Citation: P. Radoglou-Grammatikis, E. Kioseoglou, D. Asimopoulos, M. Slavvas, I. Nanos, T. Lagkas, V. Argyriou, K. E. Psannis, S. Goudos and P. Sarigiannidis, "Surveying Cyber Threat Intelligence and Collaboration: A Concise Analysis of Current Landscape and Trends," 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Naples, Italy, 2023, pp. 309-314, doi: 10.1109/CloudCom59040.2023.00057.

Surveying Cyber Threat Intelligence and Collaboration: A Concise Analysis of Current Landscape and Trends

Panagiotis Radoglou-Grammatikis[†‡], Elisavet Kioseoglou[†], Dimitrios Asimopoulos[§], Miltiadis Siavvas[¶],
Ioannis Nanos[‖], Thomas Lagkas[**], Vasileios Argyriou[††], Konstantinos E. Psannis[‡‡],
Sotirios Goudos[x] and Panagiotis Sarigiannidis[†]

***Abstract*—The evolution of cyberattacks has been significantly impacted by the rise of Artificial Intelligence (AI). In particular, AI-driven attacks leverage Machine Learning (ML) and Deep Learning (DL) methods to automate tasks like identifying vulnerabilities, crafting convincing phishing emails, and evading conventional security measures. These cyberattacks can adapt in real time, making them more elusive and challenging to detect. Furthermore, AI has enabled the development of AI-powered malware that can learn and evolve, making it even more dangerous. As AI continues to evolve, both attackers and defenders are engaged in a relentless arms race, with cybersecurity professionals striving to harness AI for threat detection and response while cybercriminals seek to exploit AI's capabilities for their malicious purposes. This ongoing battle underscores the need for proactive and adaptive cybersecurity strategies to mitigate the evolving threats posed by AI-driven cyberattacks. Based on the aforementioned remarks, it is evident that efficient and adaptable countermeasures are necessary. In this paper, we focus our attention on Cyber Threat Intelligence (CTI) mechanisms. CTI is the process of collecting, analysing, and sharing information about potential cybersecurity threats to help organisations proactively defend against cyberattacks. In particular, after providing an overview of the CTI use cases, a brief analysis of existing solutions follows, highlighting the current trends and directions for future work in this research field.**

***Index Terms*—Cybersecurity, Cyber Threat Intelligence, Information Sharing, Proactive Defense, Survey**

I. Introduction

Cyberthreats are continuously evolving, taking full advantage of emerging technologies, such as Artificial Intelligence (AI). Ransomware attacks remain a major concern, becoming more sophisticated and targeting not only individuals but also critical infrastructure and supply chains. Nation-state actors continue to engage in cyber espionage and disruptive attacks, often focusing on political, economic, or technological objectives. The expansion of the Internet of Things (IoT) has also introduced vulnerabilities, leading to an increase in attacks targeting interconnected devices. In addition, social engineering techniques like phishing and spear phishing are becoming more personalised and convincing, exploiting human psychology to gain unauthorised access to sensitive information. The rise of AI and machine learning is both a potential solution and a concern, as these technologies are leveraged by both attackers and defenders to optimise their strategies. As a result, a comprehensive and adaptable cybersecurity approach is crucial to mitigate these evolving threats.

Based on the aforementioned remarks, Cyber Threat Intelligence (CTI) refers to the information collected, analysed, and disseminated about potential and current cybersecurity threats and vulnerabilities. It is a proactive approach to cybersecurity that involves gathering data from various sources, such as security research, hacking forums, malware samples, and network monitoring, to understand and predict potential cyberthreats. CTI encompasses a wide range of data, including indicators of compromise (IoCs) such as IP addresses, domain names, hashes of malicious files, patterns of attack behaviours, and tactics, techniques, and procedures (TTPs) used by threat actors. This information is then analysed to identify patterns, trends, and potential risks. In this paper, we provide a brief

[*] *This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070450 (AI4CYBER). Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.*

