Methodology to Improve the Quality of Cyber Threat Intelligence Production Through Open Source Platforms*

Rogerio Machado da Silva[0000−0001−8790−4392], João José Costa Gondim[0000−0002−5873−7502], and Robson de Oliveira Albuquerque[0000−0002−6717−3374]

Professional Post-Graduate Program in Eletrical Engineering - PPEE, Department of Eletrical Engineering, University of Brasília, Distrito Federal, Brasília 70910-900, Brazil rogerio.machado@aluno.unb.br
gondim@unb.br
robson@redes.unb.br

Abstract. In cyberspace, boundaries are constantly being crossed in the name of progress and convenience, and invariably result in new vulnerabilities and potential attacks. Traditional security approaches are not able to contain the dynamic nature of new techniques and threats, which are increasingly resilient and complex. In this scenario, the sharing of threat intelligence is growing. However, the vast majority of data is shared in the form of unstructured textual reports, or extracted from blogs and social media. These data sources have been imposing great limitation on security analysts due to the high volume and low quality of Cyber Threat Intelligence (CTI). Among the various aspects that impose limitations on the use of CTI, we focus on data quality. Inaccurate, incomplete or outdated information makes actions reactive, in no way different from traditional approaches. However, quality threat intelligence has a positive impact on incident response time. In this work we propose an Indicator of Compromise enrichment process to improve the quality of CTI, based on the intelligence production cycle, we conduct research to define metrics capable of evaluating the CTI produced through open source licensed threat intelligence platforms.

Keywords: Quality of Cyber Threat Intelligence · Intelligence production cycle · Open Source.

1 Introduction

The advancement of connectivity introduces significant advantages to society [32]. As new technologies are created, a wide range of new vulnerabilities are also incorporated [32]. As a consequence cyber threats grow in volume and sophistication [1, 16, 39, 11, 18, 21, 25], and constitute complicating factors for cyber defense professionals [17, 21, 28, 38]. In addition, attackers have collaborated

* Supported by ABIN TED 08/2019.

with each other, sharing tools and services to increase the effectiveness of their attacks [30].

As a mitigation measure institutions have adopted proactive defense mechanisms against cyber attacks [27, 2]. In this context Cyber Threat Intelligence (CTI) is one of the measurements used, it refers to the set of information collected and organized about cyber threats that can be used to predict, prevent or defend cyber attacks [2, 26].

We identified, through literature review, the factors that influence the quality of CTI, as well as the selection of the Threat Intelligence Platform (TIP) to be used. We defined the hypothesis that this problem can be addressed by applying the intelligence cycle to improve quality using the proposed methodology. First we apply procedures to improve the planning and data collection phase by determining the gaps that need to be addressed, and then we improve the processing and analysis of the data.

The main contribution of this research is to propose an Indicator of Compromise (IoC) enrichment process to improve the quality of CTI, based on the intelligence production cycle. In this way the security analyst will be able to be more assertive and proactive as the CTI is based on an intelligence production process, which throughout its flow, describes the event, identifies the author, positions the event in a timeline and geographically, and describes the mechanisms employed.

The rest of this paper is structured as follows: section 2, related work; section 3, definitions; section 4, methodology; section 5, procedures; section 6, discussions; and section 7, conclusion.

2 Related Works

There are many works around the CTI theme that approach various aspects, of this universe, few approach the production and sharing platforms or the quality of the sources, data and intelligence produced.

Despite the increase in technology and the growing usage of threat intelligence platforms, there are still limitations. There is a large volume of threat information produced and shared in many different formats [2, 42]. This contributes to TIPs providing information with little or no processing. Thus, security analysts have difficulty finding relevant and quality intelligence [2]. In this context, existing approaches remain mostly reactive [4, 27, 39, 41].

Research points to the lack of a defined process, besides not considering the intelligence cycle [28, 39], however, there are studies that point to the need for the implementation of the intelligence cycle in the process of obtaining CTI. [34] Nonetheless, no studies have been observed that contemplate the intelligence cycle in its scope [28].

Another challenge related to CTI is the assessment of the quality of shared information [1, 2, 12, 20, 22, 30, 33, 39, 43, 44]. There is no consensus on the characteristics that indicate the quality of the information. However, four characteristics are among the most cited [2, 3, 43]:

- Opportunity: it is related to the origin of an event and the reaction time or use of certain information;
- Relevance: indicates the relationship of the information with the organization's service and network assets;
- Accuracy: measures how much the information allows to improve the response to an incident and;
- Completeness: indicates the information's ability to describe an incident.

