by popularity and license model.

Standard	Popularity	License Model	References
STIX	++++	Permissive license granted by MITRE	[9,12–14,16,20,36,37,41]
TAXII	++++	Permissive license granted by MITRE	[9,13,16,20,32,36,37]
CybOX	+++	Permissive license granted by MITRE	[9,16,36,45]
IODEF	++	IETF TLP 5.0	[9,12,20,36,37]
RID	++	IETF TLP 5.0	[32,36,37]
OpenIOC	+++	Apache 2.0	[9,16,17,36]
VERIS	+	Attribution-ShareAlike 4.0 International	[20,37]
X-ARF	+	Open Source (GNU General Public License)	[35,37]

Legend: very high (++++) high (+++) medium (++) low (+).

4.1. Standards Selected for Analysis

Given the presented results, the standards selected for further analysis and evaluation are **STIX, TAXII, IODEF, RID, CybOX and OpenIOC**. Following, a succinct presentation of the selected standards is provided.

4.1.1. Structured Threat Information eXpression

STIX is a language created by MITRE and developed to capture, specify, characterize and communicate information in the context of cyber threat intelligence [41]. It provides mechanisms to represent structured information in different scenarios of the cyber threat ecosystem.

The language was designed with principles such as interoperability, extensibility, focus on automation and machine readability. In the first version, STIX was modeled in the XML format and it was composed of eight cores. The second version was developed using serialization in JSON format [46].

Its structural architecture has been significantly modified, is currently composed of twelve main objects that correspond directly to concepts embedded in the context of CTI [47]. With its holistic architecture, STIX is able to present information in a standardized, comprehensive and structured manner while allowing application in different use cases. In addition, it is directly integrable with other languages in the TI context [17].

Cyber Observable eXpression is a language created by MITRE and developed to specify, characterize and communicate information about cyber observables in a standardized way. With the release of the second version of STIX, it is no longer used as an independent language. It was integrated into the second version of STIX that defines a structured representation for observable objects in the cyber domain, called *Cyber Observable Object* [48].

This standardization can be used to describe different types of data, from a host characterization to information about digital forensics. The objects are represented using serialization in JSON format [49].

4.1.2. Trusted Automated Exchange of Intelligence Information

TAXII is an application layer protocol created by MITRE that defines a set of services to exchange TI information messages between organizations [50]. It was projected specifically for the transport of information formatted in the STIX language but is not limited to it. TAXII uses Hyper Text Transfer Protocol Secure (HTTPS) as the transport protocol and supports different sharing models, including *hub-and-spoke*, P2P and *publish-subscribe*.

4.1.3. Incident Object Description Exchange Format

IODEF is an Internet Engineering Task Force (IETF) initiative that aims to facilitate information sharing between organizations and increase the possibility of mitigating cyber threats [51]. In the first version, the data model was focused on representing incidents. Bringing a more holistic approach, the second version of IODEF was designed with significant evolution in its structural part, which now includes structures for the description of indicators, attackers and incident response methodologies [52]. Both versions use the XML format.

4.1.4. Real-Time Inter-Network Defense

RID is an IETF initiative created to facilitate the process of sharing data about security incidents mainly structured under the IODEF format. It outlines a proactive internal communication network, capable of integration with mechanisms for detecting, identifying, mitigating and responding to incidents, aiming to compose a complete solution in the treatment of security incidents [53]. RID messages are transported under the HTTPS protocol and, in order to provide more security, the protocol adds another layer of security to manage sessions.

4.1.5. Open Indicator of Compromise

OpenIOC is a framework that offers a standardized, structured and machine-readable format used to record, define and share information encompassed in the context of cyber attacks and incidents [54]. This format is written in XML, with a relatively light and small design. Its architecture is composed of more than 500 specific types of data incorporated to represent indicators.

4.2. Evaluation of the Standards

After the selection and definition of the standards, an evaluation was made based on academic literature, the study of official documentation and practical demonstrations.

Taking into account the aforementioned criteria, the evaluation of the standards was made and it is summarized in Table 5. Regarding the results illustrated in Table 5, two considerations must be highlighted. First, as explained before in Section 4.1.1, since CybOX and STIX were usually used together and both standards are maintained by the same organization, CybOX was integrated into the second version of STIX and it is no longer used as an independent language. Thus, as CybOX is now a part of STIX structure it was considered more plausible to evaluate them as a single standard. Second, it was noticed that even though TAXII and RID are autonomous protocols, they are mostly used combined with STIX and IODEF, respectively. It stems from the fact that TAXII and RID are protocols designed specifically to facilitate the transport of STIX and IODEF. Hence, it was chosen

to evaluate these protocols as pairs (STIX/TAXII and IODEF/RID) considering the fact that their functions are complementary.