[†] P. Radoglou-Grammatikis, E. Kioseoglou and P. Sarigiannidis are with the Department of Electrical and Computer Engineering, University of Western Macedonia, Campus ZEP Kozani, 50100, Kozani, Greece - E-Mail: {pradoglou, ekioseoglou, psarigiannidis}@uowm.gr

[‡] P. Radoglou-Grammatikis is also with K3Y Ltd, William Gladstone 31,1000 Sofia, Bulgaria - E-Mail: pradoglou@k3y.bg

[§] D. Asimopoulos is with MetaMind Innovations P.C., Kila, 50100 Kozani, Greece- E-Mail: dasimopoulos@metamind.gr

[¶] M. Siavvas is with Centre for Research and Technology Hellas/Information Technologies Institute, Charilaou-Thermi Rd, Thermi, 57001, Thessaloniki, Greece - E-Mail: siavvasm@iti.gr

[‖] I. Nanos is with Sidroco Holdings Ltd, Petraki Giallourou 22, Office 11, 1077 Nicosia, Cyprus - E-Mail: inanos@sidroco.com

[**] T. Lagkas is with the Department of Computer Science, International Hellenic University, Kavala Campus, 65404, Kavala, Greece - E-Mail: tlagkas@cs.ihu.gr

[††] V. Argyriou is with the Department of Networks and Digital Media, Kingston University London, Penrhyn Road, Kingston upon Thames, Surrey KT1 2EE, UK - E-Mail: vasileios.argyriou@kingston.ac.uk

[‡‡] K. E. Psannis is with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, 156 Egnatia Street, Thessaloniki Greece - E-Mail: kpsannis@uom.edu.gr

[x] S. Goudos is with the School of Physics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece - E-Mail: sgoudo@physics.auth.gr

analysis of CTI solutions, highlighting the current trends and directions for future research works.

The rest of this paper is organised as follows. Section II summarises the use cases of CTI. Section III describes existing works in this field. Next, section IV summarises trends and research directions. Finally, section V concludes this paper.

II. Use Cases of Cyber Threat Intelligence

As presented in Fig. 1, CTIS is composed of five main stages: (a) Planning and Direction, (b) Collection, (c) Analysis, (d) Production and (e) Dissemination and Feedback. Commonly, organisations adopt CTI mechanisms to:

- **Enhance Proactive Defense**: By staying ahead of potential threats, organisations can implement measures to detect and prevent attacks before they occur.
- **Incident Response**: CTI helps organisations respond more effectively to security incidents by providing information about the nature and scope of the threat.
- **Patch and Vulnerability Management**: Understanding emerging threats can help prioritise which vulnerabilities to address first.
- **Risk Assessment**: CTI assists in evaluating the potential impact of various threats on an organisation's systems and data.
- **Cybersecurity Strategy**: It aids in developing a strategic approach to cybersecurity, focusing resources on the most relevant and likely threats.
- **Sharing Insights**: Organisations can share CTI within their industry or sector, contributing to a more collaborative approach to cybersecurity.
- **Decision Making**: CTI provides actionable insights that aid in making informed decisions about security measures and investments.
- **Understanding Attackers**: By studying threat intelligence, organisations can gain insights into the motivations, techniques, and intentions of various threat actors.

III. Analysis of Existing Works

In [1], M. Mena and B. Yang present an implementation of the blockchain protocol in a home network with IoT devices with the aim of providing a decentralised system that shares CTI between service providers and consumers. As a proof of concept, the authors designed a network simulation environment with the following components: an `Ethereum` blockchain network, a `GNS3` server and another server that acts as a gateway to the rest of the network. `Bonesi`, an open-source tool that simulates botnet behaviour, was used to simulate a Distributed Denial of Service (DDoS) attack. The analysis was focused on three different metrics: network performance, Ethereum network performance and network security capabilities. There were two scenarios to test the framework. One tested network performance without the attacks to create a baseline for normal network activity, and the other tested the Ethereum network performance under DDoS attacks. A comparison was made between two groups, one without blockchain instances (control group) and another with blockchain instances (experimental group), during the streaming of a `Youtube` performance. The DDoS attack triggered a blockchain transaction through `Snort`, which was then broadcast to the rest of the network, which in turn automatically stopped the attack. The impact on the response time for the home networks was a small delay of 2%, and connection speed was better in the control group. There was also a creation of a blockchain-based CTI report that took only 55 seconds to reach the other blockchain nodes when the attack was detected.

