The Monetization of Threat Intelligence as a Part of the Digital Economy

Denis Petkov

Abstract*: *The ongoing process of monetizing threat intelligence (TI) is increasingly viewed as a cardinal factor in the cybersecurity sector, with cybersecurity brokers being the main driving force behind it. With the rise of the digital economy, society is becoming increasingly reliant on threat intelligence when it comes to maintaining resilient and modern business operations. The following research examines in what manner cybersecurity brokers collect, analyze and distribute threat intelligence in order to elevate decision-making and foster growth in both private and public sector. Furthermore, the study includes how brokers monetize TI, the business models they employ as well as the added stakeholder value. A mixed-methods approach is used by the author by including case studies of EDIH Trakia's CYBER4ALL STAR project, which shed light on the effectiveness and accessibility of threat intelligence on the small-to-medium enterprise (SME) level. The key insights of the paper highlight how stakeholders use threat intelligence in order to foster a more rational approach to allocation of resources effectively, development of a robust cybersecurity posture and to voice ethical and legal concerns regarding privacy and transparency of data. The conclusion focuses on the need for a stronger regulatory initiative when it comes to efforts in ensuring a responsible monetization of TI in the scope of a continually growing cybersecurity market.

Keywords* : *Cybersecurity brokers, Cyber Threat Intelligence, Digital Economy, Monetization, Proactive solutions

I. INTRODUCTION

The interconnectedness of the digital economy is actively transforming business operations on a global scale, granting stakeholders the ability to collaborate through modern solutions such as vast data networks, systems and applications. While having significant benefits, this process contains intrinsic vulnerabilities for institutions of all sizes. Modern vulnerabilties of this sort include a plethora cyberattacks, ranging from ransomware to sophisticated corporate espionage. The volume of such cyberintrusions is escalating in both boldness and complexity, therefore generating substantial risk for the modern business climate. As a result, the demand for cybersecurity measures which are proactive in nature as surged, thus elevating the search for Threat Intelligence (TI), an asset often defined as the bedrock of contemporary digital security strategies.

Threat Intelligence (TI) refers to the cyclical algorithm of collecting, analyzing and putting to use data assets regarding potential or emerging cyberthreats. The objective of TI is to empower stakeholders by providing actionable insights which assist in the anticipation, mitigation and control of digital risks. Furthermore, Threat Intelligence delivers a complex understanding of an adversary's preffered modus operandi by laveraging a multitude of data sources – open web, dark web forums and proprietary channels. Thanks to this model, institutions change reactive measures into a stance of proactive security, staying ahead of potential threats and thus highlighting the transformative potential of Threat Intelligence.

The business potential of Threat Intelligence and its wide applications in the private sector elevate its unique dual nature of serving both as a defensive tool and as a strategic business asset. On an operational level, TI bolsters organizational security by reducing threat exposure, improving response times and enhancing the overall security posture. Strategically speaking, Threat Intelligence delivers value as an asset which can be capitalized and marketed due to its provision of competitive advantages. Enterprises offering such solutions are faced with the opportunity of transforming and thus monetizing raw data into products and services. As for the benefits available, they are not limited to fiscal gain, as TI can also serve as a boon to corporate reputation, customer trust and stakeholder confidence.

The goal of the paper you are reading is to explore the transformative role of threat intelligence as a part of the broader spectre of the digital economy and to emphasize its inherent potential as a monetizable asset. This is achieved by the definition of business applications and monetization models. The research also points that while it is indispensable for business operations and cybersecurity, TI also introduces ethical and legal dilemmas which require careful navigation.

II. THREAT INTELLIGENCE AND KEY BENEFICIARIES

The concept of Threat Intelligence in cybersecurity encompasses the use of evidence-based knowledge when safeguarding assets and informing decision-making. This becomes possbile thanks to insights derived from indicators of compromise, adversary operations, procedures and contextual threat data - gathered from open sources, dark web activity or shared, following a stakeholder agreement. The core idea behind TI is to provide organizations with the intel they needed when combatting threats, sometimes before they even materialize. On an operational level, the model focuses on real-time responses to immediate risks like identifying and neutralizing ongoing phishing schemes or ransomware campaigns. On the other hand, the strategic side of TI boosts the processes of long-term goal setting and decision-making. Often times, this type of TI focuses on the emerging threat landscapes and on industry-specific trends and vulnerabilities.

