INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN: 2455-0620 [Impact Factor: 6.719]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 8, Issue - 3, MARCH - 2022 Publication Date: 31/03/2022

DOIs:10.2015/IJIRMF/202203006 --:-- Research Article

Summary of Cyber Threat Intelligence

[1]Wang Zhiqun, [2]Adeyemo Oladele David, [3]Akinsoto Emmanuel Akinrayo
[1, 2, 3]Department of Information Engineering
Huzhou University, Zhejiang Province, China
Email – [1]hwzq@zjhu.edu.com, [2]oladeleadeyemo@gmail.com, [3]akinsotoemmanuel@gmail.com

Abstract: *In an ever-increasing connected world where everything seems to have connection to the internet, the rise in cyber-attacks world over has made it very important to continue to seek ways to keep organisations secured. Effective Cyber threat information dissemination is a component of cyber security to achieving success for any organisation looking to stay secured. Cyber Threat Intelligence (CTI) refers to the effective collection of data about cyber threats. As large volumes of threat data become available, the challenge remains determining how to utilize the data for effective intelligence. This research aims to review trends in the cyber threat intelligence field by highlighting existing methods for gathering threats and addressing cyber-attacks based on research findings and examine interoperability of sharing platforms of cyber threat intelligence that allow organisations to be proactive in mitigating risk and keeping secure.*

Key Words: *Cyber Security, Cyber-attack, Cyber-threat, Internet, Malware*

1. INTRODUCTION:

EC-Council 1defines cyber intelligence as “the knowledge that allows you to prevent or mitigate cyber-attacks by studying the threat data and provide information on adversaries.” Cyber threat intelligence (CTI) is a relatively new concept that is yet to gain traction in its implementation in organisations. Cyber threat intelligence is rooted in cybersecurity and intelligence 1. CTI is the potpourri of intelligence studies, computer science, computer security fields, amongst other works 3. Different literatures highlight various frameworks and approaches to implementing this concept into the defense strategy of organisations. There’s yet to be to an agreed definition and approach to CTI. CTI holds different meanings and the definition differ by company, industry, organization size and many other factors and these determine the approach to be implemented 4. As early as the twentieth century, Intelligence connected itself to communications technology bringing along massive implications for itself, diplomacy, security, and privacy 5. History has ensured that intelligence gathering and sharing is foremost in strategy development for organisations and nation-states. For example, *Newsweek*, 6 reported the attack by MOONLIGHT MAZE, by an organization with government support that interacts with Russia's top military labs which led to a large amount of data including classified naval codes and information to be accessed. This was a novel attack. The probing which targeted the Pentagon, NASA, Energy Department, private universities had been on for nearly 2 years since1998 7. The effect of the lack of CTI in the early ages of cyber-attack was captured thus:

> In 2007, Israel bombed an unfinished nuclear reactor in Syria, shielded by a U.S. Air Force developed program than tricked Syrian radar. A few months later, the nation of Estonia was shut down by a Russian cyber-attack. In 2008, fifty-four Georgian government websites were disabled... The Aurora Generator Test showed an electricity generator blown up by cyber action. The Natanz reactor in Iran was blown up by Stuxnet, and Iran wiped out tens of thousands of hard drives in Saudi Arabia 8.

There exists a history of non-linear war – a term for information warfare and cyber warfare – where lack of or poor cyber intelligence led to serious consequences for nations states. In 2016, the power grid of Ukraine was allegedly brought down by Russia using a spear-phishing attack that began in March 2015 9 (Gardner, 2018). In 2007, a series of massive coordinated cyber attacks took place on Estonian public and private sectors, which affected banks, parliament, ministries, newspapers, and TV stations which took them offline following a disagreement between Estonia and Russia 9 (Rehman, 2013, as cited in Gardner, 2018). The defacement of the Georgian parliament website and multiple denial of service (DoS) attacks that took many Georgian sites offline happened in 2008 which was attributed to Russian hackers’ cyber campaign 9 (Hollis, 2011; Markoff, 2008, as cited in Gardner, 2018). In terms of precedence, Hollis 9 (2011, as cited in Gardner, 2018) described it as the first recorded case of coordinated cyberspace domain attack. In one of the shocking events of 2008, a pipeline in Turkey, fitted with sensors and cameras to monitor its movement went up in smoke without a distress signal. The alarms on the pipeline had been shut down and communications cut off by hackers. Robertson 10 described that blast as a watershed event even though it is disputed that cyber attack is the cause of the explosion.11

GhostNet was a malware-based cyber espionage network. It was a network of computers that had been compromised and located in numerous countries globally. What the network did was cause the download of Trojan through infected computers which gave access for control. According to the *New York Times* 12, in terms of countries affected, *GhostNet* was huge in terms of discovery. Hackers attack every 39 seconds 13. Famous corporate breaches included Yahoo, who in 2017, had user account information exposed and Equinox, in 2018, that announced that 143 million U.S citizens had sensitive personal data exposed. All activities of hackers3. Microsoft also was attacked. In January 2001, its websites were target of a DDoS attack due to poor configuration of the network 14. These incidences were successful where there was little information and intelligence to guard against the attacks. Penetration had taken place and damage done long before they were detected and reported. This is why cyber threat intelligence is a topical discussion among security professionals who continue to seek ways to understand malware and techniques used by attackers. The goal of this work is to highlight the advances that have been made in threats as well as threat intelligence. To identify the present practices in terms of threat intelligence and the key elements of effective cyber threat intelligence. The paper is divided into sections. The first section introduces the cyber threat intelligence and the key events in the history of cyber threats as the internet grew. The second section reviewed related literature in the evolution of the internet and cyber threat intelligence. The third section examines cyber threat intelligence with definitions of key terminologies. The fourth section surveys the evolution of cyber threat intelligence. The fifth section concludes the paper.