There is conclusive evidence that inaccurate, incomplete, or outdated threat information is a important challenge [2, 6, 39]. To ensure the quality of CTI throughout the collaboration process is crucial to its success. The exchange and use of meaningful threat information depends on measuring and ensuring its quality. This need is reinforced when it is stated that the quality of shared information has an impact on the time required to respond to an incident [31].

3 Definitions

3.1 Intelligence Cycle

A generalized definition of intelligence is described as the conversion of a subject from a completely unknown stage to a state of complete understanding, that is, based on a defined framework, random and general data is filtered to achieve a more relevant data set, when it is processed and converted into information [23].

Most TIPs focus on the data collection phase, thus, the other phases of the intelligence cycle take a back seat [1, 29], generating little or no CTI, as a consequence many TIPs are just replicators and repositories of IoC.

Although, the efforts to employ the intelligence production cycle, few phases are supported by TIP [23], especially the planning phase [28]. The few studies that address the intelligence cycle in CTI, indicate the planning phase as the stage of data source selection [3, 9]. However, the contributions of the planning phase go much further. In this phase the scope, objectives and deadlines are established, as well as the parameters and techniques that will be used [7], and the resources that may be used. Based on the known aspects, the questions that need answers are verified [7]. This phase is crucial to the quality of the CTI [15].

3.2 Threat Intelligence Platform

The collect, treatment and processing of data can be very time consuming [41], in face of the large volume of data [37], especially when performed by humans, besides being financially burdensome. To overcome this challenge, organizations have adopted tools that manage the flow of information, convert it into knowledge [39], and facilitate sharing [36].

The selection of the platform used in this research was based on recent studies that point to Malware Information Sharing Platform (MISP) as the most complete and flexible Threat Intelligence Platform available in open source [9, 12, 20, 34, 23, 39]. These studies took into account aspects such as integration capacity, support for consolidated standards, availability of documentation and community responsiveness. Although the MISP is the most complete TIP, it does not cover all phases of the intelligence cycle.

3.3 Enrichment

The use of appropriate processes, combined with the automation power of TIP, increases the capacity in CTI production, and also contributes to unburdening security analysts [5]. The challenge is to handle the large daily volume of new Indicator of Compromise, which require evaluation to verify possible relationships [22].

In this context, data enrichment is related to obtaining context information derived from a set of raw data, apparently unrelated [24], increasing the value of the information to later transform it into knowledge [9].

The most common method to gain knowledge from a specific data is by cross-checking it with IoC from different external sources [2, 6, 21, 13], in order to take advantage of the enrichment capacity of the different communities that made this data available [2].

Otherwise the correlation of data from various sources can be augmented with a set of data collected within the organization itself [12, 14]. Comparison with internal data allows for identifying relevance and priority of the resulting data in the form of IoC, as well as producing situational awareness through additional context [12, 40, 14].

Through data enrichment, it is possible to contribute to three aspects that influence the quality of CTI:

- Relevance: as the relationship between external and internal events increases, the greater the relevance of information that makes sense to the organization;
- Accuracy: when security analysts gain situational awareness through understanding contexts, supported by data enrichment, the response to an incident if can be improved;
- Completeness: as data enrichment produces more comprehensive information, the ability to describe an incident increases.

On the other hand, many approaches expect to find context from raw data [2, 43], however, from an intelligence cycle perspective, the data needs to be organized in a way that supports answers that complement a predefined context [12, 14]. Without context there are no elements needed to underpin decision making. Without action CTI has no impact and proves useless, further burdening security analysts and adding no actionable intelligence.

4 Methodology

Based on the definitions presented, we verified the importance of knowing the context in which the organization is inserted. Thus, we employed the knowledge construction matrix, allied to the 5W3H method, during the intelligence cycle to create situational awareness and clarify the objectives at each stage of the process. The construction of knowledge goes through four stages [8] that lead from ignorance to actionable intelligence as represented in Fig. 1.