4.2.1. Data Model Architecture

From an architectural perspective, STIX is the language with the most holistic architecture and it is applicable in different use cases. The four entities considered essential to delineate a holistic contextualization of the cyber threat intelligence scenario can be fully represented and characterized by the classes that compose the STIX schema. IODEF and OpenIOC also have a satisfactory architecture but with some flaw points. Both standards do not have the necessary resources for an adequate definition of defense mechanisms or courses of action. Besides, OpenIOC has some shortcomings in the process of characterizing a threat actor in a more specific way.

4.2.2. Intelligence Process

From the process perspective, STIX has the capability to meet most of the proposed requirements. The use of serialization in JSON format provides a common and structured format, with relatively low overhead and machine-readability. The twelve objects that compose STIX architecture are well described and documented providing an unambiguous data model with coupled relationship mechanisms. When used together with TAXII, it offers a reliable transport mechanism. Finally, since it has a significant practical application, most of the TI platforms and tools have integration methods with this standard.

IODEF and OpenIOC are based in the XML format, so they also provide a common and structured format with machine-readability. However, IODEF can present some problems due to free text fields that compose its data model. Regarding the relationship mechanisms, OpenIOC provides logic operators (AND/OR) to create connections between indicators, on the other hand, besides the interconnections on the data model, IODEF does not present specific mechanisms to relate information.

IODEF and OpenIOC are supported in many platforms and tools and can be integrated with different systems. IODEF can be used together with the RID protocol, providing an efficient and secure transport, while OpenIOC does not focus on implementing transport mechanisms.

4.3. Synthesis

As a result of the evaluation, it can be said that STIX is de-facto standard in the threat intelligence context. First, STIX is the most popular and compatible one, being supported by many platforms and tools and used by most organizations. Second, due to its holistic architecture and its capability of addressing a lot of scenarios in the threat intelligence scope, can be considered the most complete standard.

Even though the other standards are still supported by some platforms and have satisfactory applicability, the features offered by STIX have stood out. So, considering the characteristics of STIX and the capacity of possible results it can generate, it can be said that the standard has the most satisfying performance.

Table 5. Evaluation of TI standards.

	STIXv2 [46,47] & TAXII [52]	IODEFv2 [52] & RID [53]	OpenIOC [54]
Holistc Architecture			
Threat	++++	++++	++++
Incident	++++	++++	+++
Threat Actor	++++	++++	++
Defense	++++	++	+
Intelligence Process			
Common formatting	++++	++++	++++
Structured format	++++	++++	++++
Low overhead	+++	+++	+++
Machine readability	++++	+++	++++
Unambiguous data model	++++	+++	++++
Relationship mechanisms	++++	++	+++
Interoperability	++++	+++	+++
Transport mechanism	++++	++++	+
Practical application	++++	++	+++

Legend: very high (++++) high (+++) medium (++) low (+).

5. Platforms Evaluation Results

Results regarding the selection and evaluation of the platforms are presented and explained. From the searching process of TI platforms, a massive number of projects were identified. The most relevant results count more than 30 different platforms. In References [16,55] a significative number of platforms were analyzed, totalizing 30 and 23, respectively. In Reference [20], a smaller number of platforms are mentioned and considered consolidated in the area.

In more specific studies [19,36,56] only open source and popular platforms are evaluated. Another work [14] proposed a framework to evaluate some platforms and described the results from three of them. Some reliable and relevant sources also mentioned emerging platforms that have great potential [57,58]. A considerable part of the platforms presented was excluded according to the exclusion method applied that considered the adherence to the intelligence flow. Thereby, a total of 16 platforms were ranked in terms of popularity and the results are presented in Table 6.

Table 6. TI platforms described by popularity and license model.

Platform	Popularity	License Model	References
Accenture CIP	+	Closed source	[16,55]
Anomali STAXX	+++	Closed source with free version	[16,20,55]
MISP	++++	Open Source (GNU General Public License)	[13,14,16,19,20,36,55]
CRITs	+++	Open Source (GNU General Public License)	[16,19,36]
OpenCTI	+++	Open Source (Apache License)	[9,57,58]
Facebook TE (beta)	++	Open Source (BSD License)	[16,20]
Falcon Intelligence	++	Closed source	[16]
MANTIS	++	Open Source (GNU General Public License)	[16,19]
McAfee TIE	+	Closed source	[16,55]
Microsoft Interflow	+	Closed source	[16,55]
Soltra Edge	+++	Closed source	[16,19,20,55]
ThreatQ	++	Closed source	[14,16,20,55]
ThreatConnect	++	Closed source	[16,20,55]
EcleticIQ	+	Closed source	[16,20,55]
IBM X-Force	++	Closed source	[16,20,55]
CIF	+++	Open Source (GNU General Public License)	[13,16,19,36]

Legend: very high (++++) high (+++) medium (++) low (+).

