World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:10, 2022

Using Social Network Analysis for Cyber Threat Intelligence

Vasileios Anastopoulos

***Abstract*—**Cyber threat intelligence assists organisations in understanding the threats they face and helps them make educated decisions on preparing their defences. Sharing of threat intelligence and threat information is increasingly leveraged by organisations and enterprises, and various software solutions are already available, with the open-source malware information sharing platform (MISP) being a popular one. In this work, a methodology for the production of cyber threat intelligence using the threat information stored in MISP is proposed. The methodology leverages the discipline of social network analysis and the diamond model, a model used for intrusion analysis, to produce cyber threat intelligence. The workings of the proposed methodology are demonstrated with a case study on a production MISP instance of a real organisation. The paper concludes with a discussion on the proposed methodology and possible directions for further research.

***Keywords*—**Cyber threat intelligence, diamond model, malware information sharing platform, social network analysis.

I. Introduction

THE ever-increasing number and sophistication of cyber-attacks pose the need for organisations to understand how the threat actors operate and to properly adjust their defences. Cyber threat intelligence (CTI) is a tool for achieving this understanding and various defenders already employ such programs reporting varying levels of maturity. Establishing CTI-sharing communities enables the participants to benefit from collective knowledge and experience. Shared situational awareness, improved security posture, knowledge maturation and defensive agility are among the resulting benefits. CTI-sharing is accompanied by challenges such as establishing trust, automation and interoperability, protecting information and enabling its consumption. Leveraging CTI makes it easier for an organisation to understand the threats it is facing and make better-informed decisions on incident response, both technically and procedurally [1]. According to a recent report, even small organisations increasingly invest in CTI programmes, demonstrating it as a mature field whose benefits are well understood and perceived [2]. There is a tendency toward automation of tools and processes with the profound aim of allowing analysts to focus on higher-level analytical activities instead of performing repetitive tasks. CTI is not only consumed by organisations but it is also disseminated using tools such as vendor-created or open-source threat intelligence platforms [2]. Their uses vary from the strategic (resource prioritisation and allocation) to the tactical (threat alerting and response).

V.A. is with the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia (e-mail: vasileios.anastopoulos@ccdcoe.org).

The MISP is an open-source software solution for the collection, storage, distribution and sharing of cyber security indicators and threats and can be used for the analysis of malware and cyber security incidents. An *indicator* is 'a technical artefact or observable that suggests an attack is imminent or is currently underway or that a compromise may have already occurred' [1]. Indicators of malware, attacks, financial fraud or any other intelligence can be shared within a community of trusted members [3]. MISP is a popular solution and is operated by many enterprises and organisations [4] for storing, correlating, sharing and consuming indicators with organisations operating their own instances or participating in sharing communities. The indicators stored in MISP are of great value for organisations since they can be used to detect and block attacks [2]. Further analysis of the indicators can lead to the production of CTI to facilitate decisions such as resource prioritisation and allocation.

This paper seeks to provide a means of producing CTI using the data stored in CTI platforms, while its contribution is a methodology for achieving this. The novelty of this work is the application of social network analysis (SNA) concepts and techniques to the MISP software solution to produce CTI.

In MISP an organisation creates events and each event is described by various attribute values, which can be in the form of free-text or specific data types (domain names, internet protocol (IP) addresses, file hashes, etc.). In this work, it is assumed that when an organisation creates an event it has been affected by it in some way since it detected and reported it. The relationship between organisations, events and attributes is modelled as a social network and SNA is applied to identify groups of indicators (attribute values) and organisations that should be prioritised for incident response. The selection of SNA measurements and the prioritisation of indicators and organisations is achieved by leveraging the diamond model (DM) of intrusion analysis [5]. The workings of the proposed methodology are demonstrated with a case study using a data set from a production MISP instance of the Computer Incident Response Centre, Luxembourg (CIRCL) [6].

The remainder of this paper is organised as follows: In Section II, related work is discussed and in Section III, the proposed methodology is presented. In Section IV, the workings of the proposed methodology are demonstrated by applying it to a dataset from a real organisation. This work is concluded with Section V, which summarises the findings and proposes directions for future work.