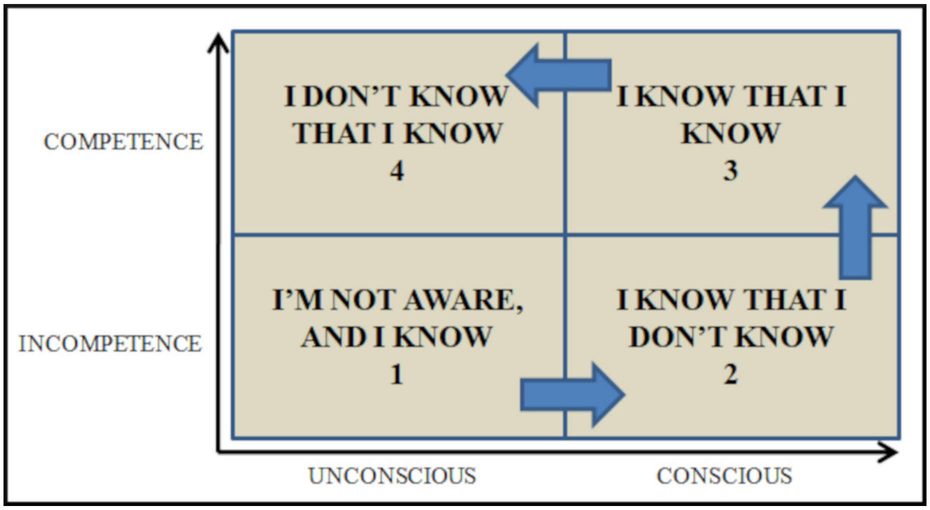
I DON'T KNOW THAT I KNOW 4
I KNOW THAT I KNOW 3
COMPETENCE
I'M NOT AWARE, AND I KNOW 1
I KNOW THAT I DON'T KNOW 2
INCOMPETENCE
UNCONSCIOUS
CONSCIOUS

Fig. 1. Matrix of Knowledge Construction

What I don't know that I don't know represents the state of ignorance, the total absence of knowledge about a certain object. In this phase we do not know our vulnerabilities, capabilities, nor the evident threats. We can correlate it with the Planning and Direction Phase of the intelligence cycle.

What I know that I don't know refers to the awareness that there is something to be discovered, however, we do not have this knowledge. It is the knowledge of a certain vulnerability, but without knowing who, what, or how it can be exploited. It expresses the state of consciousness about the goal to be reached, following the premise that this goal must be useful, that is, it needs to be translated into action. It is the most labor-intensive step of the CTI process due to the large amount of data. We can correlate it with the result of processing the collected data.

What I know that I know corresponds to awareness and mastery over a certain subject, the initial stage for standardizing and expanding knowledge. In this stage the objective is to massify the knowledge. We can associate this phase with the result of the analysis phase of the intelligence cycle, as well as the planning of future actions.

What I don't know that I know is the apex of knowledge, at this point knowledge is strongly rooted, so that certain processes are automated to the point of going unnoticed. This way, when we verify a certain threat or incident, we automatically trigger defense mechanisms without the need for effort or the search for new knowledge in order to mitigate the effects of the threat. It is about proactivity, so measures to eliminate vulnerabilities are taken before they can be exploited by a threat. We associate it with the outcome of the deployment and dissemination phase of the intelligence cycle. Here are also the consequences, inferences and deductions from what is known that have not yet been made explicit.

We adopted the 5W3H method as a guide. It originates from Aristotle's seven circumstances [35]. This method is related to a set of eight questions: what, who, why, when, how, how much, and how long. It is widely applied in several areas in order to obtain contextualization of a theme in its completeness [34]. The 5W3h questions in conjunction with the phases of knowledge construction, contribute to the awareness of the maturity level in relation to what is known and the goals for generating actionable intelligence.

The 5W3H method will initially be employed in the planning phase. The advantage of this approach is that it is easy to see which questions are unanswered. In the following phases we seek answers to the questions that were not answered in the planning phase, so in each cycle of collection, processing and analysis we check the completeness of the context, seeking answers to all questions of the 5W3H method. The more questions in the 5W3H that are answered, the greater the completeness of the CTI and consequently higher the quality. If at the end of this process there are answers to most of the questions, we probably have actionable intelligence [34].

The "what" defines the object to be studied, which in the context of threat intelligence, refers to threats or incidents. The "where" refers to the geographical location where the event originated, and may also be the path taken to the destination. The "When" determines the date and time when the event occurred. The "How" defines the tactics, techniques, and procedures employed. The "How much" refers to the ability to cause damage, it may also be related to funding. "How long" indicates the duration of the event, incident, or threat. "Who" associates the threat or incident organization or individual responsible. "Why" explains the motivations of the person responsible for the event. In Fig. 2 you can see the relationship of the elements of the 5W3H method to entities involved in an incident or threat.

About the selected TIP, besides the advantages already mentioned, the MISP platform has integration with several enrichment tools, however, many of them are not Open Source, or their free versions impose limitations that make their large scale use unfeasible. Since in this paper we propose to work with open source software, we use only open source plugins and integrations. On the other hand, the methodology employed should be independent of TIP, despite the limitations described above.