2. RELATED WORK:

The internet is described as a network that is universal and publicly accessible 15. The internet's evolution as a technology since inception can be ascribed to the involvement of public investment and private capital. Public investment as represented by the Department of Defense (DoD) and private capital as seen in the privatisation of the network in the mid-1990s 16. From what started as a military experiment as Advanced Research Projects Agency Network (ARPANET) in the 1960s to what is known as the commercial internet from about 1995, the internet has led to increased and quick access to information and has seen the rise of innovators and inventors who have built global enterprises off the back of this evolution 16. With close to 3.8 billion internet users world over, the internet has resulted in a surge in activities around e-commerce, internet advertising, education, immigration, healthcare, governance and work in the process creating new industries and careers 17. The severity of an attack on a computer does not have to take so long before it is felt, an example being the Slammer worm of 2013, whose effect took 10 minutes before it was felt globally 15. Threats have evolved from traditional such as Trojans, viruses, worms to a new generation which include advanced persistent threats (APTs), polymorphic threats, zero-day threats and composite threats 18. These attacks are more targeted at web servers, cloud computing services and mobile networks part of the new trends in cybersecurity 19. The safety of computers networks at the growth level achieved can only be possible with information sharing 20. The reason behind security researchers looking at new ways of extracting intelligence is the rise of cyber-threats as reported by companies and anti-virus vendors 21. Between 2001 and 2013, there were several cyber attacks aimed at compromising the cybersecurity tripod 14. Security was not high on the list of features of the Internet when it started out 22. Because cyber-threats are real it becomes important for owners and operators of asset to make adequate investments in cybersecurity 11. This is because a cyber-attack on a critical infrastructure is not a matter of if but rather how long before it happens 23. So it has become pertinent for organizations to aggregate and distribute real-time cyber threat information. There's a limit in terms of measuring the quality of intelligence source 24. Meanwhile, gathering and sharing of intelligence is not what only matters but also the transformation of threat information to threat intelligence so as to mitigate against attacks or at least execute timely disaster recovery 25. When determining the quality of a CTI source, certain factors must be considered 24. This is because attacks can take the form of stealing sensitive personal information or accessing and taking control of the victim's machine for further malicious purposes 26.

Cyber threat intelligence is a subject with no yet-agreed definition mainly driven by vendors 27. Threat intelligence is a fusion of strategy and practicality 28. Threat intelligence can be considered to be the evolution of the age long security approach 4. It was suggested that current research work around CTI is concentrated on the tactical level 2. Although it is was argued that a quantitative method combined with the current method of using qualitative means to gauge quality of information source can make the process robust 24. Threat intelligence sources include internal threat intelligence, external threat intelligence, data feeds and crowdsourced platforms 4. With CTI, there's an increased ability to understand threats, those behind them and their routine which gives an increased ability to apply appropriate measures 29. It is not uncommon to see organisations hire qualified threat data analysts and professionals saddled with the responsibility of converting voluminous threat data into useful intelligence 30. This is not limited to large size organisations. Some challenges of CTI as a solution include lack of methodology, bias, failure to use intelligence report (also known as Cassandra), unreliability of data, lack of transparency of vendors and difficulty in attribution 3. It was suggested that the current issues plaguing CTI include threat data overload, threat data quality, interoperability issue in TISP and privacy and legacy 31. As part of ways to tackling these challenges, legislations have been put in place to further strengthen CTI 24. For interoperability issues, standards format such as STIX, TAXII, CybOX have been introduced 30. CTI sharing is the way forward to effectively tackling the menace of cyber threats 32. Leading organisations in the future will be those who effectively utilise intelligence gathered to mitigate against attacks 33.

3. CYBER THREAT INTELLIGENCE:

Cyber threat intelligence (CTI) can be described as the process of taking different bits of information about a cyber attack, understanding how it happened and the meaning 34. It helps to predict and pre-empt cyber attacks 28. Also referred to as threat intelligence, it is the method of forewarning an organisation based on data acquired from different sources that has been analysed. Common sources of data breaches are malware, insider threats, social engineering, weak and stolen credentials, application vulnerabilities, wrong configuration and error on the part of users. Threat intelligence in itself is an evolution in the process of securing data, files and infrastructure. The sophistication in attacks led to the advancement in information gathering from multiple sources to safeguard assets in an environment. The exchange of threat intelligence provides a strong support for dealing with cyber attacks in the new era 35. In his definition, CTI is adversary based, risk focused, process oriented and tailored for diverse consumers 3738. Adversary based because it seeks to identify the motivation and intentions as well as the methods of the attackers. CTI is focused on minimising the risk that key assets and infrastructure are exposed to by the activities of the attackers such that business activities are not affected. CTI aims to give knowledge advantage over cyber threat actors 3. In this light, threat intelligence should be evidence-based knowledge of threats that lead to decision. It was pointed out that threat intelligence aims to align the business goals with cyber security goals 4.

The definition of cyber threat intelligence is not complete if it doesn’t capture relevant threat data that undergoes the stages of collection, analysis and processing that lead to actionable intelligence which assists decision making, all well-timed 31.

3.1. Cyber Attack:

A cyber attack is action targeted at the online activities of an organisation with the intent to make it lose control, ownership or access of its data (NIST). About $445 billion is what is estimated to be the toll of Cyber attacks per year 29.