II. Related Work

CTI has attracted research interest with various aspects of CTI and CTI platforms being studied. Researchers are applying supervised machine learning, natural language processing and deep learning techniques to process shared CTI data ([7]-[10], as cited in [11]). In [12], the authors deal with the shortcomings of the resource description framework (RDF) and other existing knowledge graphs in describing cyber threats and intelligence. They propose a hand-curated knowledge graph that uses unstructured threat-related data to extract information. The work in [13] addresses the problem of the limited use that text-intensive and semi-structured data have for security experts due to their extent and lack of readability. The authors seek to improve the accessibility of security experts to CTI. They propose a concept for the interactive visual analytics of threat intelligence presenting information in a graph database connected to a visual interface. This visual interface helps the security experts in incident analysis and the inclusion of knowledge into CTI information.

There is also work in evaluating existing CTI platforms and standards. In [14], the authors propose a methodology for evaluating threat intelligence standards and CTI platforms, while in [15] existing CTI relevant ontologies, taxonomies and sharing standards are evaluated to measure their high-level conceptual expressivity. The quality of CTI is assessed in [16] and the quality of open-source CTI feeds is evaluated in [17]. The risk of sharing CTI data sets is assessed in [18] with the authors proposing a quantitative risk model for performing the assessment. In [19], the authors present a novel trust taxonomy to establish a trusted threat-sharing environment. They compare and analyse popular CTI platforms and providers and the proposed taxonomy is demonstrated through case studies.

A prototype application is developed in [11] where the authors automatically process MISP data aiming to prioritise them. They aim to address the needs of small and medium-sized enterprises by providing recommendations tailored to their context. In [20] and [21], the authors deal with the topic of sharing indicators in an efficient way that considers their validity and freshness. They propose a scoring model for prioritising, or decaying, attributes in MISP that uses MISP event attributes such as taxonomies, sightings and the reliability of the source. The scoring methods are evaluated using a phishing dataset with encouraging results. The authors in [22] propose an enriched threat intelligence platform to integrate security data from public sources with the data generated by the monitored infrastructure's detection and response systems such as security information and event management (SIEM) systems or intrusion detection and prevention systems (IDPS). This is achieved using heuristic analysis to correlate the receiving open-source intelligence (OSINT) data with the potential security issues of the monitored infrastructure, thus resulting in a threat score for the received OSINT data used in continuance to prioritise them. Following, these enriched data are sent to security systems (SIEM, IDPS, etc.) for visualisation, storage and processing and is shared with external organisations.

As far as it is known, there is no published work seeking to analyse and prioritise indicators through the application of SNA concepts and techniques on CTI platforms including MISP.

III. Proposed Methodology

In the context of this work, *threat intelligence* is defined as, 'threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes' [1].

An *organisation* that is registered to a MISP instance can enter data creating an *event* [3]. An *event* contains generic information such as time and risk level of the incident and a short description and is further described by adding *attributes*. An *attribute* is described by a *category,* a *type* and a *value,* among other things. The *value* of the *attribute* is the actual indicator related to the stored *event.* The relations among organisations, events and attributes are shown in Fig. 1. An *organisation* can be related to many *events* while the same *event* may affect many *organisations;* an *event* can be described by many *attributes* and an *attribute* may describe many *events.* The relationship between the data structures allows us to model the data as a social network and consequently use the SNA methods and techniques to analyse it [23].

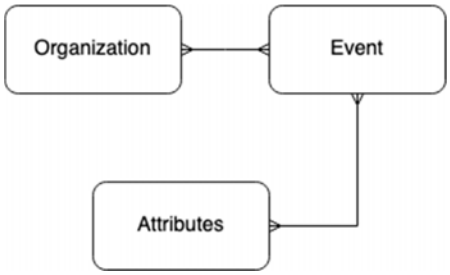

Fig. 1 MISP entity relationships diagram

The DM is a model for intrusion analysis and describes an *adversary* that uses some *capability* over some *infrastructure* against a *victim*. These activities are called *events*, with their core features being adversary, capability, infrastructure and victim. *Meta-features* are also defined in the model (timestamp, phase, result, direction, methodology, resources) and an extension of the model itself, adding the features of *social-political* and *technology.* The vertices of the model are linked with the edges (see Fig. 2), highlighting the relationships between the features. This enables the analyst to pivot across edges and within vertices exposing more information about adversary operations, capabilities, infrastructure and victims [5]. The *infrastructure* feature is used to describe, 'the physical and/or logical communication structures the adversary uses to deliver a capability, maintain control of capabilities and effect results from the victim' [5]. It can be a domain name, an IP address, an email address or something broader like a USB device. This work encompasses the indicators that organisations use to describe the events they create in MISP. The meta-feature of a *shared threat space* is also used with two or more victims in a shared threat space as long as they share features that satisfy the needs of one or more adversaries. The identification of the shared threat space is thought to be the cornerstone of strategic and proactive mitigation [5] as it allows