In [2], the authors aim to address the rare use of CTI by Small and Medium-sized Enterprises (SMEs) by conducting a systematic review of current approaches in sharing CTI and presenting a prototype that uses a `Malware Information Sharing Platform (MISP)`. The prototype is particularly useful for less digitally mature SMEs.The literature review was conducted using a combination of an active learning phase and a backward snowballing phase. It was determined that structured open-source intelligence sources and, more specifically, the `VERIS Community Database (VCDB)` are more suitable for the SME's needs. However, these sources need to be complemented by the ENISA rankings. The proposed solution uses `MISP` in conjunction with the `GEIGER` application. The CERT-RO CTI feed in `MISP` provides GEIGER with processed `MISP` events via its Application Programming Interface (API). Then, a process of prioritising the CTI threats with the help of `VCDB` data for digitally dependent SMEs,digitally-based SMEs and digital enablers takes place. This classifies threats depending on which of them are related to the SME users. The threat prioritisation is done periodically with the help of an exponential smoothing algorithm. The change in the threat prioritisation and in the relevant countermeasures that need to be implemented does not take into account internal data from SMEs and eliminates the need for a security expert.

Following the previous paper, in [3], the authors present an overview of `MISP`. First, it shows the data format of the events. Then, the different sharing models are analysed. The concept of taxonomies, with the triple tag structure, is also analysed. The next section is about the synchronisation protocol. There are three mechanisms present in the protocol, namely, the push and pull mechanism and the cherry-pick technique. All three are analysed in great detail. Finally, there are also statistics about the use of `MISP`. A distribution of events per month from 2013 to 2016 is presented with a peak of published events in 2015 and 2016.

In [4], the authors present `LUUNU`, a blockchain-based, `MISP`, Model Cards and Federated Learning (FL) enabled CTI sharing platform. This platform provides transparency and credibility to the CTI sharing by storing CTI data on the `MISP` storage in the form of Model Card objects. The anonymity of the organisations that report these data is ensured with the use of a Self-sovereign identity-enabled mobile wallet. The `LUUNU` architecture has five layers: the first is the Stakeholder Layer, which contains incident reporters/viewers and admins. The second is the Smart Contract Layer. This is where the

