Cyber Threat Intelligence; Current Trends And Future Perspectives

Abstract:

Many organizations are continually put in danger by sophisticated and malevolent cyber attacks in today's rapidly developing threat landscape, which is evolving at a rapid rate. Cybercriminals, who are more skilled, more organized, and have more financial resources than in the past. Cyber Threat Intelligence, abbreviated as CTI, has emerged as a popular topic and is now being considered by many organizations as a potential solution to the growing number of cyber attacks. The purpose of this work is to conduct a literature review on the previous research that has been done on CTI. The most fundamental question about what CTI is is investigated through the process of doing a literature study. This is done by contrasting several definitions in order to identify areas of agreement and disagreement. It has been discovered that neither the organization nor the suppliers have a comprehensive grasp of the information that is deemed to be CTI; hence, further study is required in order to define CTI. This article also listed existing CTI products and services, including as threat intelligence data feeds, threat intelligence standards, and tools that are being utilized in CTI. This study outlines four research issues in cyber threat intelligence and assesses contemporary work carried out in each of those areas. These difficulties were determined based on an assessment of the CTI definition, standards, and technologies. When an organization is inundated with a massive amount of threat data, the need for trained threat data analysts who are able to fully utilize CTI and transform the data into actionable information becomes more vital than it has ever been before. The problem of poor data quality is not a recent development; nonetheless, because to the increasing use of CTI, further study in this field is required.

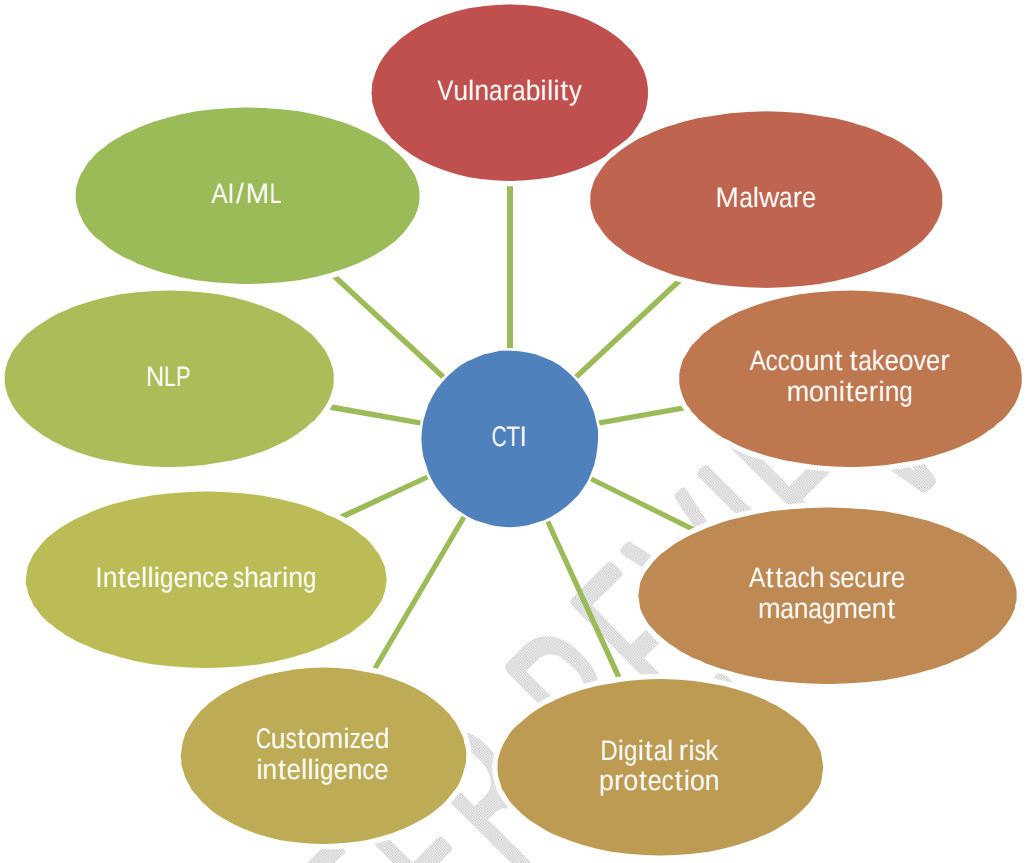
1) Introduction:

There has been an extraordinary growth in the number of cyber attacks, which have progressed and gotten more sophisticated as a result of the introduction of the Internet of things (IoT). In

today's world, adversaries launch attacks on their victims utilizing a diverse arsenal of methods and strategies, with goals that might range from the theft of sensitive information to the destruction of data to the pursuit of financial gain. Understanding the attacker has become both more difficult and more crucial as a result of the fact that this knowledge, once it has been converted into information that can be used, may be applied to the process of automatically adapting network defenses to better defend the network from potential threats [1, 2]. The primary focus of cyber-threat intelligence, also known as CTI, is on an adversary's capabilities, objectives, and goals, as well as the methods by which these may be accomplished. Intelligence is the information and knowledge that is obtained about an enemy by observation and analysis; intelligence is not simply data, but the product of an analysis and it must be actionable to fulfill the demands of contemporary defensive systems that have to deal with and respond to cyber-attacks. Indicators, which are system artifacts or observables connected with an attack, security warnings, incident reports, and threat intelligence, are some examples of CTI. CTI also include any additional pertinent information about recommended (or susceptible) security tool setups [2-4] .

The effective dissemination of CTI is essential to the processes of cyber-threat detection and prevention because it makes it possible to construct multi-layer automated tools with highly developed and efficient defensive capabilities that continuously analyze the vast amounts of heterogeneous CTI related to the tactics, techniques, and procedures (TTPs) of attackers, indicators of ongoing incidents, etc. [5-7]. Standardized and structured representations of CTI are necessary in order to permit a level of interoperability that is satisfactory across the many stakeholders[7]. This is because there are numerous architectures, products, and systems that are being utilised as sources of data for information sharing methods. In light of this, considerable efforts have been made over the course of the past decade to standardize the data formats and exchange protocols related to CTI. These efforts have included recent efforts aimed at promoting the CTI for "things" [8]; the initiative making security measurable (MSM) constitutes the most prominent effort towards improving CTI sharing among the various stakeholders [9, 10].

Fig . 1 Cyber Threat Intelligence technology



1.1.Why Threat Intelligence?

The gathering and analysis of threat intelligence is an essential component of any ecosystem devoted to cyber security. A cyber threat intelligence program, sometimes abbreviated as CTI at times, can do the following [11]:

- Data loss may be avoided if an organization implements a well-structured CTI program that allows for the detection of cyber threats and the prevention of data breaches that result in the release of sensitive information [12].
- Give instructions on how to take precautions for safety: CTI is able to recognize and analyse threats, which allows it to spot patterns that hackers employ and assist enterprises in the implementation of security measures to protect themselves from future assaults [13].
- Notify others around you: Hackers continue to improve their skills every day. Experts in cyber security often discuss the strategies they have observed with other members of their

community in order to build a collective knowledge base that may be used to combat online criminal activity [14].

