Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence

Jyri Rajamäki and Stephen McMenamin
Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
Stephen.McMenamin@student.laurea.fi

Abstract: Open-source intelligence (OSINT) is crucial for enhancing organizational cybersecurity by proactively identifying and mitigating potential threats using publicly available information. This study, part of the DYNAMO project, explores the production of cyber threat information (CTI) through OSINT, its application in safeguarding against cyber threats, and the necessary elements for secure information exchange between organizations. The authors employed an integrative literature review of various sources, including industry literature, articles, blog posts, studies, and organizational websites, which were then systematically analyzed using content analysis. The research focuses on OSINT tools and techniques emphasizing the need for expertise in discerning relevant data and respecting privacy rights. Human judgment is highlighted as crucial in ethical decision-making despite the significant role of technology in data collection. Platforms like the Malware Information Sharing Platform (MISP) facilitate the sharing of threat information, promoting prevention and identification of cyber-attacks. Ethical considerations, adherence to data protection legislation, and compliance with directives like the revision of the Network and Information Security Directive (NIS2) and artificial intelligence regulations are paramount. In conclusion, OSINT is a valuable tool for cybersecurity, requiring expertise, transparent processes, and a balanced integration of technology and human skills. The ethical dimensions of OSINT and the role of artificial intelligence merit separate in-depth studies.

Keywords: OSINT, Cyber threat intelligence, Cyber information sharing, DYNAMO project

1. Introduction

Open-source intelligence (OSINT) is conducted by various entities, including law enforcement agencies, defense forces, investigative journalists, and cybersecurity professionals. Malicious actors, such as cybercriminals or state-sponsored threat actors, also leverage OSINT techniques. The objective is to gather information about organizations or individuals that can be exploited in cyberattacks or pose a threat to security. This information is utilized in cyberattacks, prevention efforts, criminal investigations, or to support business strategies (SANS Institute 2023; Fruhlinger, Sharma & Breeden 2023).

OSINT is, in many ways, a counterpart to Operational Security (OPSEC), a process through which organizations protect information that should not be made public. For example, an employee's social media post may inadvertently contain sensitive information about the organization, or IoT devices connected to the public network may reveal information beneficial to threat actors regarding the organization's technologies. OSINT enables the proactive identification of potential threats and suggests measures to mitigate them (Fruhlinger et al. 2023; Rose 2020).

The DYNAMO project, funded by the European Union, aims to create a platform to reduce cyber threats to critical sectors such as energy, health, and transportation infrastructure. The platform supports all stages of cyber resilience - preparation, prevention, protection, response, and recovery - tailored to the needs of critical infrastructure. Its goal is to enhance the security of organizations and society (DYNAMO 2023; Packham 2022).

One component of the platform involves generating Cyber Threat Intelligence (CTI) through Indicators of Compromise (IoC), enhancing an organization's information and cyber monitoring capabilities (DYNAMO 2023). IoC are clues or observations of threatening activities, such as blacklisted IP addresses, remnants of identified malicious files, or URLs classified as phishing sites (Gaucheler 2023). OSINT is a crucial part of producing IoC, providing in-depth information about potential threats.

2. Methodology

The research methodology used included an integrative literature review, critically examining various sources to form a comprehensive understanding of the topic. Throughout the study, several tools designed for OSINT were tested, as recommended in research articles and blog posts. The testing yielded examples of data types generated through intelligence gathering and possibilities for collecting threat information. The tools were tested either in their web interface or a virtual Kali Linux environment. Usage instructions for the tools were generally found in the tool's documentation, and a list of tools used in the study is provided in the bibliography.

The study integrated threat intelligence from OSINT into the research on information sharing, along with relevant legislation and ethics. Sources included legal documents, directive proposals, and scientific articles and research written by industry professionals. For information retrieval, search engines such as Google, Google Scholar, and DuckDuckGo were primarily used. Examples of search terms used in these search engines include "OSINT," "OSINT in threat intelligence," "OSINT regulations," "OSINT ethics," "Threat intelligence sharing," and "Open-Source intelligence legislation." Specifically, in the section focusing on OSINT techniques and benefits, research literature was complemented with research material found in blogs and articles by industry experts, providing a unified perspective. Sources were objectively analyzed using content analysis methodology, and the study aimed to utilize the most recent information available.

