Exploring the Value of a Cyber Threat Intelligence Function in an Organization

Jacques Ophoff, Anzel Berndt

Exploring the Value of a Cyber Threat Intelligence Function in an Organization

Anzel Berndt[1] and Jacques Ophoff[1,2][0000-0003-0634-5248]

[1] University of Cape Town, Cape Town, South Africa
[2] Abertay University, Dundee, United Kingdom
VWYANZ001@myuct.ac.za, j.ophoff@abertay.ac.uk

Abstract. Organizations can struggle to cope with the rapidly advancing threat landscape. A cyber threat intelligence (CTI) function broadly aims to understand how threats operate to better protect the organization from future attacks. This seems like a natural step to take in hardening security. However, CTI is understood and experienced differently across organizations. To explore the value of this function this study used a qualitative method, guided by the Socio-Technical Framework, to understand how the CTI function is interpreted by organizations in South Africa. Thematic analysis was used to provide an in-depth view of how each organization implemented its CTI function and what benefits and challenges they've experienced. Findings show that CTI tasks tend to be more manual and resource-intensive, but these challenges can be resolved through automation. It was noted that only larger organizations seem to have the budget and resources available to implement the CTI function, whereas smaller organizations put more reliance on tools. It was observed that skills for the CTI function can be learned on the job, but that formal education provides a good foundation. The findings illustrate the value the CTI function can provide an organization but also the challenges, thereby enabling other organizations to improve preparation before such a function is adopted.

Keywords: Cyber Threat Intelligence, Socio-Technical Framework.

1 Introduction

Cyber threat intelligence (CTI) is a collection of data regarding threat actors, exploited vulnerabilities, malware, and any other possible cybersecurity threat. It is a crucial function in knowing the threat actor by understanding how they operate [1]. A global study by the SANS Institute observed that security teams often find themselves lagging doing analyses on artefacts, trying to predict what could happen in the future. In order to bridge this gap, the CTI function has grown in "popularity, usefulness and applicability" [2]. When using threat intelligence data organizations can improve decision-making in response to the looming danger the threat actor presents to the corporation. The CTI function also looks at how to counter these attacks to proactively develop detective and reactive mitigations [3].

According to a SANS survey the global number of organizations adopting this function is increasing, with 41% of respondents having adopted a CTI function [4]. However, there is still a large gap in adoption which is particularly true for developing countries, such as South Africa, making them an easier target for cyber-attacks [5]. Is this poor take-up due to the lack of skills required to fully understand their attacker's methods [2], or could it be due to the lack of understanding the value of this function? In developing countries organizations are primarily focused on improving their profits and decreasing their expenses, and thus cybersecurity is considered a side factor and is usually less of a priority [5]. The consequences of not adopting the CTI function are twofold. Firstly, it renders the organization incapable of analyzing the vast number of cyber-attacks happening globally each day. Secondly, it presents a risk because this function examines the attacks' features in order to implement defensive mitigations, and the organizations miss out on the benefits of this [1].

This study explores the gap in understanding the CTI function inside an organization by examining the value this function brings along with the challenges experienced when implementing this function. It aims to answer the following primary research question: What value does a cyber threat intelligence function provide an organization? The study explores this topic through interviews with several CTI professionals in South Africa, thus adding insight in a developing country context. This study will explore the perceived gap in the understanding of the CTI function inside organizations by presenting the benefits this function brings along with the challenges experienced when implementing this role. The findings should be valuable in giving organizations greater understanding and a better chance of thoroughly preparing for such an implementation by planning for the possible challenges. It also provides a list of skills required for the CTI function which can assist in designing security curricula and training programs within organizations.

The remainder of this paper proceeds as follows. Section 2 provides a review of relevant CTI literature. In Section 3, the research design is discussed in detail. This is followed by the data analysis and discussion of the project findings in Section 4. Finally, this paper concludes by discussing the limitations of this study, along with opportunities for future research.

