Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity

Jyri Rajamäki and Krista Tiitta
Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
krista.tiitta@student.laurea.fi

Abstract: This work-in-progress paper addresses the need to improve intelligence processes and enhance an organization's response to cyber threats while managing associated risks and improving Business Continuity Management (BCM). The paper focuses on the role of Open-Source Intelligence (OSINT) in Cyber Threat Intelligence (CTI) gathering and presents an operational process for its implementation. The process includes defining goals, selecting open sources, data collection, filtering, analysis, and reporting. Testing in an international financial sector organization yielded positive results, demonstrating the process's value in threat intelligence. Future research should clarify the role of artificial intelligence in OSINT.

Keywords: Business continuity management, Cybersecurity, Cyber threat intelligence, Design science research, OSINT

1. Introduction

The fundamental pillars of information and cybersecurity include ensuring and protecting the confidentiality, integrity, and availability of data. Organizations are tasked with securing their information as effectively as possible, which also includes protecting their IT infrastructure and personnel while minimizing the attack surface. Failure to secure and protect information can have significant financial implications, additional work for staff, legal repercussions, and damage to the organization's reputation (Gatlin, Yampolskiy & Yung, 2021). Cyber Threat Intelligence (CTI) is information based on knowledge, skills, and experience that helps reduce potential attacks and malicious events in cyberspace (DYNAMO, 2023).

The case organization - an international player in the financial sector - had recognized weaknesses and deficiencies in utilizing open-source intelligence (OSINT), and there were no established processes related to it. For this reason, a Design Science Research (DSR) project shown in Figure 1 was launched to design a new operational process for the case organization.

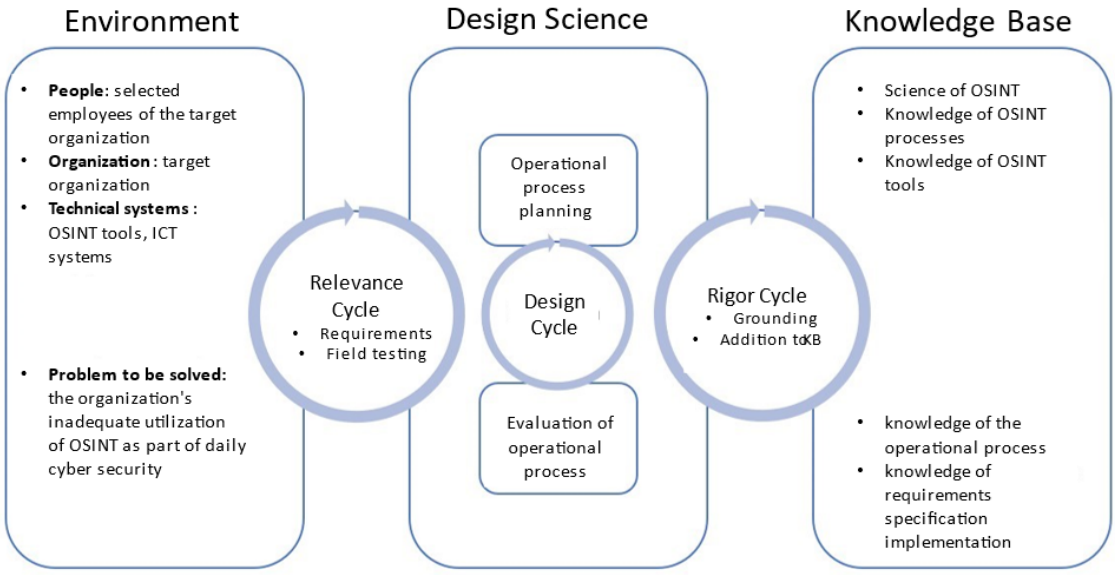

Figure 1: The DSR framework applied in the study (modified from Hevner, 2007)

To maintain anonymity in this study, the requirement specification for the OSINT intelligence operational process is presented in a simplified manner. The requirement specification defines the needs and starting point for process planning. The starting point and needs for process planning in this study are based on the case organization's requirements and the real problem. The goal is to develop a functional, clear, and efficient operational OSINT process. The requirement specification also includes a general description of the process,

which covers the scope of the operational process, functionalities, users, constraints, functional requirements (what the process includes and what is required for it to meet its intended purpose), and non-functional requirements (scalability, performance, and usability, i.e., qualitative requirements).

2. OSINT

Open Source Intelligence (OSINT) is a multifaceted concept that encompasses the systematic collection and analysis of information obtained from publicly accessible and legally obtained sources. These sources span a broad spectrum, ranging from the digital realm, including the Internet and social media, to more traditional media channels such as newspapers, magazines, television, and radio. The key characteristic of OSINT is its inclusivity, as it extends to any information or data that is available to the public. This inclusivity is particularly relevant in the contemporary era, given the exponential growth of open-source information facilitated by the widespread use of digital platforms, with social media platforms being a prominent contributor to this abundance of data (Akhgar & Bayerl, 2015; Azzopardi et al., 2014).