We apply the cycle of intelligence production using open source data as shown in the Fig. 3 and following paragraphs.

In the direction and planning phase, the first step is to become aware of the current scenario of the organization, this phase reflects on all subsequent processes and can be taken up again when necessary. Through a survey of the

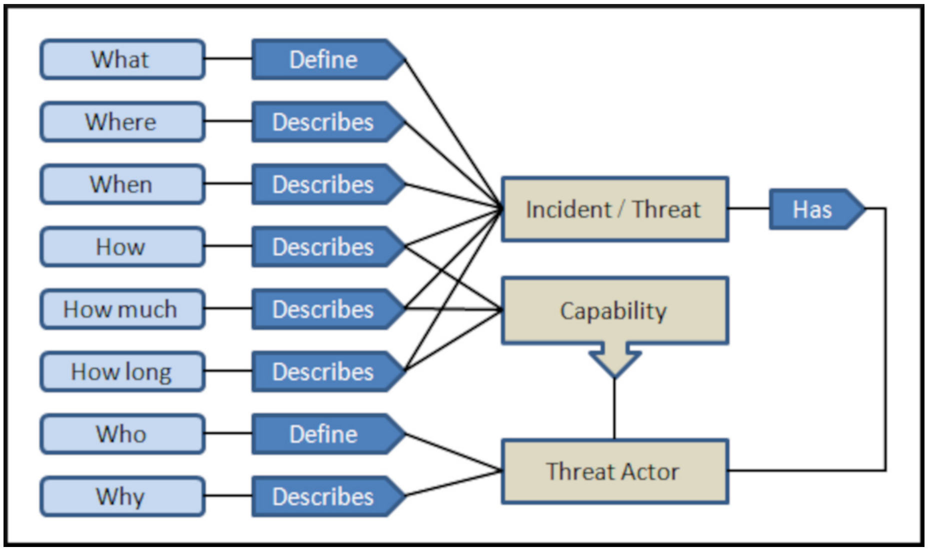

Fig. 2. Relationship Diagram [34]

technologies used, main applications and applications, as well as the topology and subsequent risk analysis, the requirements and priorities of the organization are listed. In this stage we leave the stage of ignorance, "I don't know what I don't know", to the stage of partial awareness, "I know that I don't know".

At this point it is already possible to understand the internal scenario and based on the definition of priorities, assess the existing vulnerabilities for each asset, whether software or hardware. It is crucial to understand which external factors have an influence on the organization and the elements that may be of interest to threat actors. It is also fundamental to collect internal data for comparison with data from external sources, to prove the existence or not of adverse actions.

The 5W3H method helps to delineate the relevant aspects that need to be known in order to build the context. This brings us to the stage where we are aware of the unanswered questions. Then we start planning to define the relevant data sources to complement the context by means of the unanswered questions of the 5W3H method.

After defining the sources and collecting data, it is necessary to verify credibility and validity, as well as evaluate the possibility of enrichment according to the type of data and plugins available. This phase also needs prior planning, in order to define what kind of enrichment can contribute to the completeness of the context.

Supported by the 5W3H model and based on the information created through the enrichment, correlation and patterns of the data from external sources and also the presence or absence of relationships with the organization's own data, we become more aware of the context. At this point new planning is established with

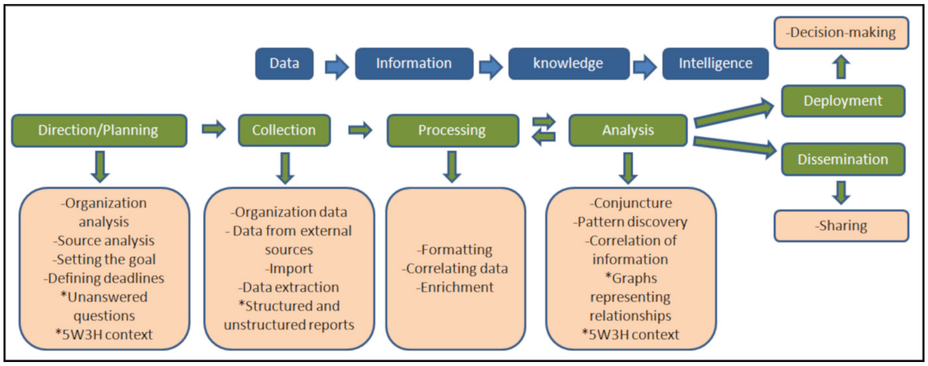

Fig. 3. Cycle for intelligence production

the purpose of proposing pertinent actions, that include safeguarding guidelines, security patching, and incident mitigation, among others.