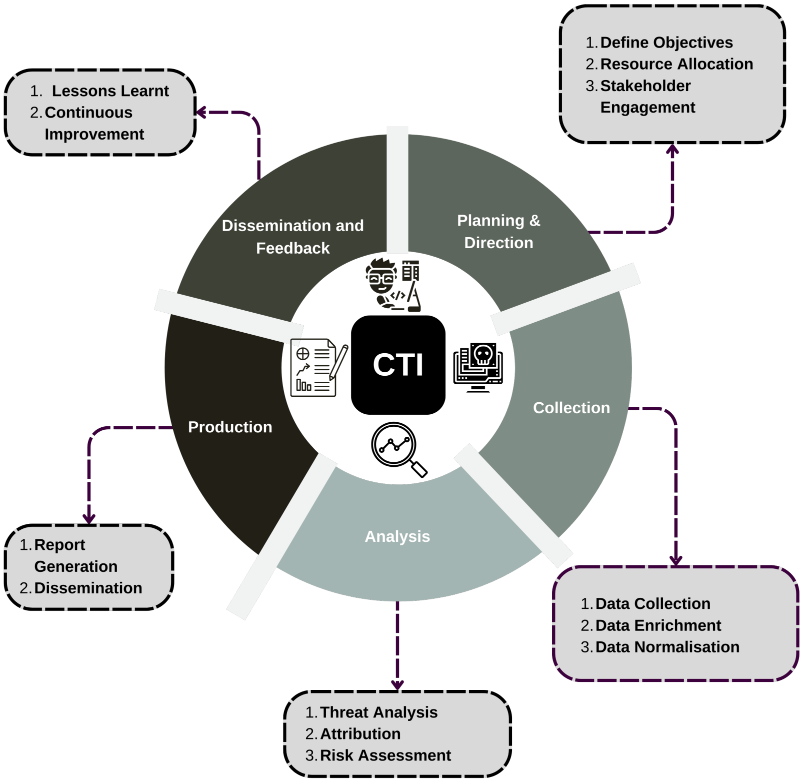

Fig. 1: Lifecycle of Cyber Threat Intelligence

user's digital identity proofs are stored, along with CTI, FL and notification contracts. Another service is the encoding of CTI data and ML information into Model Card objects. The Blockchain Storage Layer contains the nodes of each organisation. The `MISP` Layer stores the Model Card objects and allows the blockchain smart contracts to interact with it via its API. The fifth layer, called the Data Analytic Layer, provides the FL service. That is a service that uses FL models to detect cyberattacks. The functionality of `LUUNU` is to register the organisation on the platform as a blockchain node so that they can report incidents, which are then encoded into the Model Card and saved in the `MISP` database. The `LUUNU` platform is implemented on top of the `Rahasak` blockchain. The FL functions originate from `Pytorch` and `Pysyft`. The Model Card service is built with `TensorFlow Model Card` Toolkit, and the operation handling of the blockchain is managed with `Apache Kafka`.

In [5], the authors present the Enriched Threat Intelligence Platform (ETIP), whose functionality is to collect, relate and aggregate OSINT data and data from the monitored infrastructure. The OSINT data are stored in the `MISP` database, and the infrastructure data are stored in the Heuristic Component database. The `MISP` platform was selected based on criteria such as the integration with Security Information and Event Management (SIEM) and Intrusion Detection Tool (IDS) tools because the goal is to feed the enriched data to an IDS or an SIEM. The ETIP architecture has two modules: the Composed IoC module, which collects IoCs and interrelates them, making them more enriched and the Context-Aware Intelligence Sharing module, which contains a `MISP` instance and a heuristic component. The heuristic component receives data from `MISP`, and its purpose is to produce a Threat Score(TS) for the received data. To compute the TS, the Weighted Mean(WM) function was used, and it is calculated by summing the individual heuristic values times and the individual weight factor. The weighting criteria of this factor are relevance, accuracy, variety and timeliness. If there is a match with the `MISP` attributes, a score is computed according to these criteria. Finally, depending on whether the TS score is high enough, the enriched IoCs will help analysts determine the risk score on tools such as IDS and SIEM.

The goal of this paper [6] is to describe the data interaction methods used to evaluate the information exchanged in `MISP` and to propose a scoring technique for decaying information. A feature of `MISP` called taxonomies is used to evaluate attributes. Taxonomies are a classification method with its own vocabulary. The taxonomies are part of the scoring model through tagging. A data interaction method in `MISP` is the sightings, which provide information about the validity of an attribute, categorising it into priority or decaying attributes. Each attribute has a decaying function. There are also some parameters that need to be considered for its overall score: the base score of an attribute, which is calculated with the help of its weighted applied tags and the source confidence, the difference in time between the current time and the time of the attribute's last sighting and the decay rate or the speed at which the attribute's score decreases. The two parameters of the model are the end time of an attribute and the variable decay rate. Two models are considered for calculating the score, one with exponential digression and another one with a polynomial function. The polynomial function was more advantageous.

