Information & Security

J. Rajamäki, S. McMenamin & K. Tiitta
vol. 55, no. 1 (2024): 15-31
https://doi.org/10.11610/isij.5511

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

The Importance of Open-Source Intelligence in Assessing Risks of Cyberattacks

Jyri Rajamäki (✉), ***Stephen McMenamin, and Krista Tiitta***

Laurea University of Applied Sciences, Espoo, Finland
http://laurea.fi

ABSTRACT:

Open-Source Intelligence (OSINT) is becoming increasingly vital in cybersecurity as digital platforms evolve. Advanced OSINT tools, incorporating artificial intelligence and machine learning, enhance organizations' ability to process and analyze large amounts of open-source data. This paper highlights OSINT's role in risk assessment to prevent cyberattacks. The research focused on OSINT tools and techniques, emphasizing the need for expertise in identifying relevant information and respecting privacy. An OSINT operational process was developed for a critical sector company and then used to conduct a vulnerability assessment. The organization is kept anonymous due to its national security role. The goal was to integrate OSINT into the organization's cybersecurity framework. Permission was obtained before conducting a thorough OSINT test, using tools such as Maltego, SpiderFoot, Google, and Google Maps. Data collection was swift, and relevant information was easily found. The collected data was analyzed, cross-verified, and compiled into a report, which was then reviewed with the subject to provide protection advice online. The paper demonstrates OSINT's effectiveness in enhancing organizational security and provides recommendations for using OSINT to identify vulnerabilities, reduce risks, and strengthen cybersecurity practices.

ARTICLE INFO:

RECEIVED: 31 AUG 2024
REVISED: 22 OCT 2024
ONLINE: 28 OCT 2024

KEYWORDS:

cyberattack risks, open-source intelligence, OSINT, risk assessment

✉ Corresponding Author: E-mail: jyri.rajamaki@laurea.fi

Introduction

The role of Open-Source Intelligence (OSINT) in cybersecurity is likely to expand as digital platforms continue to grow and evolve. The development of advanced OSINT tools, including those leveraging artificial intelligence and machine learning, will further enhance the ability of organizations to process and analyze vast amounts of open-source data.[1, 2] As the field of cybersecurity evolves, OSINT will play an increasingly important role in protecting organizations against emerging threats.[3]

The three-year Erasmus+ funded project, Digital Education Tools for Security Risk Management (SECUREU), aims, among other things, to develop best practices for the field of security and risk management through international collaboration.[4] This study consolidates two sub-studies produced in the DYNAMO project into a unified case description, which can be offered as a depiction of one of the best practices in security and risk management. The preliminary results of these sub-studies were presented as posters accompanied by short work-in-progress papers at the ICCWS 2024 conference.[5, 6]

This study highlights the importance of OSINT in assessing risks to prevent cyberattacks. The first part of the research focused on OSINT tools and techniques, emphasizing the need for expertise in distinguishing relevant information and respecting privacy. Subsequently, we developed an OSINT operational process for a company operating in a critical sector and used that operational model to conduct a vulnerability assessment. The organization was kept anonymous in our work due to its critical role in national security. The goal was to integrate OSINT intelligence into the organization's cybersecurity framework and risk management.

Based on the research, the designed operational process included steps and guidelines for implementing OSINT intelligence within the target organization. With OSINT, we successfully profiled the company's network software, hardware, IT personnel, and detailed potential vulnerabilities related to these findings.

We sought permission from key individuals before conducting a thorough OSINT test on them. The intelligence-gathering operation had well-defined objectives, focusing on acquiring comprehensive information about the individual to facilitate potential targeted phishing attacks or other cyber threats. Social media platforms were the primary sources of data. Specific tools designated for this OSINT investigation included Maltego, SpiderFoot, Google, and Google Maps. The data collection process was efficient, and relevant information pertinent to the intelligence objectives was obtained with relative ease.

The collected data underwent analysis to ensure its relevance, cross-verified through multiple sources. The information obtained was of such high quality that it could be effectively utilized for targeted phishing attacks or other forms of manipulation and coercion. Following analysis, the findings of the intelligence were compiled into a report and delivered to the subject of the investigation. Subsequently, the intelligence report was reviewed with the subject of the investigation, providing them with advice on how to better protect themselves

online. Adjustments to the individual's online behavior did not require significant changes.

In summary, our research findings provide empirical evidence of the effectiveness of OSINT in enhancing organizational security posture. The ultimate purpose of this paper is to provide other organizations the opportunity to utilize our research findings and to generate tactical and strategic recommendations for leveraging OSINT in identifying vulnerabilities, reducing risks, and developing stronger cybersecurity practices to prevent cyberattacks.