3.2. Cyber threats:

This refers to a threat as any situation or action with the capacity to negatively affect normalcy 41. Threats can be regarded as one of adversarial, accidental, structural and environmental 42.

3.3. Cyber security:

According to the ITU, “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.” Cybersecurity refers to techniques of ensuring unauthorized access to assets and infrastructure do not take place 19.

3.4. Indicators of Compromise (IOC):

IoC refers to parts of the defense system that signals malicious activity. These actionable signals get fed into the defense system 44

3.5. Tactics, Techniques and Procedures (TTPs):

TTPs describe the ways of an actor. Tactics describe behaviours at a high-level, while techniques refers to detailed behaviour from the perspective of a tactic and procedures refer to much deeper descriptions from the perspective of a technique 45. TTPs magnify in details the actions of an attacker and methods used 46.

3.6. Threat Data:

Threat Data or Intelligence refers to the process of acquiring, via multiple sources, knowledge about threats to an environment 4. Sources include industry and community groups, internal sources and intelligence feeds from CTI vendors 47. Options for organisations include implementing a threat sharing platform that manages the threat feeds gathered together with a qualified threat data analyst to analyze, transform the threat data gathered into useful intelligence 30. Cyber Threat Intelligence (CTI) can be gathered from social media where threat information are put out in real time 48.

3.7. Cyber Threat Information:

Cyber threat information refers to information that equips an organisation against cyber threats 45. Cyber threat information includes indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents".

3.8. Importance of cyber threat intelligence:

The corona virus pandemic has exacerbated malicious activities on the internet with a recorded 600% rise during the pandemic 49. Cyber threat intelligence needs to be timely, accurate, actionable, relevant and contextual 44. This is what makes is relevant to an organisation. The power it gives to take actions as a step that protects infrastructure from cyber attack is a key benefit of CTI in cybersecurity. Cyber-attack is on the increase because of the low cost of entry and the affordability to develop attack software and protocols 50. 51 suggested some benefits of Cyber Threat Intelligence for organisations when adopted to include:

- Provides strategic intelligence for C-level executes and board of directors,
- Affects policy changes and long-term strategic decision in organisation.
- Provide knowledge that can influence high-level decision-making in organisation because CTI provides situational picture of threat landscape and situational awareness.
- Operational CTI provides context to TTPs and name potential adversaries which are capable to threaten the organisation.
- Organisational CTI supports CSOC (Cyber Security Operations Centre) for better security.
- Tactical threat intelligence assists CSOC operations by providing needed intelligence to block and needed knowledge about Indicators of Compromise (IoC).

Threat information sharing provides access to threat information that might otherwise be unavailable to an organization 45.

3.9. Intelligence cycle:

The UK's National Crime Agency (NCA) defines intelligence as information that has been analysed to determine its relevance and reliability 52. The intelligence cycle is "a representation of a set of sequential and repeated operations – educing decision makers' requirements for information; collecting relevant data; evaluating the data for reliability; analyzing their significance; disseminating the resulting intelligence product to decision makers; and then starting the process all over again by passing the decision makers' updated requirements to the collectors" 53. When the entire processes in the cycle are followed, end user requirements are met efficiently 55. The intelligence cycle is critical for decision making in commercial organisations as shown in difference in its usage from government institutions 53. Also known as the intelligence process flow, the entire cycle is made of up phases which include planning and direction, data collection, processing and analysis and dissemination as shown in Figure 1. At the planning and direction phase, the goal is to ascertain the exact requirement of the end user. This helps to establish the required data and information and how to collect them. The collection is about collection data and information that meet the requirement identified in the first phase. The data is collated from multiple sources and these sources are determined by their relevance to the desired information. Raw data from all sources and then converted into intelligence at the processing and analysis phase. Dissemination phase is the product of the intelligence being shared with end users using the right format.

Strategic Intelligence: Supports the organisation and protect it from potential threats. Top level strategy formulation and execution depend on the outcome of strategic intelligence 2.
Operational Intelligence: EC-Council describes operational threat intelligence as focusing on knowledge about the attacks while revealing details on different factors and how an attack is done 1 .
Tactical Intelligence: focuses on real-time decision to mitigate threats 56.

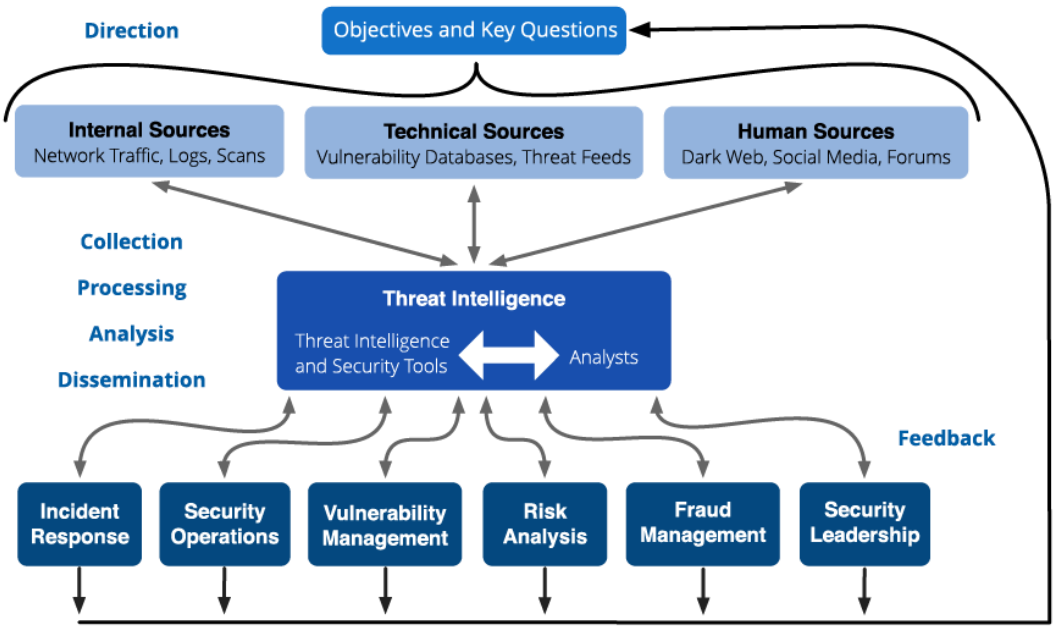

Figure 1: Threat intelligence lifecycle (Cascavilla et al., 2021)

There are 3 levels of intelligence as shown in Figure 2.