the prediction of future attacks based on the current attacks on the members of the threat space. The DM proposes analytical pivoting approaches, among which the *infrastructure-centred approach* is leveraged in the proposed methodology. This analytic approach focuses on the infrastructure of the adversary where starting from an element of his infrastructure, more elements and related infrastructure can be discovered. For example, a victim communicating with an IP address can lead to the identification of more victims, since any system communicating with this IP address could also be compromised by the same adversary.

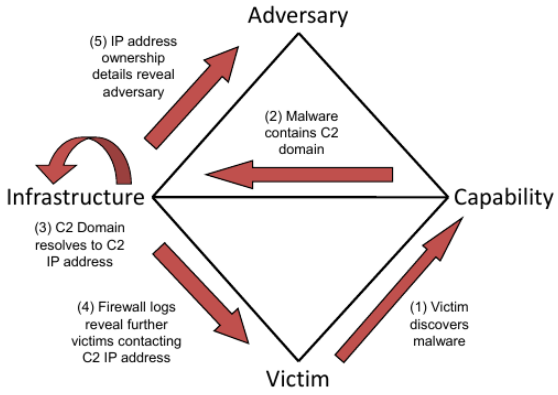

Fig. 2 DM features relationships

SNA [23] is based on the assumption of the importance of relationships among interacting units. It is part of the social and behavioural sciences, though a discrete research perspective, and it includes models, theories and applications that are expressed with relational concepts or processes [23]. In the SNA perspective an *actor* (or *node*) is a social entity. It can be a discrete social unit (an individual, group of people, corporate department, etc.), and though termed actors it is not implied that they have the ability to act. *Social ties* (or *links*), connect actors, establishing a tie between a pair of actors and are channels for the transfer or flow of resources, either material or nonmaterial. A *relation* is the collection of ties of a specific kind among members of a group (or set) of actors. A *social network* consists of a finite set, or sets, of actors and the relation, or relations, defined on them. They are composed of nodes and links. When the link from node A to node B is different from the link from node B to node A, the network is *directed.* When it is the same, the network is *undirected*. A node can have one or more attributes and a link can be binary or valued. Using graph theory notation, G = (V, E) is a social network G with |V| nodes and |E| links among them and it is represented by a |V| x |V| adjacency matrix. When a link exists between node $v_i \in V$ and node $v_j \in V$, this is indicated by a value in the $e_{ij} \in E$ cell. This is a 1-mode network since the links are formed among the nodes of the same set. Formally, the term *mode* refers to a distinct set of entities where structural variables are measured, while *structural variables* measure ties of a specific kind between pairs of nodes. A *2-mode* network is formed between two distinct sets of nodes, M and N, represented by the |M| x |N| incidence matrix.

Affiliation networks are 2-mode networks consisting of a set of actors and a set of events and describe collections of actors rather than simply ties between pairs of actors [23]. An event does not necessarily consist of face-to-face interaction. It can correspond to various occasions such as the participation in a party, a club, a committee, a board of directors, etc. When two actors participate, for example, in the same committee, they are affiliated (linked) by the same committee (event). An affiliation network is represented by an affiliation matrix |A| x |E|. When row actor *i* affiliates to column event *j*, a value of 1 is present in *the ij* cell. *Folding* [24] the affiliation network uses matrix algebra to first transpose its matrix to the desired dimension and then multiply it by the initial incidence matrix. This results in |A| x |A|, the array of linkages among actors through their participation in events, where a value in the *ij* cell indicates the number of events the two actors share; |E| x |E|, the array of linkages among events through the participation of actors, where a value in cell *ij* indicates the number of actors the two events share. These 1-mode networks that derive from the affiliation network are valued and undirected and the linkages among the members of one mode are based on the linkages established through the second mode. A property of affiliation networks is the *duality* in the relationship between actors and events, which analytically means that both the ties between the events and between the actors can be studied.