Security playbooks present the necessary steps and processes to mitigate cyberattacks, or they can also automate security functions in an efficient way. In [7], the authors introduce a metadata template to integrate security playbooks and, more specifically, the `Collaborative Automated Course of Action Operations(CACAO)` playbook into the `MISP` threat intelligence platform and a cyber threat intelligence ontology named Threat Actor Context ontology(TAC). A `CACAO` playbook can consist of a series of actions for cyberdefense functions such as threat hunting or attack emulation. It is represented in JSON format and can be digitally signed. To integrate the `CACAO` playbook into shareable threat intelligence, a metadata template was created to map the metadata of `CACAO`. The template contains elements such as `id`, `description`, `impact` and `severity`. The `MISP` platform allows the creation of objects, which are templates that represent complex structures of attributes that share a contextual bond. The object named `course of action` describes the measures of responding to an attack. Based on that, the proposed template elements now become the attributes of a new object, called `MISP` Security Playbook object, that can also be linked to other objects, such as attack emulation objects. Finally, the TAC ontology, which is based on the STIX 2.1 standard, a standard that also includes `course of action`, can be converted into an ontological representation. This representation is also based on the proposed metadata template.

Because IoCs may not always be as effective in identifying an attack and their value may decay with time, in [8], the authors proposed a solution that shares ML models for threat detection. To protect these models, they enforced a cryptographic scheme so that only authorised parties in the community have access to them. The sharing of ML models is happening through a `MISP` object template. The goal is to investigate a variety of ML models against a DDoS scenario to determine which one provides a good classification of malicious and benign traffic. The first model to be tested was the Decision Tree Classifier with a depth of 2. The classification was almost perfect, but when tested against a scenario where the attacker sends a modified HyperText Transfer Protocol (HTTP) payload, it misclassified the malicious traffic as benign. Next, a Random Forest Classifier with 20 decision trees was tested. The performance was better than the previous model, but the modified HTTP payload was still misclassified. The third model was a 'OneClassSVM' where the attack is considered an outlier. The performance was not as good as the other two, but it correctly classified the modified HTTP responses as malicious. The fourth model was a Multi-Layer Perceptron (MLP) binary classifier. The classifier not only had excellent performance, but it also identified the modified HTTP payload correctly as malicious. This model could be a good contribution to the threat intelligence community. Finally, a set of autoencoders was trained in an unsupervised way on benign traffic. The modified HTTP payloads were correctly classified as malicious. Next, the authors defined a taxonomy for adversarial ML threats. Finally, a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme was used for the encryption of the data on the `MISP` database.

In [9], the authors present an investigation of available formats, languages, and sources of threat feeds along with their suitability for several use cases related to security. The categories of the examined CTI sources were internally sourced, such as system logs and events or network events, externally sourced observables or feeds and open-source intelligence. The CTI format and languages investigation mainly focused on CTI standards specifically used for CTI representation, such as `STIX`, `CybOX` and `CVRF`, application-specific or vendor-specific formats such as `MISP`, commonly used standards that were not initially intended for CTI sharing and legacy formats referred in the literature but no longer in use. The analysis that the authors provide is focused on the CTI source feeds, formats and languages. First, they examined the CTI source originality, whether they are original or retransmitted. Then, they presented the range of CTI types (like IP, URL, domain) in the CTI source feeds. Based on that range, they defined rich CTI as CTI with more than two types in the feed and sparse CTI. It was found that only half of the examined feeds contained rich CTI. Moreover, various CTI formats and languages were searched for efficiency regarding different use cases. These use cases could be Email Blocklists, Spam filters, Network IDS (NIDS) or malware analysis.

