

Role of Open Source Intelligence (OSINT) in Cybersecurity and Threat Analysis

Ernest O. NONUM., Oghenetega AVWOKURUAYE., Tochukwu M. EZEMONYE

Department of Computing Sciences, Admiralty University of Nigeria, Delta State

DOI : <https://doi.org/10.51583/IJLTEMAS.2025.140300023>

Received: 18 March 2025; Accepted: 22 March 2025; Published: 07 April 2025

Abstract: Open-Source Intelligence (OSINT) has existed prior to modern technology. Military and political organizations employed OSINT to gather intelligence on their adversaries and opponents, respectively, for strategic decision making. In this era, OSINT is used both for cyber attacks by bad actors and for detecting cyber attacks. Its importance in cyber security cannot be overemphasized, especially when coupled with artificial intelligence. The objectives of the study were outlined, including delving into the basics of OSINT, its use in cyber security and investigations of some selected tools and techniques employed in OSINT. This study relies on a desk research approach, where existing data from various sources are reviewed to get background knowledge on the topic under study. The reasons for undertaking this study are also stated. The use of OSINT comes with challenges, limitations, privacy concerns, legal and ethical considerations, and OSINT threats. The study provides insights on how they are tackled, as well as OSINT applications.

Keywords: Open Source Intelligence, OSINT, Cyber security, Threat Analysis

I. Introduction

Open-Source Intelligence (OSINT) plays a crucial role in modern cybersecurity and threat assessment, serving as a key tool for organizations aiming to secure their digital resources. According to the Office of Director of the US National Intelligence, Open-Source Intelligence refers to information that is publicly accessible in various formats such as printed or electronic media, including sources like radio, television, newspapers, journals, the internet, commercial databases, as well as videos, images, and drawings. This intelligence can be sourced from various platforms including the dark web. Information does not equate intelligence (Ritu, 2023), but when the collated open-source findings are critically analysed with the right mindset, the result becomes intelligence. As the digital landscape evolves, it is becoming increasingly vital for organizations to leverage OSINT to detect and mitigate emerging risks and vulnerabilities.

Initially used primarily by national security and law enforcement agencies, OSINT has become an essential resource for businesses and cybersecurity professionals. By analyzing open-source data, security teams can identify potential threats, understand adversary tactics, and spot weaknesses in their systems. This intelligence supports proactive defense strategies and enhances incident response during security breaches. OSINT collection can be categorized into two main methods: passive and active. Passive OSINT involves gathering information without direct engagement, such as monitoring social media or reviewing public databases. Active OSINT, on the other hand, requires direct interaction, such as conducting interviews or participating in online forums. Both methods are crucial for building a comprehensive threat profile and understanding the broader context of cyber risks. Despite its advantages, OSINT presents several challenges. The vast amount of publicly available data can result in information overload, making it challenging for analysts to identify useful insights. Additionally, malicious actors may exploit open-source information for harmful activities like social engineering or reconnaissance prior to launching an attack. As a result, organizations must adopt effective strategies and use advanced tools that integrate artificial intelligence and machine learning to efficiently process and analyze OSINT data. In conclusion, the role of Open Source Intelligence in cybersecurity is becoming increasingly significant as organizations face a growing array of cyber threats. By effectively utilizing OSINT, security teams can improve their situational awareness, strengthen their defense strategies, and better protect their critical assets from evolving cyber risks.

Several authors traced the origin of open-source intelligence (OSINT) from the beginning of the World War II, with the establishment of radio broadcast services, BBC Monitoring Service in 1939 by Great Britain, and Foreign Broadcast Monitoring Service (FBMS) in 1941 by the United States, aimed to collect and exploit information from open sources (Ludo, 2023). While some authors opined that OSINT have been in practice from time immemorial, even though the term was not coined until in the 1990s. FBMS evolved to Foreign Broadcast Intelligence Service (FBIS) under newly established CIA in 1947, the after the World War II, and further transformed to Director of National Intelligence's Open Source Center in 2005 (Shaurer and Störger, 2013). "Open-Source Intelligence" as a phrase and "OSINT" as an acronym were first publicly used by Robert Steele in an article from 1990.

The rapid rise of cyber breaches of which ByBit (2025) is of recent on large scale, necessitated the need for effective cybersecurity and threat analysis. OSINT as tools and techniques leverage on open-source information to stay ahead of bad actors by identifying vulnerabilities, profile targets and thus reducing attack surface. Despite its potentials, it comes with myriad of challenges, such as data overload, data privacy and reliability issues. However, its potentials has not been efficiently harnessed and integrated into cybersecurity practices. This study aims to fill these gaps by examining the fundamentals, importance, tools

and techniques, case studies, role of Artificial Intelligence in OSINT and threat analysis. The objectives of this research are as follows:

- i. Delve into the fundamentals of open source intelligence (OSINT).
- ii. Examine how OSINT is utilized within cybersecurity practices.
- iii. Analyze both the advantages and constraints of employing OSINT in cybersecurity contexts.
- iv. Investigate specific tools and techniques and tools employed for OSINT in cybersecurity applications.
- v. Evaluate the ethical and legal considerations surrounding OSINT usage in cybersecurity environments.
- vi. Analyze real-world case studies of OSINT utilization in cybersecurity incidents.
- vii. Investigate potential future applications of OSINT in cybersecurity.

This study is warranted due to the escalating need for effective cybersecurity strategies in response to the growing frequency and complexity of cyber threats. Open Source Intelligence (OSINT) comes with sophisticated layer of insight, tracking threat actors across digital forums, social networks, and more, enabling preemptive actions against potential attacks (Nema, 2024). Bad actors leverage OSINT to profile potential targets, understand its patterns, and identify vulnerabilities that may be exploited. Given its cost-effectiveness and ability to adapt to emerging threats, OSINT has become an essential tool for improving cybersecurity practices. This study will also educate internet users to limit what they share on the public domains, especially sensitive information in order to reduce their attack surface. Additionally, this research will address challenges related to information overload and misinformation, exploring how advanced technologies can optimize OSINT analysis for better security outcomes.

II. Literature Review

Thematic Review

This review organizes the literature around the following themes that are relevant to OSINT's role in cybersecurity and threat analysis.

OSINT as a Preventive Cybersecurity Tool: DiSiEM (2017) opined that all Security Operation Centres (SOC) analysts try to be updated about possible threats against the IT infrastructure of their organizations by following cybersecurity OSINT. This theme emphasizes the proactive value by particularly identifying vulnerabilities, and staying ahead breaches like ByBit (2025), thereby reducing their attack surfaces.

Challenges of Data Overload, Authenticity and Reliability: Harvesting information from the internet for OSINT can be tedious. The internet, one of the sources of OSINT contains billions of information, and determining the collected data authenticity and its reliability can be complicated. A problem of the authenticity and confirmation of open source information arise, if basic information are collected from other, unverified OSINT sources (Szabó, 2019, as cited in, Dobak, 2023). OSINT data therefore still requires review and analysis to be of use to decision makers.