The proposed methodology starts with the construction of the affiliation network, the undirected 2-mode social network that relates the actors (organisations) to the event attributes (indicators). The first node set, $O = \{org_1, org_2, ..., org_n\}$, consists of the organisations (actors) and the second node set, $I = \{ind_1, ind_2, \ldots, ind_m\}$, consists of the indicators (events) that affect those organisations. The affiliation matrix is represented by |O| x |I|, where the presence of a value in the *ij* cell indicates that org_i is affected by ind_j and a link, if formed among them (Fig. 3). Following, the |O| x |I| matrix is folded resulting in the |O| x |O| and |I| x |I| arrays. The former (Fig. 4) consists of the organisations that are affected by the same indicators; the value in the *ij* cell corresponds to the common indicators between org_i and org_j. The latter (Fig. 5) consists of the indicators that affect the same organisations; the value in the *ij* cell corresponds to the common organisations affected by ind_i and ind_j.

Having constructed the two 1-mode networks, the measure of *total degree centrality* is calculated for each node. *Total degree centrality* is the number of links a node has and is used to identify the nodes that actively participate in the social network. It is distinguished into *in degree* and *out degree*, when the links are directed to or from the node, respectively. The total degree centrality of a node is equal to its normalised in degree, plus its out degree. Let G = (V, E) be the graph representation of a square network and a node v. The total degree centrality of node v = deg / 2 * (|V| - 1), where deg = card $\{u \in V | (v, u) \in E \vee (u, v) \in E\}$([23] as cited in [25]). A node with high degree centrality is a well-connected node and can potentially directly influence many other nodes [26]. The total degree centrality is measured for the |O| x |O| 1-mode social network and the nodes (organisations) are ranked in descending order. The most highly valued are those organisations that are affected by the same

indicators as many other organisations.

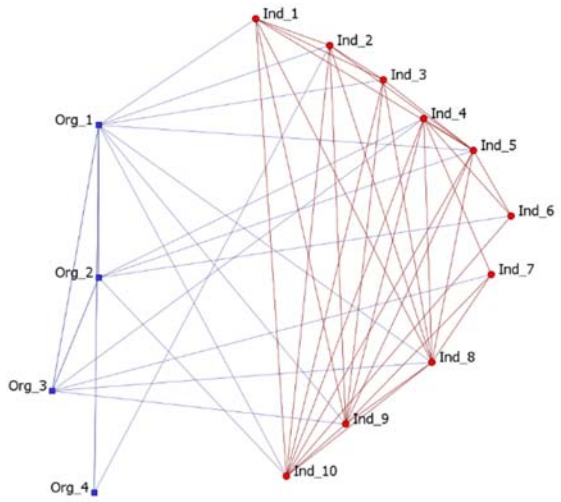

Fig. 3 |O| x |I| affiliation network

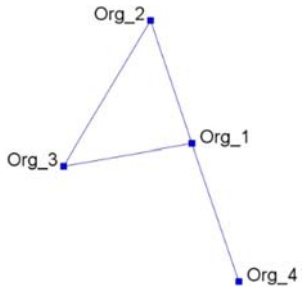

Fig. 4 |O| x |O| 1-mode social network

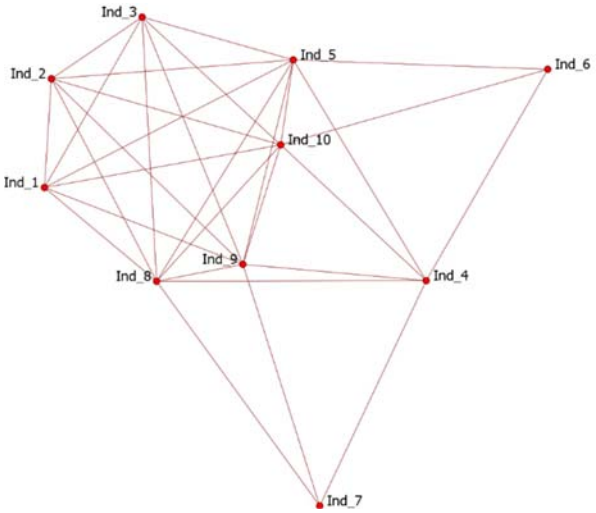

Fig. 5 |I| x |I| 1-mode social network

Following, the *m-slices* are identified. An *m-slice* is a maximal subnetwork that contains those links with a multiplicity greater than or equal to *m* and the nodes incident with these links [27]. This allows the identification of groups of organisations based on the multiplicity of common indicators they are affected by; the higher the m-slice value, the higher the multitude of common indicators affecting the group of organisations.