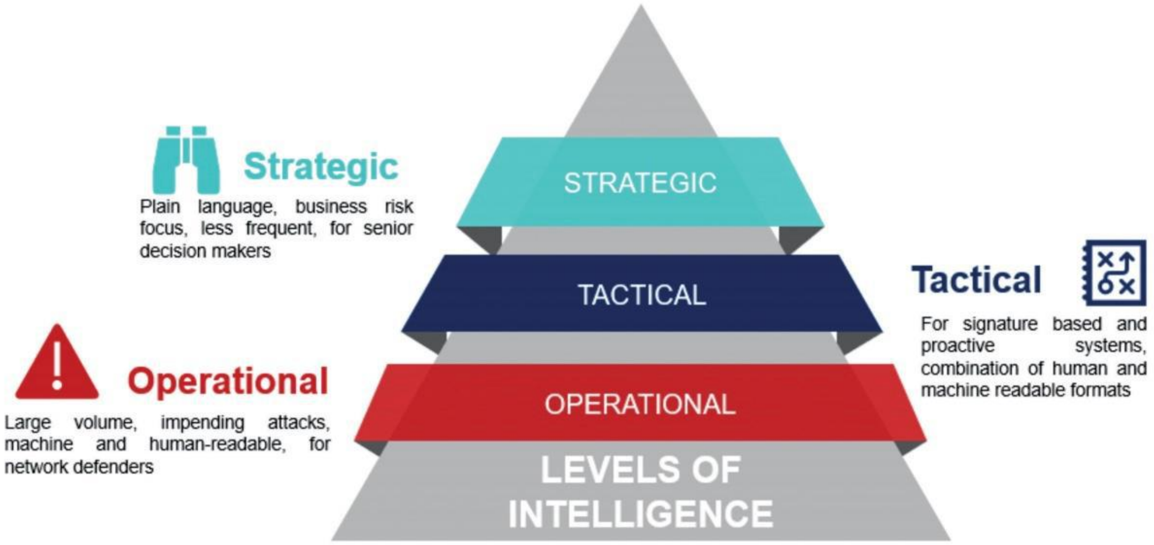
Strategic
Plain language, business risk focus, less frequent, for senior decision makers
STRATEGIC
TACTICAL
Tactical
For signature based and proactive systems, combination of human and machine readable formats
Operational
Large volume, impending attacks, machine and human-readable, for network defenders
OPERATIONAL
LEVELS OF INTELLIGENCE

Figure 2: The three levels of cyber threat intelligence (Win & Thaw, 2019)

4. CTI AND ITS EVOLUTION:

CTI is highly useful to organizations because it is the outcome of the analysis of the intent, capabilities and opportunities of adversaries in cyberspace 57. To fully understand how important it is gather useful information needed for decision making, we examine the early manifestations of threats to organisations. The first worm to spread itself across digital networks was the Morris-worm. In 1988, it became one of the earliest public documented cases 59. Also known as the internet worm, it was a non-destructive worm launched from an MIT computer and spread to internet-connected computers causing them to be slow. One of the consequence of that incident was the creation of Defense Advanced Research Projects Agency (DARPA) of the Computer Emergency Response Team (CERT) for information coordination and to respond to computer vulnerabilities and security 58. Security professionals have continued to develop measures to gather, analyse and build tools to be proactive in defending infrastructure. These are necessary to reduce disruptions and losses 14. CTI community gained relevance and started building up with the Mandiant report in 2013 3. There is an increased usage of CTI as of today with diverse options addressing the needs of organisations. A more informed perception of the value of CTI has led to its embrace by organisations 57. Though having its root in technology, there's the school of thought that argues that CTI has addressed its challenges using technology rather than intelligence analysis and methodology 3. The greatest challenge of CTI is in the collection of precise and actionable intelligence 28. Failure to aggregate the volume of information gathered without action makes it ineffective. Collaboration is the way forward for cyber security; this is why standards are used in CTI to ensure timeliness of efforts. From the days of concentrating on IoCs, CTI now covers TTPs, threat behaviors, attack surface awareness and strategic assessments which has resulted in a shift in organisations demanding automated data gathering and strategy-level reports 57. CTI tools, technologies, capabilities and integration are improving 47. Organisations are more focused on reports that can aid decision making rather than raw threat data. Collection and processing of data are more automated as organisations develop intelligence requirements by themselves. These are opened more opportunities in terms of job roles and careers as CTI has become a field of its own 57. There are organisations that are dedicated to the study of CTI today who continue to provide information on trending tools, techniques and information to enhance threat intelligence 37.