The content of the rest of the paper is as follows: The following chapters describe the research methodology and the results of the literature review. After this, the way in which the OSINT tools have been tested will be explained. Then, the planning and testing of the operational process is described. Finally, the findings and suggestions for further research are discussed.

Research Design and Methods

The research comprised (1) a literature review, (2) testing of selected OSINT tools based on this review, (3) designing of an OSINT operational model for a company operating in a critical sector, and (4) testing of this operational model. In an integrative literature review, different sources were critically examined to form a comprehensive understanding of the subject. The information retrieval primarily utilized search engines such as Google, Google Scholar, and DuckDuckGo. Examples of search terms used include "OSINT," "OSINT in threat intelligence," "OSINT regulations," "OSINT ethics," "Threat intelligence sharing," and "Open-source intelligence legislation." In addition to scientific literature, the research material included consistent information and insights found in blogs and articles by industry experts. The reliability of the sources was assessed by ensuring that multiple sources corroborated with each other. The sources were analyzed objectively using content analysis methods, and the study aimed to use the most recent sources available.

Throughout the study, various OSINT tools were evaluated, as recommended by research articles and blog posts. The testing provided examples of the types of intelligence data that could be gathered and the potential for collecting threat information. The tools were tested either through web interfaces or within a virtual Kali Linux environment. Instructions for using the tools were primarily sourced from their documentation, and the complete list of tools utilized in the study is included in the reference list.

After this, and using the design science research (DSR) methodology,[7] an OSINT operational process was developed for an international organization operating in a critical sector. With the help of this operational model, a vulnerability assessment was carried out in the target organization. In this context, a comprehensive OSINT investigation was conducted on a key individual, who had given prior consent. The organization's identity is withheld in this article due to its critical role in national security. The goal was to integrate OSINT intelligence into the organization's cybersecurity.

Literature Review

OSINT involves systematically collecting, evaluating, and analyzing information from publicly accessible sources, including the Internet, social media, traditional media outlets, and more. Its inclusivity and accessibility make it a powerful tool for various stakeholders, including cybersecurity professionals, malicious actors, and state intelligence agencies.[8, 9]

The advent of digital platforms, especially social media, has exponentially increased the availability of open-source information.[10] While this abundance of data provides opportunities for enhanced threat detection, it also presents challenges related to data accuracy, reliability, and the potential misuse of information.[11]

The Role of OSINT in Cyber-Attack Risk Assessments

Although OSINT is a framework rather than a single technology,[12] it has evolved into an essential tool in security and intelligence operations.[13] It is widely used in criminal investigations, counterterrorism,[14] monitoring Advanced Persistent Threat (APT) actors, and combating cybercrime.[15] Its cost-effectiveness and lower risks, compared to traditional espionage methods, have contributed to its growing significance.[16]

In cybersecurity, OSINT is crucial for identifying vulnerabilities within an organization's IT infrastructure. The concept of a "Red Team," which involves a group simulating adversarial attacks against the organization, often begins with an OSINT-driven information-gathering phase.[17, 18] OSINT aids in penetration testing and Red Teaming exercises by exposing potential vulnerabilities and resources that may have unintentionally leaked beyond the organization's security perimeter. These insights enable security professionals to proactively address weaknesses and mitigate associated risks before malicious actors can exploit them.[19] Unfortunately, OSINT has also become an important tool for hackers in modern cyber warfare.[20]

Challenges and Limitations of OSINT

Despite its advantages, OSINT is not without challenges. The vast amount of information available through open sources can lead to issues with data accuracy and reliability. Verifying the credibility of OSINT sources is crucial, as inaccurate or outdated information can lead to incorrect risk assessments. Additionally, the ethical and legal implications of using publicly available data, particularly when it involves personal information, must be carefully considered.[21]

Another challenge is managing and filtering the large volumes of data obtained through OSINT. Organizations must employ sophisticated tools and techniques to process this data effectively, distinguishing relevant information from noise.[22]

Integrating OSINT into Cybersecurity Practices

To maximize the benefits of OSINT, organizations should integrate it into their existing risk assessment frameworks.[23] This involves adopting methodological approaches that incorporate OSINT into cyber threat intelligence processes. The process typically includes defining objectives, collecting and processing data, analyzing findings, and continuously reviewing and refining strategies based on the intelligence gathered.[24]

OSINT also provides what is often termed the "attacker perspective," allowing organizations to see their vulnerabilities through the eyes of potential adversaries. This perspective is critical in understanding how cybercriminals might exploit vulnerabilities, enabling organizations to implement more effective defenses.[25]