1.2.Types of Cyber threat Intelligence:

Threat information in the field of cyber security is frequently organized into these three categories: strategic, tactical, and operational. Let's take each of these in turn and look at it:

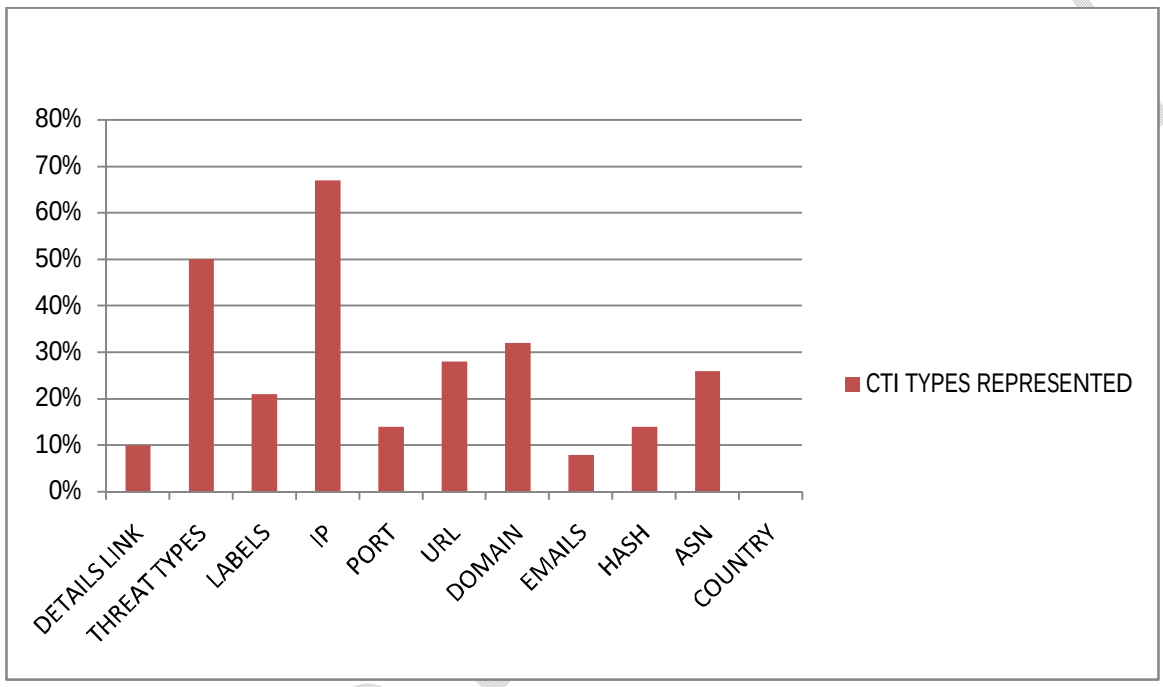


Fig. 2. Representation of CTI types

1.2.1. Information on the strategic threats:

This is often a high-level study that is aimed for audiences that are not technically oriented, such as the board of directors of a firm or organization. It explores larger business decisions that may be impacted by cyber security issues, as well as overarching trends and motives, in this area, and tackles those issues as well. Reports from the media, white papers, and research are examples of open sources that are frequently used as the foundation for strategic threat information. This implies that anybody may access these sources [15].

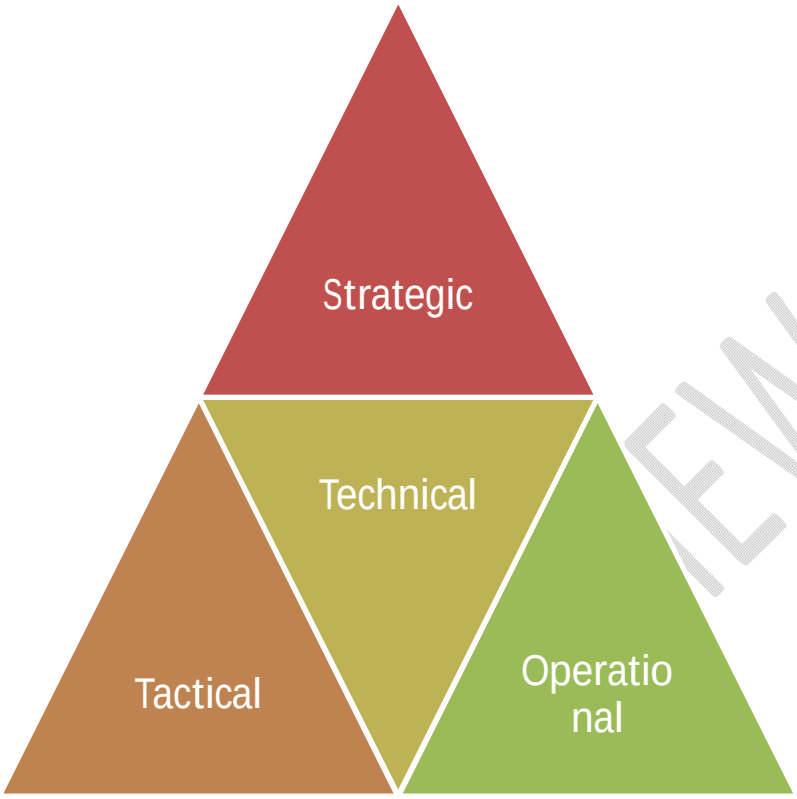
1.2.2. Intelligence on the tactical threats:

This is geared at an audience with a higher level of technical expertise and focuses on the very near future. It detects straightforward indications of compromise, or IOCs, which grants IT teams the ability to hunt down and eradicate certain dangers that are present within a network. IOCs can be things like bad IP addresses, known malicious domain names, unexpected traffic, red flags for logging in, or an increase in the number of file and download requests. The generation of tactical intelligence is typically accomplished via the use of automation since it is the kind of intelligence with the lowest learning curve. As a result of the rapid obsolescence of many IOCs, its typical lifespan is rather brief [16].

1.2.3. Intelligence about operational threats:

There is always a "who," "why," and "how" lurking in the shadows of a cyber assault. By analyzing previous cyber assaults and generating judgments about their intentions, timing, and level of complexity, operational threat intelligence is intended to provide answers to these issues. Intelligence on operational threats has a longer lifespan and demands a greater investment of resources than intelligence on tactical threats. This is due to the fact that cyber attackers are unable to alter their strategies, methods, and procedures (also known as TTPs) as readily as they are able to change their tools, such as a particular strain of malicious software [17].