Application in Profile Threat Actors: OSINT plays a role in profiling threat actors. Zachxbt, an on-chain analyst demonstrated this by meticulously analyzing ByBit (2025) Crypto breach and noted that transaction timing, wallet connections match Lazarous Group. Hence, he linked the attack to Lazarus Group, North Korea's elite cybercrime unit.

Cost-Effectiveness and Accessibility: World Customs Organization Report (2024) noted the cost-effectiveness and accessibility of OSINT in Customs administration, when compared with obtaining other classified or proprietary information. It is also considered cost-effective and easily accessible than other forms of intelligence, like human intelligence.

Conceptual Review

This conceptual review aims to evaluates the core concepts that support the role of OSINT in cybersecurity and threat analysis, in line with the study's objectives to establish theoretical foundation.

- i. **Meaning and Definition of OSINT:** Open-Source Intelligence
WCO (2024) defines OSINT Open-source intelligence (OSINT) refers to the process of collecting, analysing, and utilizing information that is publicly and commercially available to support intelligence and decision making processes.
- ii. **Cybersecurity:** According to Cisco, cybersecurity involves safeguarding systems, networks, and programs against digital threats and attacks.
- iii. **Threat:** A threat is a potential negative event or malicious act that exploits a vulnerability in a system or application with the intent to damage data, steal data, or disrupt digital life in general.
- iv. **Threat Analysis:** Threat analysis is the process of identifying and assessing the characteristics of potentially harmful threats and files.

Review of Related Works

Open Source Intelligence (OSINT) is a form of intelligence gathering that has evolved considerably since its beginnings in military and political domains, where it was primarily used for espionage and strategic intelligence collection. Schaurer, F. and Störger, J. (2013) viewed the concept of OSINT as the gathering, processing, analysis, production, classification, and distribution of information obtained from sources and methods that are publicly accessible and legally available for use by the public, in response to official national security needs.

OSINT originated from the military settings, where the process is used for espionage and strategic intelligence gatherings (Steve, 2023). Prior to World War II, monitoring radio broadcasts and news sources was crucial for military and political decision-making (Homeland Security Today, 2024). The military relied on these earliest forms of intelligence gathering using newspapers, radio broadcasts, journal, press clippings to gather valuable information about their adversaries during World War II, These sources are still in use today.

Publicly available data increased tremendously with the advent of the internet in the 1990s. Allowing investigators to quickly find and access relevant information on a global scale from websites, forums, social media platforms, and search engines. With the increase of digital devices, especially smartphones, there has also been a corresponding increase in cyberattacks. As internet users increasingly share sensitive information about their personal lives and workplaces online, bad actors take advantage of this information to monitor their targets. They identify weaknesses or vulnerabilities and develop ways to exploit them based on what is shared. Example, a photo of EXIF file format contains metadata of the image, which could be exploited by a malicious actor. Geolocation data embedded in EXIF metadata can reveal the location where the photo was taken, date and time it was captured, image orientation, camera setting, software information etc.

It is noteworthy that there are other forms of intelligence gathering. Such as SIGINT, HUMINT, GEOINT and MASINT. OSINT is distinct from these forms in that it does not require special clearance and relies on publicly available information while the other forms often involve covert or unauthorized access to private data or individuals and require specialised tools to collect data.

OSINT is also sourced in the dark web of the internet. In the dark web, exploits in their development phase are transacted. These allow analysts to be aware of zero day flaws, and act accordingly.

Steps of OSINT

Efim (2024) outline the steps of OSINT as shown in the Fig 1 below:

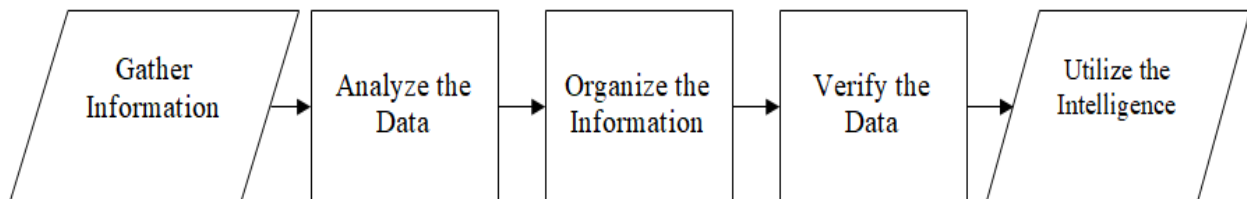


Fig 1: OSINT Steps

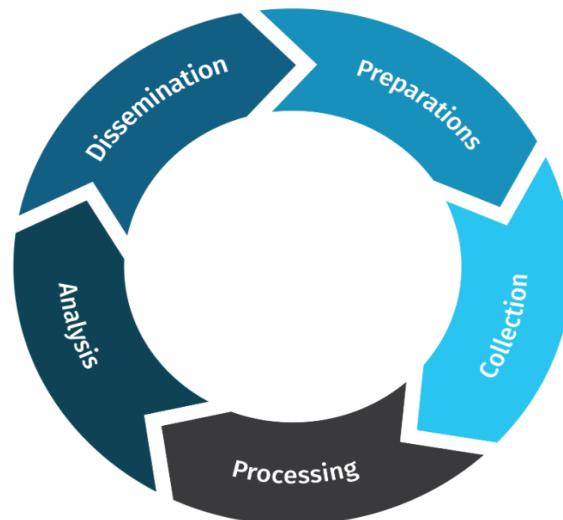


Fig 2: OSINT Cycle

Source: SANS Institute

Parts of OSINT Activity

Data Collection: This is the foundation of OSINT. It is the process of gathering data from publicly available sources such as the internet using search engines like Google, Intelligence X, Shodan, Duckduckgo or from non-internet sources - books, newspapers, journals etc. According to Kriesch (2024), “data collection includes exploring sources, monitoring sources, collecting data, and storing open source data”.

Data Processing: This involves separating unwanted data from wanted ones which are then converted to meaningful data. Also, during the indexing process, all data should be compiled to gather metadata and attributes, which can then be analyzed and correlated afterward (Kriesch, 2024).

Data Exploitation: It is also referred to as the analysis phase (Yogish P & Krishna P, 2021). It involves verifying the originality or authenticity and credibility of the processed data and contextualization. Contextualization is the process of assembling various sources of open source information into an output that give a comprehensive understanding of a subject (Williams, 2018 cited in Yogish P & Krishna P, 2021).

Data Interpretation: This stage involves transforming the open source information to open source intelligence (Gibson et al., 2016).

Importance of Osint in Cybersecurity

OSINT plays a role in detecting potential threats early in the attack lifecycle. By analyzing data for keywords associated with a potential attack, security analysts can learn to spot when cybercriminals are in the planning stages by monitoring multiple channels, searching for mentions of a data breach. Potential warning signs could include discussions of weaknesses, credentials that have been compromised being sold on dark web marketplaces, or hackers preparing Distributed Denial of Service (DDoS) attempts.