The pervasive use and accessibility of the Internet have fundamentally altered the way individuals and organizations communicate and share information. The advent of social media platforms and real-time messaging services has ushered in a new era of instantaneous interaction. However, this convenience comes with risks, as it has led to the inadvertent exposure of sensitive information. This unintentional disclosure has raised concerns about the potential misuse of such data, including its exploitation for nefarious purposes like harassment, terrorism, or identity theft (Azzopardi et al., 2014).

OSINT has evolved into a pivotal tool in various security and intelligence operations. It finds applications in diverse fields, including criminal investigations, counterterrorism efforts, the monitoring of Advanced Persistent Threat (APT) actors (i.e., sophisticated hacking groups that may be state-sponsored), and the fight against cybercrime. OSINT's growing significance can be attributed to its cost-effectiveness and reduced risks when compared to traditional espionage methods (Oikarinen, 2020).

Within the realm of information security, OSINT intelligence serves as a valuable resource for identifying vulnerabilities within an organization's IT infrastructure. The concept of a "Red Team" exemplifies this approach, wherein a group simulates adversarial attacks against an organization. These simulated attacks include an initial phase of information gathering, a process that often relies on OSINT techniques (BreachLock, 2023).

Open Source Intelligence plays a crucial role in penetration testing and Red Teaming exercises. It aids in the identification and exposure of potential vulnerabilities and resources that may have inadvertently leaked outside an organization's security perimeter. These findings empower security experts to proactively address vulnerabilities and mitigate associated risks before malicious actors can exploit them. Some common vulnerabilities identified through OSINT intelligence include the inadvertent exposure of sensitive data, the use of outdated and unpatched software, and the existence of open ports on IT devices (BreachLock, 2023).

OSINT is often characterized as providing an "attacker perspective" because it offers cybercriminals insights into the same vulnerabilities and findings that security professionals may discover. Once attackers identify a vulnerability, exploiting it becomes relatively straightforward. Consequently, many small and medium-sized organizations are susceptible to cyberattacks, with attackers often combining OSINT intelligence with social engineering techniques in targeted phishing campaigns (BreachLock, 2023).

Threat Intelligence is a critical component in an organization's cybersecurity strategy. It is the practice of proactively identifying, assessing, and mitigating threats targeting the organization. Effective threat intelligence relies on the systematic collection and analysis of data, including publicly available information relevant to the organization. The threat intelligence process typically involves six stages: defining objectives, data collection, data processing, data analysis, reviewing results, and providing feedback (Martins & Medeiros, 2022).

In today's interconnected digital landscape, OSINT serves as a valuable resource for security professionals seeking to gain a comprehensive understanding of potential cyber threats. The vast expanse of the internet offers a wealth of information on a wide range of topics, including current threats, emerging trends in the cyber domain, and the evolving tactics and techniques employed by cybercriminals. Information security experts and their teams can leverage data extracted from open sources to protect their organization's IT infrastructure effectively. This includes preemptively addressing zero-day vulnerabilities and implementing additional security measures to safeguard against potential threats (BreachLock, 2023).

In summary, OSINT is a versatile and invaluable tool within the domain of cybersecurity. It facilitates the systematic gathering, analysis, and utilization of information from publicly accessible sources, enabling organizations to enhance their threat assessment and mitigation strategies.

3. OSINT Operational Process

In the case organization, the OSINT operational process will primarily be used for threat intelligence purposes. Ideally, threat intelligence is a part of every organization's cybersecurity strategy. Monitoring existing and potential new threats, consistent data collection, and analysis enhance an organization's ability to protect itself from cybercrime. The Threat Intelligence Lifecycle consists of six phases: defining objectives for threat intelligence, data collection, data processing, data analysis, results review, and feedback (Snyk 2023). Figure 2 presents the operational process designed for the case organization.

