

1. Introduction

Open Source Intelligence (OSINT) enables organisations to better protect their networks and systems from otherwise unknown threats [1].

39% of UK businesses identified a cyber attack in 2022 [2]. To protect against a cyber attack you must understand your attack surface and attack vectors.

This project shows how structured OSINT can be used to improve the investigation of cyber security incidents.

2. Project Aims

- ◆ Compare OSINT tools and techniques.
- ◆ Create Standard Operating Procedures for OSINT investigations and incidents.
- ◆ Create a new efficient and accurate weekly process.
- ◆ Increase automation.

References:

- [1] Hutchins, "Intelligence-Driven Computer Network Defence," [Online]. Available: <https://www.lockheedmartin.com>. [Accessed 8 March 2023].
- [2] "Cyber Security Breaches Survey 2022," HMG Department for Digital, Culture, Media and Sport, 2022.
- [3] "The Cyber Kill Chain," Lockheed Martin, [Online]. Available: <https://www.lockheedmartin.com>. [Accessed 8 March 2023].
- [4] Pastor-Galindo et al., "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," IEEE Access, vol. 8, pp. 10282-10304, 2020.
- [5] "What is robotic process automation (RPA)," IBM Cloud, [Online]. Available: <https://www.ibm.com/topics/rpa>. [Accessed 1 July 2023].
- [6] "Rosetta: Understanding text in images and videos with machine learning," Meta AI, 2018 September 2018. [Online]. Available: <https://ai.meta.com/blog/rosetta-understanding-text-in-images-and-videos-with-machine-learning/>. [Accessed 20 July 2023].

3. Methods

1. Use surveys and focus groups to understand current process and to establish key requirements.
2. Categorise and compare OSINT tooling and techniques.
3. Map OSINT tools to each stage of the Cyber Kill Chain [3]
4. Map attack surfaces to understand potential attack vectors and unintended exposures.
5. Use attack surfaces and appropriate tools and technique to create Standard Operating Procedures to search for unintended exposures.
6. User testing and evaluation.

5. Sample Processes

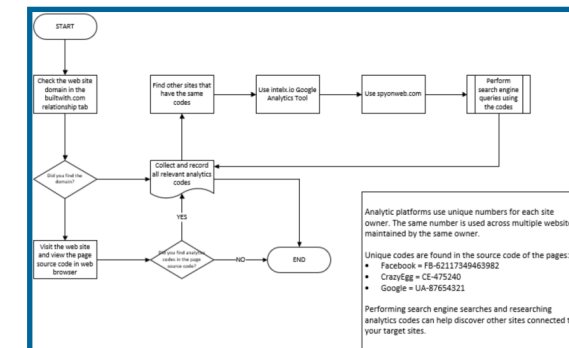


Figure 3:
New Analytic Code analysis process

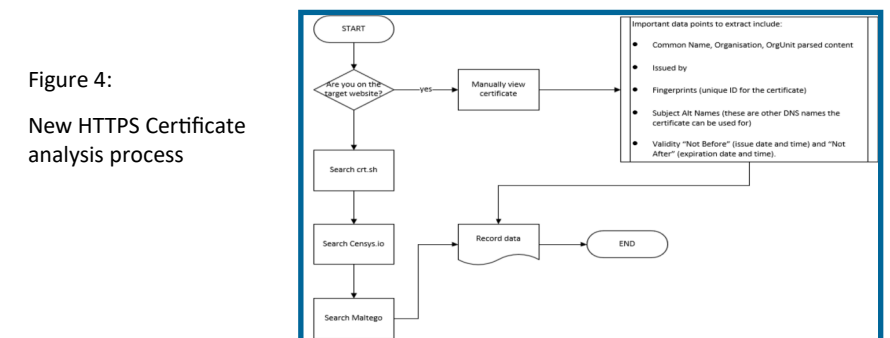


Figure 4:
New HTTPS Certificate analysis process

4. Results

- ⇒ Improved detection (77 additional indicators found).
- ⇒ Accuracy improved by 187%
- ⇒ New typo squatting process.
- ⇒ News and social media monitoring automated.
- ⇒ Breach data identification automated.
- ⇒ Time saved 52 minutes.
- ⇒ Confidence improved by 54.3%

Figure 1: Efficiency

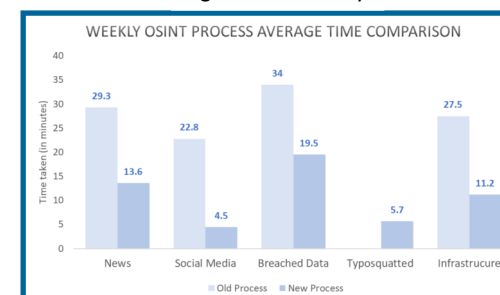
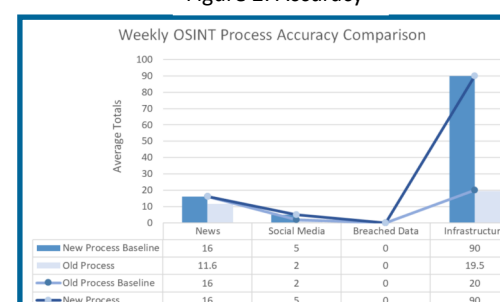


Figure 2: Accuracy



6. Feedback

"The new process helped me find a lot more pivot points faster."

"Finished the investigation much quicker and confident nothing has been missed!"

7. Conclusion and Future Work

OSINT is an unexploited goldmine [4], Standard Operating Procedures have shown to improve investigations considerably. Next steps include using Robotic Process Automation (RPA) [5] and Facebook's Rosetta Text Extraction System [6].