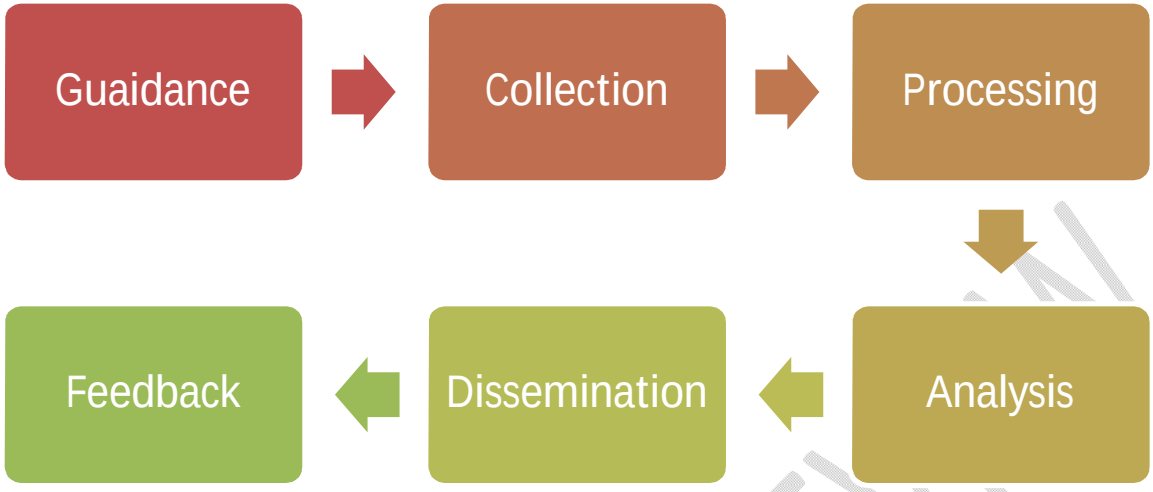
Fig .3 **Intelligence about operational threats**



2) Life Cycle Of Threat Intelligence In Cyberspace

When discussing threat intelligence, professionals in the field of cyber security frequently refer to the idea of a lifecycle. A typical example of a cyber threat lifecycle would involve these stages: direction, collection, processing, analysis, dissemination, and feedback [18].

Fig 4 **Life Cycle Of Threat Intelligence In Cyberspace**



2.1.Phase 1: Providing Guidance

During this stage of the process, the primary focus is on the goal-setting for the threat intelligence program. It may include the following [19]:

- Having a clear understanding of which components of the organisation require protection and maybe developing a priority ranking for those aspects.
- Identifying the types of threat intelligence that are required by the company in order to safeguard assets and react appropriately to attacks.
- Having an understanding of the effects a cyber breach may have on an enterprise.

2.2. Phase 2: The Collection Stage [20]

During this phase, we will be collecting data to support the goals and objectives that were established in the previous phase. Data quantity and quality are both crucial to avoid missing severe threat events or being misled by false positives. In this phase, organisations need to identify their data sources – this might include:

- Metadata from internal networks and security devices
- Threat data feeds from credible cyber security organizations
- Interviews with informed stakeholders

- Open source news sites and blogs

2.3.Phase 3: Processing [21]

All the data which has been collected needs to be turned into a format that the organization can use. Different data collection methods will require various means of processing. For example, data from human interviews may need to be fact-checked and cross-checked against other data.

2.4.Phase 4: Analysis[22]

Once the data has been processed into a usable format, it needs to be analyzed. Analysis is the process of turning information into intelligence that can guide organizational decisions. These decisions might include whether to increase investment in security resources, whether to investigate a particular threat or set of threats, what actions need to be taken to block an immediate threat, what threat intelligence tools are needed, and so on.

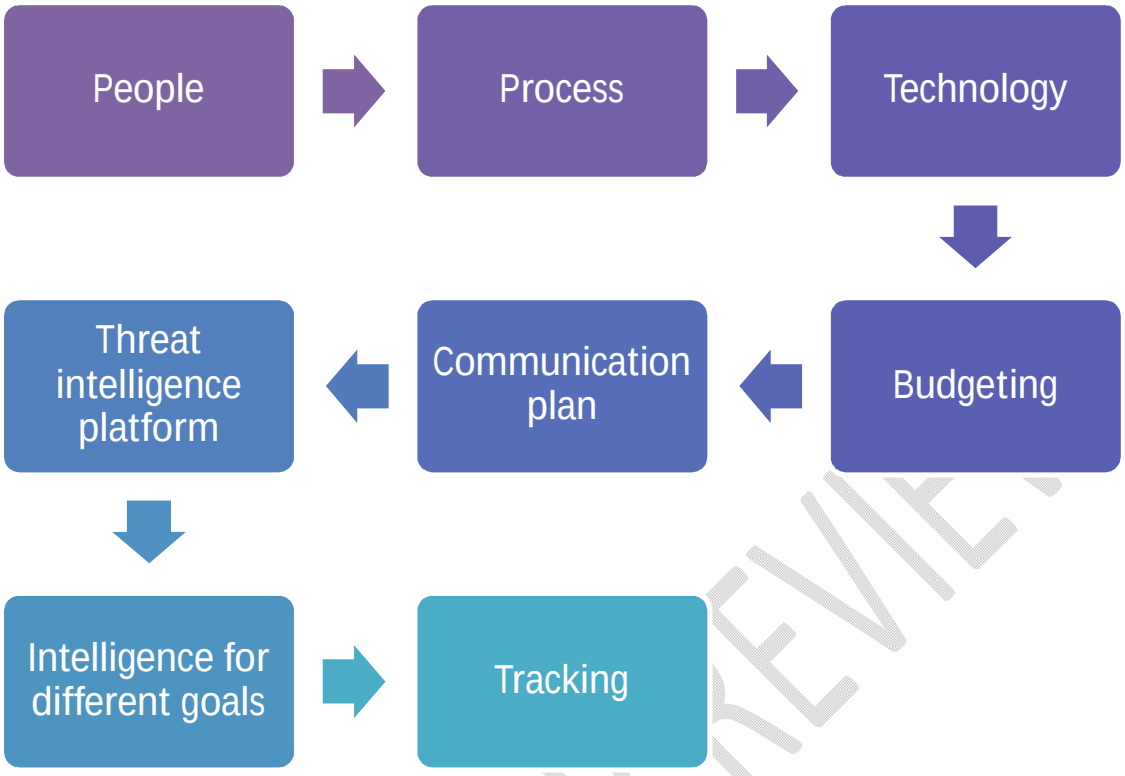
2.5.Phase 5: Dissemination[22]

Once analysis has been carried out, the key recommendations and conclusions need to be circulated to relevant stakeholders within the organization. Different teams within the organization will have different needs. To disseminate intelligence effectively, it's worth asking what intelligence each audience needs, in what format, and how often.

2.6.Phase 6: Feedback [23]

Feedback from stakeholders will help improve the threat intelligence program, ensuring that it reflects the requirements and objectives of each group. The term 'lifecycle' highlights the fact that threat intelligence is not a linear, one-off process. Instead, it's a circular and iterative process that organizations use for continuous improvement.

Fig .5 Feedback phase



1) Sources from CTI

In this part, a number of CTI sources that have been investigated are presented. These CTI sources can be classified as internal, externally supplied observables or feeds, or externally open-source intelligence [24-27]. It is essential to emphasise that the investigation of CTIs was carried out by installing and making use of the tools that were supplied by the manufacturers, in addition to reading and studying the documentation that was provided by those manufacturers and a variety of other internet resources.

2) Need of CTI:

The use of certain security tools allows for the automatic identification and mitigation of certain risks. Human security and IT teams are responsible for dealing with threats that are either more severe or more elusive. These teams need to triage the risks, study how the dangers operate, and figure out how to avoid them [28]. These two use scenarios are made possible by the CTI system:

- The Cyber Threat Intelligence Centre (CTI) offers data to cyber security technologies in order to assist those tools in better understanding the dangers that require attention as well as the strategies, methods, and procedures (TTP) that may be utilized to mitigate such threats [29].
- CTI makes available knowledge that can assist security analysts and IT operations teams in the development of security strategies and the swift implementation of such plans in order to defend networks from serious attacks [30].