2 Background

Prior research describes CTI as a collection of data from several sources which consists of indicators of comprise which is in turn used to understand threat actors, malware and vulnerabilities to provide actionable intelligence used to protect an organization [1-3, 6]. Veerasamy [3] explained that CTI can be used during a cyber-threat attack to answer important questions such as: who is attacking us; why is there an attack; what are they attacking; how are they attacking; and, how can the attack be stopped? SANS defines CTI as the practice to collect data from several sources which creates a better knowledge base and understanding of cyber threats in the wild and how this gathered information relates to your organization. This gathered information

can comprise indicators, context, and hopefully actionable advice in order to make an enlightened decision for the required mitigation to the threat [2].

Gartner defines CTI as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" [7]. This is reiterated in a study by Mavroeidis & Bromander [8] which defined CTI as providing "evidence-based" data on a known cyber threat that could potentially be a new threat or an existing threat to an organization. Having a better understanding of what CTI is, it is important to understand the importance of the CTI function and the next section will explain this in more detail.

2.1 The Importance of a CTI function

The CTI function is important because it can enable other cybersecurity teams to detect and respond more efficiently as it does not rely solely on signature-based detections but on understanding the techniques of a threat actor better, so that the threat can be mitigated in a more proactive manner [3, 9, 10].

The threat landscape is continuing to advance at a rapid rate and current cybersecurity teams don't have the capabilities to keep up with this [3]. The CTI function is a natural step towards hardening the security of an organization in order to prepare for the "known and unknown threats" [2]. In order to improve the detection and response to threats IT security teams are increasingly relying on the CTI function to improve their mitigation strategies [10].

Security controls normally rely on signature-based detection, so any new type of malware or technique used by the threat actor goes undetected. This is where the importance of the CTI function lies: to understand these new techniques and implementing mitigations [3]. The CTI function influences the Security Operations Centre (SOC) and Incident Response (IR) teams by providing them with greater insight into the current type of threats and attacks, while decreasing the time it takes to detect and respond to threats, because of a better understanding of the attack [10]. Up-to-date knowledge about threats, vulnerabilities, exploits and threat actors is vital to successfully defend against a cyber-attack and the CTI function provides this important service to an organization's IT security team [9].

2.2 Benefits of a CTI function

To understand why the adoption of CTI is important one needs to understand the benefits and value it presents. This section looks at the benefits some organizations experience with the CTI function. The first theme is proactive defense capabilities which is seen as a CTI function to enable the organization to proactively stop malware, ransomware, and advanced attacks by having indicators of compromise which consists of threat and vulnerability details [3, 8, 10-12]. The CTI function enables the organization to have an innovative capability in detecting and preventing cyber-attacks [8]. These abilities are derived from gathering intelligence of intricate threats

and threat actors, which gives more insight and develops “detective and reactive actions” [3]. This enables the organization to recognize changes in the techniques, tactics, and procedures (TTP) of a threat actor in order to plan accordingly for the appropriate protection [2].

To proactively protect the organization, the CTI function studies threat actors before they attack to learn their goals, strategies, techniques, tactics, and procedures [3, 11, 13, 14]. CTI is not just about knowing about the threats but also about understanding the threat actors’ abilities and motivation [3]. By building up CTI data you are defining the threat actors’ goals and strategies, which will give greater focus on what they would attack in your organization [13]. Understanding the threat actor and their TTP’s is crucial in the CTI function but sharing this information amongst peers is just as important [14].

By sharing data, the CTI function can familiarize itself with the ever-changing threat landscape quicker by using sharing platform technologies which could mean the early prevention of a cyber-attack [7, 8, 14-16]. Through this exchange of data participating organizations can positively influence “collective knowledge, experience, and capabilities” in order to achieve a better understanding of the threats [17]. Another benefit is a degree of protection for other community members by hindering the threat, whether this involves the spreading of malware or a threat actor possibly attacking another organization [17]. However, sharing requires “standard formats and protocols” and a significant understanding of the different terminologies amongst communities [8]. The benefits of a CTI function don’t come without challenges, which are discussed next.

2.3 Challenges for the adoption of a CTI function adoption

Challenges include lack of funding, the time required to implement, not developing enough proactive intelligence, and a skills shortage. Implementing a CTI function which consists of analysts and tools has been experienced to be a very costly function [4, 9]. According to Brown [4], in order to provide the CTI function with the required time to analyze and disseminate the intelligence gathered, an automation tool is of great use. However, such tools are expensive and only a limited number of organizations can afford to invest in such tools; often smaller organizations are not able to participate in the threat intelligence market [9]. Time and effort to implement are some of the leading challenges experienced with this function [2, 12, 18].