Benefits of OSINT in Cyber-Attack Risk Assessments

The proactive use of OSINT in cyber-attack risk assessments offers numerous benefits.[26] It enhances situational awareness by providing real-time insights into emerging threats, allowing organizations to detect anomalies and potential risks before they escalate into full-blown attacks.[27] OSINT is particularly effective in identifying common vulnerabilities such as open ports, outdated software, and exposed sensitive data, which can be exploited by attackers.[28]

State-of-the-art OSINT Technologies

The OSINT Framework[29] is a comprehensive reference framework for OSINT tools, making it easy to find the right tool for any situation. The framework lists free tools or resources that are useful for open-source intelligence gathering. Some tools may require registration or payment to access all features.

The use of advanced search operators in search engines (dorking, search engine hacking) is a technique that allows one to find, for example, leaked documents or security vulnerabilities from search engines like Google.[30]

When examining some multipurpose OSINT tools, Maltego is a Java-based software that runs on Windows, Mac, and Linux. Maltego comes with over 70 API connections to various data sources, and you can also integrate your data sources. Maltego specializes in discovering and visualizing relationships and connections between people, companies, domains, and other open data, presenting them as easy-to-read charts and graphs.[31, 32] The Harvester is an open-source intelligence-gathering tool that can search for email addresses, names, subdomains, IP addresses, and URLs. The tool is designed to find open intelligence information about an organization or domain. It uses popular search engines like Bing and DuckDuckGo, as well as lesser-known sources like CertSpotter and DNSdumpster.[33] Spiderfoot is an open-source tool that can search for and collect IP addresses, domains, subdomains, ASN numbers, email addresses, phone numbers, names, usernames, and Bitcoin addresses. The tool has over 200 modules that can be used to search for publicly exposed information from

your organization, such as leaked login credentials.[34] ThreatMiner utilizes multiple data sources (e.g., VirusTotal and Alienvault OTX) to search for indicators of compromise based on domains, IP addresses, email addresses, and file names. It operates through its web interface and can be integrated via API with platforms like MISP or Splunk.[35]

Additionally, there are many OSINT tools and techniques focused on a single task. Using a real name or username, we can easily gather information about a specific user. Email investigation examines the email header and body to obtain information about the sender and recipient. Tools based on phone numbers allow us to quickly obtain the phone number owner's details and device information using the phone number. An Internet Protocol (IP) address helps collect information such as the device's geographic location, time zone, area code, and Internet Service Provider (ISP). Blacklisted IP addresses are continuously updated, which can aid in training deep learning (DL) models to detect cyberattacks. Image search tools help gather images related to various items such as crimes, education, news, historical images, politics, and elections. Reverse image search helps collect information about a specific image, such as the device used to capture it, the location, and the image source. Image manipulation check tools help analyze images and gather information such as image metadata, the location where the image was captured, and hidden pixels. Video search tools help find information such as the type of content in the video and the video's metadata. Geospatial search tools help collect location information and analyze incidents at specific locations, street views, and other target location-related information. OSINT tools and techniques for air traffic monitoring help gather information about flight paths and current locations, track the target's real-time location in motion, and monitor air traffic at any location at any given time. Maritime traffic can be tracked using a vessel's Automatic Identification System (AIS) identifier, which provides the vessel's name, location, destination, type, and other information. Package tracking tools help monitor packages, including the smuggling of drugs, weapons, and illegal items.[36] Appendix 1 lists some tools for the aforementioned OSINT techniques. Table 1 presents the tools and techniques tested in this study.

OSINT Tool Testing

As part of this research, we evaluated tools suitable for OSINT investigations, focusing on commonly used, free, and open-source options. Various techniques, such as search operators, regular expressions, and multitasking tools, were explored. The testing included search engine operators, providing examples of commonly used operators to refine search results. Tools such as OSINT Framework, Maltego, TheHarvester, SpiderFoot, and ThreatMiner were tested for various aspects of OSINT investigations, including social media analysis, website technology detection, and domain name investigation. Regular expressions were used to structure and extract specific data from unstructured sources. Multipurpose tools like Maltego, TheHarvester, and SpiderFoot were assessed

for their ability to map relationships, gather organizational information, and perform passive intelligence.