Considering that the scope of this work is restricted to open source or free platforms, about half of the platforms were excluded. Next, the popularity criteria was applied to select the platforms.

5.1. Platforms Selected for Analysis

Given the presented results, the platforms selected for further analysis and evaluation are **MISP, CIF, CRITs, OpenCTI and Anomali STAXX**. Following, a succinct presentation of the platforms is provided.

- **Malware Information Sharing Platform**: MISP is an open source TI platform that allows the sharing, storage and correlation of indicator of compromise (IOCs) [59]. The tool provides a database of indicators, including technical and general information about cyber threats, which are stored in a structured format and with a flexible data model. The stored data is automatically correlated to describe the relationships between attributes and indicators.
- **Collaborative Research into Threats**: CRITs is an open source web-based tool that integrates a repository of malware and cyber threats with other software capable of offering mechanisms for analyzing and correlating the information [60]. This initiative was developed by MITRE with the main objective of assisting the cybersecurity community in the process of analyzing and sharing data about threats [61].
- **OpenCTI**: It is an open source framework with the main objective of aggregating, in a comprehensive way, general and technical information from the CTI context [62]. It assists organizations in the process of managing their content about cyber threats, allowing the structuring, storage, organization and graphic visualization of this information.
- **Collective Intelligence Framework**: CIF is a system focused on speed, performance and integration used in threat information management [63]. It assists users in formatting, normalizing, processing, storing, sharing and building threat data sets. The system extracts information about cyber threats from a wide range of sources and creates a sequential and chronological grouping about a specific threat [64].
- **Anomali STAXX**: It is a tool that provides bidirectional sharing between sources of threat intelligence that use the STIX and TAXII standards [65], facilitating access to information about cyber threats. The platform provides an intuitive dashboard to present data obtained from different sources.

5.2. Evaluation of the Platforms

After the definition of the platforms, an evaluation was made based on academic literature, study of official documentation and practical demonstrations. According to the aforementioned criteria, the evaluation of the platforms was made and it is summarized in Table 7.

5.2.1. Data Model Architecture

From an architectural perspective, MISP and OpenCTI are the ones with the most holistic approach and applicable in diverse scenarios. Additionally, when used correctly, both platforms have the capacity to address efficiently the 5W3H method and provide full support to the decision making process. The other platforms have some points of failure regarding to the representation of entities incorporated on the cyber threat spectrum. Besides, the platforms are not focused in classification and correlation mechanisms. As a result, not all aspects of the 5W3H method are supported.

5.2.2. Intelligence Process

The evaluation from the process perspective provided some significant findings. First, all the platforms support the importation and exportation of information in at least one of the most common formats such as XML, CSV and JSON. Also, with the exception of CIF, the platforms are

compatible with STIX, considered the consolidated standard in the TI ecosystem, along with other standards.

MISP can be contemplated as the most flexible platform considering the compatibility with different formats. Next, about the collection process, all the platforms have the capability to perform automatic gathering of information.

For CIF and Anomali STAXX, this feature is built-in, while for the other platforms some integration might be necessary. Other important point to analyze are the correlation and classification mechanisms, which are well performed by MISP and OpenCTI. The other platforms are not focused on this stage of the CTI process and provide only some filtering or aggregation mechanisms.

Regarding the information visualization, except CIF that is based on command line, the platforms use dashboards to present the information. MISP, CRITs and Anomali STAXX provide a generic dashboard for all the information in the platform, while OpenCTI builds personalized dashboards for the different information in the platform. It also provides intuitive and complete relationship graphics based on STIXv2. MISP and CRITs offer services for relationship visualization as well.

Considering the integration between platforms, systems and tools, MISP and OpenCTI are the most adjustable ones. CIF has some extension codes to use in the integration with some Intrusion Detection Systems (IDSs) and the other platforms do not have specific mechanisms for this kind of integration. About the sharing criteria, Anomali STAXX can communicate with any platform using TAXII, while MISP, CIF and CRITs focus on establishing a reliable group of instances.