Current CTI functions mostly rely on events that already occurred, but data should be studied prior to attacks in order to provide a proactive stance [6, 11, 19]. Most CTI functions primarily focus on internal intelligence data like anti-virus logs and some threat feeds, but this is a reactive approach which depend on events that have already happened. A more proactive stance should be taken when implementing the CTI function – one where more external threat feeds are analyzed to discover threat actors and malware before an attack happens [11].

Finally, a lack of skilled staff is seen as one of the prime challenges experienced in the CTI function [10]. The lack of trained staff creates a gap in the industry because a normal cybersecurity team lacks the visibility into the threat landscape without the

CTI function [3, 10, 20]. According to Veerasamy [3] the skills gap for the CTI function is the leading challenge currently seen in the industry.

2.4 NICE Framework: SP800-181 – CTI Skills Standard

In order to formalize essential CTI skills, the NICE (National Initiative for Cybersecurity Education) Framework categorizes the CTI function as a threat/warning analyst with its specialty area being warning/threat analysis. Its description of this role is as follows: "Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyses and disseminates cyber threat/warning assessments" [21]. The NICE standard specifies the tasks, knowledge, skills, and abilities that are required for the threat/warning analyst, which relates to the CTI function.

According to the NICE framework, the CTI function requires the ability to perform a total of 30 tasks, knowledge in 47 areas, with a set of 17 different skills, and a set of 16 abilities. Some skills include performing non-attributable research, but also the ability to conduct research using the deep web. The CTI function should also have the skills to create a solution to a problem where the data is incomplete, as well as identifying cyber threats that could endanger the organization by understanding the target threat systems and using multiple analytical tools and techniques. The CTI function also requires skill in reviewing and writing about threat intelligence collected from multiple sources and presenting these briefings to different knowledge levels in the organization [21].

3 Research Methodology

To explore the topic and answer the research question a qualitative research design was employed. A qualitative study focuses on a smaller number of people but tends to produce rich data [22] through a process of "deep attentiveness, of empathetic understanding" [23]. This allows the researcher to entice certain themes from the raw data without the restrictions of using a more controlled methodology [24]. This study is based on the participants' experiences of the CTI function in their organization.

Empirical data was collected through semi-structured interviews with a selected sample of participants. Performing interviews is a method of collecting data by analyzing the participants' words, making observations, and documenting the participants' perspectives of the phenomenon [24]. A non-probability sampling method was used to target South African employees who had been working in a cyber-security team in their current organization for at least six months. Ethical clearance was obtained before data collection commenced, and participation in the study was voluntary. A total of seven participants were interviewed. After the interviews were transcribed the transcriptions were loaded into Nvivo12 for analysis.

To provide a valid interpretation during a qualitative study it is important to provide information on the dependability, credibility, transferability, and authenticity of the data collected [25]. By following the sampling method, the validity is improved

and increases the quality of the study [26]. To prove dependability during the research study the theoretical framework will be used to identify themes and relationships between the participants' feedback [25]. Credibility will be established by linking the information gathered from the participants to the research question. The applicability depends on the sample that was chosen through the sampling process where the inclusion/exclusion criteria was identified [25]. Transferability is proven by using the Socio-Technology Framework, which the interview questions are constructed from.

3.1 Theoretical Framework

A theoretical framework functions as a "structure and support" for a study [27]. This research uses the Socio-Technical Framework as theoretical lens. The framework was developed when implementation problems were experienced and were possibly connected to a "failure to achieve the expected benefits" [28]. These issues consisted of behavioral problems due to poor designs linked to the members and their functions within an organization. The Socio-Technical framework was designed to create an increase in effectiveness through "meeting task requirements" [28]. This framework was also designed to provide a "realistic view" of an organization and its internal functions. It can be used for rebuilding current and implementing new functions [28].