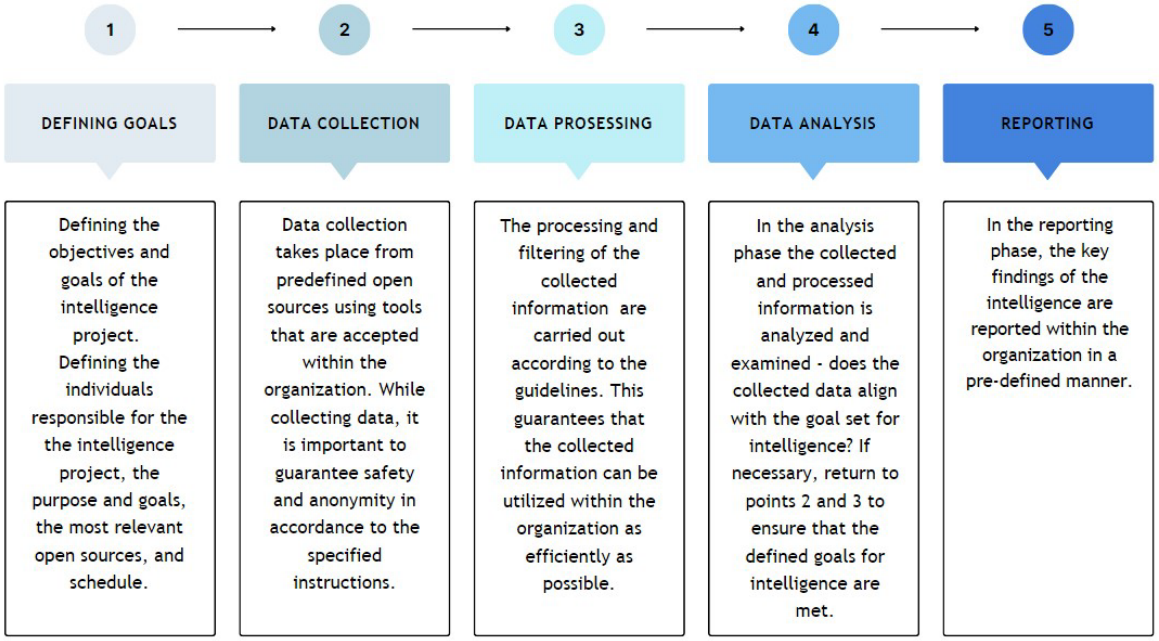

Figure 2: Designed OSINT Operational Process

The operational process begins with defining the goals of intelligence gathering. In this phase, the purpose of intelligence gathering is determined, and the individuals responsible for gathering the intelligence are selected. Intelligence gathering is mainly carried out by pre-designated employees within the organization who have an intelligence orientation. Additionally, the most relevant open sources are selected to maximize the effectiveness of intelligence gathering. At the same time, the intelligence project's timeline is defined.

During the data collection phase of the process, information is gathered from the open sources identified in the first phase of the operational process. Data is collected using approved tools within the organization for intelligence purposes. Common tools used for OSINT intelligence include Maltego and SpiderFoot. When conducting active intelligence gathering in addition to passive intelligence gathering or when collecting data from the dark web, one's own actions must be protected as defined within the organization.

In the third phase of the process, during the data collection phase, the collected data is filtered and processed. Filtering and processing of collected data are carried out according to the organization's guidelines. The collected data should align with the intelligence objectives set for the process.

In the fourth phase of the process, the processed and filtered data is analyzed and examined. At this stage, it is determined whether the collected data meets the intelligence objectives. If the analyzed data aligns with the intelligence objectives, the process can proceed to the final phase (reporting). However, if it is determined that the analyzed data does not meet the intelligence objectives, steps two and three of the process are repeated to achieve the intelligence objectives, ensuring that the analyzed data is accurate and its utilization is efficient. If steps two and three need to be repeated, new open sources may also be identified from which information is sought.

The final phase of the operational process is the reporting phase. At this stage, the analyzed information is reported. The findings of the intelligence gathering are reported in a manner defined within the organization to pre-determined individuals and/or units. The produced report should be clear and concise so that even individuals who are not technology-oriented can understand the information presented in the report. Based on the report and the information gathered in the intelligence process, potential follow-up measures are defined to enhance the organization's security.

4. Testing of the Operational Process

The operational process was tested by conducting an OSINT investigation on an organization's employees. Permission was obtained from the individual before conducting the investigation. Clear objectives were defined for the intelligence gathering. The goal was to gather as much information as possible about the individual, which could be used for targeted phishing attacks or other forms of manipulation. This paper's main author conducted the OSINT investigation. The timeline was set for April 2023, but the intelligence objectives were achieved in early April. Social media primarily served as the source of information. Specific tools were designated for this OSINT investigation, including Maltego, SpiderFoot, Google, and Google Maps. Data collection was swift, and the information that aligned with the intelligence objectives was found relatively effortlessly. The collected data was analyzed to ensure its relevance. The relevance of the information was cross-verified through multiple sources.

There was no need to revisit steps two and three of the operational process in this investigation. Sufficient information that matched the intelligence objectives was collected from the individual. The quality of the information was such that it could have been used for actions like targeted phishing or other forms of manipulation. Following the analysis of the information, a report was created from the findings of the intelligence and presented to the subject of the investigation. Subsequently, the intelligence report was reviewed with the target individual, who was provided with guidance on improving their online security. Corrective actions in the individual's online activities did not require major changes.

