**OPEN SOURCE INTELLIGENCE (OSINT) IN CYBER SECURITY.**

By

**MUOFHE LINDELANI**

**201807997**

DISSERTATION

Submitted in fulfilment of the requirements for the degree of

**HONOURS OF SCIENCE**

In

**COMPUTER SCIENCE**

in the

**FACULTY OF SCIENCE AND AGRICULTURE**

**(School of Mathematical and Computer Sciences)**

at the

**UNIVERSITY OF LIMPOPO**

**Supervisor:** Prof. Mokwena SN

**Co-Supervisor:**

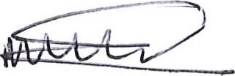
**2023**

# DEDICATION

I dedicate this research paper to my parents (**Angel Tshililo and Edith Khushi)**, my two brothers and two sisters **(Salani Muofhe, Patrick Sephuma, Angel Sephuma and Aretha Musie**), all my 2023 classmates, and most important to myself.

# DECLARATION

I declare that the research titled Open-source intelligence in Cyber security which is submitted under the supervision of Prof. Mokwena SN, is my own work and that all the sources used and quoted in this study have been cited and acknowledged by accurate reference and that this paper has not been part of any other project or article.

 09 October 2023

**……………………. …………………….**

**Signature Date**

# ACKNOWLEDGEMENT

I want to thank the following persons for their respective contributions to this

dissertation:

* Almighty God for guidance throughout since the beginning of the year.
* My parents for their unconditional love, financial support and encouragement
* A special thank you to my supervisor, Prof. Mokwena SN, for his guidance, support and encouragement.
* My classmates in everything for their willingness to participate in this study.
* The University of Limpopo: Department of Computer Science, Faculty of Science and Agriculture, in the School of Mathematical and Computer Science for giving me permission to conduct the study.
* The faculty dean, school director, the computer science HOD, and as well as all the computer science lecturers for the 2023 academic year for their leadership, support, and undying patience.

# ABBREVIATIONS

OSINT – Open source intelligence.

VPN - Virtual private network.

SSL - Secure socket layer.

S-HTTP - Secure Hypertext Transfer Protocol.

SET - Secure electronic transaction.

ABSTRACT:

The rapid change of technology, brought about by the Fourth Industrial Revolution, posed a change in cyberspace. The goal of this study is to minimise the escalating cyber threats against the security of e-Commerce systems. As online transactions continue to grow, cyberattacks have become a critical challenge, targeting both businesses and consumers. Cybercriminals exploit vulnerabilities in e-Commerce platforms to perform a range of crimes, from financial fraud to identity theft. This research investigates the role of OSINT in supporting and strengthening the security of e-Commerce systems by identifying and mitigating these threats. The research methodology employs the OSINT approach to data collection, analysis, and dissemination. This research contributes to the ongoing dialogue surrounding cybersecurity by highlighting the important role of OSINT in protecting e-Commerce platforms. By understanding the methodologies employed by cybercriminals and leveraging OSINT's capabilities, businesses and consumers together can work towards fortifying the digital landscape against evolving threats.

Keywords

Open source intelligence (OSINT), Maltego, Cyberattacks, E-Commerce, online shopping.

TABLE OF CONTENTS

[DEDICATION i](#_Toc149314909)

[DECLARATION ii](#_Toc149314910)

[ACKNOWLEDGEMENT iii](#_Toc149314911)

[ABBREVIATIONS iv](#_Toc149314912)

[ABSTRACT v](#_Toc149314913)

[Keywords v](#_Toc149314914)

[LIST OF TABLES viii](#_Toc149314915)

[LIST OF FIGURES ix](#_Toc149314916)

[CHAPTER 1 PROPOSAL 1](#_Toc149314917)

[1.1. INTRODUCTION 1](#_Toc149314918)

[1.2. PROBLEM STATEMENT 2](#_Toc149314919)

[1.2.1. This is how others have tried to solve this problem 2](#_Toc149314920)

[1.2.2. Weaknesses of SSL & VPNs 3](#_Toc149314921)

[1.2.3. How does the study aim to improve the use of open source intelligence? 3](#_Toc149314922)

[1.3. MOTIVATION OR RATIONALE 4](#_Toc149314923)