There are four themes derived from this framework and a total of 13 questions drafted from the themes. The four themes are: Structuring the CTI function inside current IT Teams; Skills their CTI function possesses; The technologies used in the CTI function; and Tasks pertaining to the CTI function. Based on these themes, and CTI literature reviewed, the interview questions were derived through a five-stage process [29].

4 Data Analysis and Findings

During the data analysis phase of this research study a thematic analysis process was used. A thematic analysis process includes searching for important themes derived from the specific phenomenon being researched. This includes "a form of pattern recognition" where the different themes change into the different categories that are being examined during the analysis phase [30].

The data analysis process consisted of six stages: 1. Developing the coding manual; 2. Testing the reliability of codes; 3. Summarizing data and identifying initial themes; 4. Applying template of codes and additional coding; 5. Connecting the codes and identifying themes; and 6. Documenting themes [30].

During Stage 5 the codes are connected to the identified themes in the data. During this phase, the Socio-Technical framework was used to form the structure of a 'map' that includes the themes and sub-themes and presents the relationship between themes. A primary contribution of this study is the thematic analysis map (Figure 1) which indicates the different relationships observed between the main themes of structure, technology, tasks, and people (skills).

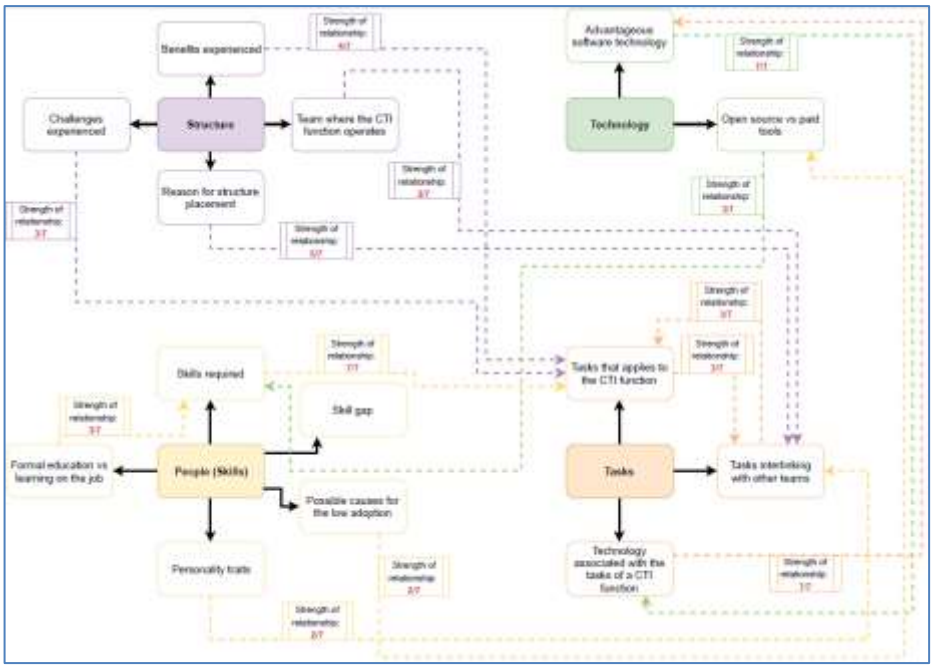

Fig. 1. Thematic Analysis Map

As seen in the thematic analysis map the benefits experienced with the CTI function in the structure had a strong relationship with the tasks that applies to this function. The team where the CTI function operates and the reason for placing the CTI function in the team also had a strong relationship with the tasks interlinking with other teams due to the nature of the function. The challenges experienced with the function were mostly related to the tasks that apply to the CTI function. The technology that is advantageous for the CTI function had the strongest relations with the technology associated with the tasks of a CTI function. Open-source versus paid threat intelligence had a strong relationship with the skills a CTI function requires, due to open-source tools requiring more skills to make it operational. The skills required by the CTI function were mostly related to the tasks required by the function. Possible causes for the low adoption of the CTI function has some relations to the open-source versus paid tools due to the CTI function being too expensive to implement and by using open-source tools, the cost to adopt the CTI function could be reduced. The personality traits a CTI function should possess had some relations with the tasks interlinking other teams, due to the function requiring the ability to continuously work other cybersecurity teams in order to gain the maximum benefit of the function. Formal education versus learning on the job has some relationships with the skills required as a CTI function. The tasks that applies to the CTI function has a strong relationship with the tasks interlinking with other teams, due to the CTI functions' requirement to work continuously with the defense and pent testing teams.

