e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

A REVIEW: THE ROLE OF OPEN-SOURCE INTELLIGENCE IN MODERN CRIME INVESTIGATION AND SECURITY THREATS

Prasanna Tanaji Gaikwad[*1], **Vikram Hankare**[*2]

[*1,2]Department of Forensic Science, Yashwantrao Chavan Institute of Science (Autonomous), Satara, Maharashtra, India

ABSTRACT

Open-Source Intelligence is modern method of investigation which help to minimize the business threats and also play important role in the crime investigation. Various techniques and methods are used to help the organization which decrease the crime as well as threat rate. The fundamental use of open-source intelligence is to protect the business from external threats. It covers fundamental methods, information cycle models, entity classification, search engine capabilities, social network research, and penetration tests. web-based applications and services that automate data extraction processes. It covers various methods, including graphical interfaces and command-line interfaces, and their usage, ensuring users can easily explore and understand the tools effectively. Use of OSINT effectively in investigation which help us to solve crime.

Keywords: OSINT, Threat, Cyber Crime, Open Source, Threat Hunting.

I. INTRODUCTION

Introduction: -

The study reviews open-source intelligence gathering and profiling, focusing on mitigating techniques. (1). The CIA analyses publicly available information, collecting newspapers, journals, and radio broadcasts to protect national interests.

OSINT USE CASES: -

1. The study concluded that OSINT can provide mission-relevant information, improve police mission accomplishment, and protect the population. The German police are now hiring personnel for OSINT investigations, similar to foreign law enforcement agencies.
2. Cyber Risk Management involves monitoring public sources for efficient risk assessment, using tools tailored to organization requirements. Service providers like Black Kite use Open-Source Intelligence and non-intrusive cyber scans to identify potential security risks. (2)

CLI Tool: -

The Harvester is an open-source intelligence tool (OSINT) created by Christian Martorella for obtaining email addresses, employee names, open ports, subdomains, and hosts banners from public sources like Google, Bing, and LinkedIn. It is a simple Python tool with various information-gathering functions, requiring Python installation in the system. (3)

emergence and evolution of Open-Source Intelligence: -

The Open-Source movement emphasized the importance of Open-Source Intelligence as the Internet opened up unrestricted information sources. As communities developed, the focus shifted from generating ideas (Gc) to maintaining a continuous stream of innovative ideas and creative initiatives. To avoid relying solely on Gf, these communities developed external maintenance tools. (4) the basis for information-gathering methods, and its potential benefits and disadvantages in cybersecurity attacks. (5) OSINT is a method of intelligence generation that involves collection phase involves obtaining publicly available data from open sources, particularly the internet, which is crucial for intelligence generation. The analysis phase involves interpreting the collected data to obtain valuable information. Knowledge extraction uses this information for sophisticated inference algorithms to detect patterns, predict values, or correlate events. (6) Cyber-threat intelligence (CTI) is a knowledge-based system that generates reputation information for network resources based on security data from SIEM systems. This information can be used in industrial infrastructures and internal IT and OT networks. However, the system's performance relies on data accuracy. A new model analyses data reliability and validity using comparative analysis, using approximately 40,000 datasets to validate the use of CTI data. (7) OSINT, often associated with military intelligence, is used by global corporations, banks, and diverse sectors for decision-making, strategic advantage, and business security, alongside government bodies, international organizations, and privacy-conscious individuals. OSINT enhances law enforcement and security by collecting vast data from internet users, enabling intelligence gathering about suspects and detecting potential perpetrators. It also aids in power evaluation by analyzing OSINT results. (8)

Advanced open-source investigation technique: -

1.Integrate internal and external databases

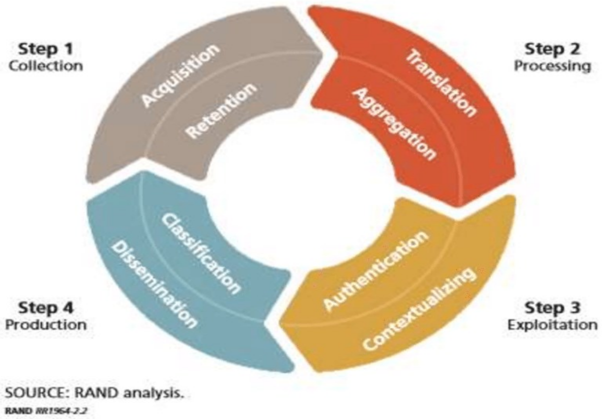
Internal and external data are crucial for businesses to identify potential intelligence. Investigation tools that integrate both types of data can help identify hidden connections and suspicious behaviors. Social Media intelligence increasingly important as people share their lives on social media. It combines original content and metadata to resolve complex problems like financial crime and fraud. Centralizing investigation processes is essential to avoid inefficiency and reduce data loss or exposure risks.

