DOI : https://doi.org/10.56452/7-5-200

ISSN: 0974-5823 Vol. 7 No. 5 May, 2022

International Journal of Mechanical Engineering

Threat Intelligence and Sharing for Collaborative Defense

Neeraj Panwar

Asst. Professor, School of Computing, Graphic Era Hill University,

Dehradun, Uttarakhand India 248002

Abstract: Collaborative defense and the exchange of threat intelligence have emerged as important weapons in the fight against cyber threats. Cooperation and the exchange of threat intelligence data across organizations can help businesses improve their level of cybersecurity and reduce their susceptibility to cyber-attacks. To embrace such initiatives, however, presents a number of challenges, including concerns around privacy and trust, incompatibility between systems, organizational pushback, the have to comply with laws and regulations, issues in operations, and scalability. Recent technological advancements, such as federated threat intelligence sharing, automated threat intelligence sharing, artificial intelligence and machine learning, industry-specific collaborative defense initiatives, and threat intelligence sharing via blockchain, have helped to ease some of these issues. Within the scope of this research, we investigate the practices that are now in use and propose a structure for the sharing of threat intelligence and the coordination of defenses. We also discuss the challenges that come along with implementing such a system, as well as the possible benefits of doing so. Before making a final decision to install a system for collaborative defense and threat intelligence sharing in their industry and environment, businesses should first determine its potential costs, advantages, and risks. This should be done before making a commitment to using the system.

Keywords: Cybersecurity, threat intelligence sharing, industry-specific collaborative defense programs, blockchain-based threat intelligence sharing, and cyber threats.

I. Introduction

Cybersecurity is a moving target because there is a continuous influx of new threats, each of which is becoming more sophisticated. As a result, the objective of cybersecurity is constantly changing. Because of the ever-evolving nature of the threats that organizations have to face, businesses are looking for novel approaches to strengthen their defenses and enhance the safety of their systems, data, and users. This is because of the nature of the threats themselves, which are always altering [1]. The most effective method for enhancing network security is to disseminate knowledge regarding potential threats to the network as well as defensive strategies. Multiple organizations combine their resources, knowledge, and people as part of a collaborative defense plan in order to confront possible threats in a manner that is more effective than fighting them individually [2]. It is impossible for a single organization to protect itself from all of the potential cyber dangers; however, if many organizations work together, those businesses may be able to improve their defenses and make themselves less susceptible to attacks. This is the thinking that underpins this strategy. "Threat intelligence" refers to the process of gathering information about prospective threats or attacks, analyzing that information, and then sharing that analysis with other people. Indicators of compromise

(IOCs) and knowledge of the strategies, methods, and procedures (TTPs) utilized by threat actors are two examples of the types of data that are included in this category. Both of these types of data are referred to as "threat actor data." [3]. Tasks that include discovering and prioritizing hazards, as well as producing effective solutions, are made a great deal simpler with the help of threat information.