5 Procedures

Collecting information from various sources is fundamental to generate solid knowledge, however, the credibility of the data and the suitability of the source, under the aspects of authenticity, trust, and competence, must be observed.

In this way, our approach is based on structured and unstructured reports of the Pegasus case, which for the purposes of our experiment we admit are from reliable sources in view of having already been widely discussed by companies with expertise in the field of cyber security, in addition to the fact that they have differentiated resources compared to other institutions, having, for example, the advantage of receiving numerous feedbacks from applications installed in the infrastructure of their customers.

Pegasus is spyware developed by Israel's NSO Group. It has been used as a surveillance tool against high-ranking government officials, human rights activists, journalists, and heads of State [10].

6 Discussions

Based on the proposed methodology we verify the results achieved sustained by the 5W3H model (see Fig. 4)

The information presented was extracted only from eight selected reports. Due to the characteristic of the case analyzed, other reports could result in differences mainly in ”where” and ”who”.

Considering that the reports and data used in the use case are not recent, most domains no longer exist or have a registration date later than the report date. The average number of expired domains (available for re-registration) is

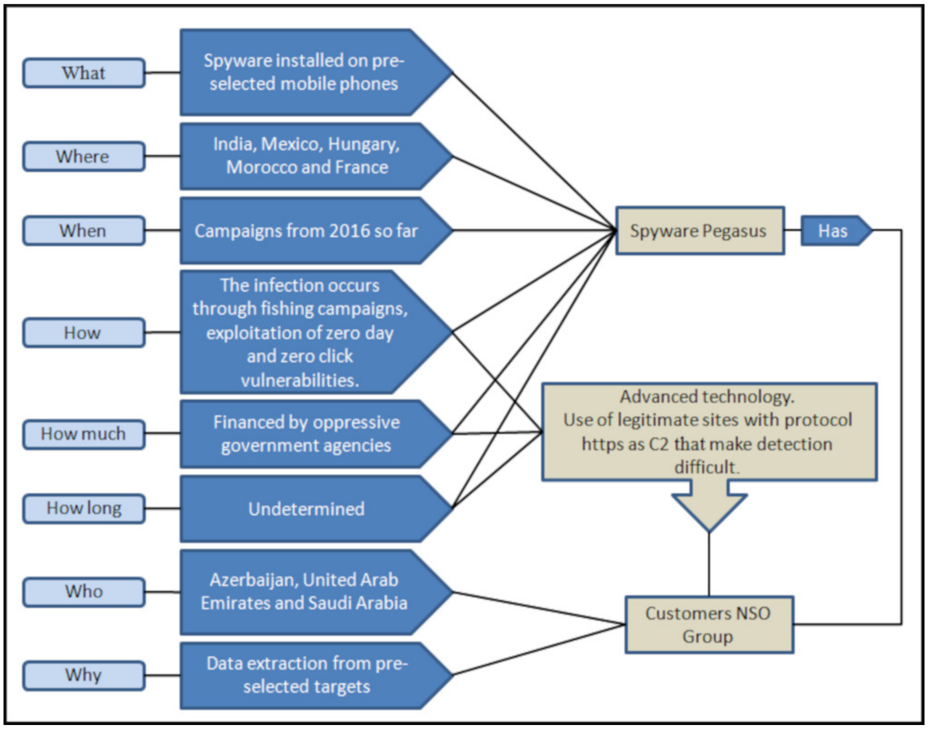
What
Spyware installed on pre-selected mobile phones
Where
India, Mexico, Hungary, Morocco and France
When
Campaigns from 2016 so far
How
The infection occurs through fishing campaigns, exploitation of zero day and zero click vulnerabilities.
How much
Financed by oppressive government agencies
How long
Undetermined
Who
Azerbaijan, United Arab Emirates and Saudi Arabia
Why
Data extraction from pre-selected targets
Spyware Pegasus
Has
Advanced technology. Use of legitimate sites with protocol https as C2 that make detection difficult.
Customers NSO Group

Fig. 4. Result Analysis

68%, ranging from 58% to 80% in reports from August 2016, July 2021, September 2021, December 2021, February 2022, April 2022, and June 2022. This is of concern, given that throughout this research we have identified tools for detecting Pegasus spyware based on IoC sets from these reports. Consequently, occurrences of false positives may be observed.

