A Survey on Cyber Threat Intelligence Pitfalls: Prevention Techniques and Challenges

Vani Krishnaswamy[1], Dr. S. P Swornambiga[2]
[1]*Assistant Professor, Department of Computing-Decision and Computing Sciences, Coimbatore Institute of Technology, Coimbatore, India*
Research Scholar, CMS College of Science & Commerce, Coimbatore
[2]*Associate Professor, Dept of Computer Applications, CMS College of Science & Commerce, Coimbatore, India*

***Abstract*—Cyber Threats can be identified and analyzed with the help of Threat Intelligence. Threat Intelligence gathers data, process data and analyses the data for a potential threat. And it also involves in examining the data to spot the problem and to deploy solution for the spotted problem. A cyber-attack refers to the deliberate and malicious exploitation of computer systems, networks, and technology-dependent enterprises. The primary objective of a cyber-attack is to compromise the confidentiality, integrity, or availability of information, disrupt operations, or gain unauthorized access to sensitive data. Cyber-attacks can be carried out by individuals, groups, or even nation-states with various motives, including financial gain, political influence, espionage, or causing disruption. By leveraging cyber threat intelligence, organizations can proactively strengthen their defences, respond more effectively to incidents, and make informed decisions to reduce the overall risk of cyber-attacks. It's a dynamic and evolving field that plays a critical role in modern cyber security strategies.**

***Index Terms*—Cyber Threat, Threat Intelligence, Cyber Attack, Vulnerability, Mitigate**

I.INTRODUCTION

Cyber Threat Intelligence (CTI) is a crucial component of cyber security that focuses on gathering, analysing, and disseminating information about potential cyber threats. It involves the collection of data related to cyber threats, the analysis of that data to understand the threat landscape, and the dissemination of actionable intelligence to help organizations defend against cyber-attacks. Cyber Threat Intelligence is the knowledge and analysis about potential cyber threats, including information about threat actors, their motives, tactics, techniques, and procedures (TTPs), as well as indicators of compromise (IoCs).

Threat Intelligence can be categorized as following and its pictorial representation is given in Fig 1.1.

- Tactical Threat Intelligence: It is used to collect, analyze and disseminate the real time intelligence on current cyber threats affecting to the organizations systems or network infra structure. The goal of tactical CTI is to provide and protect organization infrastructure by the security team to make informed decisions and respond effectively to the threats.
- Strategic Threat Intelligence: Strategic Threat Intelligence is a branch of cyber threat intelligence that focuses on providing high-level insights and analysis to support long-term planning and decision-making at the organizational level. It involves understanding the broader threat landscape, the capabilities of threat actors, and the potential impact of cyber threats on an organization's overall strategy.
- Technical Threat Intelligence: Technical Threat Intelligence focuses on the technical aspects of cyber threats, providing detailed and actionable information about the tools, techniques, and procedures (TTPs) employed by threat actors. This form of intelligence is crucial for enhancing an organization's ability to detect, respond to, and mitigate specific technical threats.
- Operational Threat Intelligence: Operational Threat Intelligence is a branch of cyber threat intelligence that focuses on providing actionable and tactical information to support day-to-day

cyber security operations. It involves the analysis of current threats, vulnerabilities, and ongoing incidents to enable organizations to respond effectively and enhance their security posture.

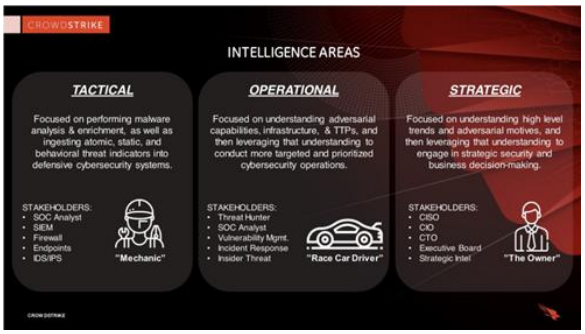


Fig. 1.1Threat Intelligence Classification

II. THREAT INTELLIGENCE LIFECYCLE

Threat Intelligence Life Cycle is a defensive mechanism to protect the organization from cyber criminals. It consists of following steps. The Fig 1.2 depicts the Threat Intelligence Life cycle.

Requirements: The requirements phase of the threat intelligence life cycle is the initial stage where the goals, objectives, scope and methodology for the process of collecting threat intelligence are planned out based on the requirements of key stakeholders involved. This phase is crucial for ensuring that threat intelligence processes correctly align with business and risk management objectives and provide output that can be considered by relevant stakeholders. It in involves identifying the type of intelligence that needs to be collected and the goal of the project and is essential for clarifying and scoping the intelligence needs of the organization.