3. OSINT for Cybersecurity

OSINT refers to intelligence derived from collecting, evaluating, and analyzing publicly available information. Various entities, including cybersecurity professionals, malicious hackers, and state intelligence services, employ advanced techniques to extract specific information from vast datasets to achieve their objectives (SANS Institute, 2023; Fruhlinger et al., 2023). Intelligence involves the collection of national or international threat information, serving to warn about potential threats or opportunities, gathering information on individuals, or contributing to counterintelligence efforts (Office of the Director of National Intelligence, 2023). OSINT is utilized in several ways (SANS Institute, 2023):

- Security and Intelligence: Gathering information on potential threats to security, such as terrorism or cyberattacks, and collecting intelligence on foreign governments, businesses, or individuals.
- Business and Market Research: Collecting information on competitors, industry trends, and consumer behavior for strategic business decisions.
- Investigative Journalism: Gathering information on politics, business, and criminal activities.
- Academic Research: Researchers use OSINT to collect information on trends, opinions, and economic indicators.

OSINT is employed by governments, law enforcement agencies, defense forces, investigative journalists, human rights researchers, private investigators, law firms, corporate cybersecurity and surveillance teams, and penetration testers. It is also used in private life, such as in people searches (Maor, 2022). OSINT is collected from various sources, including libraries, news, articles, websites, social media, blogs, search engines (including specialized ones like Shodan), the deep web, the dark web, images, videos, source code, or metadata (Kaspersky, 2023; SANS Institute, 2023).

Information can be categorized into structured and unstructured types. Structured sources offer defined data in a specific format, while unstructured sources provide data primarily in text form. OSINT techniques can be passive, semi-passive, or active (SANS Institute, 2023):

- Passive: No interaction with target systems, including scanning public websites or retrieving data from open application programming interfaces.
- Semi-Passive: Involves network scanning, directing traffic to target servers to obtain information while mimicking normal internet traffic.
- Active: Interaction or engagement with the target, such as adding a target as a friend on social media or sending messages.

Organizations can tailor their responses to potential cyber threats by proactively using OSINT to understand threat actors' tactics, techniques, and procedures. Shifting from reactive to proactive defense, organizations can protect themselves from cyberattacks by detecting anomalies through OSINT (Slinde, 2023). Information beneficial to attackers includes open ports, vulnerable and outdated software, poorly defined cloud storage, credentials in source code, and system details like device names, IP addresses, and configurations. External sources like social media and information shared by suppliers and partners can also be relevant for attack planning (Yadav, Kumar & Singh, 2023; Imperva, 2023).

4. OSINT Tool Testing

This study examined tools suitable for OSINT investigations, focusing on commonly used tools, with an emphasis on free and open-source tools. It explored various techniques such as search operators, regular expressions, and multipurpose tools. The OSINT Framework is presented as a comprehensive reference for OSINT tools that provide a wide range of resources for intelligence gathering. The study covers search engine operators and provides examples of commonly used operators to refine search results. It tested the OSINT Framework,

Maltego, TheHarvester, SpiderFoot, ThreatMiner, and other tools for various aspects of OSINT investigations, such as social media analysis, website technology detection, and domain name investigation. Techniques like regular expressions were looked at for structuring and extracting specific data from unstructured data. Multipurpose tools such as Maltego, TheHarvester, and SpiderFoot were tested for their abilities in mapping relationships, gathering information about organizations, and conducting passive intelligence.

The study also tested search engines such as Shodan, TinEye, and Grep.app, which specialize in finding connected devices, reverse image search, and finding code repositories. We tried tools like Have I Been Pwned to check compromised email addresses. Also covered were tools such as Wappalyzer for detecting website technologies, PhishTank for identifying phishing sites, and DNSdumpster for investigating domain names. The discussion ranged from retrieving historical data using the Wayback Machine and Intelligence X to exploring the dark web using Tor web search engines such as Ahmia and Dark.fail. The importance of tracking cryptocurrencies in investigations was also discussed and challenges and opportunities in tracking transactions and addresses in the field of digital currencies were highlighted.