The goal of this paper [10] is to capture the changes in a threat actor's behaviour and the polymorphism in their actions over time. The tendency of some threat actors to use obfuscation techniques prevents security analysts from associating an event with a particular threat group. To resolve this issue, the authors used a proof-of-concept ontological representation of Threat Actor Library (TAL) to identify threat actor types from CTI objects. TAL is a threat agent library, and it is used for risk assessment. It enumerates twenty-one threat actor types, such as government spies and radical activists. Several threat actor knowledge bases are presented to show how they could benefit from a more structured and automatic way to query them. For example, the `MISP` Threat Actor Cluster uses the term espionage for both an incident type and a motive, which creates ambiguity. The domain ontology for threat actor profiling created by the authors refined TAL to remove ambiguities that may occur. As an example, the object property `hasDefiningMotivation` on the ontology refers to the object of an attack that was influenced by motivation. It could also be `hasPersonalMotivation`. A threat actor type object could be a `HostileThreatActorType` or a `NonHostileThreatActorType`. Finally, the `Lazarus Group` case is presented to evaluate how a polymorphic group can be identified in an automatic way using deductive reasoning. Being polymorphic, it has exhibited behaviour that could be categorised as organised cybercrime, hacktivists or cyber vandals. Examining some attacks, such as the DarkSeoul attack, and characterising them using the proposed domain ontology, the Lazarus Group was revealed to be the one behind them.

The goal of this paper [11] is to determine the criteria that evaluate different TIPs. This was achieved by conducting a literature review to gather studies related to threat intelligence sharing (TIS) and TISPs. Out of the 40 collected papers with the greatest relevance to the study, a set of 62 criteria was extracted. The 62 criteria were grouped into two main categories: functional and non-functional criteria. The functional criteria contain the Phases of TIS, which are Collection, Aggregation, Analysis and Dissemination of TI. Each one of them contains subphases with Available Functions and Degrees of Automation existing in every phase. The functional criteria also contain Cross-Phase Support, which consists of Information Security, Data Privacy, Data Quality, Trust, Import and Export, Collaboration(which contains Anonymity Levels), Reporting and Additional Functions. The non-functional criteria contain Architecture and Interfaces (Type of Platform, Architecture, APIs, User Interface), Content and Standardization (Data Origin, Threat Intelligence and Standardization), Provider and Users and Usage Fees, License and Distribution (Usage Fees, License, Geographical Focus and Sectoral Focus). All these criteria are part of the evaluation framework, which was then used to test ten TISPs, with three of them included and analysed in the paper. These were MISP, OTX and ThreatQ.Some similarities derived from the framework were that all of them provide collection, aggregation and dissemination of TI, all of them use the STIX, TAXII and OpenIOC standards and all of them process external data sources apart from internal. On the other hand, not all of them have the same data quality and reporting functions, as only OTX offers comprehensive reporting and individualisation. Regarding the content, MISP focuses on IoCs while the other two on TTPs.

In [12], T. Schaberreiter et al. introduce a framework to evaluate trust in the quality of CTI sources. The approach proposed here is based on a closed-world assumption. This means that information provided by a specific set of CTI sources is all the information that exists in the world of CTI. The advantage of the closed world assumption is that every time a new CTI is shared with the world, the evaluation parameters of trust can be re-evaluated. There are two main aspects in this framework: the first one describes a set of quantitative evaluation parameters and the way they are computed. These are Extensiveness, Maintenance, False Positives, Verifiability, Intelligence, Interoperability, Compliance, Timeliness, Completeness and Similarity. The second main aspect is the derivation of a trust-based quality indicator to assess the quality of each source that exists in the worldview. The trust indicator(TI) of each intelligence source in the worldview depends on the weighted sum of the respective parameters. It also depends on the interval t at which the trust indicator is recalculated. The selection of this time interval is dependent on the rate at which the parameters change values and the specific needs of the use case. The Extensiveness quality indicator is calculated as a computational example. The data sample contains three STIX messages from MISP.