Collection: The collection phase is a crucial stage in the Threat Intelligence Life cycle, where organizations gather information from various sources to build a comprehensive understanding of the threat landscape. The success of the entire threat intelligence process depends on the quality, relevance, and diversity of the collected data. This may include gathering intelligence on specific threat actors, tactics, techniques, procedures (TTPs), or emerging threats. Gather information from publicly available sources such as news articles, social media, and public databases. Acquire data from proprietary sources, threat intelligence feeds, industry forums, and information-sharing communities. Monitor alerts and advisories from government agencies, law enforcement, and cyber security organizations.

Processing: The processing phase in the Threat Intelligence Life cycle involves organizing, analyzing, and refining the collected data to extract meaningful insights and actionable intelligence. This phase is crucial for transforming raw information into a format that can guide decision-making and improve an organization's cyber security posture.
In this phase, the raw data collected during collection phase is filtered, structured, and enriched with contextual information. This phase is crucial for ensuring that the data is relevant, accurate and actionable for the analysis and production phase. It consists of following steps.

- Filtering: Relevant data is separated from irrelevant data, ensuring that only useful information is proceeded to the next phase.
- Structuring: The remaining data is structured to facilitate easier analysis and comparison during the production phase.
- Enriching: The data is enriched with contextual information, such as geographical data, company information, and threat actor profiles to provide a more comprehensive.

Analyzing: The analysis phase of the Threat Intelligence Life cycle involves interpreting and extracting meaningful insights from the processed data, turning it into actionable intelligence that can inform decision-making and enhance an organization's cyber security posture. The analysis phase plays a pivotal role in extracting meaningful insights from raw data, providing decision-makers with the knowledge needed to proactively defend against cyber threats. It requires a combination of technical expertise, critical thinking, and collaboration to effectively turn threat intelligence into actionable guidance for the organization.

Dissemination: In this phase, where the intelligence report is distributed to relevant stakeholders. During this phase, the intelligence reports are shared with the appropriate stakeholders such as security teams, executives and third-party vendors to inform decision making and response efforts. The dissemination phase

involves the use of various communication channels such as email, dashboards and reports to share the intelligence with the relevant stakeholders.

Feedback: The stakeholders provide feedback on the intelligence report to determine whether the analysis was timely, relevant and actionable. During this phase, stakeholders may have changes to their priorities or adjustments to how data should be disseminated or presented. The feedback gathered is used to refine the threat intelligence processes and improve the quality of the intelligence produced. Establishing performance metrics to measure the effectiveness of the threat intelligence and continuous improvement are critical during this phase.

Fig 2.1 Threat Intelligence Life Cycle

III BENEFITS OF THREA T INTELLIGENCE

Suppose the organization is practiced with CTI along with its security aspects the following benefits are obtained.

- Reducing Risk: The risk of data loss can be reduced, prevention or minimize disruption of business operations from cyber criminals and increase the understanding of threat and its future attacks can be obtained.
- Efficientt Resource allocation: CTI enables organizations to allocate resources more efficiently by focusing on the most relevant and critical security threats, potentially reducing overall cyber security costs.
- Enhanced security controls: When the CTI is integrated into an organization then the security response time and cut down time can be lowered. And also, the false positives are minimized as well.
- Investing wisely in infrastructure: When the CTI is landscaped in to organization then the relevant threats targeting the business can be identified and addressed based on the decision made by CTI.
- Lowering Expenses: The Business Expenses can be lowered when the proper CTI is activated and executed according to the stake holders' requirements along with risk can be mitigated. With this the efficiencies in financial and human resources can be increased.

IV THREAT INTELLIGENCE TOOLS

To stop cyber-attacks, business need to focus on CTI tools to be integrated in the organization. Few tools are described below.

- Authentic8: A remote and isolated browser that allows security teams to analyze suspicious information without exposing their identity or resources.
- Bit Defender: Bitdefender is known for its antivirus and anti-malware solutions, which aim to detect and remove a wide range of malicious software, including viruses, ransomware, spyware, and other types of malwares.
- ThreatConnect: ThreatConnect is a cyber security platform that provides solutions for threat intelligence, security orchestration, and risk management. The platform is designed to help organizations understand and mitigate cyber threats effectively.
- Recorded Future Fusion: Provides real time threat intelligence and research on cyber threats helping organizations stay informed about emerging threats and trends.
- SolarWinds: Offers security tools that provide real time visibility and control over application access, user activity and network traffic.
- CrowdStrike: Provides advanced threat protection, including threat intelligence, threat hunting and 24/7 threat response.
- Proof point: Offers a comprehensive threat intelligence solution that protects against phishing, malware and other advanced threats.
- Kaspersky Threat Intelligence: Kaspersky Threat Intelligence offers a range of solutions and services aimed at helping organizations detect, analyse, and respond to cyber threats.