By monitoring social media platforms and other sources, organizations can stay one step ahead of cybercriminals. DiSiEM (2017) opined that all Security Operation Centres (SOC) analysts try to be updated about possible threats against the IT infrastructure of their organizations by following cybersecurity OSINT. Thus, reducing surface attack and proactively staying ahead of cyber attackers.

OSINT activities are performed to identify vulnerabilities within an organization's infrastructure. For example, performing OSINT can expose employee's weak or compromised passwords, leaked databases of customers. Consider how an organisation will lose reputation if their customers' information is exposed to the public.

Dark web monitoring can be performed by individuals, businesses, governments, law enforcement agencies, cybersecurity professionals to stay ahead of bad actors and be aware of potential threats. (Alanoud A, et al., 2023). Dark web monitoring is used for OSINT in cybersecurity to monitor and track activities that take place on the dark web, which is not easily accessible. Only specialized software, such as the Tor browser, is used.

Security teams can leverage OSINT to trace the attacker's digital footprints, such as social media activity, IP addresses, and forum communications. This information aids security professionals in understanding the execution of the attack, identifying the threat actors, and supporting law enforcement in taking legal action.

Role of Artificial Intelligence in Osint

Artificial Intelligence (AI) involves the imitation of human cognitive processes by machines, particularly computer systems. It is the use of advanced technology to automate data collection and analysis. AI in the areas of machine learning, pattern recognition and natural language processing plays a major role in OSINT. According to Yoyish P & Krishna P (2021), AI tools have significantly reduced the challenging task of OSINT activity due to the enormous amount of data available. It has made OSINT activity much faster, accurate and reliable.

AI enhances better search options. For example, generative Ai like ChatGPT enables investigators to obtain numerous Google search queries for a key keyword. Such as “Generate a list of Google search queries using the legal name “Ezemonye Tochukwu” to find various types of information”. Generative AI can be used by investigators to craft a persuading message for social engineering targeted at a profile, for the essence of obtaining information. AI tools like lenso.ai are used to process and analyse images.

III. Methodology

To collect data for this study, we employed a desk research method (secondary research). Existing data from various sources were thoroughly reviewed to gather background information on the topic. The reviewed sources comprised books, journals, and online resources from web and videos. In addition, insights obtained through discussions with colleagues were incorporated into the study. Consequently, this paper utilized content analysis, drawing conclusions from a range of literature on the subject.

IV. Discussion, Finding and Analysis

Some Osint Tools & Techniques for Cybersecurity

Google Dork

Dorking is the practice of utilizing advanced search operators such as intitle, inurl, filetype, OR, AND, -, *, etc in search engines, especially Google, to find hidden information that is not easily discovered through regular search queries. Nazrul (2024) opined that dorking is a powerful method that allows users to retrieve specific data, such as file types, website vulnerabilities or sensitive information that may be unintentionally exposed online. Google dork has been in use since 2002.

Case Study: In this case study, An OSINT expert was tasked with searching for any article on insecurity by Ezemonye using google dorking/hacks.

Keyword used: intext:"insecurity" AND "Ezemonye"

Findings: The output in Fig 3, shows a works written by different authors in which Ezemonye is cited. The quotation mark as used in the Google dork, searches for a specific term, AND is used as addition.

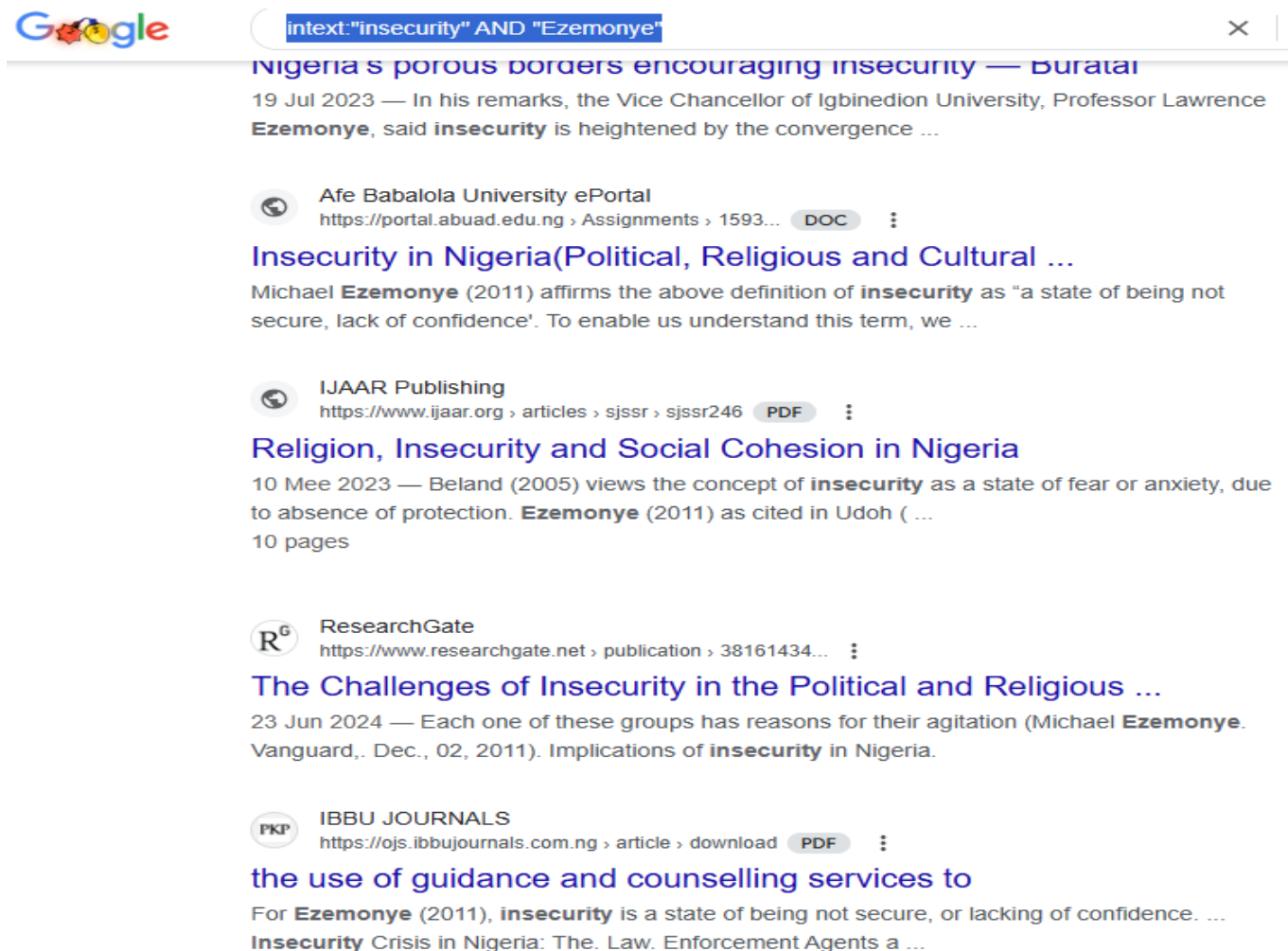


Fig 3: Case Study I

Source: Google

Case Study:

Keyword used: "Ernest Nonum" *engineer

Findings: The output indexes only searches related to Ernest Nonum as engineer.