In [13], the authors propose a platform for ORchestrated Information SHaring and Awareness(ORISHA) which is backed by a distributed Threat Intelligence Platform (TIP). In this case, the TIP is a network of several MISP instances. The benefits of ORISHA are the improvement of the detection accuracy for the Threat Detection Systems(TDS) and the sharing of reliable threat detection information among organisations with different TDSs. The ORISHA platform consists of three parts: the distributed TIP, responsible for storing data and delivering them to the other components/other MISP instances. The TDS layer includes ensemble-based IDS (EBIDS), an ML-based intrusion detection method for classifying network flows as attack-related or normal. The cooperation and active learning among the TDSs with the goal of improving their detection capabilities is very similar to a Query-By-Committee (QbC) strategy. Let's assume that TDS1 detects an anomaly in network traffic. This triggers the creation of a MISP security event. When the event is distributed in the TIP, a second IDS (TDS2) analyses it. If the classification is different than the one TDS1 gave, the event is returned to TDS1, which uses the re-evaluated event for its training set. In the opposite case, the event now has two consensus labels, and it is validated by an expert and later retrieved by other TDSs.To evaluate the platform, a series of experiments are conducted, where the different entities in the TIP share anomalies detected by their own TDSs. To measure the performance of the classification models, AUC, AUC-PR and F-measure were used as metrics. The experimental results showed an improvement in terms of accuracy of detection due to the implementation of the ORISHA.

In [14], K. Rantos et al. propose a layered model to address the interoperability challenges that organisations face when exchanging CTII. The four interoperability layers that represent the security issues that organisations have to confront when CTII is about to be shared are the following: legal interoperability, which covers legal restrictions and the impact on data privacy while sharing, policy and procedures, which are formal statements of the organisations objectives, along with instructions to achieve them, semantic and syntactic interoperability, that concerns the different data types and standards of CTII, such as STIX, MISP, CAPEC, MAEC, IODEFv2 and IDMEF and finally technical interoperability that involves protocols proposed for the transmission of CTII and the protection of information during sharing. The authors conducted an analysis of various CTII sources with respect to interoperability and focused on semantic and syntactic standards as well as policies. The analysis showed that 50% of the sources chose the JSON format, while 59% and 31% chose plaintext and CSV, respectively. Only a small percentage opted for CTII-oriented standards such as MISP. The majority of the sources provide information in generic formats only and not CTII-related ones. As far as policies are concerned, only 15 out of 32 sources provide open and public information.

In [15], the authors present an evaluation methodology for both threat intelligence standards and threat intelligence platforms. Because of the overwhelming number of results found in the literature, the standards and platforms that are unable to cover two or more stages of the threat intelligence production process flow were excluded. Then, the most popular free and open-source standards and platforms were selected. To evaluate them, a holistic architecture model was developed based on the 5W3H (what, who, why, when, where, how, how much and how long) method. For example, the field describes the way the cyberattack took place and the related techniques. Four additional entities, namely Threat, Incident, Threat Actor and Defense, are added to the architecture. Based on the popularity, the chosen standards were `STIX`, `TAXII`, `IODEF`, `RID`, `CybOX` and `OpenIOC`.Based on the holistic architecture and applicability in different use cases, `STIX`, combined with `TAXII`, was the best choice. In the same manner, the platforms selected for analysis were `MISP`, `CIF`, `CRITs`, `OpenCTI` and `Anomali STAXX`. Based on the holistic architecture and some processual criteria, such as collection process, correlation and classification mechanisms, visualisation and integration with other security tools and platforms, `MISP` and `OpenCTI` were the two most complete platforms.

IV. Trends and Research Directions

Based on the analysis of the previous works, the following trends and research directions are identified:

Automation and AI: The use of automation and AI in CTI has been growing. These technologies can help process and analyse vast amounts of data more quickly and accurately, enabling faster threat detection and response.

Contextual Threat Intelligence: Contextualising CTI by considering factors such as industry-specific risks, geopolitical events, and an organisation's own infrastructure enhances the relevance and effectiveness of threat intelligence.

Dark Web Monitoring: Monitoring underground forums, marketplaces, and other parts of the dark web has become crucial for understanding cybercriminal activities, sharing intelligence, and staying ahead of emerging threats.

Threat Actor Attribution: While attribution remains challenging, there is growing interest in accurately attributing cyberattacks to specific threat actors, groups, or nation-states. This can help organisations understand motives and respond effectively.