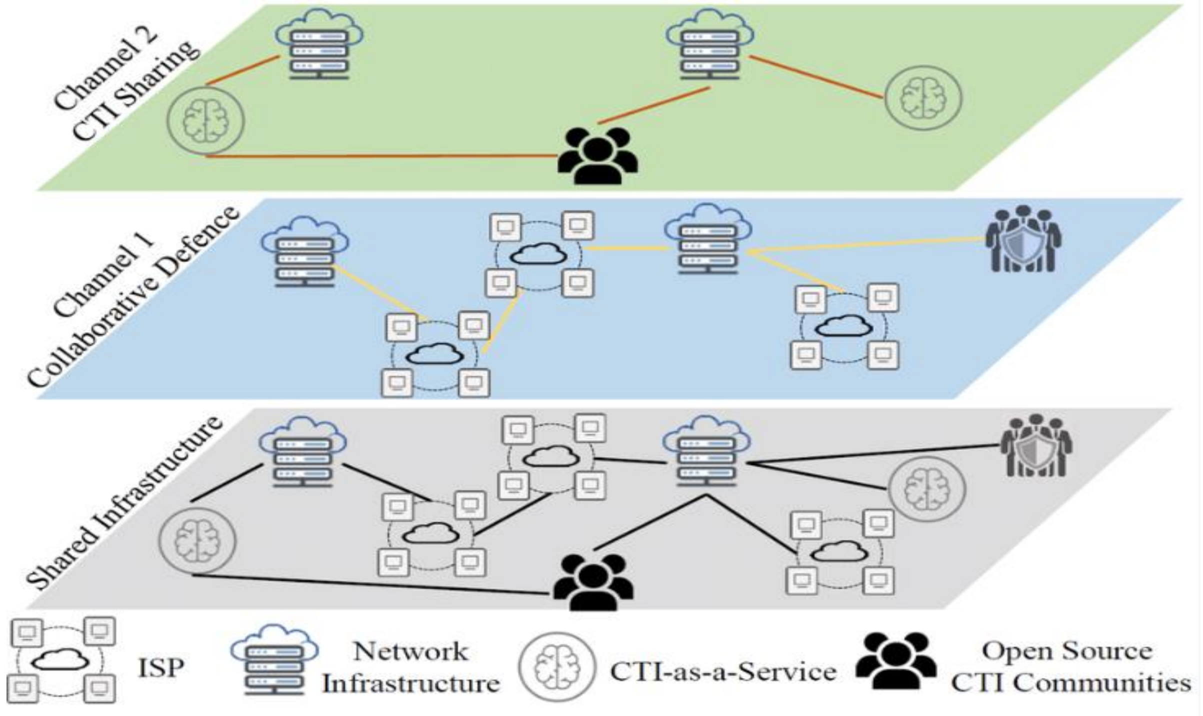

Figure 1. Basic block diagram of Threat intelligence and sharing for collaborative defense [4]

Figure 1. depicts the basic block diagram of threatintelligence and sharing threat intelligence refers to the process wherein businesses communicate with one another to discuss and share information regarding potential dangers. This can be done in an informal environment with a group of peers that you trust, or it can be done in a formal setting with standards and protocols that have been decided in advance. The goal of the sharing of threat intelligence is to improve the security posture of all parties affected by raising their awareness of and capability to respond to threats [4]. This is something that can be done regardless of the mode in which threat intelligence is shared. The level of sophistication and complexity of the threat landscape has gradually increased over the past few years, which has led to an increase in the necessity of collaborative defense and the sharing of threat intelligence. In recent years, there has been a progressive increase in the level of sophistication and complexity of the threat environment. Organizations that are a part of bigger ecosystems, such as those that operate in the same industry or region, are coming to a stronger awareness of the relevance of collaborative defense and the exchange of threat intelligence. This is because these organizations are part of larger ecosystems. The organizations that are a part of these ecosystems are able to better protect themselves against prospective attacks and decrease the harm that would be caused by attacks that are successful as a result of exchanging threat awareness and coordinating their defenses. The exchange of threat intelligence and the coordination of defenses each come with a lot of benefits, but they also each come with certain obstacles. For one thing, businesses could be cautious to share confidential information with their competitors for a variety of reasons, including trust and confidentiality concerns [5]. This is because competitors are seen as potential threats to their business. It is possible to run into a range of technical and logistical issues while attempting to disseminate threat intelligence. Two examples of these challenges are discrepancies in the data formats or standards that are employed. In spite of these obstacles, it is projected that in the years to come, as the threat landscape continues to alter, the sharing of threat intelligence and working together on defense will become increasingly crucial. When it comes to protecting their systems, data, and users against new and unanticipated threats, businesses that place a high value on working together and sharing information are more likely to be successful. The following is an analysis of the features that are required to the successful sharing of threat intelligence and collaborative defense, as well as a look at some of the potential and challenges that come with the implementation of techniques of this sort.

