Fuzzy Systems and Soft Computing
ISSN : 1819-4362

THE EVOLUTION AND CHALLENGES OF THREAT INTELLIGENCE IN MODERN CYBERSECURITY

Unnamalai K, Research Scholar, University of Madras, Government Arts College for Men, Nandanam
Dr Suriakala M, Research Supervisor & Assistant Professor, Government Arts College for Men, Nandanam

Abstract
In today's day and age, Individuals and organisation globally are reliant computers or mobile phones to stay connected and it has become imperative to protect our data and information is exposed to cyber-attacks, including extortion, ransomware, and data theft. It is important to ensure robust cybersecurity to safeguard all security breaches and digital presence. Cyber Threat Intelligence (CTI) is the solution as it marks transition from reactive to proactive methods in Cyberspace. This paper covers the lifecycle of CTI and its types. Challenges of CTI including threat actors, attack patterns, emerging threats, and trends are addressed. Additionally, this paper discusses the pivotal role of Artificial Intelligence (AI) and Machine Learning (ML) in achieving security via threat intelligence.

Keywords: Cyberattacks, Cyber Security, Threat Intelligence

1. Introduction

Organisations have traditionally addressed security threats and incidents after they happen, adopting a reactive approach to cybersecurity. This method entails identifying, evaluating, and lessening the effects of hostile activity or security breaches. Threat intelligence are gathering, examining, and disseminating data regarding new and developing cyberthreats, weaknesses, and attack strategies in order to remain one step ahead of the competition. It includes information related to protecting an organisation from external and inside threats, as well as the processes, policies and tools used to gather and analyse that information. The lifetime of threat intelligence is not a linear process, but rather an iterative one that necessitates continuous improvement and adjustment to the dynamic cyber threat environment. Being proactive entails foreseeing issues, demands, or changes in the future and acting accordingly. Proactive in the framework of cybersecurity means the same thing. Proactive cybersecurity refers to all actions taken prior to an attack occurring. Companies frequently wait until it's too late to adequately prepare for any cyber-attacks. Rather than reacting to an incident after it occurred, the goal of these security measures is to stop attacks before they start. Scott Ainslie et al [1] explains that the notion of intelligence should be seen as a "working concept" that encompasses three views: that of an organisation, a process and a result. The following are the threat intelligence types which plays main role in the current scenario:

1.1 Strategic threat intelligence

Strategic threat intelligence is employed to highlight the "who" and "why," that is, the reasons behind threat actors' actions that impact the state of contemporary threats. It is non-technical, explains the motivations and goals behind the assaults, and aims to identify the individual responsible for cyber operations and threats as well as their intended targets. Threat intelligence technologies that manage data gathering and processing can lighten the workload for analysts and improve productivity even for those with less professional experience [2].

1.2. Tactical threat intelligence

The above type of threat intelligence was providing information about TTP's tactics, techniques and procedures which are used by threat actors [2]. Tactical threat intelligence is mainly intended for the

people who are directly involved in the protection of IT and data resources. Tactical threat intelligence provides the best ways to defend against or mitigate the attacks and also the way how an organisation may be attacked using the latest methods being used. Machine-readable data such as URLs, domain names, file names, IP addresses and hashes are used by tactical threat intelligence and these are called IOC [11]. Tactical threat intelligence deals with low-level and technical deals of the attackers and individual attacks. Tactical threat intelligence is used produced for the following teams incident response (TR) team, SOC analysts, IT and IT tools including SIEM, firewalls, IDS/ IPS, endpoints, Risk analysts

1.3. Technical threat intelligence

Defenders should not only be aware of threat actors and the nature of attacks they are facing. defenders are also aware of data fundamentals associated with these cyberattacks, which are known as Indicators of Compromise (IOC).[4] The IOC are linked with TTI and often confused with intelligence. By conducting the analysis with internal data intelligence which is relevant to the organisation, an actionable decision is able to recover from any incident. IOCs are commonly divided into three distinct categories such as network, host-based indicators and email indicators. [4]

1.4 Operational threat intelligence

Operations intelligence is focused on recent or impending events. It is used continuously to assess an operation's or program's expected and current capabilities; it does not conclude with long-term forecasts [7]. Operational threat intelligence's main goals are to improve overall cybersecurity posture, facilitate incident response activities, enable preemptive threat detection, and help with vulnerability management. Operational threat intelligence is a tool used by CISOs, CIOs, and other security-related decision-makers to find criminals who are likely to target their companies and to respond with safety protocols and other measures designed to stop those attacks [8].