Fig .6 Significance of CTI

When companies make investments in cyber threat intelligence, they have access to a database of risks that provides detailed information on a variety of dangers in technical form. The security posture of the organization may be significantly strengthened by granting access to this information to either the security staff or automated systems. CTI stands for computer-to-computer intelligence and is operational intelligence that offers analysts and security systems actionable insights [31, 32]. An efficient CTI system draws a separate line between the gathering of threat data and the gathering of threat intelligence:

The gathering of information about cyber threats results in the production of raw data, which is of little use unless it is analyzed and organized in a manner that can be used for conducting security investigations [33, 34].

The collecting of data is the foundation for cyber threat intelligence, which then gives data that may be utilized to identify, stop, and mitigate attacks. It does this by employing analysis to create operational intelligence from raw security data, which includes information such as the sorts of attacks that may be impending, vulnerabilities in the network, the identification of threat actors, and the underlying cause of each threat [35, 36].

3) Current status of CTI:

Artificial intelligence (AI) and machine learning (ML) are examples of some of the more cutting-edge technology that CTI has used as it has transitioned from its more conventional, manual data processing methods to these more cutting-edge technologies. Despite this, CTI continues to confront a number of obstacles and constraints, including a lack of data standardization and difficulties in accurately assessing the authenticity of sources. CTI analysts should work on having a better understanding of the available data sources and implementing a consistent data collecting and analysis approach in order to handle these problems. These should be the primary areas of their attention [37, 38].

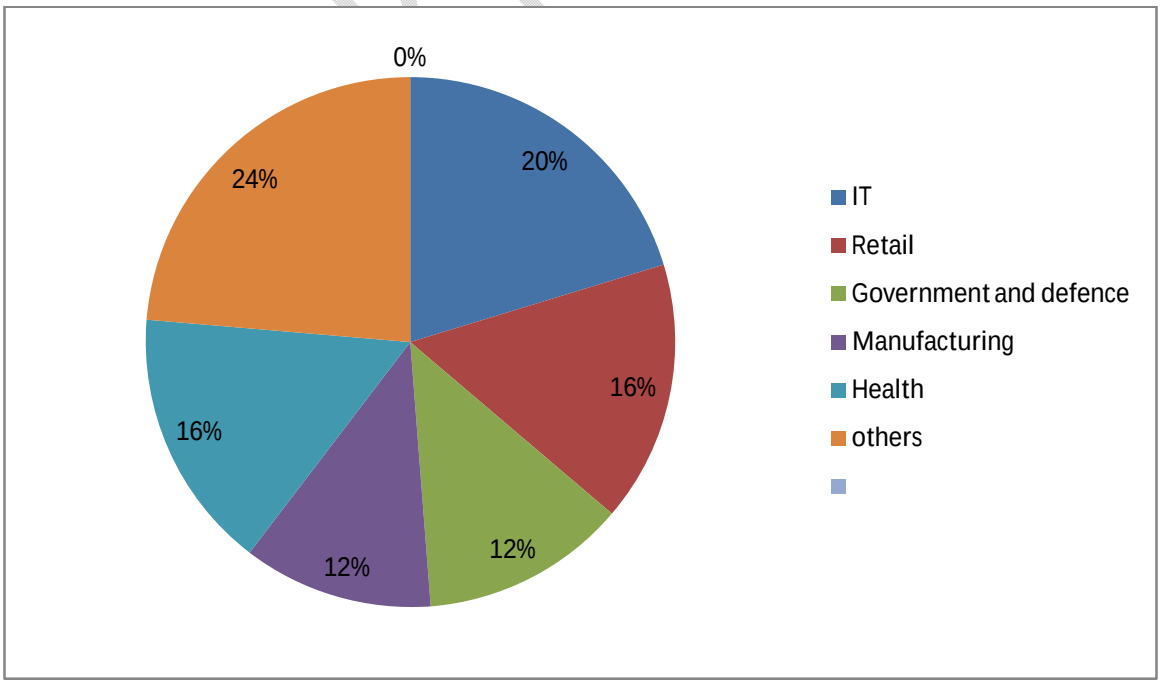


Fig . 7 Percentage **Of cyberattacks by sectors**

5.1.Challenges:

There are other important components for efficient network security, such as firewalls and antivirus software, in addition to these two mainstays. Continuous detection and reaction are obligatory, and they must work hand in hand with real-time threat intelligence that is kept up to date at all times. In most cases, this falls outside the jurisdiction of an organization's own IT departments and security staff. As a result, the organization will need to hire external analysts or reaction teams that are outsourced [39, 40].

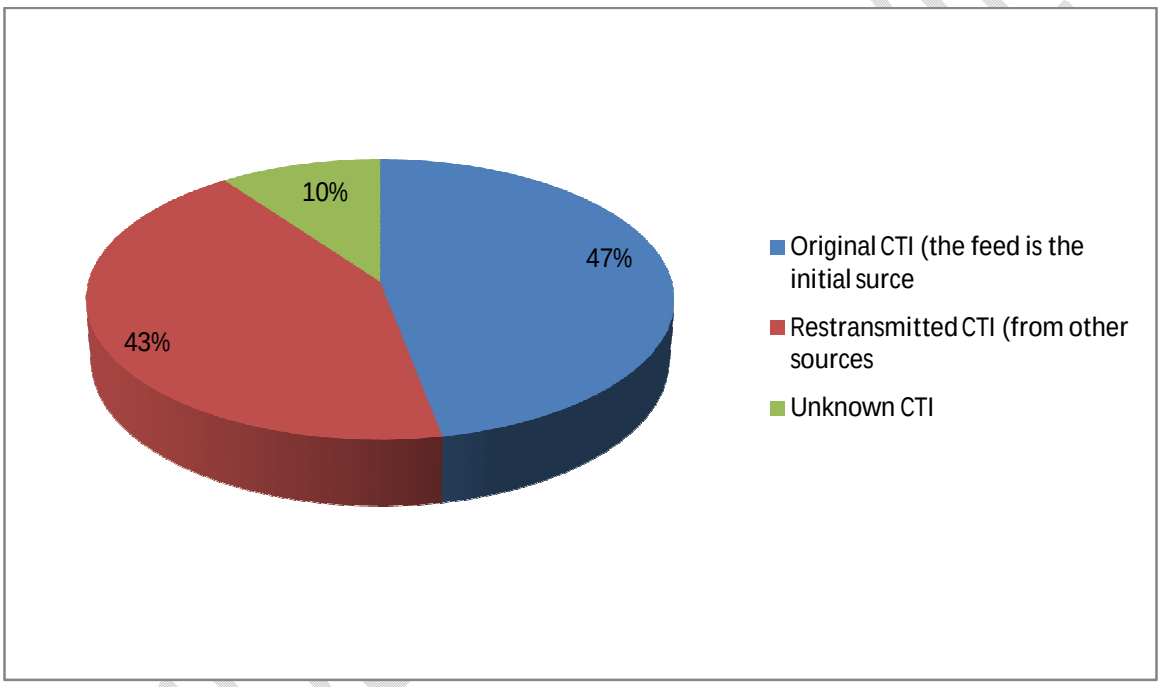


Fig .8 CTI source originality

The implementation and upkeep of data collecting technology specifically targeted for businesses is an expensive venture. When it comes to the gathering and analysis of internal data, security information and event management (SIEM) systems are widely utilized. These systems are designed to collect and aggregate data from all different parts of an organization. However, establishing one's own threat intelligence solution might be tough for those who are not professionals in the topic. The centralization of this data is vital to the analysis of risks. Because

of this, the majority of businesses choose to include threat intelligence platforms rather than constructing their own solutions based on data received from SIEMs or other independent sources of threat intelligence feeds. This is because incorporating these platforms is much simpler [41-45].