Finally, all platforms have available documentation and for MISP, OpenCTI and Anomali STAXX it is very extensive and elaborated. For CIF, there were some difficulties in finding and organizing the documentation that is limited in details and present succinct descriptions and CRITs have a satisfactory amount of information and details.

5.3. Synthesis

As a result of the evaluation, it can be said that, currently, there are some satisfactory TI platforms. Each of them has some differentials that can optimize the process of creating threat intelligence. Therefore, it is important to analyze the context in which they will be applied and the goals that must be achieved in order to decide which platform to use.

6. Discussion

To achieve great cyber threat detection and preventive capabilities, most organizations need to rely on available open source TI platforms. Similarly, these platforms need consolidated standards to provide an automated, shareable and reliable service. Thus, it is essential to analyze the features and operation modes of these two strands of the threat intelligence domain.

By evaluating some common TI standards, it is notorious that STIX, combined with TAXII features, can be considered the most holistic and applicable one. In addition, statistics show that it also is the most used standard among organizations [45]. Therefore, an important step is a definitive consolidation of this standard, so the goal of establishing broad integration and interoperability between organizations can be accomplished. Besides, the definition of an accepted standard can provide the optimization of processing, analysis and sharing tasks performed by TI platforms because it focuses efforts on a predefined data model and one based on STIX would certainly be holistic and very applicable.

Regarding the TI platform analysis, several interesting solutions were found. Some of them focus on providing speed and performance, others brought great efforts on the visualization of the information, while a few implement a little bit of each feature. As a matter of fact, diverse types of systems, with different goals, are defined as threat intelligence platforms. This probably derives from the fact that there is currently no standardized definition for the concept or process of cyber threat intelligence. As CTI is a very extensive domain, it would be relevant to establish scopes to

better characterize the platforms available, making it easier to decide which platforms are best applied in each use case.

Taking into consideration that TI platforms have different goals, it can be said that currently there is no fully complete platform, with the capacity to attend all the CTI processes adopted in this work. Thus, a possibility to expand and optimize the results obtained with the application of the CTI processes would be the integration between different TI platforms, with complementary objectives. Adopting this perspective, it is possible to reconcile different aspects such as performance and visual mechanism, achieving a fully developed CTI process, which provides everything from data collection to the transformation of data into actionable intelligence.

For the reasons discussed it is still necessary to carry out research and work in order to characterize the concept of CTI in a more specific way. Not only a definition should be established, but also the processes that are involved in this domain. Thereby, the wide range of systems available, denominated as TI platforms, could be better used and applied, and new systems that will be developed could be better designed, being able to adopt specific and more optimized processes or a complete approach that fulfills all predefined requirements for creating threat intelligence.

Table 7. Evaluation of TI platforms.

	MISP [59]	**OpenCTI [62]**	**CIF [63,64]**	**CRITs [60,61]**	**Anomali STAXX [65]**
Holistc Architecture					
Use case applicability	++++	++++	+++	+++	+++
Adherence 5W3H method	++++	++++	+	++	+
Intelligence Process					
Import formats	OpenIOC, STIX, CybOX, JSON, CSV, XML	STIX, CybOX, JSON, CSV, XML	XML, JSON, Zip	CSV, STIX, CybOX	STIX
Automatic gathering	Using MISP feeds	Using connectors with sources or other platforms	Automatic synchronization with different sources	Possible integration with gathering tools	Automatic synchronization with configured feeds
Export format	MISP, OpenIOC, CSV, XML, JSON	CSV, STIX	CSV, JSON, HTML, XLS	CSV, STIX, CybOX	CSV, JSON
Graphic visualization	General and intuitive dashboard and relationship graphics	Diverse dashboards and STIXv2 based graphics	Command line interface with possible integration with visualization tool	Simple dashboard and an extension service for generating relationship graphics	General dashboard
Correlation	Automatic for every data in platform	Automatic for every data in platform	Not addressed	Necessary an extension service	Not addressed
Classification	Based on the type of the indicator	Based on STIXv2 objects	Based on the type of the indicator	Based on a proposed data model	Using a searching mechanism based on the type of indicator
Integration	IDS, SIEMs and other TI platforms	Other TI platforms	IDSs (Snort, Splunk, Bro, Bind)	Not addressed	Not addressed
Sharing method	Reliable group of instances using different models	Particular instance to share between users	Reliable group of instances using a centralized service	Reliable group of instances	With any system that supports TAXII
Additional					
Documentation	Extensive and well elaborated	Extensive and well elaborated	Limited detail with succinct descriptions	Satisfactory quantity and detailing	Extensive and well elaborated
License model	Open Source (GNU General Public License)	Open Source (Apache License)	Open Source (GNU General Public License)	Open Source (GNU General Public License)	Closed source with free version

Legend: very high (++++) high (+++) medium (++) low (+).