2.Life cycle of Threat Intelligence

The life cycle of CTI is the process of gathering, processing, analysing and applying threat intelligence. It is an iterative cycle which requires constant refinement and adaptation to current cyber security trends. The six distinct phases of the threat intelligence lifecycle are shown in figure 1.

Fig 1.: Life cycle of Threat Intelligence

2.1 Phase 1: Direction: The lifecycle of CTI begins with goals, objectives, scope, and methodology-based stakeholder requirements. Identifying the Requirements plays a vital role as Threat Intelligence ensures in reducing the risk and aligns with business so that the output is actionable for the stakeholder.

The Security team investigates who the attackers are, their goals, what the potential attack surface would look like, and what steps should be taken to increase defences against a probable attack [10].

2.2 Phase 2: Collection: The most important requirement is the collection or gathering of information. This can be done gradually through various methods like extracting metadata and logs from security devices and internal networks, gathering information from knowledgeable sources, threat feeds from cybersecurity vendors or organisations, dark web forums by infiltrating closed sources, harvesting and scraping from websites and forums [9].

2.3 Phase 3: Processing: The transformation of collected information into usable format by the organisation is the next Processing phase. The raw data collected has to be processed either by human or machine. Irrelevant data has to be filtered and data has to be structured as it has to be used in the analysis phase. This helps in clustering similar data and collecting metadata [9].

2.4 Phase 4: Analysis: The processed information is analysed and converted into intelligence by threat intelligence analysts to make decisions. They work to create meaningful relevant context and actionable intelligence from the structured and formatted data from the processing phase. Threat Correlation, adversary profiling and behavioural analysis are the key aspects of this phase [10].

2.5 Phase 5: Dissemination: Distribution of intelligence reports to appropriate stakeholders and sharing of intelligence with trusted entities is the Dissemination phase. The Threat Intelligence team presents their analysis as a report to the stakeholders. Optimal community engagement and secure distribution is necessary for this phase [9].

2.6. Phase 6: Feedback: Getting Feedback on the intelligence report is the final stage. This helps to understand whether the report is timely, relevant, and actionable. Stakeholders might have changed their priorities or their view on how disseminated data should be presented. The effectiveness of threat intelligence can be achieved by improving performance metrics [9].

3. Challenges in Threat Intelligence

A basic framework for structuring intelligence activities is the cyber threat intelligence lifecycle. It is challenging to implement, and individuals will face numerous obstacles throughout the threat intelligence lifecycle. The following are the major issues need to addressed

3.1 Overloaded Data Transmission

The threat intelligence lifecycle involves Collecting large quantities of data, Pre-processing, refining with the help of and sharing key pieces of intelligence during Dissemination [8]. During the collection phase, an immense amount of data is provided, which is subsequently sorted. The process of sorting through the noise, determining what is important, and then adding your gathered data to the relevant intelligence is time-consuming and resource-intensive.

3.2 Quality of Data

The calibre of the information extracted from the threat intelligence lifecycle depends on the quality of the data. It is always Garbage in and Garbage out. This is due to the fact that the data absorbed during the Collection phase is essential to the Processing, Analysis, and Dissemination stages. Gathering incomplete, shaky, or out-of-date data will result in poor intelligence reports since the judgements will be predicated on shaky facts. It can be difficult to guarantee the reliability and correctness of the data accumulated.[11]

3.3 Intelligence data sharing barriers

The most difficult step in the threat intelligence lifecycle is dissemination. There are numerous obstacles in the way of disseminating threat intelligence within your company or to the general public. Among these are restrictions imposed by law or regulation, problems with trust, inconsistent data-sharing procedures, different report platforms and styles, and a lack of product and network compatibility.[8]

3.4 Providing feedback

The feedback stage is the most disregarded and underappreciated phase of the threat intelligence lifecycle. CTI teams frequently lack continuous improvement, don't have procedures in place to get feedback from their analytical skills consumers, and don't include metrics to evaluate the success of their intelligence operations [6]. CTI teams are simply sharing information with those within their organisation without thinking about if it adds value, and they are doing this without taking the time to gather feedback and make improvements to current processes.[8][11]

4. Role of AI and ML in Threat Intelligence

Because AI & ML offers real-time monitoring, automated incident response, behavioural analytics, and enhanced threat detection, cybersecurity benefits greatly from AI & ML. Nevertheless, users have to look at how cybersecurity experts are equipped with more potent tools to combat the ever-changing environment of cyberthreats in the integration of AI with ML technology.