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

OSINT Operational Process

Process Design

An OSINT operational process was designed for the target organization, which is used primarily for threat intelligence purposes, which is a core component of any organization's cybersecurity strategy. By consistently monitoring both existing and new threats and collecting and analyzing relevant data, an organization can significantly improve its defenses against cybercrime. The Threat Intelligence Lifecycle consists of six key stages: definition of objectives, data collection, data processing, data analysis, review of results, and feedback.[37]

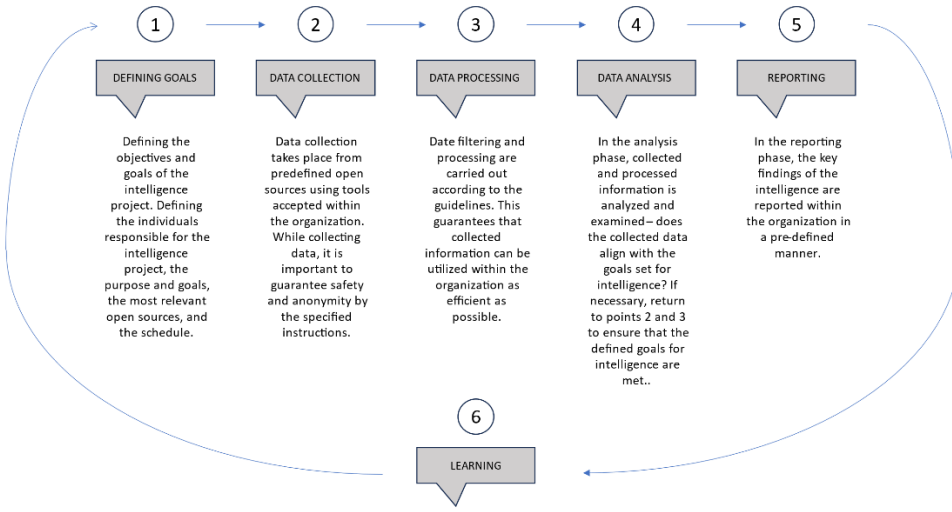

Figure 1: Designed OSINT Operational Process.

The operational process designed for the target organization (Figure 3) starts with the first step, i.e., defining the objectives of the data collection. At this stage, the purpose of the intelligence work is clarified, and the persons responcible for the execution of the task are selected. This role is usually assigned to pre-designated employees who are familiar with intelligence operations. In addition, the most important open sources are identified to ensure that data collection is as efficient as possible. At this stage, the schedule of the intelligence project is also defined.

The second step includes data collection, where information is collected from identified open sources. This data collection is performed using organizationally approved tools such as Maltego and SpiderFoot. When conducting active intelligence gathering – especially when processing data from the dark web – special care is taken to ensure that the organization's actions are protected in accordance with established guidelines.

In the third step, the collected data is filtered and processed according to the guidelines defined in advance by the organization. This step ensures that the information is aligned with the intelligence objectives set in the first step of the process.

In the fourth step, the filtered and processed data is analyzed to determine its relevance to the intelligence objectives. If the analysis confirms that the data meets these objectives, the process can proceed to the final stage of reporting. However, if the information does not meet the intelligence objectives, steps two and three are repeated. During this iteration, new open sources can be identified to ensure that the information collected is accurate and useful.

The last step of the operational process is reporting. At this stage, the analyzed data is compiled into a report, which is then presented to predetermined individuals or units in the organization. The report is written in a clear and concise manner so that even people without a technical background can easily understand the findings. Based on the report, possible additional measures are identified to improve the organization's security position further.

Process Testing

The operational process was tested by conducting an OSINT investigation on an employee of the organization, with prior permission obtained from the individual. The intelligence gathering began with clearly defined objectives: to collect as much information as possible about the person that could be used for targeted phishing attacks or other forms of manipulation.

Social media platforms were the primary sources of information, and specific tools were designated for this investigation, including Maltego, SpiderFoot, Google, and Google Maps. Data collection was efficient, and relevant information aligned with the intelligence objectives was found with relative ease. The collected data was thoroughly analyzed to confirm its relevance, with cross-verification from multiple sources. In this case, there was no need to revisit the data collection and processing steps, as sufficient information meeting the intelligence objectives was gathered.

The quality of the information was such that it could have been effectively used for targeted phishing or other forms of manipulation. After analyzing the data, a comprehensive report was created, detailing the findings of the investigation. This report was then presented to the subject of the investigation. Following the presentation, the report was reviewed with the individual, and guidance was provided on improving their online security. The required corrective actions were minimal, indicating that significant changes to the individual's online behavior were not necessary.