4.1. Threat Intelligence sharing platforms:

Threat intelligence is the analysis of internal and external threats to an organization in a systematic way 31. When cyber threats information is not shared, it often leads to breaches and failure in the intelligence cycle. Threat intelligence sharing can help organisations utilize shared knowledge, experience and capabilities to better understand and approach likely threats. This gives an edge in decision making with regards to techniques, tools and strategies to deploy 45. When threat information is shared, it allows organisations to access information yet to be encountered and better positions them to address any threat that may arise from such information. The majority of organizations involved with CTI fall into categories: those who produce intelligence, those who consume intelligence that has been produced by someone else, and those who both produce their own intelligence and consume intelligence that others have produced 57. With the gathering of threat data is a two-prong challenge that arises – information overload; a situation where there's so much data with no idea of where to start from or how to handle the information or information dearth; a situation where there's inadequate data to make meaning decision from. Inadequate data may arise from lack of trust, poor interoperability and non-disclosure of sensitive information which make it necessary to establish sharing rules. Sharing rules could include information sharing goals and objectives, identifying existing internal sources of cyber threat information and outlining the scope of information sharing activities 45.

Where threat intelligence becomes vital to an organisation is translating that information into proactive actions that keep organisations safe from attacks. De Melo e Silva describes the relevance of standards and platforms 60. The entire activity of selecting and processing data into meaningful formats requires some measure of time, effort and expertise 61. Threat Intelligence Sharing Platform is responsible for transforming threat data into useful intelligence with tools to help in incident response 30. It must be noted that before integrating Threat Intelligence into an organization's defense, the perimeter must be defined 4. The value of any CTI implementation is in the mitigation of organization-specific threats 57. TSIP are of two categories, Content Aggregation and Threat Intelligence Management System with the former providing threat data feeds while the latter derives business value from the collected information 30. There are tools that aid threat intelligence sharing 30. To convert threat intelligence into action, there has to be a combination of external and internal sources that enables security teams in organisations properly evaluate threats to its infrastructure. This combination is important as it reduces the time needed from the infection to detection to remediation 4. Effective actionable intelligence has to be timely, accurate, relevant and actionable. When properly implemented, CTI helps to achieve quite a lot from better insight of threats to robust incident detection as well as response 47.

4.2. CTI Tools and Providers:

There is an increased demand for CTI. Organisations are in need of comprehensive overview of threats documented in long-form reports 57. But not every organisation has the wherewithal internally to address CTI 37. In response to the increase in demand for CTI solutions, quite a number of vendors use TSIP which are software solutions that allow for exchange of data, information and intelligence 62. CTI solutions can either be vendor-based or open source 63. For many vendors, the market for CTI-related products and services is a huge money-spinning asset 3. With a projected growth, the threat intelligence market remains vital to organisations who continue to look out for solutions for detecting cyber threats and future vulnerabilities 36. Providers arm organisations and decision-makers with relevant information needed to stay protected against threat 31. Providers can be categorised into those who provide threat data feeds, threat indicators or comprehensive cyber threat intelligence, which is more expensive 3738. Majority of proprietary vendors are from the US and China 35. They include FireEye, IsightPartners, Dell Security, CrowdStrike, Qihoo 360, ThreatBook and Singhand. Other vendors outside these countries are Kaspersky, Group-IB, Sophos and Digital Shadows from Russia and England respectively. Other notable providers include IBM X-Force and Threat Tracer, S-ISAC, OASIS, Facebook Xchange, HP ThreatCentral, Checkpoint IntelliStore, Alienvault OTX. Open Source Intelligence (OSINT) refers to intelligence gathering from open and available sources including publications, social-networking sites etc 64. Popular open source tools include Security Information and Event Management (SIEM), HoneyDB, Infosec - CERT-PA, Disassemblers, Stixify, JamesBrine, ThreatMiner, PhishTank and VirusTotal 65.

4.3. CTI Approach:

The concept of CTI is to share threat data and give room for proactive defense against intrusion attempts. The secret to any CTI intervention is sharing 66. When adequate information is shared, it makes it possible to profile threats and handle effectively. Threat intelligence is effective when defined, sources identified, expectations, actionable steps laid out and information is presented in a structured and standard format. Before implementing threat intelligence, an organisation must develop a plan. Part of the plan includes carrying out an audit. The plan identifies what should be secured and the goal for implementation. It also identifies what are likely targets for attackers. These details help in formulating policies and processes that ensure its security and become a document. The document serves as a checklist that guides the actions of the incident response (IR) team of the organisation. This is because trapping a breach early in its track is what keeps infrastructure safe. And there are different approaches to tracking breaches. CTI can be used at the tactical level to thwart malicious activities using threat indicators, perform patch management, prioritize event response or perform reaction and remediation 37.

4.3.1 Community-Based Approach

Community-based approach involves members of the intelligence community validating threat data to ensure quality before sharing among members 30. Some of the standards include:

Structured Threat Information Expression (STIX): This is a structured representation of threat intelligence using a standard language. Developed by MITRE, STIX is a language that specifies, captures, categorizes and communicates threat information using a structured format 46. STIX has become the de facto standard for Structured Threat Information Exchange 67. The language is flexible, can be automated and in human-readable format. STIX's flexibility gives room for varied application. It is described to be expressive because of the variety of threat information captured which include observables, indicators, incidents, TTP, exploit targets, courses of action, threat actors and campaigns 46.

Part of the downsides of STIX include strict policies for classification and trust, unclear use of terminology and too much flexibility. It is also known to cause lack of precision in the expression of CTI 59.

