International Journal of Computer Science and Information Technology Research (IJCSITR)
2024, Vol. 5, Issue. 1, (Jan-June) pp. 11-14
Journal ID: 9471-1297
website: www.ijcsitr.com

The Future of Threat Intelligence-Driven Security: Integrating Emerging Technologies for Enhanced 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.USA.

Abstract

From identity theft to disinformation and social engineering schemes, threat actors and state-sponsored hacker groups continue to ravage businesses and disrupt critical government operations. With world uncertainties around warfare, economy, and politics, the increasingly sophisticated threat environment is becoming more overwrought with cyber risks – and the tremendous development of advanced technologies like generative artificial intelligence (GenAI) has become a major cause of concern. In the future, we anticipate witnessing state-sponsored hacker groups leveraging artificial intelligence to launch successful disinformation campaigns, to interfere with electoral processes. We also expect threat actors will use scaled spear-phishing schemes, augmented with various social engineering tactics to imitate senior company and government officials to steal sensitive information. Nevertheless, we expect industry leaders will leverage modern technologies to bolster information security defenses, resulting in enhanced decision-making.

Keywords

cyber threat intelligence (CTI), threat intelligence-driven security, threat intelligence (TI), emerging technologies

*Corresponding author: Arjun Krishnaiah Somanakoppa

How to Cite: Jangampeta, S., & Makani, S. T. (2024). The future of threat intelligence-driven security: Integrating emerging technologies for enhanced decision-making. International Journal of Computer Science and Information Technology Research (IJCSITR), 5(1), 11-14.

Article ID: IJCSITR_2024_05_01_002

Article Link: https://ijcsitr.com/index.php/home/article/view/IJCSITR_2024_05_01_002

1. Introduction

Threat intelligence (TI) has become a critical component of cybersecurity in most organizations, allowing them to collect and analyze information to acquire insights into cybersecurity threats. Specifically, cyber threat intelligence (CTI) has gone a long way from the earlier manual data analysis techniques to more sophisticated technologies like machine learning (ML) and artificial intelligence (AI). Nevertheless, the technology still faces various challenges, like inadequacy of information standardization and the difficulty in determining the credibility of data sources. Addressing these concerns calls for the integration of CTI with consistent information-gathering and analysis techniques.

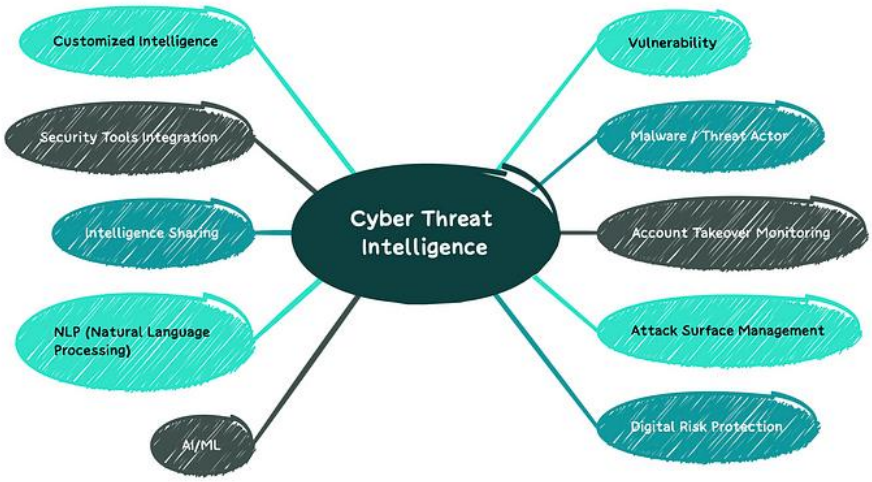

Figure 1. CTI mindmap

The future of threat intelligence-driven security is anticipated to incorporate many sophisticated technologies and tools, like automation and predictive analytics. Additionally, threat intelligence-driven cybersecurity is anticipated to be more firmly integrated with tools like security information and event management (SIEM) to offer more exhaustive visibility into the cyber threat landscape. Besides, the development of state-of-the-art solutions like quantum computing and blockchain is expected to impact CTI as well.