II. Background Study

As new cybersecurity threats and assaults appear on the scene on a regular basis, the landscape of cybersecurity threats and assaults is always altering to accommodate them. Because of this, businesses do not have a choice but to maintain a state of perpetual vigilance and to continue to reinforce their defenses in order to stay one step ahead of their competitors. The most effective method for enhancing network security is to disseminate knowledge regarding potential threats to the network as well as defensive strategies. If corporations join forces, they might be able to bolster their defenses and make the internet a more secure place for users of all ages and backgrounds [7]. The idea behind collaborative defense is that it is difficult for a single institution to protect itself from all cyber hazards; but enterprises may protect themselves more effectively by working together to combat these threats. The sharing of threat intelligence enables enterprises to get a more in-depth understanding of the threat landscape and better prepare themselves for prospective assaults. As a result, it is a vital component of joint defense since it enables these organizations to better prepare themselves [8]. The activity of exchanging threat intelligence is not a new one, but in recent years, due to the increased complexity and degree of sophistication of modern threats, it has become more crucial than it has ever been before. The exchange of threat intelligence has become an increasingly significant practices for organizations that are a part of bigger ecosystems, such as those that are active in the same market or that are in the same region [9]. The organizations that are a part of these ecosystems can better protect themselves against prospective attacks and decrease the harm that would be caused by attacks that are successful as a result of exchanging threat awareness and coordinating their defenses. One alternative involves sharing information informally amongst a group of peers who can be relied upon, while other possibilities require making more official arrangements with mutually agreed-upon standards and processes [10]. The goal of the sharing of threat intelligence is to improve the security posture of all parties affected by raising their awareness of and capability to respond to threats. This is something that can be done regardless of the mode in which threat intelligence is shared. The exchange of threat intelligence and the coordination of defenses each come with a lot of benefits, but they also each come with certain obstacles. For one thing, businesses could be cautious to share confidential information with their competitors for a variety of reasons, including trust and confidentiality concerns [11]. This is because competitors are seen as potential threats to their business. It is possible to run into a range of technical and logistical issues while attempting to disseminate threat intelligence. Two examples of these challenges are discrepancies in the data formats or standards that are employed. In spite of these obstacles, it is projected that in the years to come, as the threat landscape continues to alter, the sharing of threat intelligence and working together on defense will become increasingly crucial [12]. When it comes to protecting their systems,

DOI : https://doi.org/10.56452/7-5-200

data, and users against new and unanticipated threats, businesses that place a high value on working together and sharing information are more likely to be successful.

III. Existing Methodology

Organizations can work together on defense and share threat intelligence with the help of a variety of strategies and tools. For example:

A. ISACs are reliable platforms where businesses may exchange threat data and coordinate their security measures. Organizations that meet specific criteria for cybersecurity maturity and information sharing are often invited to join one of the several ISACs that serve specific industry and areas.

B. Platforms for collecting, storing, and analyzing threat intelligence are called Threat Intelligence Platforms (TIPs). Organizations can make use of the visualization tools and other capabilities available in TIPs to better understand the threat intelligence collected from a range of sources.

C. OSINT, or Open-Source Intelligence, is data collected from open sources and utilized to uncover potential threats or attackers. When combined with traditional methods of gathering intelligence, open-source intelligence (OSINT) can provide a more complete picture of a potential threat.

D. Automated Indicator Sharing (AIS) is a universally accepted method of exchanging indicators of compromise (IOCs) amongst businesses. The purpose of AIS is to speed up the time it takes to detect and respond to potential threats by automation of the process of sharing IOCs.

E. Hunting for security risks, or threat hunting, is the practice of actively looking for vulnerabilities and other signs of compromise within an organization's own computer systems and networks. This may include analyzing log files, network traffic, and other data sources for signs of malicious activity.

F. Red teaming is the practice of pretending to attack an organization in order to find its weak spots and security flaws. Organizations can benefit from red teaming since it aids in the detection of possible risks and the creation of efficient countermeasures.

Feeds of threat intelligence data that may be integrated into a company's security architecture are known as Cyber Threat Intelligence (CTI) feeds, and they occur in real time or very close to real time. CTI feeds can be used to automate the detection and response to threats, and may contain IOCs, TTPs, and other forms of threat intelligence data.