Each code that is connected to the corresponding theme and sub-themes is documented during Stage 6 of the thematic analysis. These relationships will be explored in more detail in the following subsections. Due to space limitations certain sub-themes will not be discussed. (A total of seven participants were interviewed but two of the participants worked for the same organization. To ensure the anonymity of the participants the findings will refer to them as O1 – O6.)

4.1 Structuring the CTI function

The first main theme is the structuring of the CTI function. This theme consists of four sub-themes: where the CTI function was implemented in the organization (not discussed), the reason for implementing the function in the specific structure (not discussed), the benefits, and challenges (not discussed) experienced when the CTI function was implemented.

Benefits experienced when the CTI function was implemented. This section will explore the benefits the organizations experienced after the CTI function was implemented in the said structure. O1 noted "greater visibility across potential threats" although this required more of a manual process when investigating specific threat indicators, tools, and tactics. Another benefit was greater confidence that the organization is not in the position of getting compromised and that the *organization is adequately defended*. O2 experienced an increase of automation on some of the work that was normally manual and very time-consuming. This drove them to build their own threat intelligence platform which sped up the process and made the team *more effective*. O3 developed monitoring for a particular threat actor targeting South African banks which included rules to alert them when a specific piece of code is identified. This solution highlighted two targeted attacks on the bank which they wouldn't have known about otherwise. O4 experienced their teams to *function more effectively*. O5 noted some benefits experienced were an increased *ability to detect attacks*. They can detect new attacks as they happen by generating their own threat intelligence and not solely relying on threat feeds. So, when they identify an attack the CTI function gathers the intelligence data and compares the IOC's (indicators of compromise) to the data from their customers to see if the same attack targeted them or not. They found that because their CTI function gathers intelligence themselves the quality of data is significantly better. O6 noted that the CTI function provides a *predictive view* in order to know what is coming down the line. Another benefit mentioned was the sharing of intelligence between organizations.

According to literature CTI is seen as assistance to cybersecurity practitioners by understanding the cyber-attack methods in order to respond in a more proactive manner [1]. This corresponds with the organizations stating that the CTI function assisted in proactively building their defenses before the attack happened. Another similarity in literature was found where the CTI function needs to study malicious threat actors before they attack the organization in order to protect the organization better [11]. This corresponds with the organizations stating that the CTI function created the pro-

cess where threat actors' activity would be studied in advance and attacks down line were detected; if the CTI function wasn't present this might not have been possible. The final similarity with literature was the sharing of threat intelligence information. A higher level of CTI function data requires the need to share intelligence gathered [14]. The organizations confirmed that the CTI function enabled their organization to start sharing threat intelligence with other organizations.

Benefits that extend current literature were that the CTI function improved organizations' automation capabilities, as well as their ability to detect attacks using data from internally generated intelligence and not just threat feeds.

4.2 Skills their CTI function possess

The second main theme is the skills within the CTI function. This theme consists of five sub-themes: what skills the CTI function should possess, is formal education required or can the skills be learned on the job, personality traits someone in a CTI function should possess, the skills gap (not discussed), and the cause of the low adoption rate of the CTI function in South Africa (not discussed).