[1.4. METHODOLOGY AND ANALYTICAL PROCEDURES 5](#_Toc149314924)

[1.5. SCIENTIFIC CONTRIBUTION 6](#_Toc149314925)

[1.6. AVAILABILITY OF RESOURCES 6](#_Toc149314926)

[1.7. ETHICAL CONSIDERATION 7](#_Toc149314927)

[1.8. CHAPTER SUMMARY 7](#_Toc149314928)

[CHAPTER 2 LITERATURE REVIEW 9](#_Toc149314929)

[2.1. INTRODUCTION 9](#_Toc149314930)

[2.2. TWITTER DATASET 9](#_Toc149314931)

[2.3. CHALLENGES IN CYBERCRIMES 10](#_Toc149314932)

[2.4. SECURITY TECHNIQUES FOR CYBERCRIMES 11](#_Toc149314933)

[2.5. USING OPEN SOURCE INTELLIGENCE (OSINT) 12](#_Toc149314934)

[2.6. BENEFITS OF OSINT IN CYBERSECURITY 13](#_Toc149314935)

[2.7. BENEFITS OF OSINT FOR BUSINESSES 13](#_Toc149314936)

[2.8. SUMMARY OF THE CHAPTER 14](#_Toc149314937)

[CHAPTER 3 RESEARCH METHODOLOGY 15](#_Toc149314938)

[3.1. INTRODUCTION 15](#_Toc149314939)

[3.2. DATA COLLECTED 15](#_Toc149314940)

[3.3. DATA PROCESSING & CLEANING 15](#_Toc149314941)

[3.4. DATA ANALYSIS 17](#_Toc149314942)

[3.5. NETWORK MAPPING 17](#_Toc149314943)

[3.6. RESPONSE PLANNING 19](#_Toc149314944)

[3.7. CHAPTER SUMMARY 19](#_Toc149314945)

[CHAPTER 4 RESULTS AND ANALYSIS 20](#_Toc149314946)

[4.1. INTRODUCTION 20](#_Toc149314947)

[4.2. DATA MANAGEMENT AND ANALYSIS 20](#_Toc149314948)

[4.3. RESEARCH RESULTS 21](#_Toc149314949)

[4.3.1. Phishing in e-Commerce 21](#_Toc149314950)

[4.3.2. Spoofing in e-Commerce 22](#_Toc149314951)

[4.4. OVERVIEW OF RESEARCH FINDINGS 22](#_Toc149314952)

[4.4.1. Define the Scope of the Assessment 22](#_Toc149314953)

[4.4.2. Define the Scope of the Assessment 23](#_Toc149314954)

[4.4.3. Network mapping 23](#_Toc149314955)

[4.4.4. Response planning 24](#_Toc149314956)

[4.5. CONCLUSION 27](#_Toc149314957)

[CHAPTER 5 CONCLUSION & FUTURE WORK: 28](#_Toc149314958)

[5.1. INTRODUCTION 28](#_Toc149314959)

[5.2. RESEARCH DESIGN AND METHOD 28](#_Toc149314960)

[5.2.1 Objective 1 28](#_Toc149314961)

[5.2.2 Objective 2 28](#_Toc149314962)

[5.2.3 Objective 3 29](#_Toc149314963)

[5.2.4 Objective 4 29](#_Toc149314964)

[5.3. SUMMARY AND INTERPRETATION OF THE RESEARCH FINDINGS 30](#_Toc149314965)

[5.4. CONCLUSION 31](#_Toc149314966)

[5.5. RECOMMENDATIONS 31](#_Toc149314967)

[5.6. CONTRIBUTIONS OF THE STUDY 31](#_Toc149314968)

[5.7. LIMITATIONS OF THE STUDY 32](#_Toc149314969)

[5.8. CONCLUDING REMARK 33](#_Toc149314970)

[6. REFERENCE 34](#_Toc149314971)

# LIST OF TABLES

[Table 1 Data cleaning 16](#_Toc149224233)

# LIST OF FIGURES

Figure 1 Data cleaning with Open refine 17

Figure 2 Removing duplicates with Open refinement 17

Figure 3 Cleaning malicious phishing data 18

Figure 4 Pie chart 21

Figure 5 Bar Chart 22

Figure 6 Maltego scope assessment 25

Figure 7 Network mapping 25

Figure 8 Monitoring infrastructure network 26

Figure 9 Monitoring for information leaks entry points 27

# CHAPTER 1 PROPOSAL

# INTRODUCTION

The fourth industrial revolution brought about significant transformations in the digital realm, driven by technological advancements and the emergence of various innovative applications. Creative platforms such as blog sites, social media, and e-Commerce quickly gained immense popularity during this period. These platforms enabled end users to engage in online shopping, create and share content with others seamlessly. Using these platforms, end users were able to buy online, publish and share material with other users(Yeboah-Ofori, 2018).