7. Conclusions and Future Work

As the cyber security landscape is fundamentally changing and a new threat scenario is emerging, the development and investigation of more efficient defense mechanisms became a necessary task. In this work, an overview of the cyber threat intelligence scenario and existing standards and platforms of the threat intelligence spectrum was provided. Based on academic literature and official sites and documentations, a group of relevant standards and platforms were defined. Considering the scope of the research, a selection strategy was proposed and applied in order to determine the most popular and efficient standards and platforms that are free or open source. Then, the standards and platforms selected were evaluated based on a developed methodology that contemplates architectural and processual criteria.

From the evaluation of TI standards, we concluded that STIX is the most consolidated standard in the area, mainly due to its holistic approach, which makes it applicable in a wide range of scenarios, and compliance with fundamental requirements for a standard, such as interoperability and machine readability. Concerning TI platforms, MISP and OpenCTI were considered the most complete and flexible platforms. Although there are sophisticated solutions available, there is none that addresses the entire CTI process.

To conclude, even though some great solutions are available in the market, it is still a challenge to find a thoroughly and absolute solution for a defense based on threat intelligence, since the platforms have divergent focuses and consequently correspond to only a few stages of the threat intelligence production flow.

Future work will address assessing and validating the methodology and results here presented by executing an experimental evaluation and running tests using data sets of cyber threat data. New research will be focused on evaluating the completeness of the CTI process that can be supplied by available platforms in a practical way, using the benefits of interoperability among platforms. Along the same lines, research is to focus on the integration between complementary platforms in order to provide a more complete solution to manage and use threat intelligence. Finally, the delineation of a standardized definition for the CTI concept and process to assist in the design of new and optimized threat intelligence systems capable of establishing an efficient defense model is still a research gap.

Author Contributions: A.d.M.e.S. provided the analysis of standard and platforms existing and developed the evaluation criteria of the platforms and standards, J.J.C.G., R.d.O.A. and L.J.G.V. reviewed the evaluation criteria and proposed the tabulation format of the results. All authors have read and agreed to the published version of the manuscript.

Funding: Authors of this research received the following funding: R.d.O.A. research work was supported in part by CNPq - Brazilian National Research Council, under Grant 465741/2014-2 INCT in Cybersecurity, in part by CAPES - Brazilian Higher Education Personnel Improvement Coordination, under Grant 23038.007604/2014-69 FORTE, in part by FAP-DF - Brazilian Federal District Research Support Foundation, under Grant 0193.001366/2016 UIoT and Grant 0193.001365/2016 SSDDC, and in part by the Institutional Security Office of the Presidency of Brazil under Grant ABIN 002/2017.

Acknowledgments: Authors would like to thank CNPq - Brazilian National Research Council (Grant 465741/2014-2 INCT in Cybersecurity), CAPES - Brazilian Higher Education Personnel Improvement Coordination (Grant 23038.007604/2014-69 FORTE), FAP-DF - Brazilian Federal District Research Support Foundation (Grant 0193.001366/2016 UIoT and Grant 0193.001365/2016 SSDDC), the Institutional Security Office of the Presidency of Brazil under (Grant ABIN 002/2017), Cyber Security Laboratory and GigaCandanga.

Conflicts of Interest: The authors declare that there are no conflicts of interest.

Abbreviations

Abbreviations used throughout the manuscript:

APT	Advanced Persistent Threats
ARF	Abuse Reporting Format
CAIF	Common Announcement Interchange Format
CAPEC	Common Attack Pattern Enumeration and Classification
CEE	Common Event Expression

CIDF	Common Intrusion Detection Framework
CIF	Collective Intelligence Framework
CRITs	Collaborative Research into Threats
CTI	Cyber Threat Intelligence
CybOX	Cyber Observable eXpression
GNU	General Public License
HTTPS	Hyper Text Transfer Protocol Secure
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IOC	Indicator Of Compromise
IODEF	Incident Object Description Exchange Format
MAEC	Malware Attribute Enumeration and Characterization
MISP	Malware Information Sharing Platform
OpenIOC	Open Indicator Of Compromise
OpenTPX	Open Threat Partner Exchange
RID	Real-time Inter-network Defense
SIEM	Security Information and Event Management
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated Exchange of Intelligence Information
TI	Threat Intelligence
TIP	Threat Intelligence Platform
TISP	Threat Intelligence Sharing Platform
VERIS	Vocabulary for Event Recording and Incident Sharing
X-ARF	Extended Abuse Reporting Format