What skills a CTI function should possess. This section will explore what skills the different organizations felt a CTI function should possess. O1 mentioned the CTI function should have an *attackers' mindset* in order to understand the goals of an attacker and know their tactics and techniques. The function should also have *experience building systems or infrastructure* to fully understand what typical mistakes are made. Thus, experience is a key part of understanding the potential threat for your specific organization. Another skill that is useful is *coding or development skills*, in order to decrease manual jobs and automate certain tasks (O1/O3). If automation is not present in the CTI function the resource overhead in the team would be much greater than if some automation was present. O2 stated that he came from a previous SOC analyst function before moving over to being part of the CTI function of the team. The participant noted that a SOC background gave him the ability to perform deeper research in order to make sure of the facts. An *analytical skill* is also required to perform this function. Another skill is having the curiosity for the work of a pentester or red teamer. O3 listed a couple of skills which a CTI function should possess. These skills include *understanding attacks* – how the organization could be attacked, how to construct a payload, and the *cyber kill chain*. The CTI function should also understand how to perform reconnaissance and how malware can get onto the network so what actions would *raise a flag*. The participant noted that if you don't understand how an attack works it is impossible to derive threat intelligence data from certain data. The CTI function should also understand how to transform data into actions that should be taken in order to defend against the attack. O4 noted some skills which include having a *broad understanding of cybersecurity* and being *open-minded*. The function should also have a *low level of bias* and needs to be *analytical*, the right personality and mindset. O5 stated that the skills that are required for a CTI function are divided into different roles. From a *response perspective* the function is

required to analyze the incident in order to gather the required intelligence data from it. Looking at the *detection* side of the function, they need to understand how that data from the response team can be applied. The most important skill for this function to have the ability to perform analysis when dealing with threat intelligence. O6 noted that *analytical skills* are very important in order to work through events and understanding what happened. The function should also *know what attacks look like*. This would require the function to have some "offensive pen testing type skills".

Collectively a total of 15 different skills a CTI function should possess were identified by participants. The most important skills were analytical and offense team (pen tester) experience. According to literature some skills a CTI function should possess include analyzing intelligence, awareness of the latest attack patterns and indicators of compromise, but also knowledge on how to perform incident response and awareness on known and unknown behaviors in the organization's network [10]. This was confirmed by some of the organizations who stated a CTI function needs to be analytical, drive the outcomes with the gathered intelligence but also need a good understanding of the organizations' infrastructure.

The NIST framework states that a CTI function should perform non-attributable research and have the ability to conduct research using the deep web [21]. However, none of the participating organizations mentioned this. There were several skills mentioned by the participants not seen in literature, including: coding skills, automation skills, knowledge of how malware payloads are constructed, having the ability to reverse engineer code, and performing OSINT (open-source intelligence) investigations.

Formal education versus learning on the job required for gaining the skills. Understanding the skills that are required for the CTI function from the participants' view and literature, this section will look at if these skills require formal education or could be learned on the job. Five out of the six organizations agreed that the skills for a CTI function can be learned on the job, but four participants noted that formal education provides an advantage. O1 mentioned that the "basics like coding, network infrastructure, and protocols" can be learned through formal education. He also stated that the OSCP (offensive security certified professional) qualification is beneficial. O5 mentioned that engineers, system administrators or network engineers that have a passion for security can develop their security skillset. There were no findings in the literature review concerning which of the two options, formal education or learning on the job is a better fit in gaining the required skills for a CTI function.

Personality traits someone in a CTI function should possess. This section will explore the personality traits a CTI function should possess. O1 mentioned that someone in a CTI function should *question everything* and not accept everything at face value. O1 & O2 stated that a person in a CTI function should have the ability to interact with external companies or internal people. O2 also said that they should always *communicate clearly and quickly*. O4 stated the CTI function should be *open-minded* and have a *low level of bias*. And finally, O3 said the CTI function should *be curious*

to understand how things work. There were no findings in the literature review concerning the personality traits a CTI function should possess.

4.3 Technology used in the CTI function

The third main theme is the technology used in the CTI function. This theme consists of two sub-themes: the software that is advantageous for the CTI function (not discussed) and if open-source tools could be just as effective as commercial threat intelligence tools.

Open-source versus commercial threat intelligence tools. This section will explore the views of the participants regarding open-source tools versus a commercial threat intelligence tool. Five out of the six organizations agreed that an open-source tool can be just as effective as a paid threat intelligence tool. However, one organization disagreed saying open-source tools are not as effective as paid threat intelligence tools, stating that "support for open-source tools can be challenging", and paid threat intelligence tools generates a higher quality of threat intelligence data through a *higher level of integration and automation*. O1 noted that a commercial tool is too expensive, and an open-source tool can be used to do a value evaluation to create a better motivation for a paid threat intelligence tool. However, O1, O2 & O5 stated that an open-source tools require more skills to use effectively. O6 mentioned that only a *strict intelligence sharing space* would be able to use open-source effectively.