4) Future Perspectives:

Predictive analytics and automation are among the more cutting-edge techniques and technologies that are anticipated to be used in CTI in the future. In order to give a more complete picture of the threat landscape, CTI is also anticipated to be more closely connected with other security technologies, such as security information and event management (SIEM) systems. Future developments in new technologies like block chain and quantum computing will also have a big influence on CTI [46-51].

6.1.Zero Trust:

A security approach known as "Zero Trust" operates under the premise that all network traffic, whether internal and external, is potentially hazardous and should not be implicitly trusted. Instead, before granting access, each request for access to a resource must be rigorously vetted, authorized, and confirmed. This strategy tries to lessen the risk of data breaches and other cyber risks by reducing the attack surface [52, 53]. The corporate sector is seeing an increase in popularity of this strategy. Organizations may make sure they have access to the most recent information about newly emerging vulnerabilities and can take preventative actions to mitigate such dangers by incorporating CTI into a Zero Trust security strategy. Before they do serious harm, CTI may assist organizations in identifying and responding to efforts at credential theft, data breaches, and other malicious actions. For instance, if a company receives a CTI warning on a brand-new malware variant that targets a particular application, it may act promptly to reduce the risk by patching vulnerabilities or revising security procedures. Similar to this, if a data breach occurs, an organization can utilize CTI to immediately assess the size and severity of the breach and take the necessary steps to limit the damage [54, 55]. According to the greatest threats to an organization's assets and activities, CTI may assist organizations in identifying and prioritizing security initiatives. This can assist businesses in making better informed choices about how to manage risks and where to deploy their resources[56, 57].

6.2.Governance, social, and environmental issues

Companies now recognize the value of environmental, social, and governance (ESG) considerations in their day-to-day operations. Investors and other stakeholders assess a company's impact on the environment, society, and corporate governance using a set of criteria known as ESG. Companies are increasingly focusing on their cyber security posture as one of the ESG elements. By assisting in the identification and mitigation of cyber risks that may have an impact on a company's operations, cyber threat intelligence (CTI) may significantly contribute to the achievement of a company's ESG goals [58, 59]. A cyber assault on a business's infrastructure, for instance, may cause a data breach that exposes private customer information and causes financial loss and reputational harm. By undermining consumer confidence in the business and affecting its clients, this can have a severe effect on the environment and society. Here is yet another instance. CTI can be used to keep an eye on phishing or brand abuse websites that utilise a company's name to sell fake items or steal consumer information. This kind of cyber assault might impair a company's reputation and erode consumer confidence in its brand, which would be detrimental to the company's ESG objectives [60-66].

Businesses may safeguard their consumers' data and privacy and uphold their reputation as ethical business leaders by utilizing CTI to monitor for brand misuse sites, phishing sites, and other cyber dangers [67-71].

6.3.The Need For Competent Analysts Is Still Present.

Additionally, the value of competent analysts for CTI cannot be emphasized. Although automated data gathering and analysis are now possible because to cutting-edge technologies like AI and ML, the human factor is still very important in CTI. High-quality analysts bring a variety of abilities and experiences to CTI, including the ability to comprehend and analyze complicated data, spot trends and anomalies, and provide insights that can be put to use. Additionally, analysts with a variety of experiences and viewpoints may offer a more thorough picture of the threat environment, including new threats and attack strategies [72-74].

Additionally, top-notch analysts can contextualize and make threat intelligence relevant while also adjusting it to the unique requirements of an organization. They may collaborate closely

with internal stakeholders to comprehend the particular dangers and difficulties the organization faces and to create tailored threat intelligence and actionable advice [75-77].

6.4.Cyber threat intelligence is used

In terms of business and national security, CTI is essential. To assist organizations in preventing and addressing prospective and existing attacks, CTI may offer insights on the most recent malware/threat actor trends, threat environments, vulnerabilities, attack surfaces, and data breaches. Additionally, CTI may be extremely useful in assisting organizations in comprehending the wider social and environmental effects of cyber threats. CTI, for instance, may offer insightful information on the growth of the dark web and telegram as cybercrime enabling markets, as well as assist organizations in better understanding the dangers posed by these threats [78, 79].

6.5.Account Takeover Monitoring

Monitoring for account takeover involves looking for evidence of online leakage of a company's or an employee's login and password. This monitoring is crucial because hackers commonly use stolen or leaked credentials to gain unauthorized access to corporate resources and data. A successful cyber assault, such as phishing attacks, data theft, or other harmful actions, may be carried out considerably more easily if an attacker has access to a legitimate set of credentials. The recent LAPSU$ hacking event is a perfect illustration of the need of monitoring credential leaks. By using a sizable database of stolen credentials in this instance, the hackers were able to access sensitive data and private information of significant organizations [80].

Organizations can use a range of tools and procedures to check for credential leakage. To find any compromised accounts within their organization, they may, for instance, subscribe to threat intelligence feeds that give information on previous data breaches and leaks. Organizations can also employ automated tools to search the web and dark web for references of their brand or domain as well as any related login information, such as email addresses and passwords. Organizations must make sure they have an accurate inventory of all of their systems and applications, along with the user accounts and credentials that go with them. They should also make sure that staff members receive frequent training on the value of password hygiene and the dangers of credential leaking [81].

- There are numerous measures organizations may take to integrate credential leakage monitoring into a business environment:

- Determine the domains and email accounts the company uses to operate its online services and establish accounts.
- Utilize a credential monitoring service to systematically search the web for credentials that are exposed and that match the organization's email addresses and domains.
- Set up alerts such that they will warn security staff when matches are discovered, allowing them to take prompt action to thwart threats.
- All accounts should use two-factor authentication (2FA) to offer an extra layer of protection on top of passwords.
- Employees should receive training on how to manage and create secure, unique passwords.

Organizations may considerably lower the risk of credential-based attacks by proactively monitoring for credential leaks and deploying security solutions like MFA (Multifactor Authentication). It's critical to keep in mind that monitoring credential leakage is only one component of an all-encompassing cyber security program and should be used in conjunction with other security measures like routine vulnerability scanning, employee training, and incident response planning to make sure the company is adequately protected against cyber threats [82-86].

6.6.Management of the attack surface (ASM)

ASM, or attack surface management, is yet another crucial area where CTI may contribute. ASM entails locating and keeping an eye on a company's digital attack surface, which includes all applications, systems, and data that might be attacked. Such as credential leaks, current 1-day or 0-day vulnerabilities and in-the-wild vulnerabilities discovered from recent occurrences, CTI can offer insightful information about possible vulnerabilities in an organization's attack surface. Organizations may more effectively identify their potential weaknesses and threats by integrating ASM into CTI [87-89].