We observed that identical reports, when analyzed by different organizations, produce different results. For example, the report ”The Million Dollar Dissident - Citizen lab report” [19], available in pdf format, was analyzed by more than one security expert organization, however, the amount of IoC generated by each organization was different. We imported and enriched this report in MISP and observed that the analysis is limited due to the inherent computational complexity of natural language processing (NLP). We also verified that relevant information contained in reports available in natural language was not extracted by the tools employed for collection.

We conclude that the type of enrichment that makes the most sense for ”expired” data is to look for relationships with data spotted in the same period. In addition, when querying domain data, we noted the scarcity of Open Source tools that provide history of the registration data, which could contribute to the temporal definitions of the event. However, we were able to determine some of the tactics, techniques, and procedures employed, as well as identify the vulnerabilities exploited. Thus, we verified the ability to generate intelligence and propose actions, based on the use of the proposed method.

7 Conclusions and Future Work

Threat intelligence alone cannot protect an organization, but rather complements security components related to detection, response, and prevention in order to reduce the potential damage done by increasing the effectiveness of security components, decreasing response time, reducing damage recovery time, and reducing the time the adversary remains in the organization's environment.

As security components become more robust through information originating from CTI, threat prediction becomes closer to reality, since threat mitigation is more inherent to the security state of the organization than to the study of data transiting the network.

Analyzing the possible relationships of known data, it is necessary to verify what type of enrichment can generate usable results. Disordered enrichment often generates a lot of information that is not used and does not add to knowledge. Just as indiscriminately importing reports from multiple sources does not guarantee that you will get actionable CTI.

Although studies show that MISP is the most complete platform, it has limitations, but it was possible to generate Actionable Intelligence by applying the proposed methodology.

The use of the knowledge construction matrix, coupled with the 5W3H method, throughout the intelligence production cycle proved to be effective in creating situational awareness of the organization and clarifying the objectives of each stage of the process. In this way unnecessary data collection and enrichment is avoided.

The main advantage of the proposed methodology is that it contemplates the entire cycle of intelligence production.

Future work can be addressed to integrate tools or platforms that complement each other in order to solve limitations such as employment of the full intelligence cycle and relationship discovery and visualization.

Acknowledgement

R.d.O.A. gratefully acknowledges the technical and computational support of the Laboratory of Technologies for Decision Making (LATITUDE) of the University of Brasília; the General Attorney's Office (Grant AGU 697.935/2019); the General Attorney's Office for the National Treasure – PGFN (Grant 23106.148934/2019-67); the National Institute of Science and Technology in Cyber Security – Nucleus 6 (grant CNPq 465741/2014-2).

The authors thankfully acknowledge the support of Brazilian Intelligence Agency - ABIN grant 08/2019.