5. Using OSINT Information to Defend Against Cyber Threats

In the examples of the use of the tools, it was noticed that when inquiring about open data sources, information can be found, e.g., about the target organization's employees, finances, IP addresses connected to the organization, the technologies it uses, vulnerabilities, the relationships of persons or organizations with other persons or organizations and their physical locations. By combining this information, a threat actor can plan an effective and efficient attack. The information can also cause reputational harm if it ends up in the wrong hands.

The organization should identify what kind of threats it faces, what could be the motivations of a potential threat actor to carry out a cyber-attack on the organization, and what kind of information it perceives as a threat if it ends up being public. Once the threat area has been identified, the organization can use open data sources to find out what dangerous information is available about them. The organization must have a process by which, after the discovery of potentially dangerous information, follow-up measures are taken to reduce the risk (Hiremath 2023; Rose 2020)

Investigating open data sources is not a one-time project but should be done regularly. Technology is helpful, and the various scans should be automated so that dangerous information is detected before the threat actor and there is time to react before it is too late (Hiremath 2023; Makrushin 2022). Cooperation within the cybersecurity community is important. Sharing OSINT findings and cyber CTI (CTI) with colleagues in the field facilitates joint preparedness against changing threats. Appropriate platforms, such as ISACs (Information Sharing and Analysis Center), are essential here. (Hiremath 2023; ENISA 2023)

6. Sharing CTI in a Trusted Environment

The DYNAMO platform offers support for all phases of cyber resilience. One part of the platform is the ability to store and share CTI among DYNAMO stakeholders, paying special attention to protecting shared information. For this purpose, the project develops a trust environment for users of the DYNAMO platform. The developed module is based on open-source solutions such as the Malware Information Sharing Platform (MISP), taking advantage of its advanced storage and sharing functions, but also allowing integration with other open-source tools such as Cortex and TheHive (DYNAMO 2023). Threat actors specialize in targeting their attacks on certain sectors, such as governments or banking. Once they find a technique that works against one organization, a common next step is to try the same techniques against similar organizations. Therefore, shared CTI in an environment of trust benefits all parties and reduces the probability that similar organizations fall victim to the same threats. (Postolovski 2023)

MISP open-source threat intelligence and sharing platform’s goal is to prevent and identify targeted cyber-attacks, for example with the help of indicators of compromise. MISP gives CTI a unified structure and automatically combines similar information, making it easier to store and share information despite the large amount of information among organizations that are likely to face similar threats. MISP includes a representative state transfer (REST) application programming interface (API) for adding functionalities and external data sources (CIRCL 2023; Postolovski 2023). TheHive is an open-source Security Incident Response platform, i.e. a platform for managing information security incidents. It can be synchronized with MISP instances to investigate MISP events. The research results can be exported and distributed as a MISP event among the trust environments. Cortex is a software developed by TheHive Project for analyzing compromise indicators, which is intended specifically for use with MISP and TheHive.

When sharing CTI, a balance must be found between transparency, privacy, and confidentiality. It is good for the organization to share CTI, which helps other organizations in a trusted environment to understand the threats better. On the other hand, sharing identifiable or sensitive information should be avoided. Such information includes, for example, company names, internal IP addresses, personnel names, customer identifiers, or business-related information. The information to be shared therefore contains intelligence information only about threats, and not about the company's own business, infrastructure, employees, or customers. Checking shared CTI is important to maintain privacy and confidentiality. To reduce risks and ensure confidentiality and accuracy when sharing information, an approval chain can be used before sharing information with other organizations (Postolovski 2023).

7. Conclusions

Open-source intelligence (OSINT) is an important tool in maintaining the cybersecurity of organizations. It can be used to proactively identify and anticipate potential threats and develop measures to reduce these threats. This concerns finding information that is publicly available and that threat actors could use against the organization. This may include, for example, information related to employees, which could be used for example in phishing or password cracking.

Practicing OSINT requires expertise. The professional must be able to identify significant data from a large amount of information and assess its relevance in terms of the organization's security. Ethical and legislative aspects are central to the collection of intelligence information. The data collection must be limited so that it does not violate anyone's privacy or rights. The use of technology in data collection can lead to unethical or illegal practices if people's control and understanding of the limitations of intelligence are not a priority.

The inquiry process must have a clear reference framework, in which the goals and processes of OSINT are defined. The role of technology in data collection is significant in speeding up data acquisition, but the importance of human judgment is emphasized in ethical decisions. Documenting operations is central to ensuring ethics. Automated systems can save research steps, allowing people to focus on analysis and value creation.