Case Study: Searching for sub-domain.

An OSINT expert is tasked to find all sub-domain linked to a university official site. This can be achieved using the keyword site and the minus sign (-), as shown below.

Keyword used: site:unn.edu.ng -www

Findings: The results only all the sub domains of unn.edu.ng as seen in Fig 4. The minus sign is used to exclude a particular information that is not needed.

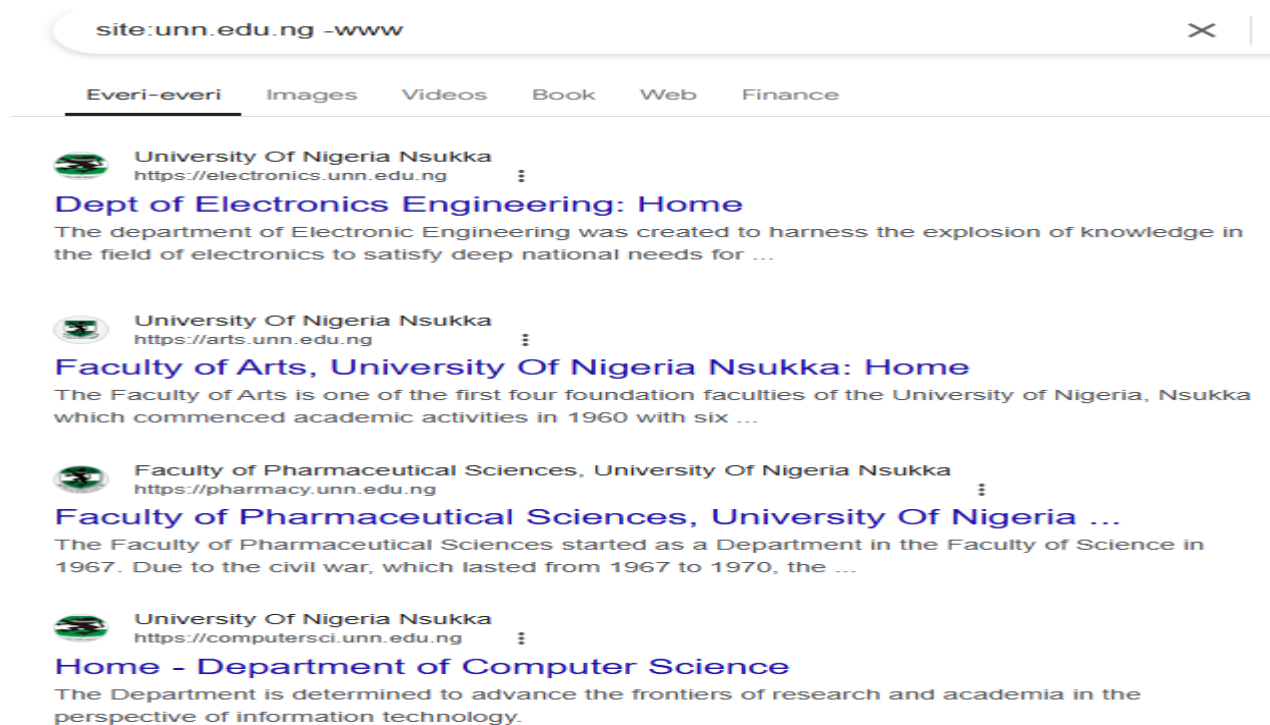


Fig 4: Searching for subdomains

Source: Google

Also, plus sign “+” or “AND” can be used to include specific information. Example shown below:

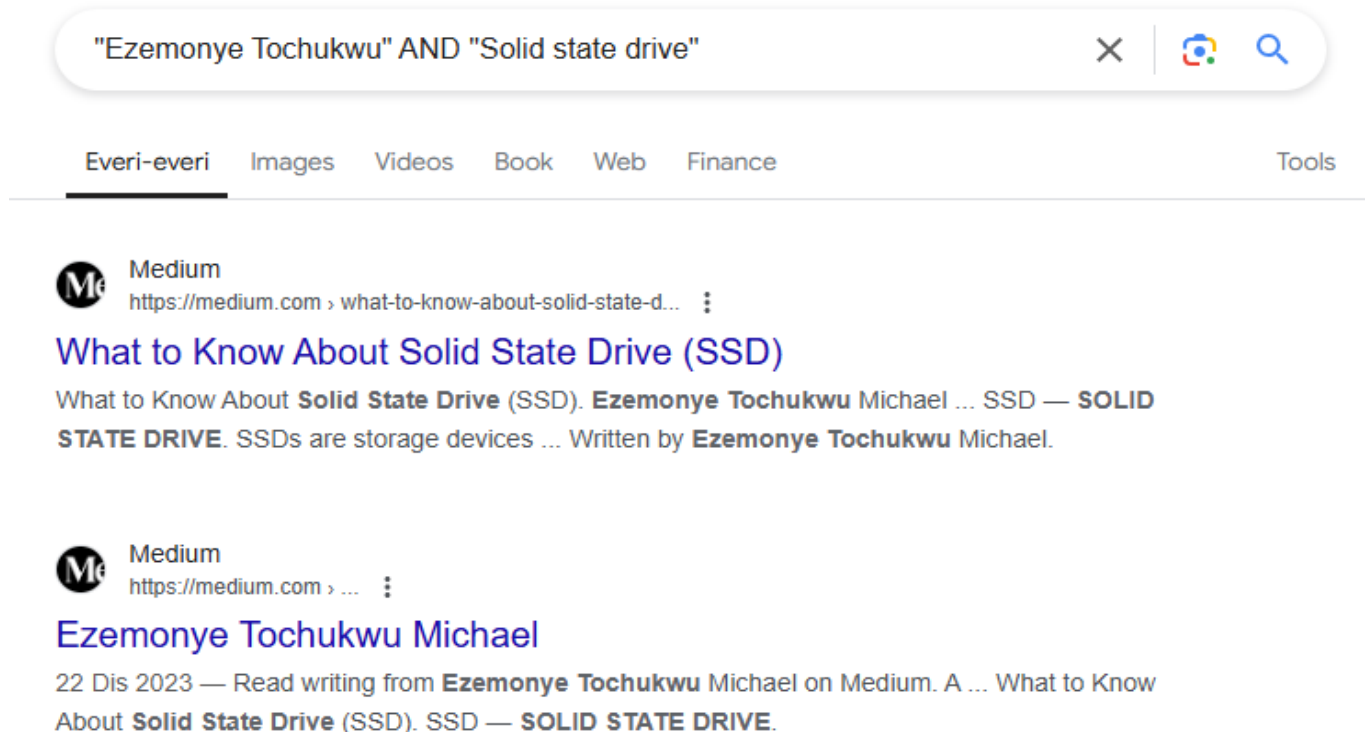


Fig 5: Case Study IV

Source: Google

Google Advanced Search (https://www.google.com/advanced_search) could be used too. Other google dork keywords can be obtained from Google Hacking Database (GHDB).