References

1. Abu, M.S., Selamat, S.R., Ariffin, A., Yusof, R.: Cyber threat intelligence – issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science **10**(1), 371–379 (2018). https://doi.org/10.11591/ijeecs.v10.i1.pp371-379
2. Azevedo, R., Medeiros, I., Bessani, A.: Automated solution for enrichment and quality ioc creation from osint. Simpósio de Informática (INForum 2018) p. 12 (2018), http://disiem-project.eu/wp-content/uploads/2018/11/INForum2018_enr-IoC.pdf
3. Basheer, R., Alkhatib, B.: Threats from the dark: A review over dark web investigation research for cyber threat intelligence. Journal of Computer Networks and Communications **2021** (2021). https://doi.org/10.1155/2021/1302999
4. Berndt, A., Ophoff, J.: Exploring the Value of a Cyber Threat Intelligence Function in an Organization, vol. 579 IFIP, p. 96–109. Springer International Publishing (2020). https://doi.org/10.1007/978-3-030-59291-2_7
5. Bromander, S.: Understanding Cyber Threat Intelligence - Towards Automation. Ph.D. thesis, University of Oslo (2021), http://urn.nb.no/URN: NBN: no-87408
6. Bromander, S., Swimmer, M., Muller, L.P., Jøsang, A., Eian, M., Skjøtskift, G., Borg, F.: Investigating sharing of cyber threat intelligence and proposing a new data model for enabling automation in knowledge representation and exchange. Digital Threats: Research and Practice **3**(1), 1–22 (Mar 2022). https://doi.org/10.1145/3458027
7. Bubach, R., Herkenhoff, H.G., Herkenoff, L.S.B.: O cilclo da inteligência e os requisitos para a produção do conhecimento. Ph.D. thesis, Universidade Vila Velha (2019), https://repositorio.uvv.br//handle/123456789/570
8. Businessballs: Conscious competence learning model, https://www.businessballs.com/self-awareness/conscious-competence-learning-model/#theories_models_change_learning
9. Chantzios, T., Koloveas, P., Skiadopoulos, S., Kolokotronis, N., Tryfonopoulos, C., Bilali, V.G., Kavallieros, D.: The quest for the appropriate cyber-threat intelligence sharing platform. In: Proceedings of the 8th International Conference on Data Science, Technology and Applications. p. 369–376. SCITEPRESS - Science and Technology Publications (2019). https://doi.org/10.5220/0007978103690376
10. Chawla, A.: Pegasus spyware – "a privacy killer". SSRN Electronic Journal (2021). https://doi.org/10.2139/ssrn.3890657, https://www.ssrn.com/abstract=3890657
11. Check, P.: Cyber securit y report 2021. Tech. rep., Check Point, San Carlos, CA (2021), https://pages.checkpoint.com/cyber-security-report-2021.html?utm_source=cp-home&utm_medium=cp-website&utm_campaign=pm_wr_21q1_ww_security_report
12. Faiella, M., Gonzalez-Granadillo, G., Medeiros, I., Azevedo, R., Gonzalez-Zarzosa, S.: Enriching threat intelligence platforms capabilities. ICETE 2019 - Proceedings of the 16th International Joint Conference on e-Business and Telecommunications **2**, 37–48 (2019). https://doi.org/10.5220/0007830400370048
13. Gao, Y., Li, X., Peng, H., Fang, B., Yu, P.S.: HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE Transactions on Knowledge and Data Engineering **34**(2), 708–722 (feb 2022). https://doi.org/10.1109/TKDE.2020.2987019, https://ieeexplore.ieee.org/document/9072563/
14. González-Granadillo, G., Faiella, M., Medeiros, I., Azevedo, R., González-Zarzosa, S.: Etip: An enriched threat intelligence platform for improving osint correlation,

analysis, visualization and sharing capabilities. Journal of Information Security and Applications **58**, 102715 (May 2021). https://doi.org/10.1016/j.jisa.2020.102715

15. Hettema, H.: Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence. Computers and Security **109**, 102396 (2021). https://doi.org/10.1016/j.cose.2021.102396, https://doi.org/10.1016/j.cose.2021.102396
16. Husari, G., Al-Shaer, E., Ahmed, M., Chu, B., Niu, X.: TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI Sources. In: ACM International Conference Proceeding Series. vol. Part F1325, pp. 103–115. Association for Computing MachineryNew YorkNYUnited States, Orlando FL USA (2017). https://doi.org/10.1145/3134600.3134646
17. Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., Tryfonopoulos, C.: InTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. Electronics (Switzerland) **10**(7) (2021). https://doi.org/10.3390/electronics10070818
18. Korte, K.: Measuring the quality of Open Source Cyber Threat Intelligence Feeds. Master's thesis, JAMK University of Applied Sciences - Finland (2021), https://www.theseus.fi/handle/10024/500534 http://urn.fi/URN:NBN:fi:amk-202105178967
19. Marczak, B.B., Scott-railton, J.: The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Tech. rep., Citizen Lab - University of Toronto, Toronto, Ontario - Canada (2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
20. Martins, C., Medeiros, I.: Generating quality threat intelligence leveraging osint and a cyber threat unified taxonomy. ACM Transactions on Privacy and Security **25**(3), 1–39 (Aug 2022). https://doi.org/10.1145/3530977
21. Nikolaienko, B., Vasylenko, S.: Application of the Threat Intelligence Platform To Increase the Security of Government Information Resources. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska **11**(4), 9–13 (2021). https://doi.org/10.35784/iapgos.2822
22. Oosthoek, K., Doerr, C.: Cyber threat intelligence: A product without a process? International Journal of Intelligence and CounterIntelligence **34**(2), 1–16 (2020). https://doi.org/10.1080/08850607.2020.1780062
23. Papaioannou, F.: Threat Intelligence Platforms evaluation. Ph.D. thesis, University of Piraeus (2021), https://dione.lib.unipi.gr/xmlui/handle/unipi/13346
24. Park, Y., Choi, J., Choi, J.: An extensible data enrichment scheme for providing intelligent services in internet of things environments. Mobile Information Systems **2021**, 1–18 (May 2021). https://doi.org/10.1155/2021/5535231, https://www.hindawi.com/journals/misy/2021/5535231/
25. Preuveneers, D., Joosen, W.: Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. Journal of Cybersecurity and Privacy **1**(1), 140–163 (2021). https://doi.org/10.3390/jcp1010008, https://www.mdpi.com/2624-800X/1/1/8/htm
26. Rahman, M.R., Mahdavi-Hezaveh, R., Williams, L.: A literature review on mining cyberthreat intelligence from unstructured texts. In: 2020 International Conference on Data Mining Workshops (ICDMW). IEEE (Nov 2020). https://doi.org/10.1109/ICDMW51313.2020.00075
27. Samtani, S.: Developing proactive cyber threat intelligence from the online hacker community: a computational design science approach. Ph.D. thesis, THE UNIVERSITY OF ARIZONA (2018), http://hdl.handle.net/10150/628454