6.7.VINT + ATOM Attack Surface Management

Organizations may discover possible holes in their digital attack surface and priorities their remediation efforts depending on the risk level of each vulnerability by combining ASM and vulnerability intelligence. This can assist businesses in better managing their cyber security risk and ensuring the protection of their most important assets. An organization's security posture may be further improved by integrating Account Takeover Monitoring (ATOM) services with ASM and vulnerability intelligence. Organizations can be made aware of compromised credentials by using ATOM services, which can be used to access sensitive systems and data without authorization. Organizations may proactively monitor their online attack surface for indications of account takeover and swiftly fix any discovered vulnerabilities or compromised accounts by combining ATOM services with ASM and Vulnerability Intelligence [90-93].

Regarding conventional ASM services, it depends on the particular service and its features. While some conventional ASM services could have capabilities comparable to ASM and Vulnerability Intelligence, others might have a broader scope or be less proficient at spotting possible vulnerabilities. The ideal strategy will ultimately rely on the unique demands and risk profile of each organization. The management of a company's cyber security risk may be approached more thoroughly and proactively by combining ASM, Vulnerability Intelligence, and ATOM services [94-96].

A thorough cyber security program must incorporate Attack Surface Management and Account Takeover Monitoring. But for these to be effective, full visibility into possible attack vectors, including covert channels like the dark web, Telegram, Discord, and others, is crucial. Threat actors frequently discuss and share information about possible targets, weaknesses, and attacks through these channels. Organizations can learn important information about new threats and possible weaknesses in their own attack surface by keeping an eye on these channels. However, because they are frequently heavily encrypted and tricky to access, monitoring these channels may be difficult. Here is when the value of data visibility is put to use. The term "data visibility" describes the capacity to observe and comprehend all of the data moving across the networks and systems of an organization. Internal and external data sources, including social media, the dark web, and other covert routes, are included in this. Organizations can uncover possible risks and

vulnerabilities before attackers may take advantage of them by having total access into these sources [97-102].

Conclusions:

CTI is essential to every cyber security program. CTI helps organizations detect and respond to cyber attacks by revealing new threats and vulnerabilities. CTI has progressed from human data analysis to AI and machine learning. CTI continues struggles with data standardization and source reliability, despite its advances. Organizations must invest in skilled analysts with various skills and expertise to deliver comprehensive, relevant, and actionable threat intelligence to solve these obstacles. To better understand the threat landscape, CTI is planned to interface with other security solutions like security information and event management (SIEM) systems. Attack Surface Management (ASM) in CTI can assist organizations identify vulnerabilities and threats. ATOM services also warn organizations about compromised credentials, which may be exploited to access vital systems and data. Organizations can monitor their digital attack surface for account takeover and promptly fix vulnerabilities and compromised accounts by combining ATOM services with ASM and Vulnerability Intelligence. Threat Intelligence may also detect risks and vulnerabilities using a variety of data sources, sophisticated analytics, and machine learning.

References:

1. Roberts, S.J. and R. Brown, *Intelligence-driven incident response: Outwitting the adversary*. 2017: " O'Reilly Media, Inc.".
2. Menges, F., C. Sperl, and G. Pernul. *Unifying cyber threat intelligence*. in *Trust, Privacy and Security in Digital Business: 16th International Conference, TrustBus 2019, Linz, Austria, August 26–29, 2019, Proceedings 16*. 2019. Springer.
3. Appala, S., et al. *An actionable threat intelligence system using a publish-subscribe communications model*. in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. 2015.
4. Wagner, T.D. *Cyber Threat Intelligence for "Things"*. in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. 2019. IEEE.
5. Zrahia, A., *Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views.* Journal of Cybersecurity, 2018. **4**(1): p. tyy008.
6. Sauerwein, C., et al., *Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives.* 2017.

7. Brown, S., J. Gommers, and O. Serrano. *From cyber security information sharing to threat management*. in *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*. 2015.
8. Liu, R., et al. *A research and analysis method of open source threat intelligence data*. in *Data Science: Third International Conference of Pioneering Computer Scientists, Engineers and Educators, ICPCSEE 2017, Changsha, China, September 22–24, 2017, Proceedings, Part I*. 2017. Springer.
9. Sauerwein, C., et al., *An analysis and classification of public information security data sources used in research and practice.* Computers & security, 2019. **82**: p. 140-155.
10. Abu, M.S., et al., *Cyber threat intelligence–issue and challenges.* Indonesian Journal of Electrical Engineering and Computer Science, 2018. **10**(1): p. 371-379.
11. *Barnum S (2014) Standardizing cyber threat intelligence information with the structured threat information eXpression (STIX). Version 1.1, Revision 1. MITRE. http://stixproject.github.io/getting-started/whitepaper.*
12. *Brown R, Lee RM (2019) The evolution of cyber threat intelligence (CTI): 2019 SANS CTI survey. SANS.*
13. *Dandurand L, Kaplan A, Kácha P, Kadobayashi Y, Kompanek A, Lima T et al (2014) Standards and tools for exchange and processing of actionable information. ENISA. https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information.*
14. *Howard JD, Longstaff TA (1998) A common language for computer security incidents. Sandia National Labs.*
15. *LandauerM, Skopik F, Wurzenberger M, Hotwagner W, Rauber A (2019) A framework for cyber threat intelligence extraction from raw log data. In: 2019 IEEE international conference on big data (Big Data). IEEE, pp 3200–3209. https://doi.org/10.1109/bigdata47090.2019.9006328.*
16. *Lee RM (2020) 2020 SANS cyber threat intelligence (CTI) survey. SANS.*
17. *Mavroeidis V, Bromander S (2017) Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within CTI. In: 2017 European intelligence and security informatics conference (EISIC). IEEE, pp 91–98.*
18. *McMillan R (2013) Definition: threat intelligence. Gartner. https://www.gartner.com/en/documents/2487216/definition-threat-intelligence. Checked on 10 Jan 2020.*
19. *Schlette D, Böhm F, Caselli M, Pernul G (2020) Measuring and visualizing cyber threat intelligence quality. Int J Inf Secur 1–18.*
20. Menges, F. and G. Pernul, *A comparative analysis of incident reporting formats.* Comput Secur, 2018. **73**.
21. Nespoli, P., et al., *Optimal countermeasures selection against cyber attacks: a comprehensive survey on reaction frameworks.* IEEE Commun Surv Tutorials, 2017. **20**.
22. Skopik, F., G. Settanni, and R. Fiedler, *A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing.* Comput Secur, 2016. **60**.
23. Tounsi, W. and H. Rais, *A survey on technical threat intelligence in the age of sophisticated cyberattacks.* Comput Secur, 2018. **72**.
24. Pala, A. and J. Zhuang, *Information sharing in cybersecurity: A review.* Decision Analysis, 2019. **16**(3): p. 172-196.
25. Chang, J., et al., *Analyzing and defending against web-based malware.* ACM Computing Surveys (CSUR), 2013. **45**(4): p. 1-35.