Threat Intelligence can be defined as a critical pillar of the modern digital economy due to its beneficiaries being located across various sectors and levels of society. Following this statement, the private sector has the opportunity to use TI as a means of reducing cyber risk exposure, to enchance decision-making processes and to refine resource allocation –

thanks to TI, companies can deploy tailored cybersecurity measures and thus cut costs. On the other hand, the public sector employs Threat Intelligence to enchance proactivity in the processes of protecting public infrastructure, mitigating cyberincidents and protecting citizen data.

On a day-to-day basis, threat data fosters trust in digital ecosystems. This becomes possible thanks to the indirect protection of service, comunnication and transaction platforms which customers interact with. A clear example of this are the safer online banking services and "safehaven" social networks who have gone a step ahead of cyberrisks by investing and becoming an proactive beneficiary of Threat Intelligence. By doing so, such stakeholders have not only gained the competitive advantages of business resilience and informed planning, but also sent a clear message to competitors, lacking behind in the digitalization race.

III. THE THREAT INTELLIGENCE CYCLE

The cycle of TI consists of six separate stages – Direction, Collection, Processing, Analysis, Dissemination and Feedback. In the Direction stage, specific organizational goals are being laid down and alligned with intelligence capacity, organizational priorities and stakeholder context. During the following stage – Collection, raw data is inflowing from a diversity of sources such as open-source platforms, dark web sites and more. As an example, a cybersecurity team might be tasked with monitoring such sources in an attempt to detect mentions of data leaks related to their institution.

After the accumulation of raw data is complete, it passes through the Processing phase, where it is destilled and in essence made applicable. Following that, the data asset goes through the Analysis stage where efforts are made in order to identify patterns, assess potential risks and generate an usable and therefore monetizable product. For example, this could be shown as pinpointing a concrete malware strain targeting specific sectors or industries. At this stage of the cycle, brokers of cybersecurity can step in deliver expertise through ensuring accuracy and relevance for different use cases.

The following Dissemination stage is where the TI is made accessible to relevant stakeholders, be it their executive leadership, management or IT and CS teams. Cybersecurity brokers are critical in this stage, as they contribute to matchmaking by knowing the right time, the right data format and the right recipient for the right information package. At the end of the cycle is the Feedback stage where evaluation and future integration is done with the means of refinement of future efforts.

IV. MONETIZATION MODELS

The key factor for monetizing Threat Intelligence is hidden in closing the divide between intelligence gathering and actionable implementation. Therefore, a certain few monetization models have emerged as dominant strategies – licensing platforms, subscription-based feeds and data partnership, each with its selling points in order to deliver tailored, scalable and impactful solutions. Of course, one cannot leave cybersecurity brokers out of the equation as they are essential facillitators in the process, solidifying the interplay between monetization and brokerage services.

The first model, Licensing Platforms provides stakeholders with advanced Threat Intelligence capabilities through the use of a software platform. Such solutions are easy to distribute as they integrate easily the use of TI into already existing cybersecurity frameworks. Of course, licensing agreemets come with customization options so the benefitiary gets their industry-specific needs met, whereas on the other side the TI distributor generates a steady revenue stream.

Consequently, Subscription-based feeds allow for real-time tailored updates in an approach that is valuable for stakeholders who require continious and dynamic updates in their operations. The intelligence bulletin has the potential to be curated by sector, by industry or by a client-specific degree of segmentation, requested by the customer. For example, a payment provider subscribed to such a feed is going to receive an early warning, highlighting the specifics of an ongoing phishing campaign targeting customers from their sector. The selling point of this model is its scalability potential, which in turn makes it perfect for small and medium enterprises (SMEs) as the providers can specifically target customer needs and fit budged constraints. It is important to note, that the model creates an opportunity for cybersecurity brokers to step in and present bundled or tiered subscription packages that in turn can reach a broader customer segment and remove the need for budged overextending.

The third model, Data Partnership, envisions the aggregation of large quantites of data through the collaboration between multiple stakeholders for the common goal of identifying systemic risks across sectors and fostering sector stability. Of course, the use of such volume of Threat Intelligence in a shared environment requires adherence to strict data security standards, which are ultimately justified due to the potential of such collective cybersecurity efforts.