According to literature in order to provide the CTI function with the required time to analyze and disseminate the intelligence gathered, an automation tool is of great use [4]. But such tools are expensive and only a limited number of organizations can afford to invest in such tools; smaller organizations are not able to participate in the threat intelligence market [9]. These statements share similarities to that found in the data gathered from the participants where the participants stated that *commercial tools are too expensive* but in the previous section, where the advantageous technology was discussed, it seems there is still a need for tools that provides automation. Due to the commercial tool being too expensive, more organizations are moving towards open-source tools but find it challenging due to the extra skills that are required and the lack of support.

4.4 Tasks pertaining to the CTI function

The fourth main theme are the tasks pertaining to the CTI function. This theme consists of three sub-themes: the tasks that apply to the CTI function, the tasks interlinking between the CTI function and other cybersecurity teams (not discussed), and the technology associated with the tasks of a CTI function (not discussed).

Tasks that apply to the CTI function. This section will explore the tasks pertaining to the CTI function. O1 stated that these tasks include the *gathering of information* in order to produce indicators that would discover malicious activity in the organization

or attacking the organization. The gathered data is correlated which requires *visibility across your organization*. The tasks also include the implementation of an alarm or trip when something bad happens. One of the main tasks is *research* and *applying context* to the information gathered but then also implementing that intelligence in your organization in a useful way. O1 also mentioned that a very important task is to make the information actionable in order to provide value to the organization. O2 noted that the CTI function "plays a big role in your IT security strategy". O3 stated the tasks include *threat modelling* in understanding the type of threat actors who would target your organization and understanding the tools and techniques and procedures the specific threat actors use. The *behavioral aspects* when hunting the threat actors in your environment are also part of the tasks related to the CTI function. Another important task is *industry sharing* which should be automated in order to handle it more effectively. O4 noted the tasks pertaining to the CTI function include the collection and dissemination of research data, but also *reporting, investigating, advising, underground checking and social media monitoring*. O5 stated that there are different tasks within the CTI function which depends on the level of maturity. A basic level of CTI maturity only ingests feed data and then pushes it through to their technologies. A mid-range level of CTI maturity *generates their own intelligence*. Here the CTI function is required to analyze incidents and understand how the threat intelligence data can be extracted from the data. A higher-level of CTI function tasks require research to be done on the dark web and finding the threat intelligence data from more advanced sources. O6 noted the tasks pertaining to the CTI function included looking at "your threat intelligence server provider platform or portal". This is to see what's happening in the world using the available feeds. Each incident data should be collected and analyzed.

According to literature, a CTI function "collects, processes, analyses and disseminates cyber threat/warning assessments" [21]. This has strong similarities to the data from the participants. Some additional tasks include research on the dark web and social media monitoring.

5 Conclusion

The primary objective of this research was to understand the value experienced in organizations when the CTI function was adopted. During the literature review the importance of a CTI function was identified. It seems like a natural step to take in hardening the security of an organization in order to prepare for the known, and unknown, threats. Empirical data was collected to examine how the CTI function was implemented, what benefits and challenges were experienced with the implementation, what skills such a function requires, and the technology that would be beneficial for such a function.

Using the Socio-Technical Framework as lens it was observed that implementing a CTI function provides significant value to the organization, but requires skilled resources, process to integrate the CTI function into current cybersecurity teams, and enough budget for tools to provide the best value to the organization.

A limitation of this study is the limited number of participants which represented only large organizations. Thus, the data does not represent smaller organizations and differences in their context. The limited number of CTI professionals represents a challenge for research in this area, which might be overcome with a broad survey methodology. In addition, it would be valuable to understand how the cybersecurity industry can ensure that a CTI function is also adopted by smaller, resource-constrained organizations.

Acknowledgements. This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838) [31].