The advancement of cloud computing technology has encouraged businesses to embrace the e-Commerce service. At the same time, traditional services such as newspapers, libraries, bill payments, government agencies, and the education sector have transitioned into the digital realm, storing their data on Web-based platforms. Consequently, Open source Intelligence (OSINT), a practise that has been around for more than half a century, initially used by defence personnel to extract valuable intelligence from publicly available data, has experienced a resurgence in popularity(Zhang et al., 2022).

Open source intelligence (OSINT), similar to other intelligence systems, follows a structured approach to gather, clean, analyse, and sharing data. With the large amount of publicly accessible data now available, OSINT has seen significant growth in various fields, becoming essential for numerous applications. Its popularity is increasing due to its cost-effectiveness, minimal risks, and reliance on publicly accessible information.

Corporate enterprises utilise open source intelligence (OSINT) for a range of objectives, such as predicting market trends, evaluating competitors, and gauging customer sentiment. Meanwhile, cybersecurity professionals are responsible for creating profiles of criminals and extremists, conducting forensic investigations into illegal activities, and identifying vulnerabilities within IT systems, with OSINT proving invaluable in uncovering weaknesses in information technology infrastructure(Santarcangelo et al., 2015).

# PROBLEM STATEMENT

Technology has bestowed upon society numerous significant advantages and opportunities. Simultaneously, it has also brought forth concerns related to data and information security, which have exposed vulnerabilities and weaknesses(Tabatabaei & Wells, 2016a).

This study focuses on examining cyber threats targeting the security of e-Commerce systems through the utilization of open source intelligence (OSINT). With the ongoing increase in online transactions, there is a corresponding increase in cyberattacks directed at the security of e-Commerce system.

E-Commerce, also known as online shopping, refers to the purchase and sale of products and services carried out over the Internet.

The problem is that cyberattacks are increasingly being issues for businesses and e-Commerce. Cybercriminals frequently focus on online shoppers with the aim of swindling their money or stealing their personal information. They employ a range of tactics, which encompass creating counterfeit online store websites, selling non-existent products, soliciting personal and payment data from online shoppers, and implanting malicious software on their network devices. These threat actors, or cybercriminals, engage in e-enabled crimes, including hacking, fraudulent use of credit cards, and the theft of personal information.

Cybercriminals take advantage of the anonymity provided by web-based communication to engage in malicious activities such as phishing, spamming, extortion, and identity theft(Gottschalk et al., 2011).

## This is how others have tried to solve this problem

Using a virtual private network (VPN) and a secure socket layer (SSL), both were used to enhance the online security and privacy by encrypting and protecting user data as they interact with the Internet through apps and websites(Kaur & Sharma, 2020).

VPNs, often used for access control purposes, serve as a safeguard for sensitive information and protect online privacy. They are particularly valuable when browsing the Internet, especially in situations involving public Wi-Fi networks or when trying to access restricted content in specific geographic regions.

SSL, or Secure Sockets Layer, is a technology that establishes a secure and encrypted link between a web browser and a web server. Its primary purpose is to improve the security of online interactions, particularly for sensitive activities such as online banking, shopping, and the exchange of private data. SSL achieves this by encoding the data transmitted between the user's browser and the server, thereby guaranteeing that the information stays confidential and is shielded from potential interception by unauthorised individuals or entities.

## Weaknesses of SSL & VPNs

VPNs are not reliable and not compatible with all network platforms. VPNs can slow down your Internet connection due to the encryption and the distance between your device and the remote server, and the connection becomes weak and sometimes even disconnect, and this can be very harmful when making online transactions, or receiving payments as intruders are always on the wait to attack.