Managing Google Dorking

Protection for Google dorks is managed in robots.txt of web servers, but it does not guarantee security. Robots.txt is a text file in a website root directory that instructs web crawlers like Google bot on which pages of a site they are allowed or disallowed to search for information. Robots.txt is used in OSINT to prevent access to sensitive information. However, google dorking can still access sensitive information from a website even if robots.txt blocks access to the pages, hence the need to secure the files properly.

To view a website's robots.txt, type on a browser URL, the web address of the target site followed by forward slash and robots.txt. Example: www.google.com/robots.txt in Fig 6

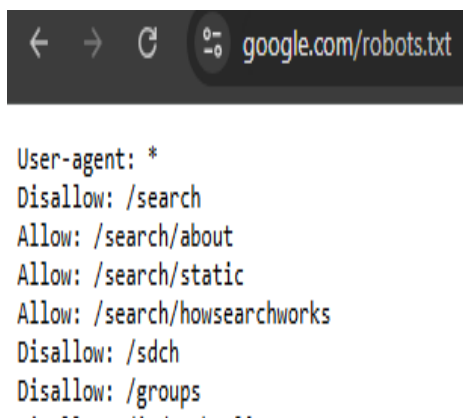


Fig 6: Robots.txt

Source: Google

OSINT Framework

According to eSecurity Institute, Justin Nordine developed and authored OSINT Framework. It is an important online tool for researchers, categorizing open source intelligence resources by source, type, and context, and is used for online investigations, including domain analysis, email analysis, social media analysis, and more.

The web address is <https://www.osintframework.com>

Builtwith

Builtwith is a tool that allows investigators to understand the technologies used in building websites. Official website is www.builtwith.com.

Wappalyzer

Just like Builtwith, Wappalyzer allows investigators to understand and analyse the technologies used in building web application. The image below shows the technology used to build www.example.com which is a HTML.

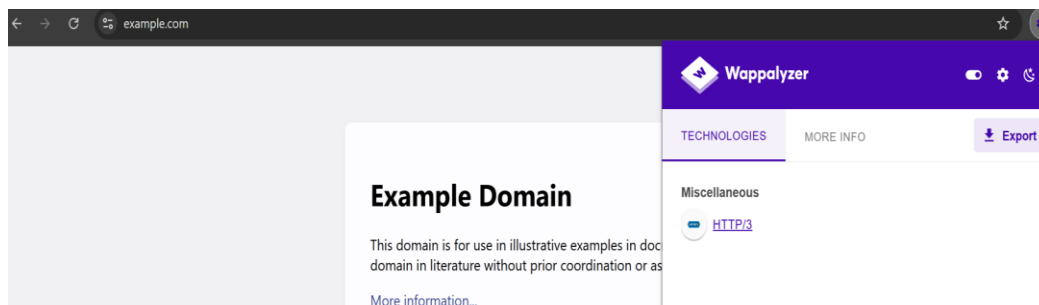


Fig 7

Have I Been Pwned

Have I Been Pwned lets you search through various data breaches to check if your email address or phone number has been exposed. The official site is <https://www.haveibeenpwned.com>

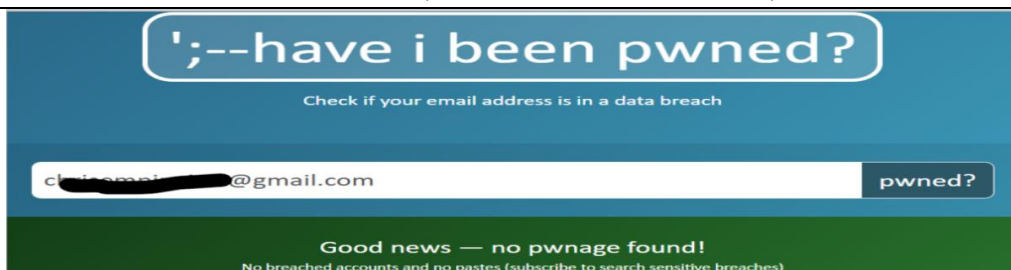
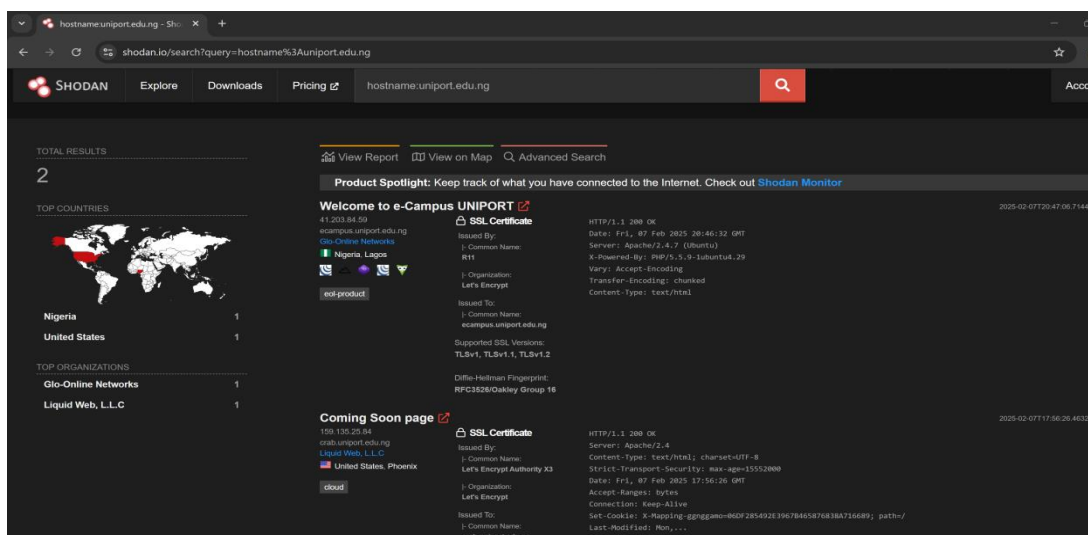


Fig 8: Have I been Pwned

Shodan (Sentient Hyper-Optimised Data Access Network)

Shodan is a search engine for internet-connected devices, created to map and collect data on internet-connected devices and systems.



the Harvester

According to Kali.org, theHarvester is a tool designed to harvest subdomain names, email addresses, virtual hosts, open ports/banners, and employee names and other publicly available data.

Nmap

Nmap is a free security scanner that is used to map networks to discover hosts on a network, open ports, OS versions, firewalls on the network etc. It is a free and open source utility used to discover networks and for security audits (Nmap.org).