26. Chuang, J., C.D. Manning, and J. Heer. *Termite: Visualization techniques for assessing textual topic models*. in *Proceedings of the international working conference on advanced visual interfaces*. 2012.
27. Clarke, V. and V. Braun, *Successful qualitative research: A practical guide for beginners.* Successful qualitative research, 2013: p. 1-400.
28. *Alhawi, O.M.K., Baldwin, J., Dehghantanha, A.: Leveraging machine learning techniques for windows ransomware network traffic detection. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 5. Springer - Advances in Information Security series (2018, in press).*
29. *Baldwin, J., Alhawi, O.M.K., Shaughnessy, S., Akinbi, A., Dehghantanha, A.: Emerging from The Cloud: a Bibliometric Analysis of Cloud Forensics Studies. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 16, p. in press. Springer - Advances in Information Security series (2018).*
30. *Baldwin, J., Dehghantanha, A.: Leveraging support vector machine for opcode density based detection of crypto-ransomware. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 6, p. in press. Springer - Advances in Information Security series (2018).*
31. *Ding, Q., Li, Z., Haeri, S., Trajković, L.: Application of machine learning techniques to detecting anomalies in communication networks: Classification algorithms. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 4, p. in press. Springer - Advances in Information Security series (2018).*
32. *Ding, Q., Li, Z., Haeri, S., Trajković, L.: Application of machine learning techniques to detecting anomalies in communication networks: Datasets and feature selection algorithms. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 3, p. in press. Springer - Advances in Information Security series (2018).*
33. *Elingiusti, M., Aniello, L., Querzoni, L., Baldoni, R.: PDF-malware detection: a survey and taxonomy of current techniques. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 9, p. in press. Springer - Advances in Information Security series (2018).*
34. *Gill, J., Okere, I., HaddadPajouh, H., Dehghantanha, A.: Mobile Forensics: A Bibliometric Analysis. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 15, p. in press. Springer - Advances in Information Security series (2018).*
35. *Haughey, H., Epiphaniou, G., Al-Khateeb, H., Dehghantanha, A.: Adaptive Traffic Fingerprinting for Darknet Threat Intelligence. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 10, p. in press. Springer - Advances in Information Security series (2018).*
36. *Homayoun, S., Ahmadzadeh, M., Hashemi, S., Dehghantanha, A., Khayami, R.: BoTShark: A deep learning approach for botnet traffic detection. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 7, p. in press. Springer - Advances in Information Security series (2018).*
37. *Pandya, M.K., Homayoun, S., Dehghantanha, A.: Forensics Investigation of OpenFlow-Based SDN Platforms. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 14, p. in press. Springer - Advances in Information Security series (2018).*
38. *Papalitsas, J., Rauti, S., Tammi, J., Leppänen, V.: A honeypot proxy framework for deceiving attackers with fabricated content. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 12, p. in press. Springer - Advances in Information Security series (2018).*
39. *Ussath, M., et al.: Pushing the limits of cyber threat intelligence: extending STIX. Springer Conference Paper Information Technology New Generations, pp. 213–225 (2016).*
40. *Ghazi, Y., et al.: A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources. IEEE-2018 International Conference on Frontiers of Information Technology (FIT), pp. 129–134 (2018).*

41. *Kim, I., et al.: Cyber threat detection based on artificial neural networks using event profiles IEEE Access, 7, 165607–165626 (2019).*
42. *Liu, H., Lang, B.: Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. MDPI (2019).*
43. *Raad Abbas, A., et al.: Detection of phishing websites using machine learning. Springer Nature Singapore Pte Ltd. 2020, Lecture Notes, vol 1989, pp. 1307–1314 (2018).*
44. *Bhanu Prakash, B., et al.: An integrated approach to network intrusion detection and prevention using KNN. Springer Nature Singapore Pte Ltd. 2020, Lecture Notes Vol-89, pp. 43–51 (2020).*
45. Buczak, A.L. and E. Guven, *A survey of data mining and machine learning methods for cyber security intrusion detection.* IEEE Commun. Surv. Tutor., 2015. **18**.
46. *Park, R.: Guide to zero-day exploits (2015). URL https://www.symantec.com/connect/blogs/guide-zero-day-exploits.*
47. *Petraityte, M., Dehghantanha, A., Epiphaniou, G.: A Model for Android and iOS Applications Risk Calculation: CVSS Analysis and Enhancement Using Case-Control Studies. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 11, p. in press. Springer - Advances in Information Security series (2018).*
48. *Shackleford, D.: Who's using cyberthreat intelligence and how? – a SANS survey (2015). URL https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767.*
49. *Shalaginov, A., Banin, S., Dehghantanha, A., Franke, K.: Machine learning aided static malware analysis: A survey and tutorial. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 2, p. in press. Springer - Advances in Information Security series (2018).*
50. *Wardman, B., Weideman, M., Burgis, J., Harris, N., Butler, B., Pratt, N.: A practical analysis of the rise in mobile phishing. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 8, p. in press. Springer - Advances in Information Security series (2018).*
51. *Yasmin, R., Memarian, M.R., Hosseinzadeh, S., Conti, M., Leppänen, V.: Investigating the possibility of data leakage in time of live VM migration. In: M. Conti, A. Dehghantanha, T. Dargahi (eds.) Cyber Threat Intelligence, chap. 13, p. in press. Springer - Advances in Information Security series (2018).*
52. *Symantec Corporation.: Internet security threat report 2019 (2019). https://www.symantec.com/content/dam/ symantec/docs/reports/istr-24-2019-en.pdf.*
53. *Ponemon Institute LLC.: Live threat intelligence impact report 2013 (2013). https://www.ponemon.org/blog/ live-threat-intelligence-impact-report-2013-1.*
54. *Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Data quality challenges and future research directions in threat intelligence sharing practice. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security - WISCS'16, pp. 65–70. ACM, New York (2016).*
55. *Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Towards a maturity model for inter-organizational cyber threat intelligence sharing: A case study of stakeholder's expectations and willingness to share. In: Proceedings of Multikonferenz Wirtschaftsinformatik (MKWI 2018), pp. 6–9. Springer, Heidelberg (2018).*
56. *Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE Computer Society Press, Los Alamitos (2013).*
57. *Serrano, O., Dandurand, L., Brown, S.: On the design of a cyber security data sharing system. In: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS '14, pp. 61–69. ACM, New York (2014).*
58. *Kokulu, F.B. Soneji, A. Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., Ahn G.J.: Matched and mismatched socs: a qualitative study on security operations center issues. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (Association for*

Computing Machinery, New York, NY, USA, 2019), CCS '19, pp. 1955–1970. https://doi.org/10.1145/3319535.3354239.