Regulatory Compliance: With the introduction of data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), threat intelligence is being used to ensure compliance and demonstrate due diligence in protecting sensitive data.

Machine-Readable Threat Intelligence (MRTI): The adoption of standardised formats for threat intelligence data enables easier sharing, integration, and automation across security tools and platforms.

Edge and Remote Workforce Focus: With the shift to edge services and remote work, CTI is adapting to address the unique security challenges associated with these environments.

V. Conclusions

The continuous evolution of cyberthreats requires the presence of adaptable and proactive countermeasures. In this paper, we focus on CTI mechanisms, investigating existing solutions in this field. Based on this analysis, trends and research directions in this field are identified.

References

[1] D. Mendez Mena and B. Yang, "Decentralized actionable cyber threat intelligence for networks and the internet of things," *IoT*, vol. 2, no. 1, pp. 1–16, 2020.

[2] M. Van Haastrecht, G. Golpur, G. Tzismadia, R. Kab, C. Priboi, D. David, A. Răcătăian, L. Baumgartner, S. Fricker, J. F. Ruiz *et al.*, "A shared cyber threat intelligence solution for smes," *Electronics*, vol. 10, no. 23, p. 2913, 2021.

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

[4] E. Bandara, S. Shetty, R. Mukkamala, A. Rahaman, and X. Liang, "Luunu—blockchain, misp, model cards and federated learning enabled cyber threat intelligence sharing platform," in *2022 Annual Modeling and Simulation Conference (ANNSIM)*. San Diego, CA, USA: IEEE, 2022, pp. 235–245.

[5] M. Faiella, G. G. Granadillo, I. Medeiros, R. Azevedo, and S. G. Zarzosa, "Enriching threat intelligence platforms capabilities." in *ICETE (2)*, 2019, pp. 37–48.

[6] S. Mokaddem, G. Wagener, A. Dulaunoy, and A. Iklody, "Taxonomy driven indicator scoring in misp threat intelligence platforms," *arXiv preprint arXiv:1902.03914*, 2019.

[7] V. Mavroeidis, P. Eis, M. Zadnik, M. Caselli, and B. Jordan, "On the integration of course of action playbooks into shareable cyber threat intelligence," in *2021 IEEE International Conference On Big Data (Big Data)*. Orlando, FL, USA: IEEE, 2021, pp. 2104–2108.

[8] D. Preuveneers and W. Joosen, "Sharing machine learning models as indicators of compromise for cyber threat intelligence," *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 140–163, 2021.

[9] A. Ramsdale, S. Shiaeles, and N. Kolokotronis, "A comparative analysis of cyber-threat intelligence sources, formats and languages," *Electronics*, vol. 9, no. 5, p. 824, 2020.

[10] V. Mavroeidis, R. Hohimer, T. Casey, and A. Jesang, "Threat actor type inference and characterization within cyber threat intelligence," in *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE, 2021, pp. 327–352.

[11] S. Bauer, D. Fischer, C. Sauerwein, S. Latzel, D. Stelzer, and R. Breu, "Towards an evaluation framework for threat intelligence sharing platforms." in *HICSS*, 2020, pp. 1–10.

[12] T. Schaberreiter, V. Kupfersberger, K. Rantos, A. Spyros, A. Papanikolaou, C. Ilioudis, and G. Quirchmayr, "A quantitative evaluation of trust in the quality of cyber threat intelligence sources," in *Proceedings of the 14th international conference on availability, reliability and security*, 2019, pp. 1–10.

[13] M. Guarascio, N. Cassavia, F. S. Pisani, and G. Manco, "Boosting cyber-threat intelligence via collaborative intrusion detection," *Future Generation Computer Systems*, vol. 135, pp. 30–43, 2022.

[14] K. Rantos, A. Spyros, A. Papanikolaou, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability challenges in the cybersecurity information sharing ecosystem," *Computers*, vol. 9, no. 1, p. 18, 2020.

[15] 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, 2020.