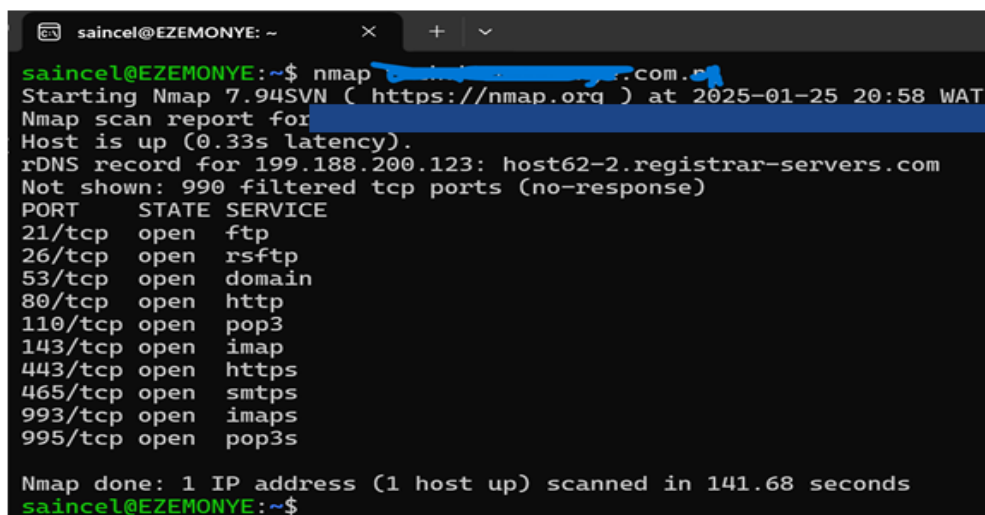


Fig 9: Scan result

Intelligence X

Intelligence X is a search engine used for searching for and collecting data from various publicly available online sources, including content from the deep web and dark web. The official website of Intelligence X is <https://www.intelx.io>.

Maltego

Maltego is a robust OSINT (Open Source Intelligence) and graph analysis tool commonly used for data mining, link analysis, and visualizing connections between individuals, organizations, websites, domains, IP addresses, and other digital assets. <https://www.maltego.com/> is the official website of Maltego.

TinEye

TinEye is a reverse image search engine and recognition tool that proffers image search solutions.

Yandex

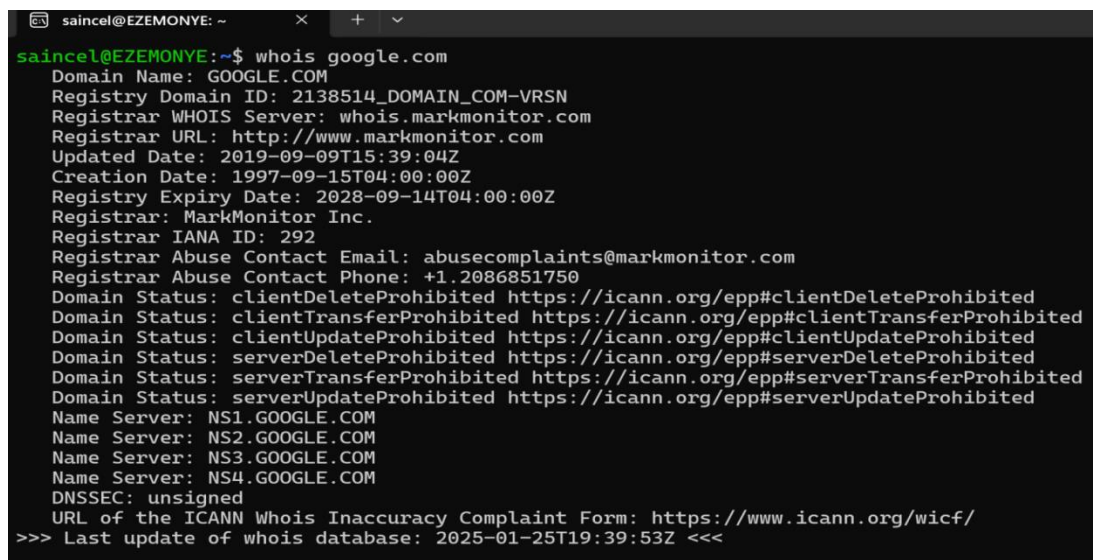
Yandex is a search engine, just like Google but most widely used in Russia and her neighbours. It has several products and services such as Yandex Search, Maps, Image, Video, Translate etc.

Google Lens

Google Lens is used in OSINT investigations to search for information based on images or real world objects using a smartphone camera or an existing image.

Whois

Whois is a tool used to get information about websites such as domain name information such as date hosted and expiring date, registered email, status, registrar, name server, registrant contact details such as name, city, admin contact, technical contact and billing contact. The image is show information on Google using whois tool.



```
saincel@EZEMONNYE: ~
saincel@EZEMONNYE:~$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-01-25T19:39:53Z <<<
```

Fig 10: whois google.com result

Source: Ubuntu 24.04.1 LTS

Creepy

A python code that uses EXIF information in publicly available images from social media and other sources to track and retrieve geolocation and display it on a map. EXIF stands for Exchange Image File Format, which is a format that shows technical data about an image.

applications of osint in threat analysis

The use of OSINT has enabled security analysts and other OSINT practitioners to develop a full profile of their targets and gain high-level intelligence by mining public records.

Publicly available information from social media or forums provide good insight, which is generally used from the stages like threat analysis, risk and threat management, etc, which ultimately enhance the overall security posture of the organization.

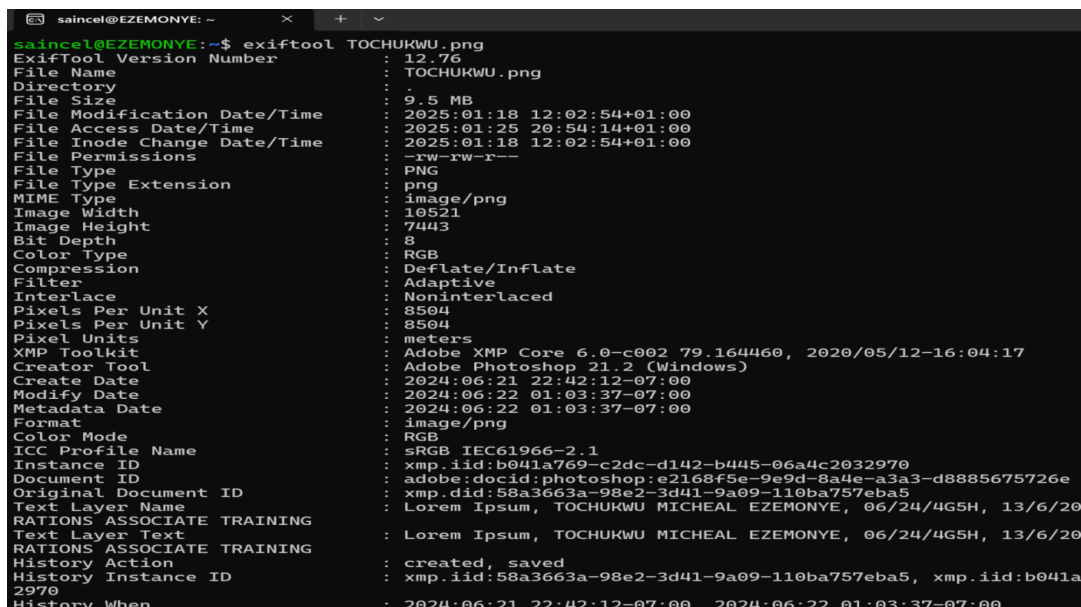
Law enforcement agencies used OSINT to collect data about security concerns in order to improve protection of people and properties.