59. *Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat intelligence sharing platforms: an exploratory study of software vendors and research perspectives. In: Proceedings of the 13th International Conference on Wirtschaftsinformatik, pp. 837–851. Springer, Heidelberg (2017).*
60. *Piazza, R., Wunder, J., Jordan, B.: StixTM version 2.0. part 2: Stix objects (2017). https://docs.oasis-open.org/cti/ stix/v2.0/stix-v2.0-part2-stix-objects.html.*
61. *Umbrich, J., Neumaier, S., Polleres, A.: Quality assessment and evolution of open data portals. In: 2015 3rd International Conference on Future Internet of Things and Cloud (FiCloud), pp. 404–411. IEEE Computer Society Press, Los Alamitos (2015).*
62. *Batini, C., Palmonari, M., Viscusi, G.: The many faces of information and their impact on information quality. In: Proceedings of the 17th International Conference in Information Quality (ICIQ 2012), pp. 212–228. MIT, Cambridge (2012).*
63. *Gascon, H., Grobauer, B., Schreck, T., Rist, L., Arp, D., Rieck, K.: Mining attributed graphs for threat intelligence. In: Proceedings of the 7th ACM on Conference on Data and Application Security and Privacy, pp. 15–22. ACM, New York (2017).*
64. *Böhm, F., Menges, F., Pernul, G.: Graph-based visual analytics for cyber threat intelligence. Cybersecurity (Cybersecurity) 1, 1 (2018).*
65. *Heinrich, B. Kaiser, M. Klier, M.: How to measure data quality? A metric-based approach. In: ICIS 2007 Proceedings pp. 108–122 (2007).*
66. *Piazza, R., Wunder, J., Jordan, B.: StixTM version 2.0. part 1: Stix core concepts (2017). https://docs.oasis-open.org/ cti/stix/v2.0/stix-v2.0-part1-stix-core.html.*
67. Batini, C., et al., *Methodologies for data quality assessment and improvement.* ACM Comput. Surv., 2009. **41**.
68. Chaturvedi, I., et al., *Distinguishing between facts and opinions for sentiment analysis: survey and challenges.* Inf. Fus., 2018. **44**.
69. Jøsang, A., R. Ismail, and C. Boyd, *A survey of trust and reputation systems for online service provision.* Decis. Support Syst., 2007. **43**.
70. Juran, J.M. and F.M. Gryna, *Juran's Quality Control Handbook*. 1988, New York: McGraw-Hill.
71. Lazar, J., J.H. Feng, and H. Hochheiser, *Research Methods in Human–Computer Interaction*. 2010, Burlington: Morgan Kaufmann.
72. Menges, F. and G. Pernul, *A comparative analysis of incident reporting formats.* Comput. Secur., 2018. **73**.
73. Pipino, L.L., Y.W. Lee, and R.Y. Wang, *Data quality assessment.* Commun. ACM, 2002. **45**.
74. Redman, T.C., *Data Quality for the Information Age*. 1996, Norwood: Artech House Publishers.
75. Riesco, R. and V.A. Villagrá, *Leveraging cyber threat intelligence fora dynamic risk framework.* Int. J. Inf. Secur., 2019. **18**.
76. Ring, T., *Threat intelligence: Why people don't share.* Comput. Fraud Secur., 2014. **2014**.
77. Sänger, J., C. Richthammer, and G. Pernul, *Reusable components for online reputation systems.* J. Trust Manag., 2015. **2**.
78. Skopik, F., G. Settanni, and R. Fiedler, *A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing.* Computers & Security, 2016. **60**.
79. Tounsi, W. and H. Rais, *A survey on technical threat intelligence in the age of sophisticated cyber attacks.* Comput. Secur., 2018. **72**.
80. Wand, Y. and R.Y. Wang, *Anchoring data quality dimensions in ontological foundations.* Commun. ACM, 1996. **39**.

81. Wang, R.Y., V.C. Storey, and C.P. Firth, *A framework for analysis of data quality research.* IEEE Trans. Knowl. Data Eng., 1995. **7**.
82. Wang, R.Y. and D.M. Strong, *Beyond accuracy: What data quality means to data consumers.* J. Manag. Inf. Syst., 1996. **12**.
83. Ogino, T., *Evaluation of machine learning method for intrusion detection system on Jubatus.* Int J Mach Learn Comput, 2015. **5**.
84. Razia, S. and V. Ramani Varanasi, *Intrusion detection using machine learning and deep learning.* Int J Recent Technol Eng, 2019. **8**.
85. Seok, S. and H. Kim, *Visualized Malware classification based-on convolutional neural network.* J Korea Inst Inf Secur Cryptol, 2016. **26**.
86. Yemunarane, K. and A. Hema, *A survey on stress detection using data mining techniques.* Int J Comput Sci Eng, 2018. **06**.
87. *Fimia L (2020) Laughing all the way to the bank—DDoS bank cyber attacks on the rise. [Blog]. https://activereach.net/newsroom/blog/laughing-all-the-way-to-the-bank-ddos-attacks-on-the-rise/. Accessed 4 Oct 2020.*
88. *Auld A (2020) Why has there been an increase in cyber security incidents during COVID-19?. [Blog]. PwC UK Cyber Threat Intelligence.*
89. *Software Reviews, Opinions, and Tips—DNSstuff (2020) What is an intrusion detection system? Definition, types, and tools—dnsstuff. https://www.dnsstuff.com/intrusion-detection-system. Accessed 7 Oct 2020.*
90. *PR, Reddy E (2018) A comprehensive survey on semantic based image retrieval systems for cyber forensics. Int J Comput Sci Eng 6(8):245–250.*
91. *Dooley J (n.d.) Software development, design and coding.*
92. *Lynn R (2021) Taming the Agile Chaos: who's who in your zoo?*
93. *Chauhan N (2020) Decision tree algorithm, explained—Kdnuggets. KDnuggets. https://www.kdnuggets.com/2020/01/decision-tree-algorithm-explained.html. Accessed 29 Dec 2020.*
94. *SHIFT Communications—Integrated Communications + PR Agency—Boston | New York | San Francisco (2021) Understanding qualitative and quantitative analysis—SHIFT Communications—Integrated Communications + PR Agency—Boston | New York | San Francisco. https://www.shiftcomm.com/insights/understanding-qualitative-quantitative-analysis/#:~:text=Qualitative%20analysis%20fundamentally%20means%20to,its%20quality%20rather%20than%20quantity.&text=Quantitative%20analysis%20is%20the%20opposite,%2C%20measures%2C%20numbers%20and%20percentages. Accessed 5 Jan 2021.*
95. *Cooney M (2020) Machine learning in Palo Alto firewalls adds new protection for IoT, containers [Blog]. https://www.networkworld.com/article/3562705/machine-learning-in-palo-alto-firewalls-adds-new-protection-for-iot-containers.html#:~:text=The%20machine%20learning%20is%20built,%E2%80%93%20with%20behavior%2Dbased%20identification. Accessed 8 Jan 2021.*
96. Mishra, P., et al., *A detailed investigation and analysis of using machine learning techniques for intrusion detection.* IEEE Commun Surv Tutor, 2019. **21**.
97. *Arnold A (2021) 4 promising use cases of blockchain in cybersecurity [Blog]. Forbes. https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/?sh=786acb493ac3. Accessed 9 Jan 2021.*
98. *Netpublikationer.dk (2021) Evaluation guidelines. http://www.netpublikationer.dk/um/7571/html/chapter05.htm. Accessed 9 Jan 2021.*
99. *Wani M, Khoshgoftaar T, Palade V (n.d.) Deep learning applications.*

100. *Porter J (2020) Amazon says it mitigated the largest DDoS attack ever recorded. [Blog] An attack with a previously unseen volume of 2.3 Tbps. https://www.theverge.com/2020/6/18/21295337/amazon-aws-biggest-ddos-attack-ever-2-3-tbps-shield-github-netscout-arbor. Accessed 4 Oct 2020.*
101. Ahmed, M., A. Naser Mahmood, and J. Hu, *A survey of network anomaly detection techniques.* J Netw Comput Appl, 2016. **60**.
102. Meryem, A. and B. Ouahidi, *Hybrid intrusion detection system using machine learning.* Netw Secur, 2020. **2020**.