The fact that a group of organisations is affected by the same indicators is an indication that the same *infrastructure* (as defined in the DM**)** is being used against them, resulting in that they belong to a *shared threat space* [5]. This information enables them to better prioritise their resources and focus their efforts [28] while sharing CTI with those that are possible to be impacted by a similar adversary is more productive and cost-efficient. Applying the *infrastructure-centred* approach of the DM enables the discovery of more related indicators thus enabling the identification of more victims, additional infrastructure and adversary information. For example, suppose that org_1 is affected by five IP addresses and org_2 has so far been affected by only two of them, likely, it will also be affected by the remaining three as both organisations belong to the same threat space and the same infrastructure is used against them.

Next, the total degree centrality is measured for the |I| x |I| 1-mode social network and the nodes (indicators) are ranked in descending order. The more highly ranked are those indicators that affect many common organisations, and thus they should be prioritised for incident response. The m-slices allow for the identification of groups of indicators that affect many common organisations. An indicator or a group of indicators that is affecting multiple common organisations should be treated with priority throughout the process of incident response [28]. For example, a domain name that has been reported by many organisations should be prioritised in incident response. On the other hand, a domain name that has affected only a few, or just one organisation, may be a sign of a targeted attack against those specific organisations.

IV. Case Study

The case study uses data stored on a production MISP instance of the CIRCL [6]. The data were accessed using the MISP REST API and the PyMISP Python library [29], [30]. The construction and analysis of the social networks were performed using the ORA-LITE version 3.0.9.9.87, a software tool developed by CASOS at Carnegie Mellon University for the dynamic assessment and analysis of meta-networks [31]. The attribute values describing the MISP events are the indicators that affect each organisation and the organisation creating an event is considered to be affected by it, since it detected and reported it. In this study, the selected indicators were the event attribute types that contain IP addresses. The proposed methodology and SNA software impose no limitation in considering more and different types, such as autonomous systems, bank accounts, cookies and more (listed in [32]).

According to CIRCL policy, the data used for this cases study are not allowed to be published and thus were anonymised. Each IP address was replaced by an 'IP' label and each organisation by an 'ORG' label. For the construction of the |O| x |I| affiliation network, 6 organisations and the 1,999 IP addresses affecting them were selected, resulting in the formation of 2,162 links among them. The resulting social network is visualised in Fig. 6 where the organisations are represented by blue squares and the IP addresses by red dots; the node labels have been omitted for readability. An

organisation reporting an IP address is assumed to be affected by this IP address and a link is formed between that organisation and the IP address.

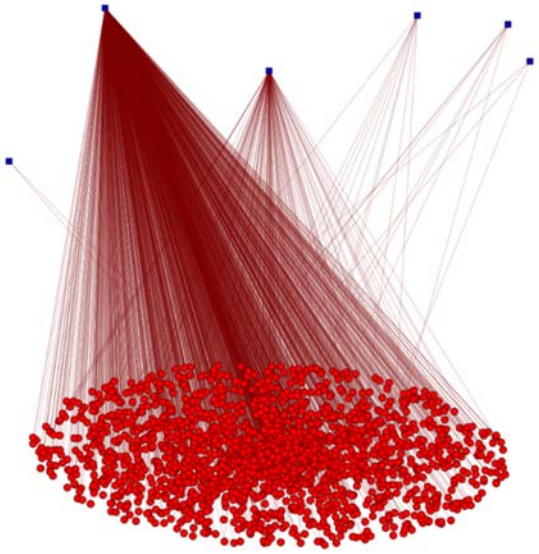

Fig. 6 Case study |O| x |I| affiliation network

Having constructed the affiliation network the proposed methodology continues folding the |O| x |I| social network to result in: the |O| x |O| 1-mode, valued social network and; the |I| x |I| 1-mode, valued social network.