Unfortunately, due to the critical nature of the target organization, we are unable to report the results in detail. However, it can be concluded that one limitation of our research is that the OSINT data was collected over a limited timeframe. Future studies should focus on developing a tool that enables continuous collection and storage of OSINT data to create an archive and assess the long-term effectiveness of OSINT in risk management. Programmatic methods, such as automation and web-scraping, would expedite the data collection process. An organization's own OSINT tools provide greater control over data sources and content filters compared to off-the-shelf intelligence tools, thereby enhancing data integrity.

Discussion

Open-Source Intelligence (OSINT) is a crucial tool for maintaining an organization's cybersecurity. It can be used proactively to identify and predict potential threats and develop measures to mitigate these risks. This involves gathering publicly available information that threat actors could exploit against the organization, including details about employees that could be used in phishing or password cracking.

Practicing OSINT requires expertise. Professionals must be able to sift through large volumes of data to identify significant information and assess its relevance to the organization's security. Ethical and legal considerations are central to intelligence gathering; data collection must be limited to avoid violating privacy or rights. The use of technology in data collection can lead to unethical or illegal practices if human oversight and understanding of intelligence limitations are not prioritized.

The intelligence process must have a clear framework defining the goals and procedures of OSINT. While technology plays a significant role in accelerating information acquisition, human judgment is crucial for making ethical decisions. Documenting activities is essential to ensure ethicality. Automated systems can streamline research phases, allowing professionals to focus on analysis and value creation.

The target organization's cybersecurity risk assessment was implemented by designing an operational process for OSINT intelligence, enhancing the organization's cybersecurity management. The research method used was design science. The design of the operational process closely followed the seven principles of DSR, and the research met these principles' requirements.

Although our research focused on a company operating a critical infrastructure network, future studies should evaluate the effectiveness of OSINT in other industries to increase the generalizability of the results. Finally, it is important to understand that OSINT is free intelligence, and many tools used to obtain OSINT are free. However, in some cases, there may be costs associated with OSINT tools, such as LinkedIn Premium for more detailed searches. Nevertheless, the resources required to obtain OSINT should be considered value-added improvements to security.

As a future study, it would be interesting to find out how different actors in the financial sector utilize OSINT intelligence and its processes to maintain the threat field, acquire targeted threat information, and mitigate the initial stages of attack vectors with the help of OSINT. The focus of such research could be on the information gathered from the dark web, specifically what information about financial actors is found there and how cybercriminals can strategically use this information against financial institutions. This could be viewed, for example, through Lockheed Martin's Cyber Kill Chain framework, which is part of the Intelligence-Driven Defense model used to identify and prevent the activities of cybercriminals.[38]

Appendix 1. State-of-the-art OSINT tools

Tool function	Name	Function
User name check	Check user name	Helps to find user availability on social media
	Namechk	Helps to find social media account of user
	Namecheckr	Find social media account
	Usersearch Team	Find someone by username or email on Social Networks, Dating Sites, Forums, Crypto Forums, Chat Sitesp and Blogs
Real name search	Truth finder	Public record search engines of America
	Piple	Helps to find the real person
	Spokeo	Search by name, phone, address, or email to confidentially lookup information about people
	TruePeopleSearch	Helps to find real person
	US search	Transparent and informative source for finding addresses, phone numbers, and email addresses
	PeekYou Developers	Helps to find friends, relatives and colleagues across the Web
	Whitepage	Find people, contact info & Background checks
	Beenverifed	Find People, Vehicle, Property and Contact Info
	Address Search	Finding someone's email or finding out who is emailing you
	Lullar	Profile Search by Email First Last Name or Username
	Yasni	People search

	ProfleEngine	Provide complete website information
	Fast People Finder	People search by name, address search, or reverse phone lookup
	Thatthem	Find people by name, find who lives at an address, find people using phone number, emailp etc
	Webmii	People search engine
	Howmanyofme	People search engine
	Genealogy	Search family history
Email investigation	Email dossier	Investigate email address
	Emailhippo	Verify the email address
	Hunter	Email verifier
	Email Checker	Email checker
	Byte plant email validator	Email validator
	Email format	Check email format
	Scam dex	Scam emails archive
	Email-header analysis	Email header analysis tool
Phone number search	Zlookup	Check about the owner of a mobile number
	ReversePhoneLookup	Info about the owner of a mobile number
	Inter800	Locate products or services via a toll-free number
	Twilio	Instantly delivers you a caller ID name and person type
	Fonefinder	Info about the owner of a mobile number
	Truecaller	Info about the owner of a mobile number
	FreeCarrierLookup	The carrier name and whether the number is wireless or landline
	PhoneLookup	Info about owner of ь mobile number
IP geolocation information	IPverse	Provide list of IPs
	IP2Location	Provide info about IP geolocation
	IPfngerprints	Geographic location of an IP address along with some other useful information including ISP, Time Zone, Area Code, State, etc
	DB-IP	IP Geo-location API and database
	IP Location	Provide info about IP geolocation
	Utrace	Provide info about IP geolocation
Blacklisted IP address	Block List	Report attacks on your server
	FireHOL	Analyzes all available security IP Feeds, mainly related to on-line attacks, online service abuse, malwares, botnets, command and control servers and other cybercrime activities
	Directory of malicious IPs	Exact moment when the address was harvested and the IP address that gathered it
Image search	Imgur	Image Sharing and hosting site