4.1 Asset Management

AI & ML can guarantee an accurate and complete log of all the devices, users, and apps that are gaining access to information systems. Sort and assess their significance to the company in order to ensure efficient administration and organisation [12][13]

4.2 Breach Risk Prediction

By taking into account variables like IT asset inventory, threat exposure, and the efficacy of security controls, AI can assist in anticipating vulnerabilities and possible security breaches. By being proactive, resources can be allocated to reduce hazards before they become significant incidents [12]

4.3 Assessment of Security Controls

To strengthen the overall security posture, assess the influence and efficacy of the security tools and procedures currently in place. This entails evaluating the effectiveness of our current security measures and pinpointing areas in need of development [13]

4.4 Response time to threats

One of the most important indicators for assessing the effectiveness of a cybersecurity team is the threat response time. Malicious attacks have a reputation for moving swiftly from exploitation to deployment. Before initiating an assault, threat actors in the past sometimes had to spend weeks sorting through networking permissions and disabling safeguards [13]

4.5 Identification and prediction of new threats

Cyberattacks are also influenced by the discovery and prediction of new threats. Unknown attack tactics, and equipment can further fool a squad into responding slowly. Sometimes, worse, concealed threats, like data theft go totally undetected [12][13]

5. Conclusion

Threat Intelligence (TI) has become an absolutely essential component of modern cybersecurity. It has evolved from being a simple indicator to a sophisticated multifaceted discipline. This paper emphasizes that as cyber threats continue to grow in complexity and scale, the integration of Artificial Intelligence and Machine Learning into TI processes has become crucial, enabling faster analysis, more accurate predictions, and automated responses.

References

[1] Scott Ainslie, Dean Thompson, Sean Maynard, Atif Ahmad, Cyber-threat intelligence for security decision-making: A review and research agenda for practice, Computers & Security, Volume 132, 2023, 103352, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103352.

[2] Leong, Yee. (2021). The Implementation of Strategic Threat Intelligence for Business Organization. Journal of IT in Asia. 9. 41-48. 10.33736/jita.3398.2021.

[3] Poopak Alaeifar, Shantanu Pal, Zahra Jadidi, Mukhtar Hussain, Ernest Foo, 2024, Current approaches and future directions for Cyber Threat Intelligence sharing: A survey, Journal of Information Security and Applications, Volume 83, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2024.103786.

[4] Goel, Nimisha & Mansi, & Sethi, Nandini. (2022). Cyber Threat Intelligence: A Survey on Progressive Techniques and Challenges.

[5] Tounsi, Wiem (2024), What is Cyber Threat Intelligence and How is it Evolving, ISBN - 9781786304483 doi - 10.1002/9781119618393.ch1

[6] Wijnbergen, Max. Bridging the Gap: From CWEs to TTPs in Cybersecurity Attack Kill Chains. BS thesis. University of Twente, 2024.

[7] M Nazmuz Sakib, Cyber Threat Intelligence

[8] Md Sahrom Abu, Siti Rahayu Selamat, Aswami Ariffin, Robiah Yusof, 2018, Cyber Threat Intelligence – Issue and Challenges, Indonesian Journal of Electrical Engineering and Computer Science Vol. 10, No. 1, April 2018, pp. 371~379 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v10.i1.pp371-379

[9] White TLP. An introduction to threat intelligence.

[10] https://learn-cloudsecurity.cisco.com/umbrella-library/cyber-threat-trends-report

[11] M. Husák, J. Komárková, E. Bou-Harb and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640-660, Firstquarter 2019, doi: 10.1109/COMST.2018.2871866.

[12] Iqra Naseer, 2024, Machine Learning Applications in Cyber Threat Intelligence: A Comprehensive Review, Asian Bulletin of Big Data Management Vol. 3. Issue 2 (2023) ISSN: 2959-0809 DOI: https://doi.org/ 10.62019/abbdm.v3i2.85

[13] Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN COMPUT. SCI. 2, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

Authors' background

Your Name	Title*	Research Field	Personal website
UNNAMALAI K	Research Scholar Assistant Professor	Cyber Security, Threat Intelligence	Nil
Dr Suriakala M	Research Supervisor, Assistant Professor	Information Security	Nil