V ISSUES AND CHALLENGES IN CTI

Considering the cyber security landscape, today's organizations consider CTI is a critical factor to reduce cyber risks, boost incident response and fortifying all the security challenges. However few challenges encountered when CTI is operationalized into an organization. Few are listed down along with the tackling those challenges.

Data overload and Noise: The security teams are overwhelmed when the flooding of data generated as CTI inputs from different sources. The CTI provides millions of threat indicators in order to solve the following risks arises from the CTI inputs.

- Numerous threats
- Vulnerabilities
- Breaches
- Threat Actors
- Filtering false positives

Which delays threat detection and response. This can be overcome by investing more on threat prioritization by the organization based on threat profile which results in more effective security strategies.

Maintaining quality and accuracy: There are considerable differences in quality and accuracy from the CTI feeds where organization rely on these feeds and generate false security decisions which in turn triggers inaccurate intelligence which increases the risk exposure and vulnerability to breaches. A high-quality CTI feeds have 6 properties.

- Applicable
- Accurate
- Timely
- Machine readable
- Consumable
- Actionable

To make high quality CTI feeds the organization must invest in reputable, feeds and regularly evaluate intelligence resources. Assessments identify the data quality gaps and enable informed decisions for effective CTI programs.

Addressing Resource constraints: CTI programs need appropriate tools with CTI feed subscriptions leads to organization struggle due to limited resources. To overcome this issue, organization should provide investment on specific threat landscape and allocate budgets that aligns with strategic security goals. The optimization of limited resources can be achieved by leveraging technology.

Bridging the expertise Gap: Many organizations lack in specific expertise to understand and analyze the CTI data. This may lead to missed threat or delaying in response or fails to act on specific threat indicators. To address this issue, organization should provide training and development for their security teams to provide specialized CTI insights and expertise.

VI MITIGATING THE CHALLENGES

Mitigating the challenges in cyber security involves the use of tools, processes and strategies to reduce the risk of potential cyber-attacks. This practice is essential in today's interconnected digital landscape, where no business is completely safe from the threat of cyber-attacks. Cyber threat mitigation empowers organizations to identify, respond to, and remove network threats, making ita top priority for successful organizations. It encompasses various elements or approaches, including threat prevention, detection and remediation. By implementing continuous risk assessments, establishing network access controls and conducting regular employee training, organizations can reduce their cyber security risk and protect their IT infrastructure.

According to the study of Hackers attack is existing for every 39 seconds on any day by A. James Clark School of Engineering, University of Maryland.

The best practices to overcome the cyber threat is given in fig 6.1&6.2,

Fig 6.1 & 6.2 Best Practices to overcome cyber threat

1. Set up Firewall:
Setting up a firewall is a crucial step in securing our computer or network from unauthorized access and potential cyber threats. Firewalls act as a barrier between our device or network and the internet, allowing or blocking data packets based on predetermined security rules.
Firewall software up to date to ensure it can effectively block the latest threats. Be aware of default settings and adjust them based on security needs. Regularly review of firewall logs to identify potential security issues. Firewall configuration is to be tested to ensure it behaves as expected without blocking essential services. Firewalls are just one component of a comprehensive cyber security strategy. In addition to a firewall, consider using antivirus software, keeping software updated, and following best practices for online security.

2. Anti-virus Program
To protect against cyber threats, using an antivirus program is essential. Anti-virus software helps detect, neutralize and remove malware, viruses and other online threats. It is recommended to choose a reputable antivirus program such as Bitdefender Antivirus Plus, AVG Antivirus or Microsoft Defender and ensure that is regularly updated to guard against the latest threats. The antivirus program should be configured to provide real-time prevention and automatic, constant scanning to prevent and remove threats. Additionally, it's important to practice safe computing habits such as keeping software up to date and avoiding suspicious links to enhance overall cyber security.

3. Home router maintenance
To safeguard home router, ensuring that the router is placed in a central location and that the firewall and Wi-Fi encryption are turned on. And also, strong Wi-Fi password to be created and changing default router login credentials are necessary. Additionally, guest network can be created. It is also recommended to disable Universal Plug and Play (UpnP) and remote administration there by denying unauthorized access to the router.