Cyber Observable eXpression (CybOX): A structured language for cyber observables 68

Common Vulnerabilities and Exposure (CVE): CVE is an international, community-based effort that maintains community-driven, open data registry of publicly known cybersecurity vulnerabilities (CVE List). It is the internationally accepted standard for identifying vulnerabilities 69

Web Ontology Language (OWL): A semantic web language designed to represent rich and complex knowledge about things, groups of things, and relations between things 70

Trusted Automated eXchange of Indicator Information (TAXII): is a free and open transport mechanism that standardizes the automated exchange of cyber threat information 71

Incident Object Description and Exchange Format (IODEF): Incident Object Description Exchange Format (IODEF) defined in RFC 5070 is to exchange enriched cybersecurity information among security experts at organizations and facilitate their operations. It provides a well-defined pattern to consistently embed structured information, such as identifier- and XML-based information 72.

Real Time Inter-Network Defense (RID): Real-time Inter-network Defense (RID) outlines a proactive inter-network communication method to facilitate sharing incident-handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident-handling solution 73.

OpenIOC: An extensible XML schema containing technical characteristics that identify a known threat, an attacker's methodology or other evidence of a compromise.

4.3.2 Risk-Based Approach

Risk-based approach is a framework that seeks to understand the threats faced. Risk is the combination of vulnerability, threat and impact. Many nations have designed their framework to address specific industries and the nature of threats faced. The framework consists largely of red team exercises, tests often carried out by independent providers in collaboration with government institutions that mimic real life attacks that help institutions be proactive. The Bank of England designed CBEST, for the financial sector of the UK 74. CREST described CBEST as a tool for identifying likely threats to financial institutions through the simulated tests carried out by stakeholders. In the Netherlands, there exists the Threat Intelligence-Based Ethical Red team (TIBER-NL). Others in the UK are BEST for the telecoms sector, GBEST for government departments and ATTEST for the aviation industry, the European financial sector uses TIBER-EU 757677.

4.3.3 Narrative-Based Approach

Operationalizing narrative-based approach consists of reports that describe in detail a series of events related to an intrusion or incident 57.

5. CONCLUSION:

Cyber Threat Intelligence (CTI) is about prevention and mitigation of attacks 78. All through the history of the internet, IT security teams have had to battle to stay one step ahead of attackers 47. As cyber attacks increase and threats take new forms and potentials, Cyber Threat Intelligence (CTI) makes it possible to not properly detect in time but always react to intent and activities of attackers. The timing of information sharing is what makes the difference in protecting against attacks 20. Internet of Things (IoT), metaverse and other technology advancement mean more connected devices will be prone to attack and so the need to exploit knowledge of adversaries is important. Organisations, large or small, must embrace the gathering and sharing of threat data to secure their infrastructure and assets. Options available for organisations to utilize CTI including making adequate budget to recruit certified threat analysts or outsource the role to CTI vendors that can provide effective solutions for securing their assets. Developing a plan and gathering threat data from sources are key in effective CTI. CTI can be gathered from hacker forums, social media and dark web using open source or vendor-based tools and solutions 79. Some challenges of CTI as a solution include lack of methodology, bias, failure to use intelligence report (also known as Cassandra), unreliability of data, lack of transparency of vendors and difficulty in attribution 3. With regards to implementation, due to being a novel discipline, we identified lack of trained personnel, funding and technical capability to integrate CTI as challenges organisations face. Limited management support and lack of time to implement new processes are other challenges 47. Awareness is also very important in organisation. Employees need to be properly trained and qualified to be aware of behaviours and analyse data that can make the organisation susceptible to attacks.

STIX standard is a ubiquitous sharing standard in CTI. This is due to its extensive flexibility as a language representation. TAXII is also a commonly deployed standard. TAXII uses as yardstick service and information exchange in terms of exchange protocols. Government institutions also utilize frameworks for staying protected against threats. Frameworks such as CBEST, TIBER-NL and iCAST. To continue to stay ahead of the curve in cyber threats it is necessary for organisations to build intelligence teams that are skilled in CTI tools 80. Several teams with job roles exist today focused on CTI. Teams in addition to traditional ones of cyber security and incident response include security operations, enterprise security and vulnerability management. Roles such as Cyber Intelligence Analyst and Threat Intelligence Analyst exist today. There are still several issues around cyber threat intelligence that can make it robust. Further research should be carried out on how to develop frameworks that can help law enforcement agencies in the fight against cyber threats

REFERENCES

1. Cyber threat intelligence. (n.d.). EC-Council. https://www.eccouncil.org/cyber-threat-intelligence/
2. Groš, S. (2020). Research Directions in Cyber Threat Intelligence. arXiv preprint arXiv:2001.06616.
3. Oosthoek, K. & Doerr, C. (2021) Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence*, 34:2, 300-315, DOI: 10.1080/08850607.2020.1780062
4. Bromiley, M. (2016). Threat intelligence: What it is, and how to use it effectively. *SANS Institute InfoSec Reading Room*, 15, 172.
5. Warner, M. (2017). Intelligence in cyber-and cyber in intelligence. Understanding Cyber Conflict: Fourteen Analogies, 17-29.
6. Newsweek Staff. (1999, September 19). 'We're In The Middle Of A Cyerwar'. *Newsweek*. https://www.newsweek.com/were-middle-cyerwar-166196
7. PBS. (2003, April 24). The warnings? | Cyber war! | Frontline | PBS. PBS: Public Broadcasting Service. https://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/
8. Kaplan, F. (2016). Dark territory: The secret history of cyber war. 978-1-4767-6325-5. Simon and Schuster.
9. Gardner, B. (2018). Social engineering in non-linear warfare. *Journal of Applied Digital Evidence*, 1(1), 1.