Methodology	**Description**	**Benefits**
Information Sharing and Analysis Centers (ISACs)	ISACs are trusted forums for organizations to share threat intelligence and coordinate their defenses.	- Provides a trusted forum for organizations to share threat intelligence - Enables organizations to coordinate their defenses and collaborate on incident response - Can help organizations to better understand the threat landscape
Threat Intelligence Platforms (TIPs)	TIPs are software tools that enable organizations to	- Can automate the process of collecting and analyzing threat

DOI : https://doi.org/10.56452/7-5-200

	collect, store, and analyze threat intelligence.	intelligence - Provides visualization tools and other features to help organizations make sense of the data - Enables organizations to more effectively defend against potential threats
Automated Indicator Sharing (AIS)	AIS is a standardized protocol for sharing IOCs between organizations.	- Can reduce the time it takes to detect and respond to potential threats - Can enable organizations to more effectively defend against emerging threats - Supports the automation of threat detection and response
Red Teaming	Red teaming involves simulating a real-world attack against an organization to identify vulnerabilities and weaknesses in the organization's defenses.	- Can help organizations to identify potential threats and to develop effective countermeasures - Provides a realistic view of an organization's security posture - Enables organizations to improve their defenses and better protect against potential attacks

Table 1. Comparative study of Various Existing Techniques

In the above table we had studied companies have the option of selecting from a variety of strategies and resources that have been developed to encourage coordinated defense and the exchange of threat knowledge. In order to determine which strategies and resources will be most beneficial, organizations need to evaluate their specific needs and highest priorities.

IV. Challenges

There is a wide variety of potential uses for a collaborative security and threat intelligence sharing system, including those in the following areas of business and organizations:

A. The exchange of threat intelligence data between various financial institutions, such as banks, insurance companies, and other financial organizations, can help improve overall cybersecurity resilience. Sharing threat intelligence data across businesses in the financial services industry can assist increase overall cybersecurity resilience and is a key target for hackers because the financial services industry is a key target for them.

B. Because the healthcare industry is becoming increasingly computerized, internet fraudsters now have access to patient medical data and other sensitive information, both of which are extremely desired as potential targets. Initiatives that encourage collaborative defense and the exchange of threat intelligence can assist healthcare companies in spotting threats and responding to them in a timelier manner. This can be accomplished through the

DOI : https://doi.org/10.56452/7-5-200

use of the initiatives' collaborative defense capabilities and the exchange of threat intelligence.

C. When government organizations and departments share threat intelligence data with one another, it can help to strengthen the overall cybersecurity resilience of an organization. Government: There are significant cybersecurity dangers facing governments at every level.

D. Manufacturing: The manufacturing industry is also rapidly adopting digital technology, and cybersecurity threats can have an effect not only on an organization's intellectual property but also on the physical production processes. This is because of the interconnected nature of the manufacturing and digital technology industries. Identifying and managing these risks may be made easier by the implementation of programs that encourage cooperative defense and the sharing of threat intelligence.

E. Energy & Utilities: Providers of essential infrastructure, energy and utility companies can have severe effects on both public safety and the economy if their services are disrupted in any manner. This is the case since energy and utility businesses are responsible for providing important infrastructure. It's possible that if these companies shared threat intelligence data with one another, it may help the industry as a whole become more resilient to cybersecurity threats.

All of these companies might potentially reap significant benefits from the implementation of a system that enables coordinated defense and the sharing of threat intelligence. Some of these benefits include shorter durations needed to respond to incidents, reduced exposure to potential risks, and improved overall cybersecurity resilience. However, it is essential to conduct an in-depth analysis of the costs, benefits, and risks connected with the introduction of such a system. Additionally, it is essential to ensure that all parties involved are kept fully apprised of the potential advantages as well as the potential challenges that may emerge.

V. Conclusion

In conclusion, combining defensive actions against cybercrime and sharing information about potential threats can be quite successful. Sharing and collaborating on threat intelligence data allows for faster incident response times, decreased risk exposure, and greater overall cybersecurity resilience for organizations. These benefits can be realized through sharing and cooperating on threat intelligence data. However, before such a system can be implemented, there are several challenges that need to be conquered. These challenges include concerns over privacy and trust, incompatibility between systems, organizational pushback, the requirement to comply with laws and regulations, difficulty in operations, and the ability to scale. In order for the concerned companies to be successful in overcoming these challenges, they will need to plan ahead, communicate openly, and collaborate frequently. Before making a commitment to building a collaborative defense and threat intelligence sharing system in their sector and environment, organizations ought to do a cost-benefit analysis of the potential advantages, risks, and drawbacks of doing so.