References

1. Conti, M., Dargahi, T., Dehghantanha, A.: Cyber threat intelligence: Challenges and opportunities. Advances in Information Security. 70, 1–6 (2018).
2. Bromiley, M.: Threat Intelligence: What It Is, and How to Use It Effectively. SANS Security Insights. (2016).
3. Veerasamy, N.: Cyber Threat Intelligence Exchange- A Growing Requirement. (2017).
4. Brown, R.: SANS Institute Information Security Reading Room: The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey. (2019).
5. Mbelli, T.M., Dwolatzky, B.: Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security. Proceedings - 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016. 1–6 (2016).
6. Qamar, S., Anwar, Z., Rahman, M.A., Al-Shaer, E., Chu, B.T.: Data-driven analytics for cyber-threat intelligence and information sharing. Computers and Security. 67, 35–58 (2017).
7. Knights, R., Morris, E., Security, V.C.W.: Move to intelligence. Network Security. 2015, 15–18 (2015).
8. Mavroeidis, V., Bromander, S.: Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017. 2017-Janua, 91–98 (2017).
9. Mtsweni, J., Shozi, N.A., Matenche, K., Mutemwa, M.: Development of a Semantic-Enabled Cybersecurity Threat Intelligence Sharing Model. Proceeedings of the International Conference on Cyber Warfare and Security. 244–252 (2016).
10. Shackleford, D.: Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey. SANS Institute. (2017).
11. Grisham, J., Samtani, S., Patton, M., Chen, H.: Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. 2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017. 13–18 (2017).
12. Shackleford, D.: SANS Institute Information Security Reading Room: CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey. (2019).
13. Bou-Harb, E., Lucia, W., Forti, N., Weerakkody, S., Ghani, N., Sinopoli, B.: Cyber meets control: A novel federated approach for resilient cps leveraging real cyber threat intelligence. IEEE Communications Magazine. 55, 198–204 (2017).

14. Skopik, F., Settanni, G., Fiedler, R.: A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers and Security. 60, 154–176 (2016).
15. Abu, M.S., Selamat, S.R., Ariffin, A., Yusof, R.: Cyber threat intelligence – Issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science. 10, 371–379 (2018).
16. Johnson, C., Badger, L., Waltermire, D.: NIST Special Publication (SP) 800-150 Guide to Cyber Threat Information Sharing October 2016. 150, (2016).
17. Johnson, C.S., Badger, M.L., Waltermire, D.A., Snyder, J., Skorupka, C.: Guide to Cyber Threat Information Sharing. NIST Special Publication. (2016).
18. Mutemwa, M., Mtsweni, J., Mkhonto, N.: Developing a cyber threat intelligence sharing platform for South African organisations. 2017 Conference on Information Communication Technology and Society, ICTAS 2017 - Proceedings. 1–6 (2017).
19. Samtani, S., Chinn, R., Chen, H., Nunamaker, J.F.: Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. Journal of Management Information Systems. 34, 1023–1053 (2017).
20. Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., Njilla, L.: Rethinking Information Sharing for Actionable Threat Intelligence. Computers and Security. 14, (2017).
21. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. 144 (2017).
22. Kerr, K.: Research Methods in Physical Education. (2005).
23. Punch, K., Oancea, A.: Introduction to Research Methods in Education. (2014).
24. Leitch, C.M., Hill, F.M., Harrison, R.T.: The Philosophy and Practice of Interpretivist Research in Entrepreneurship. Organizational Research Methods. 13, 67–84 (2010).
25. Seale, C.: Quality in Qualitative Research. Journals. Sagepub.Com. 5, 465–478 (1999).
26. Robinson, O.C., Robinson, O.C.: Sampling in interview-based qualitative research: A theoretical and practical guide Abstract. Qualitative Research in Psychology. 11, 25–41 (2016).
27. Grant, C., Osanloo, A.: Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your "House." Administrative Issues Journal Education Practice and Research. 4, (2014).
28. Bostrom, R.P., Heinen, J.S.: MIS Problems and Failures: A Socio- Technical Perspective. STS Perspective. 17–33 (1977).
29. Wilkinson, D., Birmingham, P.: Using research instruments a guide for researchers. (2003).
30. Fereday, J., Muir-Cochrane, E.: Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. International Journal of Qualitative Methods. 5, 80–92 (2017).
31. Berndt, A.: Investigating the role of a cyber threat intelligence function in an organization [Unpublished manuscript]. Department of Information Systems, University of Cape Town, South Africa. (2019).