References

1. Pokorny, Z. *The Threat Intelligence Handbook: Moving toward a Security Intelligence Program*; CyberEdge Group: Annapolis, MD, USA , 2019.
2. Bissell, K.; LaSalle, R.; Dal Cin, P. The Cost of Cybercrime—Ninth Annual Cost of Cybercrime Study. 2019. Available online: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (accessed on 4 May 2020).
3. Bissell, K.; LaSalle, R.; Dal Cin, P. The 2020 Cyber Security Report. 2020. Available online: https://pages.checkpoint.com/cyber-security-report-2020 (accessed on 4 May 2020).
4. Tounsi, W. What is Cyber Threat Intelligence and How is it Evolving? In *Cyber-Vigilance and Digital Trust*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2019; pp. 1–49, doi:10.1002/9781119618393.ch1.
5. Alshamrani, A.; Myneni, S.; Chowdhary, A.; Huang, D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 1851–1877, doi:10.1109/COMST.2019.2891891.
6. Wu, J. New Approaches to Cyber Defense. In *Cyberspace Mimic Defense*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 113–157, doi:10.1007/978-3-030-29844-9_4.
7. Abu, M.S.; Selamat, S.R.; Ariffin, A.; Yusof, R. Cyber Threat Intelligence—Issue and Challenges. *Indones. J. Electr. Eng. Comput. Sci.* **2018**, *10*, 371, doi:10.11591/ijeecs.v10.i1.pp371-379.
8. Chadwick, D.W.; Fan, W.; Costantino, G.; de Lemos, R.; Cerbo, F.D.; Herwono, I.; Manea, M.; Mori, P.; Sajjad, A.; Wang, X.S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Gener. Comput. Syst.* **2020**, *102*, 710–722, doi:10.1016/j.future.2019.06.026.
9. Zhao, J.; Yan, Q.; Li, J.; Shao, M.; He, Z.; Li, B. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Comput. Secur.* **2020**, *95*, 101867, doi:10.1016/j.cose.2020.101867.
10. Gao, Y.; LI, X.; PENG, H.; Fang, B.; Yu, P. HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. *IEEE Trans. Knowl. Data Eng.* **2020**, 1, doi:10.1109/tkde.2020.2987019.
11. Riesco, R.; Larriva-Novo, X.; Villagra, V.A. Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommun. Syst.* **2019**, *73*, 259–288, doi:10.1007/s11235-019-00613-4.
12. Rantos, K.; Spyros, A.; Papanikolaou, A.; Kritsas, A.; Ilioudis, C.; Katos, V. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers* **2020**, *9*, 18, doi:10.3390/computers9010018.
13. Ramsdale, A.; Shiaeles, S.; Kolokotronis, N. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. *Electronics* **2020**, *9*, 824, doi:10.3390/electronics9050824.