In the |O| x |O| social network visualised in Fig. 7, two organisations are linked when they are affected by the same IP address (indicator); the link value shows how many common IP addresses are affecting them. The resulting 1-mode network is composed of six nodes (organisations) and 10 links. The total degree centrality of each node in the |O| x |O| 1-mode, valued social network is measured and the nodes are ranked based on their value in descending order, Table I. Nodes ORG-1 and ORG-2 are the highest-ranked ones, with the former sharing 163 IP addresses with other organisations and the latter sharing 150. These organisations could play a central role in sharing threat intelligence and, they should be prioritised during a collaborative response due to the large number of indicators affecting them. In Fig. 7, the formation of m-slices is easily identified. ORG-1 and ORG-2 are affected by the same 141 IP addresses forming a 141-slice, while ORG-1, ORG-3 and ORG-2 form a 10-slice since they are affected by 10 or more common IP addresses. The fact that these groups of organisations are targeted by the same IP addresses is an indication that the same infrastructure (as defined in the DM) is leveraged against them, thus they belong to the same shared threat space. These organisations could share CTI to allow them to prepare against and mitigate threats faster and more efficiently. Their resources can also be better prioritised as the IP addresses used against ORG-1 could be also used against ORG-3 and ORG-2. Preparation against and detection of these IP addresses (indicators) would result in a more effective incident response and could also reveal new victims (e.g., systems communicating with these IP addresses).

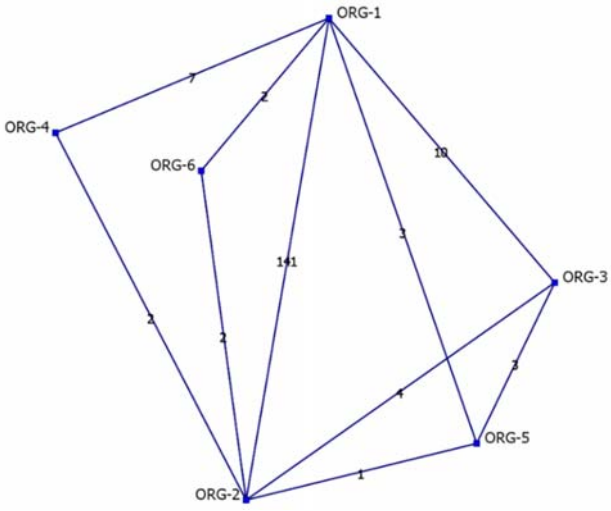

Fig. 7 Case study |O|x |O| 1-mode social network

TABLE I
ORGANISATIONS' TOTAL DEGREE CENTRALITY RANKING

Rank	Organisation	Scaled	Unscaled
1	ORG-1	0.231	163
2	ORG-2	0.213	150
3	ORG-3	0.024	17
4	ORG-4	0.013	9
5	ORG-5	0.010	7
6	ORG-6	0.006	4

TABLE II
SAMPLE IP ADDRESSES TOTAL DEGREE CENTRALITY RANKING

Rank	IP address	Scaled	Unscaled
1	IP-1	0.359	2,149
2	IP-2	0.358	2,147
3	IP-3	0.358	2,147
4	IP-4	0.358	2,147
5	IP-5	0.358	2,144
6	IP-6	0.358	2,144
7	IP-7	0.357	2,139
8	IP-8	0.357	2,139
9	IP-9	0.357	2,138
10	IP-10	0.357	2,138

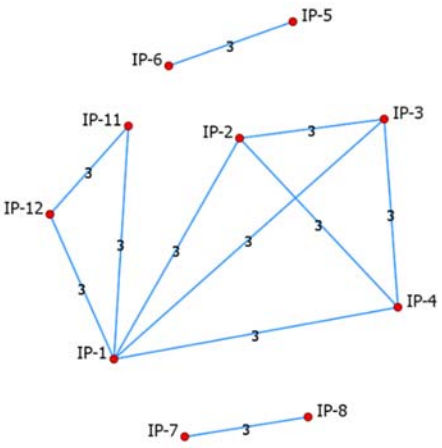

Fig. 8 Case study |I| x |I| 1-mode social network

The proposed methodology continues with the analysis of the |I| x |I| 1-mode valued social network visualised in Fig. 8, where two IP addresses (indicators) are linked when they affect the same organisation; only links valued 3 are depicted for readability. The resulting 1-mode network is composed of 1,999 nodes (IP addresses) and 1,997,001 links among them. The total degree centrality is measured and the nodes (IP addresses) are sorted in descending order. A sample list of the nodes' measurements is listed in Table II showing their ranking and values. These nodes are highly valued since they are the 10 highest ranking among the 1,999 nodes. They should be handled with priority during the incident response phases as they all affect multiple common organisations. Using the m-slices measurement a group of 6 IP addresses is identified (IP-1, IP-2, IP-3, IP-4, IP-11, IP-12) affecting organisations with a multiplicity of three, forming a 3-slice. These groups of IP addresses (indicators) should be prioritised in incident response. They could be blocked or blacklisted in a network security solution, detection signatures could be created for network or host detection and, of course, they could be shared using a CTI platform as part of a threat information or threat intelligence platform.