4, Reduction usage of public WiFi
When using public Wi-Fi, it is best to avoid it altogether or use a VPN to encrypt the internet traffic. It is important to choose a secure router such as recommended by Peplink routers and to keep it updated with the latest firmware.

5. Virtual Private Network
Using VPN, the cyber threats can be reduced but it is important to be aware of the potential dangers. VPNs can provide encryption, online privacy and device security. To use VPN safely, it is recommended to choose a reputable VPN provided, keep the VPN software up to date, and use a strong and unique password. It is also important to avoid using public Wi-Fi and to be aware of the limitations of VPNs.

6. Backup strategy
"Data loss is like doing your taxes: nobody likes it, but it's inevitable"
Develop a comprehensive backup strategy it includes regular backups, secure storage and rapid recovery protocols. Utilize a cloud back up service that offers end to end encryption, ensuring data remains secure as it moves to and from the cloud. Physical security of data centers should also be considered such as alarm system, armed guards, biometric scanners, locked server cabinets and backup generators.

7.Password Protection
Using strong password is an important step in protecting from cyber threats. Here are some tips for creating strong passwords:

- Use a password manager: Remembering long, random and unique password for every account is not possible. Rather that writing them down, use a password manager to generate and store strong passwords.
- Make them unique: Avoid using the same password across multiple accounts. If one account is

compromised, having unique passwords for each account helps prevent further security issues.

- Use Passphrases: Consider using passphrases like a sequence of words or a sentence. Passphrases are easier to remember and can be just as secure as complex passwords.
- Long Passwords are stronger: Avoid using commonly used passwords, such as "password," "123456," or "admin." These are easy targets for attackers.
- Change them regularly: Change passwords periodically, especially for sensitive accounts. Regular changes reduce the risk of unauthorized access.
- Use strong passwords: Create passwords that are complex and not easily guessable. Use a combination of uppercase and lowercase letters, numbers, and special characters. Avoid easily guessable information like names, birthdays, or common words.

8. Locking device

To lock the device, we can use the built-in features of device's operating system or a third-party app. For example, on Android devices, we can use the "Find My Device" feature to remotely locate and lock device. On iOS devices, we can use the "Lost Mode" feature in iCloud to lock your device. To set up a lock on your device, we can use a PIN, pattern, password or biometric authentication such as fingerprint or facial recognition.

9.Beware of phishing attacks

Phishing attacks are a common and effective method used by cyber criminals to trick individuals into revealing sensitive information, such as usernames, passwords, and financial details. Treat unexpected emails, messages, or calls with caution. Cyber criminals often use unsolicited communications to initiate phishing attacks. Verify the sender's email address carefully. Pay attention to misspellings or variations that may indicate a fraudulent sender. Hover over links in emails to preview the actual URL before clicking. Ensure that the URL matches the official website of the organization purportedly sending the message. Watch for signs of phishing, such as generic greetings, spelling and grammar errors, urgent requests, and unexpected attachments or links. Do not click on links or download attachments in emails, messages, or social media posts from unknown or unverified sources. Legitimate organizations typically do not request sensitive information like passwords or credit card details via email. Verify such requests through official channels before responding.

10. Attack surface reduction

In an Enterprise network the attacker gains unauthorized access in certain surface. This surface to be reduced to mitigate the cyber risk. This can be achieved by monitoring the inventory control of the enterprise assets and applications. The no longer applications can be removed. Different tools involved to find the attack surface clearance. Penetration test and Cyber risk quantification solutions help to identify, prioritize and to remediate vulnerabilities.

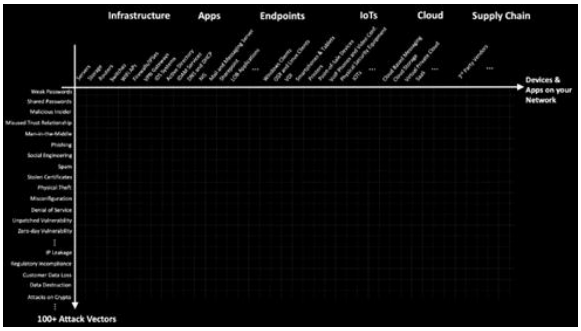


Fig 6.2 shows attack surface parameters.

