International Journal of Computer Science and Information Technology Research (IJCSITR)
2022, Vol. 3, No. 1, Jan – Dec, pp. 17-21
Journal ID: 9471-1297
website: www.ijcsitr.com

Optimizing Security Controls: Aligning Threat Intelligence with NIST CSF for Effective Decision-Making

ShivaDutt Jangampeta[1] & Sai Teja Makani[2]

[1]Senior Manager of Security Engineering, JPMorgan Chase, Plano, USA.
[2]Senior Manager, DevOps, Spotter Inc, Culver City, CA.

Abstract

In today's era of increased digital vulnerability, there is an immense need for the implementation of robust security measures. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides security experts and organizations with elaborate guidance on handling their security risks based on several fundamental functions. Lately, integrating cyber threat intelligence (CTI) has become a fundamental subject in information security, evolving with augmented supply chains and sophisticated hackers' tactics. Nonetheless, threat intelligence is not only critically useful for the detection or identification of threats, but can also be aligned with all phases of cybersecurity processes to have a consequential impact on security risk prediction and mitigation. This review discusses how organizations can optimize their security controls by aligning threat intelligence with NIST CSF.

Keywords

National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF), cyber threat intelligence (CTI), indicators of compromise (IOCs), security incident

*Corresponding author: *ShivaDutt Jangampeta*

How to Cite: Jangampeta, S., & Makani, S. T. (2022). Optimizing security controls: Aligning threat intelligence with NIST CSF for effective decision-making. *International Journal of Computer Science and Information Technology Research (IJCSITR)*, *3*(1), 17-21.

Article ID: IJCSITR_2022_03_01_003
Article Link: https://ijcsitr.com/index.php/home/article/view/IJCSITR_2022_03_01_003

I. INTRODUCTION

Cyber Threat Intelligence, or CTI is the knowledge or information collected regarding potential security threats and threat actors in a bid to bolster proactive information security controls. Fundamentally, threat intelligence encompasses the gathering, analysis, and review of cyber threat information and its modification into practical intelligence. CTI helps security teams understand hackers' tactics, techniques, and procedures (TTPs), motivations, and security risks they present to an organization [1].

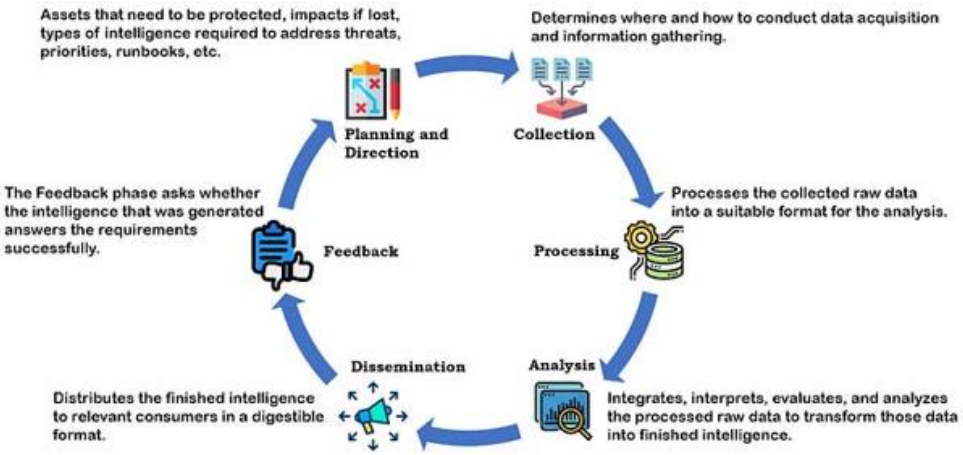

Figure 1. Threat Intelligence cycle

CTI features a broad range of information, such as indicators of compromise (IOCs), like malicious internet protocol (IP) addresses and file/domain hashes. Additionally, it covers contextual information regarding threat actors, hackers' infrastructure and tools, as well as security vulnerabilities exploited by the bad actors. It can be acquired from various sources, like open-source intelligence (OSINT), incident response information, dark web monitoring, commercial threat feeds, and collaborative data sharing platforms. CTI plays an important role in a business's overall cybersecurity response, such as threat identification, vulnerability management, threat mitigation, and incident response. It helps security teams make informed decisions regarding the deployment of security controls, bolstering their defense systems' capabilities, and prioritizing information security investment.