14. Bauer, S.; Fischer, D.; Sauerwein, C.; Latzel, S.; Stelzer, D.; Breu, R. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2020, doi:10.24251/hicss.2020.239.
15. Shin, B.; Lowry, P.B. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Comput. Secur.* **2020**, *92*, 101761, doi:10.1016/j.cose.2020.101761.
16. Sauerwein, C.; Sillaber, C.; Mussmann, A.; Breu, R. Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. In Proceedings of the 13th International Conference on Wirtschaftsinformatik, St.Gallen, Switzerland, 12–15 February 2017.
17. Skopik, F.; Settanni, G.; Fiedler, R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Comput. Secur.* **2016**, *60*, 154–176, doi:10.1016/j.cose.2016.04.003.
18. ENISA. Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms. 2018. Available online: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms (accessed on 16 March 2020).
19. Poputa-Clean, P.; Stingley, M. Automated Defense-Using Threat Intelligence to Augment Security. 2015. Available online: https://www.sans.org/reading-room/whitepapers/threats/paper/35692 (accessed on 23 March 2020)
20. Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.* **2019**, *87*, 101589, doi:10.1016/j.cose.2019.101589.
21. Sarker, I.H.; Abushark, Y.B.; Khan, A.I. ContextPCA: Predicting Context-Aware Smartphone Apps Usage Based On Machine Learning Techniques. *Symmetry* **2020**, *12*, 499, doi:10.3390/sym12040499.
22. Sarker, I.H.; Kayes, A.S.M.; Watters, P. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. *J. Big Data* **2019**, *6*, doi:10.1186/s40537-019-0219-y.
23. Sarker, I.H.; Abushark, Y.B.; Alsolami, F.; Khan, A.I. IntruDTree: A Machine Learning-Based Cyber Security Intrusion Detection Model. *Symmetry* **2020**, *12*, 754, doi:10.20944/preprints202004.0481.v1.
24. Truong, T.C.; Zelinka, I.; Plucar, J.; Čandík, M.; Šulc, V. Artificial Intelligence and Cybersecurity: Past, Presence, and Future. In *Advances in Intelligent Systems and Computing*; Springer: Singapore, 2020; pp. 351–363, doi:10.1007/978-981-15-0199-9_30.
25. Noor, U.; Anwar, Z.; Amjad, T.; Choo, K.K.R. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Gener. Comput. Syst.* **2019**, *96*, 227–242, doi:10.1016/j.future.2019.02.013.
26. Dalton, A.; Aghaei, E.; Al-Shaer, E.; Bhatia, A.; Castillo, E.; Cheng, Z.; Dhaduvai, S.; Duan, Q.; Islam, M.M.; Karimi, Y.; et al. The Panacea Threat Intelligence and Active Defense Platform. *arXiv* **2020**, arXiv:2004.09662.
27. Kazato, Y.; Nakagawa, Y.; Nakatani, Y. Improving Maliciousness Estimation of Indicator of Compromise Using Graph Convolutional Networks. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020, doi:10.1109/ccnc46108.2020.9045113.
28. Albakri, A.; Boiten, E.; Lemos, R.D. Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. In *Privacy Technologies and Policy*; Springer: Cham, Switzerland, 2019; pp. 28–41, doi:10.1007/978-3-030-21752-5_3.
29. Wu, Y.; Qiao, Y.; Ye, Y.; Lee, B. Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing. In Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019, doi:10.1109/iotsms48152.2019.8939192.
30. Tlelo-Cuautle, E.; Díaz-Muñoz, J.D.; González-Zapata, A.M.; Li, R.; León-Salas, W.D.; Fernández, F.V.; Guillén-Fernández, O.; Cruz-Vega, I. Chaotic Image Encryption Using Hopfield and Hindmarsh–Rose Neurons Implemented on FPGA. *Sensors* **2020**, *20*, 1326, doi:10.3390/s20051326.
31. Khan, M.; Masood, F.; Alghafis, A. Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. *Neural Comput. Appl.* **2019**, doi:10.1007/s00521-019-04667-y.
32. Burger, E.W.; Goodman, M.D.; Kampanakis, P.; Zhu, K.A. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security—WISCS-14, Scottsdale, AZ, USA, 3–7 November 2014; doi:10.1145/2663876.2663883.