SSL certificates can be fraudulent and can be issued by fraudulent or malicious parties, potentially allowing them to intercept and access sensitive data, and does not guarantee full protection from cyberattacks.

## How does the study aim to improve the use of open source intelligence?

This study aims to solve this problem by monitoring e commerce sites or online shopping apps and identifying any potential threats, such as phishing sites or fake accounts by utilising tools such as Spiderfoot and Maltego. This study involves the process of collecting and analysing data from diverse sources, which may include social media platforms, search engines, and online marketplaces.

Spiderfoot and Maltego are powerful OSINT tools that can help identify potential threats, investigate and asses vulnerabilities for businesses to stay up to date, and protect customer data from being intercepted by cybercriminals(Yamin et al., 2022)

# MOTIVATION OR RATIONALE

The motivation or goal of this research is to gather information using OSINT tools from multiple sources to monitor and minimise the online shopping inappropriate behaviours that have been detected in Websites, such as identity theft, money scams and private-information leaks.

* + 1. Aim

This research aims to solve the problem of cyberattacks on e-Commerce system through the use of open source intelligence tools.

Objectives

The specific objectives of this study are:

* To investigate previous e-Commerce security incidents using OSINT tools by gathering data on how to monitor, litigate, and minimise their spread against e-commerce security or online shopping.
* Identify possible potential threats and detect fraudulent activities such as fake reviews, phishing attacks, and scams targeting e-Commerce customers.
* Help businesses investigate the source of the attack and entry points by identifying hashes that are appended to the company domain or IP addresses by attackers and also trace their origin.
* Gather intelligence to prevent future attacks by providing early warning of potential cyberattacks to businesses by monitoring leaked customer credentials, weak passwords, and other indicators of poor security practises affecting the e-Commerce systems.
  + 1. Research questionnaires
* How can OSINT tools be used to gather data on how to monitor, litigate, and minimise their spread against e-commerce security or online shopping?
* How can OSINT detect fraudulent activities such as fake reviews, phishing attacks, and scams targeting e-Commerce customers?
* How can OSINT help businesses investigate the source of the attack and gather intelligence to prevent future attacks?
* Can OSINT gather intelligence to prevent future attacks of cybersecurity on the e-Commerce systems?

# METHODOLOGY AND ANALYTICAL PROCEDURES

To achieve the aim and objectives of this study successfully, useful and reliable information must be collected, cleaned, and analysing data that will lead to accurate and useful results, network mapping, and lastly response planning.

* + 1. Data collection

The data can be collected or downloaded from the <https://www.kaggle.com/> website, since many papers under OSINT domain have been published by many researchers. The data will be used to gather information from a wide range of sources, including social media platforms, blogs, and news articles, to identify possible cyber threats against e-Commerce Apps and websites. This information can include details about specific threat actors, their motives, techniques, and procedures they use.

* + 1. Data Clean up

The collected data should be cleaned and organised to eliminate or filter all irrelevant information, for analysis purposes.

Open source intelligence has great tools in place that are useful for cleaning data. This study is going to use Open refine to clean the data.

* + 1. Data Analysis

Once you clean and organise the data, the next step is to analyse it using different features and functionalities provided by OSINT tools, Jupyter Notebook, and Maltego.

* + 1. Response planning

Based on the identified potential threats, the final stage is to develop a response plan to filter threats’ risks against e-Commerce security. This involves implementing OSINT security measures such as firewalls, cybercriminals, detection systems, and authentication systems for organisations or businesses to always validate and protect their customer’s information when performing online transactions.

# SCIENTIFIC CONTRIBUTION

The findings of this study will be compared with the results of previous studies and methodology used and offer a conclusion on how efficient it is to use OSINT in the context of cyber security to monitor and minimize the cyber security potential threats against the security of e-Commerce, and how well can OSINT tools defend corporate businesses and customers from online shopping risks?

# AVAILABILITY OF RESOURCES

There are several resources available for this study using OSINT on cybersecurity to help monitor and minimize cyberattacks to defend e-Commerce security. This include data collected by previous studies, OSINT tools such as Maltego, Spider foot, and Jupyter Notebook that are going to be very useful in this study.