2. Using NIST CSF Framework to Integrate Threat Intelligence into Organization's Security Controls

While the choice of a CTI-based approach depends on an organization's cybersecurity maturity, the NIST CSF framework can be used to point out when and how to leverage threat intelligence. Typically, the NIST CSF framework features five core functions, including Identify, Protect, Detect, Respond, and Recover, and can be used to develop an exhaustive cybersecurity plan [2]. NIST CSF functions guide security teams to assess security risks, implement protective measures, identify and respond to security events, and recover from security incidents. The alignment of CTI with NIST CSF can be critically consequential in the

enhancement of an organization's level of cybersecurity maturity.

Figure 2. NIST CSF functions

A. Identify

Using threat intelligence, businesses can easily *identify* the most vulnerable informational assets that threat actors regard as lucrative, assess their susceptibility level, and prioritize security controls accordingly. For instance, threat intelligence offers insights regarding information leaks that may result in data breaches [3]. Additionally, it helps security teams monitor the company's cybersecurity regulatory requirements and assess security risks posed by supply chains and vendors. Threat intelligence helps firms maintain an up-to-date inventory of data assets, identify specific assets that require enhanced protection, and ensure the implementation of appropriate security measures.

B. Protect

Threat intelligence helps organizations proactively deploy peculiar security controls depending on the specific threats faced. For instance, organizations can leverage threat intelligence feeds to identify familiar indicators of compromise (IOCs) and deploy proactive security measures like access controls, security configurations, and patch management in a bid to *protect* their system from known threats. Additionally, organizations can leverage threat intelligence to educate their staff on emerging threats, attack methods, and social engineering techniques to reduce their impact.

C. Detect

Threat intelligence is a fundamental enabler of threat detection. Organizations can integrate CTI with security monitoring systems to enable early detection of security threats and

malicious activities, allowing expeditious incident response. For instance, organizations can leverage threat intelligence to detect security flaws in their authentication architecture, detect unwarranted access attempts, monitor for malicious activities, and even update access privileges. Also, companies can use CTI to detect IOCs, anomalous behavior, and emerging threats that might circumvent conventional security controls.

D. Respond

Threat intelligence provides vital information during security events to allow effective incident response (IR). Organizations can leverage CTI to understand the techniques/tactics adopted by threat actors, the nature of security incidents, and IOCs to effectively *respond to* security events using pre-set measures and playbooks. Besides, threat intelligence facilitates constant enhancements in incident response efficiency by generating feedback and knowledge acquired from past events [4]. Threat intelligence allows security professionals to correlate the detected activities with intellect, spot patterns, and extract insights to guide their investigative endeavors.

E. Recover

Constructive communication is paramount during the recovery stage as it guarantees alignment between security experts and the organization's stakeholders, and threat intelligence facilitates this by offering real-time information about the security event, recovery progress, and any developing threat. Additionally, threat intelligence offers invaluable insights for performing an all-inclusive root cause assessment of security events.

3. CONCLUSION

Threat intelligence enables businesses to be proactive rather than reactive when dealing with cyber-attacks. The failure to effectively understand security gaps in a data system, threat indicators, and TTPs adopted by cybercriminals is an indication of incompetence and lack of preparedness to tackle security incidents. Threat intelligence enables security teams to swiftly contain cyber-attacks and save the organization thousands of dollars, preserve its reputation, prevent insolvency, and more importantly, prevent data compromise.

With threat intelligence, security teams can acquire the understanding to empower them to avoid or mitigate potential security attacks on their network. Cyber threat intelligence is viewed as an integrated, valuable tool that facilitates the development of an effective cybersecurity strategy that can detect, protect, mitigate, respond, and recover from adversary impacts of cyber-attacks.

References

[1] D. Blum, Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment, Apress, 2020.

[2] J. N. M. Dahj, Mastering Cyber Intelligence: Gain Comprehensive Knowledge and Skills to Conduct Threat Intelligence for Effective System Defense, Packt Publishing, 2022.

[3] I. Richard O. Moore, Cyber Intelligence-Driven Risk: How to Build and Use Cyber Intelligence for Business Risk Decisions, Wiley, 2020.

[4] Carol A. Siegel, Mark Sweeney, Cyber Strategy: Risk-Driven Security and Resiliency, Taylor & Francis Limited (Sales), 2020.