Case Study - Image Analysis

Images often contain metadata that can lead to the image identification and location. While bigger social media platforms like Facebook remove such metadata before uploading, lesser platforms carry them.

An image of interest was uploaded on the dark web from an unknown person. OSINT is performed to unravel the source, location and the creation date of the image.

The pictures below show the steps followed to get the metadata of the image using EXIFTOOL.



```
saincel@EZEMONYE: ~  
saincel@EZEMONYE:~$ exiftool TOCHUKWU.png  
ExifTool Version Number      : 12.76  
File Name                    : TOCHUKWU.png  
Directory                   : .  
File Size                    : 9.5 MB  
File Modification Date/Time   : 2025:01:18 12:02:54+01:00  
File Access Date/Time        : 2025:01:25 20:54:14+01:00  
File Inode Change Date/Time   : 2025:01:18 12:02:54+01:00  
File Permissions              : -rw-rw-r--  
File Type                    : PNG  
File Type Extension          : png  
MIME Type                    : image/png  
Image Width                  : 10521  
Image Height                 : 7443  
Bit Depth                    : 8  
Color Type                   : RGB  
Compression                  : Deflate/Inflate  
Filter                       : Adaptive  
Interlace                    : Noninterlaced  
Pixels Per Unit X             : 8504  
Pixels Per Unit Y            : 8504  
Pixel Units                  : meters  
XMP Toolkit                   : Adobe XMP Core 6.0-c002 79.164460, 2020/05/12-16:04:17  
Creator Tool                  : Adobe Photoshop 21.2 (Windows)  
Create Date                  : 2024:06:21 22:42:12-07:00  
Modify Date                   : 2024:06:22 01:03:37-07:00  
Metadata Date                : 2024:06:22 01:03:37-07:00  
Format                       : image/png  
Color Mode                   : RGB  
ICC Profile Name              : sRGB IEC61966-2.1  
Instance ID                   : xmp.iid:b041a769-c2dc-d142-b445-06a4c2032970  
Document ID                   : adobe:docid:photoshop:e2168f5e-9e9d-8a4e-a3a3-d8885675726e  
Original Document ID         : xmp.did:58a3663a-98e2-3d41-9a09-110ba757eba5  
Text Layer Name               : Lorem Ipsum, TOCHUKWU MICHEAL EZEMONYE, 06/24/4G5H, 13/6/20  
RATIONS ASSOCIATE TRAINING    : Lorem Ipsum, TOCHUKWU MICHEAL EZEMONYE, 06/24/4G5H, 13/6/20  
Text Layer Text               : created, saved  
History Action                 : xmp.iid:58a3663a-98e2-3d41-9a09-110ba757eba5, xmp.iid:b041a  
History Instance ID           : 2024:06:21 22:42:12-07:00, 2024:06:22 01:03:37-07:00  
History When                   :
```

Fig 11: Image metadata

Source: Ubuntu 24.04.1 LTS

The above screenshot contains the original GPS coordinates of the image and other relevant information needed for your OSINT investigations.

Mitigating Osint Threat

OSINT is beneficial to investigators, though it comes with challenges and threats. However, OSINT threats can be reduced by being proactive. The following are some of the ways, OSINT threat can be minimized.

DeepFake Detection: Cyber criminals use DeepFake technology to create fake videos for malicious purposes. DeepFakes are image synthesis technology which creates digitally altered images of persons in a video, which are used for manipulation or misinformation. DeepFakes are detected with the use of DeepWare AI (deepware.ai). It can also be detected by observing the tones of the different parts of the body.

Advanced technologies are used to detect misinformation and disinformation and use of automated monitoring systems to scan the web for sensitive data exposure and sock puppets (an online identity used for the purpose of deception).

Legal, Ethical and Privacy Consideration

OSINT is considered legal since it involves publicly available records, however, It is prohibited by law if the information obtained is used for illegal purposes. Privacy rights should be respected by obtaining valid consent from data sources while adhering to OSINT Code of Ethics. Authenticity of Information from these data sources should be verified and attributed. It is not in the interests of individuals for their records to be exposed to the public, however, there is a need to maintain a balance between legitimate use of OSINT for information gathering purposes and respecting individual's privacy rights (Scott B, 2024).

Due to the metadata that comes with image files, some social media platforms often remove this metadata from photos due to privacy concerns.

Legal frameworks like the General Data Protection Regulation (GDPR) establish stringent rules for data collection, compelling organizations to maintain transparency and accountability.

Challenges and Limitation of Osint in Cybersecurity

OSINT activity does not come without challenges and limitations. However, OSINT experts should try to minimize these challenges in order to get an accurate open source intelligence for strategic decision-making. These challenges and limitations

range from information overload to false information available in the public domain. According to Hribar et al. (2014), unstructured data, false information available on the internet and legal issues are some of the challenges faced by OSINT (cited in Yogish P & Krishna P, 2017). Unstructured data sources are feeds that provide unstructured data where the main content is free text format (DiSiEM, 2017). Examples are news sites, X (formerly Twitter).

Performing OSINT activity is tasking and time consuming especially in that area of data collection. Hence tools are used to collect and process OSINT, and also extract only the needed parts, thereby reducing the time consumption.

In the course of performing OSINT, investigators often encounter contents that may appear encrypted or suspect messages hidden in pictures, if the size is unusual. These challenges are addressed using OSINT cryptography. Hiding messages in another, the process is termed steganography.

Information Overload: The sheer amount of available information can make it difficult to know what is of value. Determining the collected data's source and its reliability can be complicated. OSINT data therefore still requires review and analysis to be of use to decision makers. Information overload can be solved by automating data collection and processing.

Collection of Misinformation: Misinformation spreads faster on social media platforms. Websites like FactCheck.org offer resources for disproving common myths and misinformation on social media.

Future of Osint in Cybersecurity

Integration of advanced technologies such as web scraping or web crawling to automate and aid data collections and processing and automated systems for real-time monitoring.

Blockchain integration for data integrity and reliability in OSINT can enhance security by ensuring that the collected information remains immutable and can be verified.

V. Conclusion

This paper examines the fundamentals of OSINT and its role in cybersecurity and threat analysis. It also explores some techniques and tools used to gather and analyze OSINT data. OSINT investigators leverage on publicly available information, to identify, monitor and mitigate threats. By integrating OSINT into cybersecurity strategies, organizations can enhance their overall security posture, detect threats early.