All three of these OSINT tools can be useful for minimizing cyber threats on e-Commerce platforms by providing valuable insights into potential vulnerabilities, suspicious activity, and other indicators of potential threats. By using these tools to collect and analyse data from various sources, cybersecurity professionals can better protect e-Commerce platforms from potential cyberattacks(Yamin et al., 2022).

Maltego is a versatile data mining application designed for visualizing and investigating connections among individuals, businesses, and websites. It empowers users to gather information from diverse sources, such as social media, websites, and search engines, enabling them to uncover potential risks or weaknesses within e-Commerce platforms. Essentially, Maltego serves as a valuable tool for mapping and understanding relationships across the digital landscape, making it useful for various investigative and security purposes. It can be used to identify potential threats on e-Commerce platforms by analysing domain names, IP addresses, and other metadata associated with the online platforms.

Jupyter Notebook is a freely available web-based tool designed to create and distributing documents that incorporate live code, mathematical equations, and various multimedia elements, all of which aim to improve the process of data analysis and exploration.

# ETHICAL CONSIDERATION

Ethical considerations encompass the moral principles and values that provide guidance for how individuals and researchers should behave and make decisions when they are engaged in research activities(Bhandari, 2021).

In this study, ethical considerations will include privacy, data protection, transparency, and fairness.

* + 1. Privacy

When conducting this research, it is important to respect the privacy of individuals and organisations. This involve protecting sensitive data from unauthorized access, minimizing the collection of personally identifiable information, and obtaining informed consent before collecting any data from all the source of data collection.

* + 1. Data protection

It is important to protect the confidentiality of any data that will be collected during the research. This include storing the data securely and only sharing it with individuals who have a legitimate need to know.

* + 1. Fairness

Fairness must be maintained and be imperial with people when collecting data from various sources, that is, treat all people with equal respect, and ensure that their response in social media or any other data collection platform does not unfairly discriminate against any group. This includes avoiding the release of any sensitive information that could be used to harm individuals or organisations.

# CHAPTER SUMMARY

In this chapter the proposal of the whole study has been summarised; in this chapter, a comprehensive overview is provided, encompassing the study's context, its driving factors, the identified issue or challenge, the study's objectives, and the planned methodology for improving the application of open source intelligence in the field of cybersecurity.

# CHAPTER 2 LITERATURE REVIEW

# INTRODUCTION

This section will clearly outline the background and review some important literature that is relevant to how other previous researchers have tried to solve the problem of cybercrimes against the security of E-Commerce, and how this research is going to use OSINT identify these potential threats against the E-Commerce domain.

# TWITTER DATASET

Twitter is a social network with more than 192 million daily active users. Beyond serving as an individualised space for sharing content and self-promotion, it is extensively utilised by a diverse group of individuals, including hackers, vendors, cybersecurity experts, and enthusiasts, as a forum for discussing and revealing various computer security-related topics. These discussions often revolve around exploits, vulnerabilities, threats, and cyberattacks. Early detection is very important, as it allows prioritising the response, i.e., the risk treatment and response to potential incidents(Marinho & Filho, 2023).

Mittal et al., (2016a) managed to build a pipeline that collects, filters, preprocesses, extracts, classifies, and clusters the information by analysts and its cyber threat management platforms. Despite the classification module that measures the relevance of each tweet, this end-to-end system doesn’t identify the metrics that allow the evaluation of the relevance or trustworthiness of the information extracted from Twitter(Marinho & Filho, 2023).

A CyberTwitter was developed by (Mittal et al., 2016a), a system designed to collect and analyse cybersecurity information from Twitter, functioning as an Open source intelligence (OSINT) tool. This system has the ability to recognize, label, and retrieve conceptual elements linked to cybersecurity vulnerabilities. These elements cover various aspects, such as cyberattacks methods, the repercussions of such attacks, the software and hardware affected, and the involved vendors. It achieves this by using a tool known as the Security Vulnerability Concept Extractor.

This intelligence provides valuable information to human analysts, alerting them to new threats or vulnerabilities in software or hardware listed in their user system profile. Importantly, this information does not come with a specific time frame or temporal dimension(Mittal et al., 2016b).