Platforms such as MISP are used to share threat information, the goal of which is to prevent and identify targeted cyber-attacks and share CTI between actors. When sharing CTI, it is important to ensure that the shared information does not violate privacy or confidentiality. Operators related to data security can share information within the framework of the Personal Data Act when the activity serves the public interest and personal data is only processed to the extent necessary. In addition, the requirements set by, for example, the revision of the Network and Information Security Directive (NIS2) directive and the artificial intelligence regulation must be considered as they impose several new cyber security obligations on organizations in many economically critical sectors.

OSINT offers organizations an important tool for maintaining cybersecurity, but its effective and ethical use requires expertise, clear processes, and a balanced combination of technology and human skills. The ethics of OSINT activities and the utilization of artificial intelligence are topics that would be enough to consider for separate further studies. These two issues could also be combined into one research entity.

Acknowledgements

Acknowledgement is paid to DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

CIRCL. 2023. CIRCL » MISP - Open Source Threat Intelligence Platform. Referred 24.10.2023. https://www.circl.lu/services/misp-malware-information-sharing-platform/

DYNAMO. 2023. Horizon Dynamo EU. Referred 21.9.2023. https://horizon-dynamo.eu/about/

ENISA. 2023. Information Sharing and Analysis Centers (ISACs). Topic. ENISA. Referred 23.10.2023. https://www.enisa.europa.eu/topics/national-cyber-security- strategies/information-sharing

Fruhlinger, Josh, Sharma, Ax & Breeden, John. 2023. 15 top open-source intelligence tools. CSO Online. Referred 11.9.2023. https://www.csoonline.com/article/567859/what-is-osint- top-open-source-intelligence-tools.html

Gaucheler, Mathieu. 2023. Advanced IOCs Collection with OSINT and Threat Intelligence Feeds. Maltego. Referred 11.9.2023. https://www.maltego.com/blog/advanced-iocs- collection-with-osint-and-threat-intelligence-feeds/

Hiremath, Omkar. 2023. Protecting Your Organization With Open-source Intelligence (OSINT). Software Secured. Referred 23.10.2023. https://www.softwaresecured.com/protecting-your- organization-with-open-source-intelligence-osint/

Imperva. 2023. Open-Source Intelligence (OSINT). Referred 5.9.2023. https://www.imperva.com/learn/application-security/open-source-intelligence-osint/

Kaspersky. 2023. OSINT (Open-Source Intelligence). Referred 5.9.2023. https://encyclopedia.kaspersky.com/glossary/osint/

Kumar, Dinesh. 2022. 10 OSINT Tools Hackers Need to Know About. Medium. Referred 1.10.2023. https://0xtmux.medium.com/10-osint-tools-hackers-need-to-know-about- 9cbb3519ea47

Maor, Etay. 2022. How and Why to Apply OSINT to Protect the Enterprise. Dark Reading. Referred 23.10.2023. https://www.darkreading.com/attacks-breaches/how-and-why-to-apply-osint-to-protect-the-enterprise

Office of the Director of National Intelligence. 2023. What is Intelligence? Referred 21.9.2023. https://www.dni.gov/index.php/what-we-do/what-is-intelligence

Packham, Karen. 2022. RHEA to Contribute to Develop Cyber Threat Intelligence Solution for European DYNAMO Project. RHEA Group. Referred 11.9.2023. https://www.rheagroup.com/rhea-to-contribute-to-develop-cyber-threat-intelligence- solution-for-european-dynamo-project/

Postolovski, Tash. 2023. What is MISP? The Ultimate Introduction. Cosive. Referred 26.10.2023. https://www.cosive.com/blog/what-is-misp-the-ultimate-introduction

SANS Institute. 2023. What is Open-Source Intelligence? Referred 28.8.2023. https://www.sans.org/blog/what-is-open-source-intelligence/

Slinde, Johanna Sofie. 2023. Unveiling the Potential of Open-Source Intelligence (OSINT) for Enhanced Cybersecurity Posture

Rose, Zoë. 2020. OSINT – Using Threat Intelligence to Secure Your Organisation. Tripwire. Referred 11.9.2023. https://www.tripwire.com/state-of-security/osint-using-threat-intelligence-secure-organisation