11.Planning the Incident Response

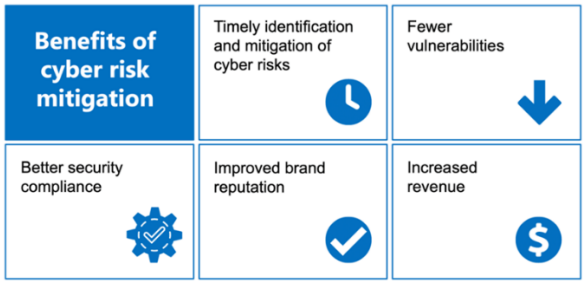
Incident Response Plan is achieved by writing set of instructions which outlines the enterprise response in case of data breaches or data leaks. By doing this further damage can be reduced and easily recover and resume its operations. A proper Incident Response Plan allows to minimize the losses and restore affected system and process. It can be used to find the root cause of the threat and provide the post incident recovery plan.

VII THREAT MITIGATION BENEFITS

Threat mitigation refers to the actions and strategies taken to reduce or eliminate the impact and likelihood of cyber security threats. Implementing effective threat mitigation measures comes with several benefits for organizations. By implementing continuous monitoring tools, organizations can constantly look for vulnerabilities within their network instead of

periodically, leading to increased protection of IT infrastructure. Additionally, a robust risk management strategy enables organizations to protect and maintain their business reputation, enhance IT team support, and meet their security goals and performance objectives.

- Enhanced security postures: Threat mitigation measures contribute to an overall improvement in the organization's security posture. By addressing vulnerabilities and potential risks, the organization becomes more resilient to cyber threats.
- Risk Reduction: Threat mitigation helps reduce the level of risk associated with potential security incidents. Proactive measures can prevent or limit the impact of threats, minimizing the likelihood of data breaches, system compromises, or other security incidents.
- Protection of Sensitive Information: Mitigating threats helps protect sensitive information, including customer data, intellectual property, and proprietary business information. This safeguards the organization's reputation and builds trust with stakeholders.
- Business Continuity: Mitigating threats helps protect sensitive information, including customer data, intellectual property, and proprietary business information. This safeguards the organization's reputation and builds trust with stakeholders.
- Improved Incident Response: Threat mitigation measures, including incident response plans, enhance an organization's ability to effectively respond to and recover from security incidents. This reduces the time it takes to contain threats and restore normal operations.



VIII CONCLUSION

Cyber Threat Intelligence (CTI) plays a critical role in contemporary cyber security strategies, providing organizations with the necessary insights to understand, detect, and respond to evolving cyber threats. The proactive and informed nature of CTI empowers organizations to stay one step ahead of cyber adversaries. In a digital landscape where cyber threats continue to evolve in complexity and sophistication, Cyber Threat Intelligence emerges as a strategic asset. Organizations that integrate CTI into their cyber security framework are better equipped to navigate the dynamic threat landscape, protect critical assets, and maintain the trust of stakeholders in an increasingly interconnected world.

REFERENCES

[1] D. Gavriluț and M. Cimpoeșu, "Malware detection using machine learning," in Proc. Int. Multiconference on Computer Science and Information Technology (IMCSIT), 2009, doi: 10.1109/IMCSIT.2009.5352759.
[2] P. Chadha, "The Four Phases of Crisis Management," blog post, Oct. 6, 2020.
[3] T. Morar and A. Nelson, "The Global Cyber Threat to Financial Systems," IMF Finance & Development, Spring 2021.
[4] G. Goldstein, "How Threat Intelligence Drives Efficiency in an Economic Downturn," Jun. 8, 2023.
[5] "Intelligence and Evidence Gathering," Authentic8 OSINT Investigation Platform.
[6] "ThreatRadar: Web Application Threat Intelligence," Imperva ThreatRadar PDF.
[7] Bitdefender, "Global leader in cybersecurity protecting consumer and business environments since 2001."
[8] ThreatConnect, "Smarter security, maximum impact."
[9] Anomali, "Detection to resolution in seconds."
[10] C. Ahlberg, "Threat Intelligence: Putting It All Together," Jan. 29, 2018. Available: Recorded Future
[11] SolarWinds, "Hybrid cloud observability and IT management platform."
[12] CrowdStrike, "The Forrester Wave™ for External Threat Intelligence Services Providers 2023."
[13] Proofpoint US, "Cybersecurity Threats & Attacks – Threat Reference."
[14] Kaspersky Threat Intelligence Portal, "Threat Intelligence Portal — Analysis."

[15] "Cyber Threat Intelligence – Issue and Challenges," Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, pp. 371–379, Apr. 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.