	Photobucket	Image hosting and video hosting website
	SmugMug	Photo sharing site
	Flickrmap	Photo and video sharing site
	GettyImages	Capturing, creating and preserving content to elevate visual communications
	Instant logo search	Logo search
	Reuters pictures	Provide archive of images, video, audio, graphics and news
	News Press	Provides trending news of different types such crime, education, and politics and elections
	Associated press images portal	Collections of historical and contemporary photographs
	PA images	Image search in UK
	European Pressphoto Agency	Photo and video coverage of breaking news
	Canadian press images archive	Press images archive of Canada
Reverse image search	Google reverse search	All related images related to the name across Google
	Karmadecay	Source of image searched majorly across Reddit.
	TinyEye	To know the interests or different accounts a person is connected through just from image
	Reverse image search	Easy to access the sites containing the image was uploaded in it as a new tab opens and shows all links in it
	Cam finds App	All the places across the web where the image is present. Limited as it's a mobile application
	Image Identification project	The content of the image based on the result of AI. AI which determines the content inside the image, useful when bulk images to be analyzed
Image manipulation check	Forensically	Magnifiers, String analyzers, Clone Detections
	Fotoforensics	ELA, hidden pixels, Metadata, Strings, etc
	Ghiro	Metadata extraction, GPS Localization, Error level analysis, etc.; a fully automated tool designed to run forensics analysis over a massive amount of images, just using a user-friendly and fancy web application
	ExifTool	Metadata editing tool
	GeoSetter	Change the geo data linked with an image.exe file to be downloaded, but can be useful in modifying the info
	Lets Enhance	Higher-resolution pic, Unblurring any blurred image of usefulness

Video search	AOL	Videos are based on different categorizations. Very Less as pinpointing the information of the victim is difficult
	Start Page video search	General web search BUT helps leave no footprints behind
	Facebook video search	Browse through videos on Facebook
	Internet archive open-source movie	All the related media files on the web; gather huge amount of intel just from the name
	Meta tube	Results spread across Facebook. Required intel from Facebook
	Earthcam	Analyze the victim's surroundings
	Insecam	Live camera feed of nearest CCTV camera
	EzGif	Editand check hidden data in a video
	Video to text converter	Analyze the metadata of the video
Geospatial search	Digital globe	Map of the location, Explore the surroundings of a victim if the location is known
	Daum	Map of location, Limited as everything in Korean
	N2yo	Live feed from satellite to know relevant data
	Wiggle	Network maps of the location
	BB Bike	Different maps, placed side by side for easy comparisons
	Newspaper map	Intel over general interests in the area, News Papers brands used majorly in the area
	USGS	The US provided a map finally with meeting the set properties, Useful in narrowing down on a target
	Google map street view	Street view of the location or around it
	KartaView	Publicly available street views datasets
	ZoomEarth	Live satellite feed with weather and all
	Mapillary	Street view if available
	Address lookup	Address of the clicker, i.e., a process to make the victim click the button and get his address
	Viamichelin	The path between the locations
	Corona project	Map made by a US secret satellite in the 1970s used to know the old name of a place
	TripGeo	The animated path between the locations provided
	Mapquest	Map with a nearest public place like restaurants etc. nearby, Easy to explore a wide area
	Maphub	Collaborative Maps
	Perry-Castaneda library map collection	Map of the selected period, Get some really old maps and new maps too WayBack Machine of Maps