Reference

1. Ludo Block (2023). The long history of OSINT, Journal of Intelligence History, DOI: 10.1080/16161262.2023.2224091 Office of the Director of National Intelligence. What is Intelligence. Retrieved from <https://www.dni.gov/index.php/what-we-do/what-is-intelligence>
2. Ritu Gill, 2023. What is Open-Source Intelligence. SANS. Retrieved from <https://www.sans.org/blog/what-is-open-source-intelligence/> Cisco. What is Cybersecurity? Retrieved from <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html>
3. Alanoud A. et al., 2023. How Dark Web Monitoring can be Used for OSINT and Investigations. Journal of Theoretical and Applied Information Technology, Vol.101. No 10. Dep of Computer Networks and Communications, CCSIT, King Faisal University, Al Hassa 31982, Saudi Arabia. Retrieved from <https://www.jatit.org/volumes/Vol101No10/15Vol101No10.pdf>
4. Nema M., 2024. The Role of Open Source Intelligence in Advancing Cybersecurity. Uniethena. Retrieved from <https://uniathena.com/role-open-source-intelligence-advancing-cybersecurity>
5. Yogish P., & Krishna P., 2021. Open Source Intelligence & its Applications in Next Generation Cyber Security - A Literature Review. International Journal of Applied Engineering & Management, IJAEM Vol. 5. College of Computer Science & Information Science, Srinivas University, Mangalore, India.
6. Kriesch S. J., 2024. Integrating OSINT and Cyber Threat Intelligence to Enhance the Security of Enterprise IoT. University of Bamberg. Retrieved from <https://www.researchgate.net/publication/381045472>
7. DiSiEM, 2017. Techniques & Tools for OSINT-based Threat Analysis. Gibson H., Ramwell S.S., & Day T., (2016). Analysis, Interpretation and Validation of Open Source Data. In Open Source Intelligence Investigation from Strategy to Implementation. Springer-Verlay.
8. Scott B., 2024. The Ethical Considerations of OSINT: Privacy vs Information Gathering. Retrieved from <https://www.medium.com/@scottbolen/the-ethical-considerations-of-osint-privacy-vs-information-gathering-63b5b2f76c55>
9. World Customs Organization (2024). Study Report. Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement. Retrieved from https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/security-programme/osint-report_final.pdf
10. Cisco, 2023. What is Cyber Threat Intelligence? <https://www.cisco.com/c/en/us/products/security/what-is-cyber-threat-intelligence.html>

11. Steve, A. 2023. A History of OSINT: From Informing Spies to Detecting Lies. Skope Now <https://www.skopenow.com/news/a-history-of-osint>
12. Schaurer, F. and Störger, J. 2013. The Evolution of Open-Source Intelligence. The Intelligencer. Journal of the US Intelligence Studies Vol 19. No. 3. https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf
13. Homeland Security Today, 2024. Evolution of OSINT: From Coup Crisis to Cutting-Edge Advancements with Social Media, AI, and Data Analytics <https://www.hstoday.us/subject-matter-areas/intelligence/evolution-of-osint-from-coup-crisis-to-cutting-edge-advancements-with-social-media-ai-and-data-analytics/> eSecurity Institute, 2023. OSINT Framework. <https://www.esecurityinstitute.com/osint-framework/> Retrieved from <https://www.x.com/zachxbt?t=3Eu1FcA3tVKNFb12guMbQ&s=09Nmap>. <https://www.nmap.org/>
14. Canonical Ltd. (2024). Ubuntu Linux (Version 24.04.1 LTS). Retrieved from <https://www.ubuntu.com/>
15. Dobak, 1., 2024. Data Collection in the OSINT Investigation. Ludovika University of Public Service. Retrieved from <https://www.researchgate.net>
16. Ludo Block (2023). The long history of OSINT, Journal of Intelligence History, DOI: 10.1080/16161262.2023.2224091 Office of the Director of National Intelligence. What is Intelligence. Retrieved from <https://www.dni.gov/index.php/what-we-do/what-is-intelligence>
17. Ritu Gill, 2023. What is Open-Source Intelligence. SANS. Retrieved from <https://www.sans.org/blog/what-is-open-source-intelligence/> Cisco. What is Cybersecurity? Retrieved from <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html>
18. Alanoud A. et al., 2023. How Dark Web Monitoring can be Used for OSINT and Investigations. Journal of Theoretical and Applied Information Technology, Vol.101. No 10. Dep of Computer Networks and Communications, CCSIT, King Faisal University, Al Hassa 31982, Saudi Arabia. Retrieved from <https://www.jatit.org/volumes/Vol101No10/15Vol101No10.pdf>
19. Nema M., 2024. The Role of Open Source Intelligence in Advancing Cybersecurity. Uniethena. Retrieved from <https://uniathena.com/role-open-source-intelligence-advancing-cybersecurity>
20. Yogish P., & Krishna P., 2021. Open Source Intelligence & its Applications in Next Generation Cyber Security - A Literature Review. International Journal of Applied Engineering & Management, IJAEM Vol. 5. College of Computer Science & Information Science, Srinivas University, Mangalore, India.
21. Kriesch S. J., 2024. Integrating OSINT and Cyber Threat Intelligence to Enhance the Security of Enterprise IoT. University of Bamberg. Retrieved from <https://www.researchgate.net/publication/381045472>
22. DiSiEM, 2017. Techniques & Tools for OSINT-based Threat Analysis. Gibson H., Ramwell S.S., & Day T., (2016). Analysis, Interpretation and Validation of Open Source Data. In Open Source Intelligence Investigation from Strategy to Implementation. Springer-Verlay.
23. Scott B., 2024. The Ethical Considerations of OSINT: Privacy vs Information Gathering. Retrieved from <https://www.medium.com/@scottbolen/the-ethical-considerations-of-osint-privacy-vs-information-gathering-63b5b2f76c55>
24. World Customs Organization (2024). Study Report. Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement. Retrieved from https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/security-programme/osint-report_final.pdf
25. Cisco, 2023. What is Cyber Threat Intelligence? <https://www.cisco.com/c/en/us/products/security/what-is-cyber-threat-intelligence.html>
26. Steve, A. 2023. A History of OSINT: From Informing Spies to Detecting Lies. SkopeNow <https://www.skopenow.com/news/a-history-of-osint>
27. Schaurer, F. and Störger, J. 2013. The Evolution of Open-Source Intelligence. The Intelligencer. Journal of the US Intelligence Studies Vol 19. No. 3. https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf
28. Homeland Security Today, 2024. Evolution of OSINT: From Coup Crisis to Cutting-Edge Advancements with Social Media, AI, and Data Analytics <https://www.hstoday.us/subject-matter-areas/intelligence/evolution-of-osint-from-coup-crisis-to-cutting-edge-advancements-with-social-media-ai-and-data-analytics/> eSecurity Institute, 2023. OSINT Framework. <https://www.esecurityinstitute.com/osint-framework/> Retrieved from <https://www.x.com/zachxbt?t=3Eu1FcA3tVKNFb12guMbQ&s=09Nmap>. <https://www.nmap.org/>
30. Canonical Ltd. (2024). Ubuntu Linux (Version 24.04.1 LTS). Retrieved from <https://www.ubuntu.com/> Dobak, 1., 2024. Data Collection in the OSINT Investigation. Ludovika University of Public Service. Retrieved from <https://www.researchgate.net>