The workings of the proposed methodology were demonstrated using a small number of organisations and indicators to ensure the readability of the visualisations, though the SNA software tools can easily handle measurements and visualisations on thousands of nodes and links.

V. Conclusions and Future Work

The problem that was dealt with in this work is the production of CTI using the data that are commonly stored in software solutions such as the MISP platform. Concepts and techniques available in the discipline of SNA are combined with the DM, a model used for intrusion analysis and the production of CTI. The result and contribution of this work is the proposal of methodology that models the MISP threat data as a social network, applies relevant SNA analysis techniques and leverages the DM model to identify groups of victims that are targeted by the same infrastructure such as IP addresses. This enables the victims to allocate their resources in a cost-efficient manner, establish CTI-sharing relationships and prioritise and focus their incident response process and capabilities.

The workings of the methodology were demonstrated with a case study using the anonymised threat data stored on a production MISP instance. During the case study, the importance of threat data semantics was identified. The fact that multiple organisations are creating events in a MISP instance can result in different semantics being used to describe similar security incidents. For example, an organisation might use MD5 hashes for malware samples, while another might use SHA256 hashes for the same purpose. In this case, even though both organisations are affected and report the same malware, the link between them is not established.

The proposed methodology is not limited to the MISP platform, it can be applied to any CTI-sharing solution as long as the data can be modelled as a social network. Leveraging the features and capabilities of SNA software facilitates the application of analysis techniques on these networks, producing measurements and visualisations. Future work could focus on the automation of the methodology, development of a software tool and development of a MISP module that could perform the task. The methodology could be also enhanced by researching more analytic pivoting approaches available in [5]: the victim-centred; the capability-centred; the adversary-centred; the social-political centred; and the technology-centred.

Acknowledgment

The author wishes to thank the Computer Incident Response Centre Luxembourg for providing the data necessary for the performance of the case study presented in this work.

References

[1] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to Cyber Threat Information Sharing," National Institute of Standards and Technology, NIST SP 800-150, Oct. 2016. doi: 10.6028/NIST.SP.800-150.

[2] R. Brown and R. M. Lee, "2021 SANS Cyber Threat Intelligence (CTI) Survey," p. 20, 2021.

[3] "Introduction · User guide of MISP intelligence sharing platform." https://www.circl.lu/doc/misp/ (accessed Nov. 03, 2021).

[4] "MISP Communities and MISP Feeds." https://www.misp-project.org/communities/ (accessed Jan. 31, 2022).

[5] S. Caltagirone, A. Pendergast, and C. Betz, "The Diamond Model of Intrusion Analysis," US Department of Defense, Technical Report OMB No. 0704-0188, May 2013.

[6] "Computer Incident Response Center Luxembourg (CIRCL)." https://misppriv.circl.lu/users/login (accessed Nov. 23, 2021).

[7] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," Comput. Secur., vol. 95, p. 101867, 2020, doi: https://doi.org/10.1016/j.cose.2020.101867.

[8] M. S. Ansari, V. Bartos, and B. Lee, "Shallow and Deep Learning Approaches for Network Intrusion Alert Prediction," Procedia Comput. Sci., vol. 171, pp. 644–653, 2020, doi: https://doi.org/10.1016/j.procs.2020.04.070.

[9] P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Skiadopoulos, and C. Tryfonopoulos, "inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence," Electronics, vol. 10, no. 7, 2021, doi: 10.3390/electronics10070818.

[10] A. Mohasseb, B. Aziz, J. Jung, and J. Lee, "Cyber security incidents analysis and classification in a case study of Korean enterprises," Knowl. Inf. Syst., vol. 62, no. 7, pp. 2917–2935, Jul. 2020, doi: 10.1007/s10115-020-01452-5.

[11] M. van Haastrecht et al., "A Shared Cyber Threat Intelligence Solution for SMEs," Electronics, vol. 10, no. 23, p. 2913, Nov. 2021, doi: 10.3390/electronics10232913.

[12] S. Dutta, N. Rastogi, D. Yee, C. Gu, and Q. Ma, "Knowledge Graph for Malware Threat Intelligence," p. 6.