# CHALLENGES IN CYBERCRIMES

Interpersonal trust, when it comes to traditional business transactions, canter around the confidence a customer has in various aspects, such as their trust in a salesperson. Previous studies have noted that consumer trust can have various focal points, including the product, the salesperson, and even friends. They define trust as a broad, overarching belief held by the consumer, which encompasses their expectations that the salesperson, the product and their social circle will fulfil their respective commitments as perceived by the consumer(Tabatabaei & Wells, 2016b).

Similarly, within the realm of e-Commerce, researchers often characterise trust as a person's readiness to open themselves up to vulnerability, their expectations, their subjective beliefs, and their reliance on parties other than themselves. This trust can also be seen as a subjective estimate of the likelihood of a positive outcome when engaging with these external parties(Tabatabaei & Wells, 2016c).

E-Commerce website owners face the dual challenge of attracting more customers and ensuring a secure and comfortable browsing experience for their visitors. On the other hand, end users must evaluate and rate e-Commerce websites while also taking steps to protect themselves in the online community. This dynamic involves website owners striving to enhance their platforms' appeal and security, while users need to evaluate websites and adopt protective measures as part of their online engagement(Yeboah-Ofori, 2018).

The rise in media warnings about security and privacy breaches, such as identity theft and financial misconduct, has hindered e-Commerce from reaching its full potential. Many consumers are reluctant to make online transactions, attributing this reluctance to a lack of trust and concerns about the safety of their personal information. It's evident that online transactions necessitate customers to share a substantial amount of sensitive personal data with the seller, which exposes them to significant risks(Yeboah-Ofori, 2018).

# SECURITY TECHNIQUES FOR CYBERCRIMES

A group of researchers examined the technologies used to ensure transaction security for e-Commerce applications, specifically focussing on the use of encryption as an approach.

Encryption involves the transformation of plain text or data into a form known as ciphertext, which is designed to be unreadable by anyone except the intended sender and recipient of the information(Khan, 2019).

The main idea of encryption was deployed to protect the data stored and to safeguard data transmission.

One of the widely recognised methods for ensuring secure communication channels is through the use of the Secure Socket Layer (SSL) within the TCP/IP protocol suite. SSL offers features such as data encryption, server authentication, optional client authentication, and message integrity for TCP/IP connections. SSL, originally developed by Netscape Communications Corporation and now managed by industry security working groups, serves as a vital security protocol for securing online communications(Dastres & Soori, 2020).

The primary goal of this convention's design is to ensure that when information is transmitted over the Internet between two communicating applications, it is protected from eavesdropping, unauthorised manipulation, or the creation of fake messages (Khan, 2019).

The Secure Hypertext Transfer Protocol (S-HTTP) is a security protocol intended for secure communication in conjunction with HTTP, the standard protocol for transferring data over the Internet. Unlike SSL, which is primarily focused on securing the connection between two computers, S-HTTP is designed to provide security at the message level. Allow individual messages to be signed, authenticated, encrypted, or a combination of these security measures. S-HTTP aims to enhance the security of HTTP by ensuring that data exchanged between a client and a server remain confidential and tamper-proof. It was developed to seamlessly integrate with existing HTTP applications, making it a versatile choice for improving the security of web-based communications(Khan, 2019).

A digital signature is a modern and secure way of confirming the authenticity of a document, and it is unique to the person who creates it. This signature is created with the intention of verifying the document and can be validated by others. It is closely tied to the document in a way that if any changes are made to the document, the digital signature becomes invalid. Essentially, a digital signature is usually a hash of the message, which is then encrypted using the owner's private key to ensure its integrity and authenticity(Zhang et al., 2022).

Secure Electronic Transactions (SET) is a crucial specification in the realm of e-Commerce, particularly for the secure exchange of credit and payment card information. Its design revolves around the achieving of three key objectives. First, SET aims to ensure the safety of all parties involved in e-Commerce transactions. This involves securing payments, verifying the identities of both cardholders and merchants, maintaining the confidentiality of payment details, and establishing standardised procedures and options for electronic security services. Secondly, SET strives to promote interoperability, making it possible for applications from various vendors and different operating systems to work seamlessly together in the e-Commerce ecosystem(Yeboah-Ofori, 2018).