2.Harness intelligent automation to improve decision-making

Open-source investigations are challenging due to vast data. AI-based decision-making cannot match the expertise of experienced investigators. improving human decision-making. This involves automated data gathering, red-flagging, cross-matching, visualization, and prioritizing human oversight. This platform augments human decision-making, not replacing it.

3. Safeguarding the security of your investigations

OSINT platforms prioritize security, ensuring investigative integrity through centralized data repositories, IP address security, direct exports, and flexible deployments on-premises or in the cloud. (9)



SOURCE: RAND analysis.

(10)

II. APPLICATIONS OF OSINT

Cybercrime is a global issue affecting intelligence departments and law enforcement teams worldwide. Mining public records for targeted intelligence is becoming a valuable tool. Innovative software tools and strategies are essential for countering cybercrime. An integrated OSINT Cybercrime Investigation Framework was developed to use open-source information for investigations. Martinez Monterrubio et al. (2021) designed a tool for open-source intelligence (OSINT) on official medical bulletins to detect false news. Med-OSINT is a modular system that processes data from various medical official bulletins and generates intelligence for decision-making. (2019) studied the establishment of concepts for assessing information flows across global computer networks while performing Martinez Monterrubio et al. (2021) designed a tool for open-source intelligence (OSINT) on official medical bulletins to detect false news. Med-OSINT is a modular system that processes data from various medical. publicly available Twitter data. They used the Security Vulnerability Concept Extractor (SVCE) to extract terms linked to security vulnerabilities and store the intelligence as Resource Description Framework triples in a cyber security knowledge base. Ziolkowska (2018) discussed how military intelligence can benefit from opensource intelligence, safeguarding citizens' lives and the country's security. Open-source data is crucial for intelligence services, including diplomatic negotiations and geopolitical plans, and can be obtained through technologies like OSINT.

III. CONCLUSION

This review article summarizes an information that are important by the perspective of the forensic investigation with this technical era. Now a days there is lots of data were available in public which are helpful in the investigation purpose in different way and available various open-source tools. Various tools were available in the open source which are helpful in the forensic investigation purpose with various criminal cases. How we can efficiently use open-source intelligence in forensic investigation which help to solve the various cases and also cyber security threats.

ACKNOWLEDGEMENTS

We are thankful to the department of forensic science, Yashwantrao Chavan Institute of science, Satara, India for the valuable and enlightening guidance and for the provoking and cooperative behavior towards us and allowing us to write the review on the topic.

IV. REFERENCES

[1] Cyber Intelligence & OSINT: Developing Mitigation Techniques. Prof. Allan Brimicombe, [1]Abel Yeboah-Ofori. 2017, nternational Journal of Cyber-Security and Digital Forensics , p. 13.

[2] Open source intelligence Introduction, legal, and ethical considerations. Lolagar, Isabelle Böhm · Samuel. s.l. : Int. Cybersecur. Law Rev. (2021) 2:317–337, 2021.

[3] Sudhanshu Chauhan, Nutan Kumar Panda. OSINT Tools and Techniques. s.l. : Elsevier Inc., 2015.

[4] Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Michael Glassman a 1, Min Ju Kang b. s.l. : Elsevier, 2011.

[5] Current Status and Security Trend of OSINT. Yong-Woon Hwang, Im-Yeong Lee ,Hyejung Le,Donghyun Kim. s.l. : Open Access, 2022. Article ID 1290129.

[6] The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. Pastor-Galindo, Javier, et al. s.l. : IEEE, 2020.

[7] A Reliability Comparison Method for OSINT Validity Analysis. Gong, Seonghyeon, Cho, Jaeik and Lee, Changhoon. s.l. : IEEE, 2018.

[8] The effect of ISO/IEC 27001 standard over open-source intelligence. Abdallah Qusef1, Hamzeh Alkilani2. s.l. : PeerJ Computer Science, 2022.

[9] Solutions, Blackdot. Advanced Open Source Investigation Techniques.

[10] Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review. Karani, Krishna Prasad. s.l. : nternational Journal of Applied Engineering and Management Letters, 2021.