2. Emerging Technologies for Enhanced Decision-Making

A. Artificial intelligence (AI) and Machine learning (ML)

AI and ML technologies will revolutionize threat intelligence-driven cybersecurity by enhancing their capability to process huge volumes of information at unprecedented speeds. The solutions will enable more complex analytics, forecasts, and automation, making threat safeguards more promptly and actionable.

B. Automated Threat Hunting

Automated threat-hunting techniques, powered by real-time intelligence will enable precise

scanning of networks to detect indicators of compromise (IOCs) even before the actual threat is realized.

C. Customization of CTI tools

CTI tools are anticipated to offer remarkable customization and individualization options, enabling organizations to tailor threat mitigation tools to fit their respective industries, threat profiles, security requirements, etc. This will make threat intelligence-driven cybersecurity more actionable.

D. Zero Trust

Zero Trust implies a security model designed to presume that all network traffic, both inbound and outbound is potentially harmful and shouldn't be trusted by default. Rather, all requests to access organizational informational assets must be authenticated, authorized, and substantiated before granting access. The zero-trust approach is meant to minimize the attack surface while reducing the risk of security breaches [1]. Recently, this security approach has become progressively popular in the world of business. By incorporating zero trust into threat intelligence-driven security, businesses will ensure that they can access information regarding emerging cyber threats and configure appropriate security controls to mitigate them.

Figure 2. Zero trust security

The advanced security model will help businesses identify and respond to security incidents, like identity theft attempts, security breaches, social engineering campaigns, and various malicious actions before they can cause substantial damage. For instance, if the security team gets a threat intelligence alert regarding emerging malware targeting a particular application, security analysts can promptly take appropriate measures to patch existing vulnerabilities or update security policies to mitigate the threat. Correspondingly, if an establishment gets notified of a potential data breach, it can promptly leverage threat intelligence to determine the severity and scope of the breach and take proper measures to contain the menace [1]. The future integration

of CTI and advanced technologies will help organizations identify and prioritize resource allocation in terms of cybersecurity investments based on the most critical cyber risks to their informational assets and business operations. Consequently, organizations can reap hugely from this approach and enable business leaders to make data-driven decisions regarding how/where to allocate informational resources and mitigate potential cyber risks.

E. Environmental, social, and governance (ESG)

Lately, organizations have heightened their awareness of the impact of Environmental, social, and governance (ESG) factors on business. Essentially, the ESG is a collection of criteria adopted by stakeholders and investors to estimate the influence of their company on Environmental, social, and corporate governance. Cybersecurity posture is a critical ESG factor that most organizations are paying attention to. It is anticipated that in the future threat intelligence-driven cybersecurity will play an essential role in promoting organizations' ESG goals by aiding to identify and thwart cyber threats that adversely impact an organization's operations. For instance, a security event on an organization's data system could lead to a data breach exposing valuable, sensitive customer data, resulting in hefty financial losses and ruining customer confidence. Consequently, both society and the environment will be negatively affected as customer trust in the company will be eroded. Similarly, threat intelligence may be leveraged to monitor abuse in the brand websites and phishing campaigns that imitate an organization's brand to market fake goods/services or steal personally identifiable information (PII) from clients. These cyber-attacks may cause reputation harm to businesses and ruin brand trust, resulting in adverse effects on the organization's ESG goals.

Integrating a company's ESG goals with threat intelligence will help organizations monitor abuse platforms, phishing schemes, and other malicious activities, enabling them to safeguard their customers' privacy and sensitive data, and preserve their reputation as trustworthy, responsible corporate patriots.

Conclusion

The future of threat intelligence-driven cybersecurity is marked by technological advancement, integration, and strategic collaboration into wider enterprise and security approaches. As businesses navigate the evolving threat environment, staying abreast of the merging trends will be critical to fostering their security stance and resilience against cybersecurity threats.

References

[1] Rebekah Brown, Scott J. Roberts, Intelligence-Driven Incident Response, O'Reilly Media, 2023.

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