28. Sauerwein, C., Fischer, D., Rubsamen, M., Rosenberger, G., Stelzer, D., Breu, R.: From threat data to actionable intelligence: An exploratory analysis of the intelligence cycle implementation in cyber threat intelligence sharing platforms. ACM International Conference Proceeding Series (2021). https://doi.org/10.1145/3465481.3470048
29. Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. The 13th International Conference on Wirtschaftsinformatik p. 837–851 (2017), https://wi2017.ch/images/wi2017-0188.pdf
30. Schaberreiter, T., Kupfersberger, V., Rantos, K., Spyros, A., Papanikolaou, A., Ilioudis, C., Quirchmayr, G.: A quantitative evaluation of trust in the quality of cyber threat intelligence sources. ACM International Conference Proceeding Series (2019). https://doi.org/10.1145/3339252.3342112
31. Schlette, D., Böhm, F., Caselli, M., Pernul, G.: Measuring and visualizing cyber threat intelligence quality. International Journal of Information Security **20**(1), 21–38 (2021). https://doi.org/10.1007/s10207-020-00490-y
32. Security, A.: Cyber Threatscape Report. Tech. rep., Accenture Security (2020), https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf
33. Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Data quality challenges and future research directions in threat intelligence sharing practice. WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016 p. 65–70 (2016). https://doi.org/10.1145/2994539.2994546
34. de Melo e Silva, A., Gondim, J.J.C., de Oliveira Albuquerque, R., Villalba, L.J.G.: A methodology to evaluate standards and platforms within cyber threat intelligence. Future Internet **12**(6), 1–23 (2020). https://doi.org/10.3390/fi12060108
35. Sloan, M.: Aristotle's as the original locus for the septem circumstantiae. Classical Philology **105**, 236–251 (2010). https://doi.org/10.1086/656196
36. Stojkovski, B., Lenzini, G., Koenig, V., Rivas, S.: What s in a cyber threat intelligence sharing platform? ACM International Conference Proceeding Series p. 385–398 (2021). https://doi.org/10.1145/3485832.3488030
37. Sun, T., Yang, P., Li, M., Liao, S.: An automatic generation approach of the cyber threat intelligence records based on multi-source information fusion. Future Internet **13**(2), 1–19 (2021). https://doi.org/10.3390/fi13020040
38. Tekin, U., Yilmaz, E.N.: Obtaining Cyber Threat Intelligence Data from Twitter with Deep Learning Methods. ISMSIT 2021 - 5th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings pp. 82–86 (2021). https://doi.org/10.1109/ISMSIT52890.2021.9604715
39. Tounsi, W., Rais, H.: A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security **72**, 212–233 (jan 2018). https://doi.org/10.1016/j.cose.2017.09.001
40. Vielberth, M., Menges, F., Pernul, G.: Human-as-a-security-sensor for harvesting threat intelligence. Cybersecurity **2**(1), 23 (dec 2019). https://doi.org/10.1186/s42400-019-0040-0
41. Wagner, T.D., Mahbub, K., Palomar, E., Abdallah, A.E.: Cyber threat intelligence sharing: Survey and research directions. Computers and Security **87**, 101589 (2019). https://doi.org/10.1016/j.cose.2019.101589
42. Zhao, J., Yan, Q., Liu, X., Li, B., Zuo, G.: Cyber threat intelligence modeling based on heterogeneous graph convolutional network. In: 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). p. 241–256 (2020), https://www.usenix.org/conference/raid2020/presentation/zhao

43. Zibak, A., Sauerwein, C., Simpson, A.C.: Threat intelligence quality dimensions for research and practice. Digital Threats p. 1–22 (Sep 2021). https://doi.org/10.1145/3484202
44. Zibak, A., Simpson, A.: Cyber threat information sharing: Perceived benefits and barriers. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. p. 1–9. ACM (Aug 2019). https://doi.org/10.1145/3339252.3340528