10. Robertson, J., & Riley, M. (2014). Mysterious' 08 Turkey Pipeline Blast Opened New Cyberwar Era. Bloomberg Business, Dec.
11. Hemsley, K., Fisher, R. (2018). A History of Cyber Incidents and Threats Involving Industrial Control Systems. *12th International Conference on Critical Infrastructure Protection (ICCIP)*, Arlington, VA, United States. 215-242, 10.1007/978-3-030-04537-1_12. hal-02076302
12. Vast spy system loots computers in 103 countries (Published 2009). (2009, March 29). The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1
13. Milkovich, D. (2021, January 12). 15 alarming cyber security facts and stats. Cybint. https://www.cybintsolutions.com/cyber-security-facts-stats/
14. Vaidya, T. (2015). 2001-2013: Survey and Analysis of Major Cyberattacks. arXiv preprint arXiv:1507.06673.
15. Lehto, M. (2015). Phenomena in the cyber world. In Cyber Security: Analytics, Technology and Automation. 3-29. Springer, Cham.
16. Naughton, J. (2016) The evolution of the Internet: from military experiment to General Purpose Technology, *Journal of Cyber Policy*, 1:1, 5-28, DOI: 10.1080/23738871.2016.1157619
17. Meeker, M. (2019). Internet Trends report highlights China's short-form videos and super apps [Internet]. TechCrunch.[cité 4 oct 2019]. Disponible sur: http://social. techcrunch. com/2019/06/12/mary-meekers-2019-internet-trends-reporthighlights-chinas-short-form-videos-and-super-apps.
18. Tounsi, W., Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks, *Computers & Security*, 72, 212-233, 0167-4048, https://doi.org/10.1016/j.cose.2017.09.001.
19. Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. arXiv preprint arXiv:1402.1842.
20. Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60, 154-176.
21. Boukhtouta, A. (2016). On the Generation of Cyber Threat Intelligence: Malware and Network Traffic Analyses. 195.
22. Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. M. F. (2009). Tracking GhostNet: investigating a cyber espionage network. *Munk Centre for International Studies*, University of Toronto
23. Hult, F., Sivanesan, G. (2014). Introducing cyber. *Journal of Business Continuity & Emergency Planning*. 7 (2), 97-102(6), 1749-9216. https://www.ingentaconnect.com/content/hsp/jbcep/2014/00000007/00000002/art00002.
24. Schaberreiter, T., Kupfersberger, V., Rantos, K., Spyros, A., Papanikolaou, A., Ilioudis, C., & Quirchmayr, G. (2019, August). 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*. 1-10.
25. Tounsi, W. (Ed.). (2019). Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT. John Wiley & Sons.
26. Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. *In Cyber Threat Intelligence*. 1-6. Springer, Cham.
27. Bank of England. (2016). CBEST Intelligence-Led Testing: Understanding Cyber Threat Intelligence Operations.
28. Guitton, C. (2017). Foiling cyber attacks, 2017 *International Conference on Cyber Security And Protection Of Digital Services (Cyber Security),* 1-7, doi: 10.1109/CyberSecPODS.2017.8074853.
29. Samtani S., Abate M., Benjamin V., Li W. (2020) Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In: Holt T., Bossler A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_8
30. Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371-379.
31. Win, K.M.N., Thaw, Y.M.K.K. (2019). Information Sharing of Cyber Threat Intelligence with their Issue and Challenges. *International Journal of Trend in Scientific Research and Development*, 2456-6470, 3 (5), 878-880, https://doi.org/10.31142/ijtsrd26504
32. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.

33. Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 44, 655-662.
34. Roberts A. (2021) Cyber Threat Intelligence – What Does It Even Mean? In: Cyber Threat Intelligence. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-7220-6_2
35. Du, L., Fan, Y., Zhang, L., Wang, L., & Sun, T. (2020). A Summary of the Development of Cyber Security Threat Intelligence Sharing. *International Journal of Digital Crime and Forensics (IJDCF)*, 12(4), 54-67. http://doi.org/10.4018/IJDCF.2020100105
36. Singh, S. (2018). "Threat Intelligence Market Worth $12.9 billion by 2023," Markets and Markets, 1 November 2018, https://www.marketsandmarkets.com/PressReleases/threat-intelligence-security.asp
37. Friedman, J. (2015). Definitive guide to cyber threat intelligence. CyberEdge Group, LLC. https://cryptome.org/2015/09/cti-guide.pdf.
38. iSIGHT Partners, "The Definitive Guide to Cyber Threat Intelligence", https://informationsecurity.report/view-resource.aspx?id=4486
39. National Institute of Standards and Technology. (n.d.). Cyber attack - Glossary | CSRC. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/Cyber_Attack
40. Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr. J.F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence, *Journal of Management Information Systems*, 34:4, 1023-1053, DOI: 10.1080/07421222.2017.1394049
41. Ross, R. S. (2012). Guide for conducting risk assessments (nist sp-800-30rev1). The National Institute of Standards and Technology (NIST), Gaithersburg.
42. Blank, M.R., & Acting Secretary. (2011). Guide for Conducting Risk Assessments.
43. International Telecommunications Union. (n.d.). Cybersecurity. ITU. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
44. Mavroeidis, V., & Bromander, S. (2017, September). 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)* 91-98. IEEE.
45. Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. *NIST special publication*, 800(150).
46. Barnum, S. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). 2012. Available online: https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the (accessed on 6 February 2022).
47. Shackleford, D. (2017). Cyber threat intelligence uses, successes and failures: The sans 2017 CTI survey. SANS Institute.
48. Le, D.B., Wang, D., Nasim, M., Babar, A. (2019). Gathering Cyber Threat Intelligence from Twitter Using Novelty Classification, 1907.01755, arXiv.
49. Cranley, E. (2020, May 23). Cybercrime against healthcare groups 'worldwide' is on the rise during coronavirus pandemic, top UN official warns. Business Insider. https://www.businessinsider.com/top-un-official-warned-of-cybercrime-spike-during-pandemic-2020-5?r=US&IR=T
50. Green, J. A. (Ed.). (2015). Cyber warfare: a multidisciplinary analysis. Routledge.
51. Matilainen, J. (2020). Using Cyber Threat Intelligence as a part of organizational cybersecurity. University of Jyväskylä, 55.
52. Panlogic. (n.d.). Intelligence: Enhancing the picture of serious organised crime affecting the UK. National Crime Agency. https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk
53. Phythian, M. (Ed.). (2013). Understanding the intelligence cycle (pp. 23-30). London: Routledge.
54. Cascavilla, G., Tamburri, D.A., Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review, *Computers & Security*, 105, 102258, 0167-4048, https://doi.org/10.1016/j.cose.2021.102258.
55. CREST (2019). What is Cyber Threat Intelligence and how is it used*? CREST Threat Intelligence Professionals*. http://www.crest-approved.org
56. Nye, R., & Mod, C. (2017). Cyber Threat Intelligence Plan.
57. Brown, R., & Lee, R. M. (2019). The evolution of cyber threat intelligence (CTI): 2019 SANS CTI survey. SANS Institute. Available online: https://www. sans. org/white-papers/38790/ (accessed on 3 February 2022).
58. Kelty, C. (2011). The Morris Worm. Limn, 1. Retrieved from https://escholarship.org/uc/item/8t12q5bj