5. Discussion

The objective of this study was to implement OSINT as a component of the case organization's cybersecurity. The implementation was achieved by designing an operational process for OSINT intelligence, enabling the organization to enhance its cybersecurity management. The research methodology was design science. The design of the operational process closely adhered to the seven principles of DSR (Hevner et al, 2004), and the research fulfilled the requirements outlined in these principles as follows:

- An operational process for OSINT intelligence was created for the case organization to address their need to improve the deficient and weak approach to utilizing open-source intelligence within the organization.
- The resulting operational process solves the case organization's problem related to the inadequate utilization of OSINT.
- The operational process was thoroughly tested, and it was found to meet the established objectives for its functionality.
- The operational process provides the case organization with a customized process for conducting OSINT intelligence within the organization. The process is based on scientific knowledge.
- A comprehensive study was conducted on the scientific theory related to OSINT intelligence, requirement specification theory, and process design theory.
- The operational process was created by using scientifically valid knowledge and applying an existing solution to the intelligence process.
- The results of the study were presented within the case organization to individuals for whom the research findings were relevant. The research results were also shared within the academic community.

The study results were validated through testing the developed operational process, and the outcomes aligned with the objectives set for intelligence gathering and testing. The case organization can utilize this operational process, particularly for threat intelligence purposes. Therefore, it can be concluded that the study successfully generated value for the case organization, achieving its research objective, and the design science research approach was effective.

As future research, it would be interesting to investigate how different financial industry players utilize OSINT intelligence and its processes to maintain a threat landscape, acquire targeted threat intelligence, and mitigate the initial stages of attack vectors using OSINT. The focus of such research could be on intelligence gathered from the dark web, specifically what information about financial industry entities can be found there and how this information can be strategically used by cybercriminals against financial institutions. This could be examined through frameworks like Lockheed Martin's Cyber Kill Chain, which is part of the Intelligence-Driven Defense model used to identify and prevent cybercriminal activities (Lockheed Martin 2023).

Another area for further research could be the challenges and opportunities brought by artificial intelligence (AI) in OSINT intelligence. What benefits does AI offer to OSINT intelligence, and what challenges may arise as AI technologies continue to evolve?

Acknowledgements

This work was supported by the DYNAMO project, which has received funding from the European Union's Horizon Europe research and innovation funding programme under grant agreement no. 101069601. The sole responsibility for the content of this paper lies with the authors. It does not necessarily reflect the opinion of the European Commission or of the full project. The European Commission is not responsible for any use that may be made of the information contained therein.

References

Akhgar, B. & Bayerl, P. (2015) "Surveillance and Falsification Implications for Open Source Intelligence Investigations", *Communications of the ACM*, Vol 58, Iss 8, 62.

Azzopardi, L., Glisson, W., Maxwell, D., & McKeown, S. (2014) "Investigating people: a qualitative analysis of the search behaviours of open-source intelligence analysts", *Proceedings of the 5th Information Interaction in Context Symposium*, pp 175-176.

BreachLock (2023) "What is Open-source Intelligence, and how is it used?" [online] https://www.breachlock.com/resources/blog/what-is-open-source-intelligence-and-how-is-it-used/

Gatlin, J., Yampolskiy, M. & Yung, M. (2021) "Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad", *Proceedings of the 2021 Workshop on Additive Manufacturing Security*.

DYNAMO (2023) "Factsheet 2: Cyber Threat Intelligence" [online] https://horizon-dynamo.eu/wp-content/uploads/2023/09/DYNAMO-Factsheet-2-1.pdf

Hevner, A. (2007) "A Three Cycle View of Design Science Research", *Scandinavian Journal of Information Systems* vol 19, pp 88-91.

Hevner, A., March, S., Park, J., & Ram, S. (2004) "Design Science in Information Systems Research", *MIS Quarterly* Vol 28 No 1, pp 80–90.

Lockheed Martin (2023) "Putting Intelligence to Work" [online] https://www.lockheedmartin.com/en-us/capabilities/cyber/intelligence-driven-defense.html

Martins, C. & Medeiros, I. (2022) "Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy", *ACM Transactions on Privacy and Security*, Vol 25, Iss 3, Article 19, pp 2-5

Oikarinen, A. (2020) "Open-Source Intelligence – It's Incredible what you can find from public sources" [online] https://www.nixu.com/blog/open-source-intelligence-its-incredible-what-you-can-find-public-sources

Snyk (2023) "Threat Intelligence Lifecycle - Phases & Best Practices Explained" [online] https://snyk.io/learn/threat-intelligence/threat-intelligence-lifecycle/