33. Mavroeidis, V.; Bromander, S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 11–13 September 2017; doi:10.1109/eisic.2017.20.
34. Asgarli, E.; Burger, E. Semantic ontologies for cyber threat sharing standards. In Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 10–11 May 2016, doi:10.1109/ths.2016.7568896.
35. Steinberger, J.; Sperotto, A.; Golling, M.; Baier, H. How to exchange security events? Overview and evaluation of formats and protocols. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015, doi:10.1109/inm.2015.7140300.
36. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233, doi:10.1016/j.cose.2017.09.001.
37. Menges, F.; Pernul, G. A comparative analysis of incident reporting formats. *Comput. Secur.* **2018**, *73*, 87–101, doi:10.1016/j.cose.2017.10.009.
38. Ferreira, H.G.C.; de Sousa Junior, R.T. Clust. Comput. Security analysis of a proposed internet of things middleware. *Clust. Comput.* **2017**, *20*, 651–660, doi:10.1007/s10586-017-0729-3.
39. de Melo Silva, C.C.; Ferreira, H.G.C.; de Sousa Júnior, R.T.; Buiati, F.; Villalba, L.J.G. Design and Evaluation of a Services Interface for the Internet of Things. *Wirel. Pers. Commun.* **2016**, *91*, 1711–1748, doi:10.1007/s11277-015-3168-6.
40. Sillaber, C.; Sauerwein, C.; Mussmann, A.; Breu, R. 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—WISCS16, Vienna, Austria, 24–28 October 2016; doi:10.1145/2994539.2994546.
41. Barnum, S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). 2012. Available online: https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the (accessed on 17 March 2020).
42. Chismon, D.; Ruks, M. *Threat Intelligence: Collecting, Analysing, Evaluating*; MWR InfoSecurity Ltd.: Basingstoke, UK, 2015.
43. Friedman, J.; Bouchard, M. *Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks*; CyberEdge Group: Annapolis, MD, USA, 2015.
44. CERT-UK. An Introduction to Threat Intelligence. 2015. Available online: http://dl.icdst.org/pdfs/files/85d0b11467a3e30bf12a5bbc6c3e543c.pdf (accessed on 4 May 2020).
45. Shackleford, D. Cyber Threat Intelligence Uses, Successes and Failures: The Sans 2017 Cti Survey. 2017. Available online: https://www.sans.org/reading-room/whitepapers/threats/paper/37677 (accessed on 12 May 2020)
46. OASIS. STIX Version 2.0. Part 1: STIX Core Concepts. 2017. Available online: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html (accessed on 18 May 2020).
47. OASIS. STIX Version 2.0. Part 2: STIX Objects. 2017. Available online: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html (accessed on 18 May 2020).
48. Corporation, M. Cyber Observable eXpression (CybOX™) Archive Website. 2017. Available online: https://cyboxproject.github.io/ (accessed on 21 May 2020).
49. OASIS. STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts. 2017. Available online: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part3-cyber-observable-core.pdf (accessed on 18 May 2020).
50. OASIS. TAXII Version 2.0. 2017. Available online: http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html (accessed on 21 May 2020).
51. Danyliw, R.; Meijer, J.; Demchenko, Y. The Incident Object Description Exchange Format. 2007. Available online: https://tools.ietf.org/html/rfc5070 (accessed on 25 May 2020).
52. Danyliw, R. The Incident Object Description Exchange Format Version 2. 2016. Available online: https://tools.ietf.org/html/rfc7970 (accessed on 25 May 2020).
53. Moriarty, K. Real-Time Inter-Network Defense (RID). 2012. Available online: https://tools.ietf.org/html/rfc6545 (accessed on 27 May 2020).
54. Inc., M. An Introduction to Open IOC. 2011. Available online: https://www.academia.edu/31820654/An_Introduction_to_Open_IOC (accessed on 27 May 2020).

55. Wagner, T.D.; Palomar, E.; Mahbub, K.; Abdallah, A.E. Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper). In *Information Security Practice and Experience*; Springer: Cham, Switzerland, 2017; pp. 576–586, doi:10.1007/978-3-319-72359-4_35.
56. Liu, R.; Zhao, Z.; Sun, C.; Yang, X.; Gong, X.; Zhang, J. A Research and Analysis Method of Open Source Threat Intelligence Data. In *Communications in Computer and Information Science*; Springer: Singapore, 2017; pp. 352–363, doi:10.1007/978-981-10-6385-5_30.
57. ANSSI. OpenCTI—The Open Source Solution for Processing and Sharing Threat Intelligence Knowledge. 2020. Available online: https://www.ssi.gouv.fr/en/actualite/opencti-the-open-source-solution-for-processing-and-sharing-threat-intelligence-knowledge/ (accessed on 29 May 2020).
58. Garnier, F. CTI & Information Fusion Benefits and Challenges. 2020. Available online: https://www.enisa.europa.eu/events/2019-cti-eu/presentations/200130-cti-info-fusion-tlp-white (accessed on 30 May 2020).
59. project, M. MISP—Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. 2020. Available online: https://www.misp-project.org/features.html (accessed on 20 May 2020).
60. Corporation, M. Welcome to CRITs. 2020. Available online: https://github.com/crits/crits#readme (accessed on 26 May 2020).
61. Corporation, M. Collaborative Research into Threats. 2020. Available online: https://crits.github.io/#nav (accessed on 26 May 2020).
62. OpenCTI. OpenCTI Documentation 3.0.2. 2019. Available online: https://opencti-platform.github.io/docs/getting-started/introduction (accessed on 29 May 2020).
63. GADGETS, C. The FASTEST Way to Consume Threat Intelligence. Period. 2018. Available online: https://csirtgadgets.com/collective-intelligence-framework (accessed on 20 May 2020).
64. Iovino, G. What Is the Collective Intelligence Framework? 2015. Available online: https://github.com/csirtgadgets/massive-octo-spice/wiki/What-is-the-Collective-Intelligence-Framework%3F (accessed on 20 May 2020).
65. Anomali. Anomali STAXX—Installation and Administration Guide. 2018. Available online: https://update.anomali.com/staxx/docs/Anomali_STAXX_Installation_&_Administration_Guide.pdf (accessed on 19 May 2020).