An examplary model of Threat Intelligence delivery to a multitute of stakeholders is that of The European Digital Innovation Hub Trakia, located in Bulgaria. By laveraging access to cybersecurity solutions such as TI in the form of state aid, the EDIH grows the Threat Intelligence market in the region by helping SMEs understand the value behind cybersecurity and the potential of TI. Moreover, by joining the Cyber4All STAR ecosystem a stakeholder contributes not only to the bridging the digital gap in the South-Central Region of Bulgaria, but also gains access to a regular communication channel used by the DIH to share cybersecurity-related information and updates.

V. CHALLENGES TO & IN THE MONETIZATION PROCESS

There are no single thoughts that the process of monetizing Threat Intelligence can be undertaken and optimized without any ethical challenges arising, especially from the misuse of the intelligence shared. The main concern in this context is the risk of external actors obtaining Threat Intelligence data, be it through security breaches or the employment of social engineering.

Secondly, a following ethical concern is whether the cycle of threat intelligence has been completed in adherence to ethical standards and not in prioritization of profit over integrity and legitimacy.

Furthermore, fair practices have to be kept at a high standard – selling intelligence disproportionately or categorizing stakeholders by their financial capacity is bound to leave vulnerable institutions exposed to potential threats.

VI. CONCLUSION

The competitive edge and economic value gained through the dual potential of Threat Intelligence as a service are going to escalate the search and the process of its monetization. The TI concept surpasses its initial purpose as an enabler of proactive cybersecurity measures in order to grow into a business asset, capable of being a boon to business operations on every enterprise level. Central to this evolution are the brokers of cybersecurity services who curate, standardize and distribute intelligence by taking on the role as middlemen who stakeholders can trust.

Looking forward, the monetization of TI is greater than a business plan – it is a business-oriented roadmap. By allocating resources in licensing platforms, subscription feeds and data partnerships public, private and governmental actors lay the groundwork for cyberintelligence ecosystems, which enforce the belief that the pursuit of profit should never compromise transparency. Furthermore, public-private partnerships are integral for bridging the digitalization gap in its ability to safeguard today while strenghtening tomorrow.

REFERENCES

[1] CyberEdge Group, LLC. (1997). The Threat Intelligence Handbook. Moving Toward a Security Intelligence Program.

[2] Dykstra, J., Gordon, L.A., Loeb, M.P. and Zhou, L. (2022). The Economics of Sharing Unclassified Cyber Threat Intelligence by Government Agencies and Departments. Journal of Information Security , 13, 85-100. https://doi.org/10.4236/jis.2022.133006

[3] European Digital Innovation Hub Trakia. (2021). Digital Europe Programme (DIGITAL) Dissemination and Exploitation Plan D 2.2

[4] Mavroeidis, V. & Bromander, Siri. (2017). Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. European Intelligence and Security Informatics Conference

[5] Даскалов, Х & Атанасов, С. (2024). КИБЕРПОЛИГОНЪТ НА ЕЦИХ ТРАКИЯ ПО ПРОЕКТ „CYBER4ALLSTAR“ КАТО СРЕДА ЗА РАЗВИТИЕ НА ЕКСПЕРТИ В СФЕРАТА НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ В ЮЖЕН ЦЕНТРАЛЕН РЕГИОН“

[6] Даскалов, Х. (2024). ЕВРОПЕЙСКИЯТ ЦИФРОВ ИНОВАЦИОНЕН ХЪБ ТРАКИЯ И ПРАВОТО НА (САМО)ЗАЩИТА В ДИГИТАЛНОТО ПРОСТРАНСТВО

AUTHOR PROFILE

Denis Petkov is an emerging professional, backed by a solid academic foundation and a profound commitment to initiatives which deliver impact to the public. A distinquished student of the The Faculty of economics and social sciences (FESS), he holds a master’s degree in Cybersecurity, awarded by Plovdiv University “Paisii Hilendarski”. The professional and academic life of Denis both focus on the business-oriented side of Cybersecurity, namely cybersecurity monetization and brokerage. Currently employed as a Senior Expert in Academic Relations at the Trakia Digital Innovation Hub, Denis specializes in the facilitation of collaborative cybersecurity-oriented efforts between the Academic sector and a multitude of stakeholders. Moreover, he holds several certifications in the Cybersecurity sphere, issued by prestigous academic entities such as the University of Maryland, New York University and the University of London. Valedictorian of The Faculty of economics and social sciences in 2024 and Student of the Year in 2023, Denis is dedicated to both professional and community engagement.