References

[1] [W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” Computers & security, vol. 72, pp. 212–233, 2018.

[2] Dr. Jamie Graves, “Reactive vs. proactive cybersecurity: 5 reasons why traditional security no longer works,” 2019.

[3] Dave McMahon, RafalRohozinski,Bell Canada , “The dark space project - defence research reports,” 2013.

[4] verizonenterprise.com , “2015 data breach investigations report,” 2015.

[5] D. Kreutz, F. Ramos et al., “Software-defined networking: A comprehensive survey,” arXiv preprint arXiv:1406.0440, 2014.

[6] T. Ryffel, A. Trask, M. Dahl, B. Wagner, J. Mancuso, D. Rueckert, and J. Passerat-Palmbach, “A generic framework for privacy preserving deep learning,” CoRR, vol. abs/1811.04017, 2018. [Online]. Available: http://arxiv.org/abs/1811.04017

[7] Takahashi, T.; Miyamoto, D. Structured Cybersecurity Information Exchange for Streamlining Incident Response Operations. In Proceedings of the NOMS 2016—2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 25–29 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 949–954. [CrossRef]

[8] Kure, H.; Islam, S. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. JUCS—J. Univ. Comput. Sci. 2019, 25, 1478–1502. [CrossRef]

[9] Graf, R.; King, R. Neural Network and Blockchain Based Technique for Cyber Threat Intelligence and Situational Awareness. In Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 30 May–1 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 409–426.

[10] Kim, E.; Kim, K.; Shin, D.; Jin, B.; Kim, H. CyTIME: Cyber Threat Intelligence Management Framework for Automatically Generating Security Rules. In Proceedings of the 13th International Conference on Future Internet Technologies, CFI 2018, Seoul, Korea, 20–22 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–5.

[11] Yang, W.; Lam, K.Y. Automated Cyber Threat Intelligence Reports Classification for Early Warning of Cyber Attacks in Next Generation SOC. In Proceedings of the International Conference on Information and Communications Security (ICICS 2019), Beijing, China, 15–17 December 2019; Springer International Publishing: New York, NY, USA, 2020; pp. 145–164.

[12] D. Sahoo, C. Liu, and S. C. H. Hoi, “Malicious URL detection using machine learning: A survey,” CoRR, vol. abs/1701.07179, 2017.

[13] SkopikF. *et al.*A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharingComputSecur(2016)

[14] G. Kaiafas, G. Varisteas, S. Lagraa, R. State, C. D. Nguyen, T. Ries, and M. Ourdane, “Detecting malicious authentication events trustfully,” in 2018 IEEE/IFIP Network Operations and Management Symposium, NOMS 2018, Taipei, Taiwan, April 23-27, 2018, 2018, pp. 1–6.

[15] Mutemwa, M.; Mtsweni, J.; Mkhonto, N. Developing a Cyber Threat Intelligence Sharing Platform for South African Organisations. In Proceedings of the 2017 Conference on Information Communication Technology and Society (ICTAS), Durban, South Africa, 8–10 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6

[16] A. Mohaisen, O. Al-Ibrahim et al., “Rethinking information sharing for threat intelligence,” in Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies. ACM, 2017, p. 6.

[17] D. Webster, R. L. Harris et al., “Sharing is caring: Collaborative analysis and real-time enquiry for security analytics,” in iThings. IEEE, 2018, pp. 1402–1409. E. U. A. for Network and I. S. (ENISA), “Exploring the opportunities and limitations of current threat intelligence platforms,” Tech. Rep., 2017.

[18] W. Pourmajidi and A. Miranskyy, “Logchain: Blockchain-assisted log storage,” in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). IEEE, 2018, pp. 978–982

DOI : https://doi.org/10.56452/7-5-200

[19] Ahuja, R., Kumar, A., & Sood, S. K. (2017). Collaborative defense using threat intelligence sharing. International Journal of Computer Science and Mobile Computing, 6(2), 76-83.

[20] Whitman, M. E., &Mattord, H. J. (2019). Principles of Information Security. Cengage Learning.