59. Bromander, S., Muller, L. P., Eian, M., & Jøsang, A. (2020). Examining the" Known Truths" in Cyber Threat Intelligence–The Case of STIX. *In International Conference on Cyber Warfare and Security (493-XII).* Academic Conferences International Limited.
60. De Melo e Silva, A., Costa Gondim, J. J., de Oliveira Albuquerque, R., & García Villalba, L. J. (2020). A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. *Future Internet*, 12(6), 108. MDPI AG. Retrieved from http://dx.doi.org/10.3390/fi12060108
61. Elmellas, J. (2016). Knowledge is power: the evolution of threat intelligence, Computer Fraud & Security, 2016 (7), 5-9, 1361-3723, https://doi.org/10.1016/S1361-3723(16)30051-3.
62. Sauerwein, C., Fischer, D., Rubsamen, M., Rosenberger, G., Stelzer, D., & Breu, R. (2021). From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms. *In The 16th International Conference on Availability, Reliability and Security (ARES 2021). Association for Computing Machinery*, New York, NY, USA, Article 85, 1–9. DOI:https://doi.org/10.1145/3465481.3470048
63. Wagner, T.D. (2019). "Cyber Threat Intelligence for “Things”," *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (Cyber SA), 1-2, doi: 10.1109/CyberSA.2019.8899384.
64. Mittal, S. (2019). Knowledge for Cyber Threat Intelligence. University of Maryland, Baltimore County.
65. Kenya CyberSecurity & Forensics Association: KCSFA [@kcsfa]. (2022, February 4). *“Here are some opensource tools for Cyber threat intelligence that you can utilize”* [Tweet]. Twitter. https://twitter.com/kcsfa/status/1489523090757402626?t=SQqdWDx_CPBtXLCdtWEdUA&s=08
66. Boi, A. Comparative Analysis of Cyber Intelligence: the Italian case.
67. Riesco Granadino, R. (2021). 21 A review of Leveraging Cyber Threat Intelligence for a Dynamic Risk Framework.
68. CybOX - Cyber Observable Expression (n.d.) | CybOX Project Documentation (Archived). github.io. Retrieved from https://cyboxproject.github.io/
69. CVE-website. (n.d.). cve-website. https://www.cve.org/About/Overview
70. W3C, OWL”, https://www.w3.org/OWL/
71. Taxiiproject. (n.d.). About TAXII (Archive). github.io. Retrieved from http://taxiiproject.github.io/about/
72. Kadobayashi, Y. (2014). An incident object description exchange format (IODEF) extension for structured cybersecurity information.
73. Hjp: Doc: RFC 6545: real-time inter-network defense (RID). (n.d.). Peter Holzer's. https://www.hjp.at/doc/rfc/rfc6545.html
74. Kaniewski J., Jahankhani H., Kendzierskyj S. (2021) Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector. In: Jahankhani H., Kendzierskyj S., Akhgar B. (eds) Information Security Technologies for Controlling Pandemics. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-72120-6_1
75. (n.d.). CREST. https://www.crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf
76. Hong Kong Monetary Authority, “Cybersecurity Fortification Initiative”, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160524e1.pdf
77. European Central Bank, “TIBER-EU Framework”, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
78. Berndt, A., & Ophoff, J. (2020, September). Exploring the value of a cyber threat intelligence function in an organization. *In IFIP World Conference on Information Security Education* 96-109. Springer, Cham.
79. Deliu, I., Leichter, C., & Franke, K. (2018). Collecting Cyber Threat Intelligence from Hacker Forums via a Two-Stage, Hybrid Process using Support Vector Machines and Latent Dirichlet Allocation, *2018 IEEE International Conference on Big Data (Big Data)*, 5008-5013, doi: 10.1109/BigData.2018.8622469.
80. Mutemwa, M., Mtsweni, J., & Mkhonto, N. (2017, March). Developing a cyber threat intelligence sharing platform for South African organisations. *In 2017 Conference on Information Communication Technology and Society (ICTAS).* 1-6. IEEE.