	Round shot	Live Cam active nearby, Explore nature, and understand a country
	Live earth map	Marks on locations where a recent natural disaster occurred, Understand the different problems different countries face with respect to natural disasters
Air movement tracking	Flightaware	Path and current location of a fight, track the live location of the target on the move
	Flight radar 24	Monitor Air Trafc at any location at any given time
	Air cargo tracker	Track the cargo loaded on the fight, Limited fights allow this feature so functionality is limited, too
	Radar box 24	Monitor Air Trafc at any location at any given time
	World Aircraft's database	Data related to fight, Dictionary of all the fights available
Maritime movements tracking	Marine traffic	Map of all the marine traffic around the world, Know the marine traffic around the required location
	Vessel finder	Map of all the marine traffic around the world, Know the marine traffic around the required location
	Cruise Mapper	Know the marine traffic around the required location
	Ship Finder	All the ships (named) at the location; Know where the major famous ships are located live
	Container prefix-list	All about different containers. Active, dead, in the dock, etc.
	Identification code of container owner	The exact location and details connected with code, Know in detail about the owner of the container
	Volza	Know the port codes of all ports on the globe to make searches easy
Package tracking	After ship	Live track after the drop
	Trackingex	Live tracking the package from the company perspective
	17 Track	Live track after the drop
	Package tracker	Live tracking the package from the company perspective
	Canada post	Locations and info about packages, Limited as restricted to only Canada
	Royal mail	Locations and info about packages, Limited as restricted to the only UK

Our research results demonstrate the significance of OSINT as an effective tool for risk assessment and enhancing an organization's security posture. Increasing attention is being paid to cybersecurity, particularly for critical infrastructure, to minimize cyber risks. As critical infrastructure companies seek ways to mitigate cyber risks, the results of this study are relevant to academic, practical, and policy-making audiences. Instead of relying on a faith-based approach to cybersecurity, we have provided evidence of a feasible method for conducting risk assessments to prevent attacks and improve network and application security. OSINT provides organizations with 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 warrant separate further studies. Further research is needed on the benefits that AI offers to OSINT intelligence and the challenges that may arise as AI technologies continue to develop.

Acknowledgment

This research is supported in part by the Secureu Project, number 2021-1-LV01-KA220-HED-000023056.

Endnotes

1 Abel Yeboah-Ofori, "Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media," *International Journal of Cyber-Security and Digital Forensics* 7, no. 1 (2018): 87–98, https://doi.org/10.17781/p002378.

2 "What is Open-source Intelligence, and how is it used?" BreachLock, August 8, 2022, https://www.breachlock.com/resources/blog/what-is-open-source-intelligence-and-how-is-it-used/.

3 Ashok Yadav et al., "Open-Source Intelligence: A Comprehensive Review of the Current State, Applications and Future Perspectives in Cyber Security," *Artificial Intelligence Review* 56, no. 11 (2023): 12407–38, https://doi.org/10.1007/s10462-023-10454-y.

4 "ERASMUS+ cooperation partnership in higher education 'Digital education tools for security risk management'," Project number: 2021-1-LV01-KA220-HED-000023056, 2022 - 2024, https://security.turiba.lv/about-the-project/.

5 Jyri Rajamäki and Stephen McMenamin, "Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence," In *International Conference on Cyber Warfare and Security*, Vol. 19, no. 1, March 2024, pp. 607-611.

6 Jyri Rajamäki and Krista Tiitta, "Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity," In *International Conference on Cyber Warfare and Security*, Vol. 19, no. 1, March 2024, pp. 612-616.

7 Alan Hevner, Salvatore March, Jinsoo Park, and Sudha Ram, "Design Science in Information Systems Research," *MIS Quarterly* 28, no. 1 (2004): 80–90.

[8] Babak Akhgar and Petra Bayerl, "Surveillance and Falsification Implications for Open Source Intelligence Investigations," *Communications of the ACM* 58, 8 (2015): 63.

[9] Leif Azzopardi, William Glisson, David Maxwell, and Sean McKeown, "Investigating people: a qualitative analysis of the search behaviours of open-source intelligence analysts," *IIiX'14: Proceedings of the 5th Information Interaction in Context Symposium*, 2014, pp. 175-176.

[10] Yeboah-Ofori, "Cyber Intelligence and OSINT" (2018).

[11] Azzopardi, Glisson, Maxwell, McKeown "Investigating people," (2014).

[12] Thea Riebe, et al, "Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey," *Proceedings on Privacy Enhancing Technologies*, vol. 2023, no. 1, Jan. 2023, pp. 477–93, https://doi.org/10.56553/popets-2023-0028.

[13] Yong-Woon Hwang, et al, "Current Status and Security Trend of OSINT," *Wireless Communications and Mobile Computing* 2022 (2022): 1–14, https://doi.org/10.1155/2022/1290129.

[14] Mohamed El-Guindy, "Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism," *Journal of Law and Emerging Technologies* 1, no. 1 (2021): 11–64, https://doi.org/10.54873/jolets.v1i1.32.