[13] F. Böhm, F. Menges, and G. Pernul, "Graph-based visual analytics for cyber threat intelligence," Cybersecurity, vol. 1, no. 1, p. 16, Dec. 2018, doi: 10.1186/s42400-018-0017-4.

[14] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, and L. J. García Villalba, "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence," Future Internet, vol. 12, no. 6, p. 108, Jun. 2020, doi: 10.3390/fi12060108.

[15] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," in 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Sep. 2017, pp. 91–98. doi: 10.1109/EISIC.2017.20.

[16] D. Schlette, F. Böhm, M. Caselli, and G. Pernul, "Measuring and visualizing cyber threat intelligence quality," Int. J. Inf. Secur., vol. 20, no. 1, pp. 21–38, Feb. 2021, doi: 10.1007/s10207-020-00490-y.

[17] H. Griffioen, T. Booij, and C. Doerr, "Quality Evaluation of Cyber Threat

Intelligence Feeds," in Applied Cryptography and Network Security, vol. 12147, M. Conti, J. Zhou, E. Casalicchio, and A. Spognardi, Eds. Cham: Springer International Publishing, 2020, pp. 277–296. doi: 10.1007/978-3-030-57878-7_14.

[18] A. Albakri, E. Boiten, and R. Smith, "Risk Assessment of Sharing Cyber Threat Intelligence," in Computer Security, vol. 12580, I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, and A. Sasse, Eds. Cham: Springer International Publishing, 2020, pp. 92–113. doi: 10.1007/978-3-030-66504-3_6.

[19] T. D. Wagner, E. Palomar, K. Mahbub, and A. E. Abdallah, "A Novel Trust Taxonomy for Shared Cyber Threat Intelligence," Secur. Commun. Netw., vol. 2018, pp. 1–11, Jun. 2018, doi: 10.1155/2018/9634507.

[20] A. Dulaunoy, G. Wagener, A. Iklody, S. Mokaddem, and C. Wagner, "An Indicator Scoring Method for MISP Platforms," Trondheim, Norway, p. 15.

[21] A. Iklody, G. Wagener, A. Dulaunoy, S. Mokaddem, and C. Wagner, "Decaying Indicators of Compromise," ArXiv180311052 Cs, Mar. 2018, Accessed: Jan. 14, 2022. (Online). Available: http://arxiv.org/abs/1803.11052

[22] M. Faiella, G. Gonzalez-Granadillo, I. Medeiros, R. Azevedo, and S. Gonzalez-Zarzosa, "Enriching Threat Intelligence Platforms Capabilities," in Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, Prague, Czech Republic, 2019, pp. 37–48. doi: 10.5220/0007830400370048.

[23] K. Faust and S. Wasserman, Social Network Analysis: Methods and Applications. Cambridge University Press, 1994.

[24] K. M. Carley, J. Pfeffer, J. Reminga, J. Storrick, and D. Columbus, "ORA User's Guide 2013," Institute for Software Research School of Computer Science Carnegie Mellon University, Pittsburgh, PA 15213, CMU-ISR-13-108, Jun. 2013.

[25] K. M. Carley and J. Reminga, "ORA: Organization Risk Analyzer*," Carnegie Mellon University School of Computer Science, Institute for Software Research International, CASOS Technical Report CMU-ISRI-04-106, Jul. 2004.

[26] Borgatti SP, "The key player problem," presented at the Dynamic social network modeling and analysis: workshop summary and papers, 2003.

[27] Wouter De Nooy, AndrejA Mrvar, and Vladimir Batagelj, Exploratory Network Analysis with Pajek, 2nd ed. Cambridge University Press, 2011.

[28] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "NIST SP 800-61, Computer Security Incident Handling Guide, Rev.2-SP800-61.pdf." Aug. 2012. Accessed: Apr. 19, 2018. (Online). Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[29] "Automation and MISP API · User guide of MISP intelligence sharing platform." https://www.circl.lu/doc/misp/automation/ (accessed Nov. 23, 2021).

[30] PyMISP - Python Library to access MISP. MISP Project, 2021. Accessed: Nov. 23, 2021. (Online). Available: https://github.com/MISP/PyMISP

[31] "Projects - *ORA-LITE | CASOS." http://www.casos.cs.cmu.edu/projects/ora/ (accessed Nov. 23, 2021).

[32] "Categories and Types · User guide of MISP intelligence sharing platform." https://www.circl.lu/doc/misp/categories-and-types/#types (accessed Nov. 23, 2021).