[15] A. Oikarinen, "Open-Source Intelligence – It's Incredible what you can find from public sources," *Nixu Insights*, April 8, 2020, https://www.nixu.com/blog/open-source-intelligence-its-incredible-what-you-can-find-public-sources, accessed August 29, 2024.

[16] Yadav, "Open-Source Intelligence" (2023).

[17] BreachLock ; "What is Open-source Intelligence, and how is it used?" (2022).

[18] Ryan Benito, et al, "An Automated Post-Exploitation Model for Cyber Red Teaming," *International Conference on Cyber Warfare and Security*, vol. 18, no. 1, 2023, pp. 25–34, https://doi.org/10.34190/iccws.18.1.978.

[19] BreachLock ; "What is Open-source Intelligence, and how is it used?" (2022).

[20] Sanjeev Arora, "The Hidden Threat: Exposing OSINT Exploitation in Cyber Attacks," *International Journal of Advanced Research in Science Communication and Technology* (April 2024): 421–25, https://doi.org/10.48175/ijarsct-17472.

[21] Ritu Gill, "What is Open-Source Intelligence?" SANS Institute, February 23, 2023, https://www.sans.org/blog/what-is-open-source-intelligence/.

[22] Kaspersky, "OSINT (Open-Source Intelligence)," 2023, https://encyclopedia.kaspersky.com/glossary/osint/, accessed August 29, 2024.

[23] Darren Hayes and Francesco Cappa, "Open-Source Intelligence for Risk Assessment," *Business Horizons* 61, no. 5 (Sept. 2018): 689–97, https://doi.org/10.1016/j.bushor.2018.02.001.

[24] Cláudio Martins and Ibéria Medeiros, "Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy," *ACM Transactions on Privacy and Security* 25, no. 3, Article 19 (2022): 2-5.

[25] BreachLock ; "What is Open-source Intelligence, and how is it used?" (2022).

[26] Hayes, Cappa, "Open-Source Intelligence for Risk Assessment" (2018).

[27] J.S. Slinde, "Unveiling the Potential of Open-Source Intelligence (OSINT) for Enhanced Cybersecurity Posture," Master's thesis, University of Agder, 2023.

[28] Imperva, "Open-Source Intelligence (OSINT)," https://www.imperva.com/learn/application-security/open-source-intelligence-osint/, accessed August 29, 2024.

[29] OSINT Framework, https://osintframework.com/, accessed August 29, 2024.

[30] Aubrey Byron, "OSINT need-to-knows: Intro to advanced search and Google dorking," September 22, 2024, https://authentic8.com/blog/osint-need-knows-intro-advanced-search-and-google-dorking.

[31] Josh Fruhlinger, Ax Sharma, and John Breeden, "15 top open-source intelligence tools," *CSO Online*, 15 Aug 2023, https://www.csoonline.com/article/567859/what-is-osint-top-open-source-intelligence-tools.html.

[32] Maltego, "Writing Custom Maltego Integrations," 28 Mar 2022, www.maltego.com/blog/writing-custom-maltego-integrations/.

[33] Christian Martorella, "theHarvester. Python," 2023. https://github.com/laramies/theHarvester.

[34] Steve Micallef, "Attack Surface Management. You're (probably) doing it wrong," *Medium*, August 26, 2021, https://medium.com/@micallst/attack-surface-management-youre-probably-doing-it-wrong-608719da1cab.

[35] ThreatMiner, "What is ThreatMiner?" *ThreatMiner.org*, 2023, https://www.threatminer.org/about.php

[36] Yadav, "Open-Source Intelligence" (2023).

[37] Snyk, "Threat Intelligence Lifecycle – Phases & Best Practices Explained," https://snyk.io/learn/threat-intelligence/threat-intelligence-lifecycle/, accessed August 29, 2024.

[38] Lockheed Martin, "Putting Intelligence to Work," www.lockheedmartin.com/en-us/capabilities/cyber/intelligence-driven-defense.html/, accessed August 29, 2024.

About the Authors

Dr. Jyri Rajamäki is an Adjunct Professor of Cybersecurity and Critical Infrastructure Protection with 35 years of experience in the ICT field. Currently, he contributes to several EU-funded research projects, with research interests in resilient cyber-physical systems and ethical governance of safety-critical and/or classified information. Dr Rajamäki has authored more than 200 scientific publications. https://orcid.org/0000-0003-4798-2462

Mr. Stephen **McMenamin** and Ms. Krista **Tiitta** have completed the Bachelor's degree programme in Business Information Technology, Cybersecurity at Laurea University of Applied Sciences. They are now proud alumni of Laurea.