# USING OPEN SOURCE INTELLIGENCE (OSINT)

This study aims to solve this problem by monitoring e commerce sites or online shopping apps and identifying any potential threats, such as phishing sites or fake accounts using Spiderfoot and Maltego, by collecting and analysing of information from various open sources, such as social media, Google search engines, and online marketplaces.

Spiderfoot and Maltego are powerful OSINT tools that can help identify potential threats, investigate and asses vulnerabilities for businesses to stay up to date, and protect customer data from being intercepted by cybercriminals(Yamin et al., 2022).

This study will improve by providing businesses and individuals with detection methods of fraudulent activities such as fake reviews, phishing attacks, and scams targeting e-Commerce customers, and providing early warning of potential cyberattacks.

# BENEFITS OF OSINT IN CYBERSECURITY

Open source Intelligence (OSINT) serves as a valuable resource to gather threat intelligence. It offers organisations a large amount of data on the methods, approaches, and strategies used by cybercriminals. Additionally, it provides valuable information on new threats and vulnerabilities. This wealth of information can prove highly advantageous in the creation and execution of more robust security strategies and countermeasures.

Open source Intelligence (OSINT) involves the collection of data on software and system vulnerabilities, including information about known exploits and available patches. This information serves a valuable purpose in helping organisations prioritize their efforts to address vulnerabilities and ensure the security and up-to-date status of their systems.

Another application of OSINT involves the identification and mitigation of phishing and social engineering attacks. OSINT can be employed to collect valuable data on the methods employed by attackers to deceive individuals into divulging sensitive information or downloading malicious software. Furthermore, it can aid in identifying individuals who have a public online presence and may pose security risks as potential weak links within an organisation's defences(Lande & Shnurko-Tabakova, 2019).

# BENEFITS OF OSINT FOR BUSINESSES

Open source Intelligence (OSINT) enhances the decision-making process by offering valuable insights and information that can help make informed decisions in different facets of a business, including areas such as marketing strategies, product development, and customer service.

Open source Intelligence (OSINT) is a valuable tool for obtaining customer insights. It involves the collection of information about customers, which includes their preferences, viewpoints, and behaviours. These data can be leveraged to enhance the overall customer experience and elevate levels of customer satisfaction(Lande & Shnurko-Tabakova, 2019).

Open source Intelligence (OSINT) can serve as a valuable resource to conduct market research. It involves gathering information and insight related to the market, such as emerging trends, consumer preferences, and industry advancements. These data can be leveraged by businesses to enhance their products or services and maintain a competitive edge in the market(Lande & Shnurko-Tabakova, 2019).

# SUMMARY OF THE CHAPTER

The study reviews of this chapter clearly give a background of how previous papers have worked to solve the cybersecurity problem, challenges that organisations and individual encounter dealing with cybercrimes, how the study will improve on the proposed solutions and the benefits of using open source intelligence in cybersecurity.

# CHAPTER 3 RESEARCH METHODOLOGY

# INTRODUCTION

This chapter aims to carry out the study research methodology to fulfil the objectives of this study successfully, useful and reliable data was downloaded, cleaned and analysed to automate accurate and useful results.

# DATA COLLECTED

Data available for use in this study were collected or downloaded from the Internet via the <https://www.kaggle.com/> website. This approach proved more convenient because various researchers had previously published articles in the cybersecurity domain, making it easier to access the existing data they had collected and used.

* + 1. Dataset Available: Cybersecurity Breaches

# DATA PROCESSING & CLEANING

The data should be cleaned and organised to eliminate or filter all irrelevant information, for analysis purposes.

Open source intelligence has great tools in place useful for cleaning data, and in this study, we utilised Open refine, a freely, available open source software tool designed for managing and improving disorganised or untidy data. This tool enables users to refine and convert data from one structure or format to another. It offers features such as data reconciliation, data normalisation, and data augmentation(Nguyen, 2010).

We check for entities such as:

Table 1 Data cleaning

|  |
| --- |
| Other = Do not contain useful information. |
| Organisation = Company or organisation. |
| Product = Product or items. |
| Vulnerability = maybe referencing the existence of a threat or vulnerability. |
| Identifier = An identifier, from a public known vulnerability. |

The last stage of our data cleaning was to look for duplicates from all of our datasets.

Figure 1 Data cleaning with Open refine

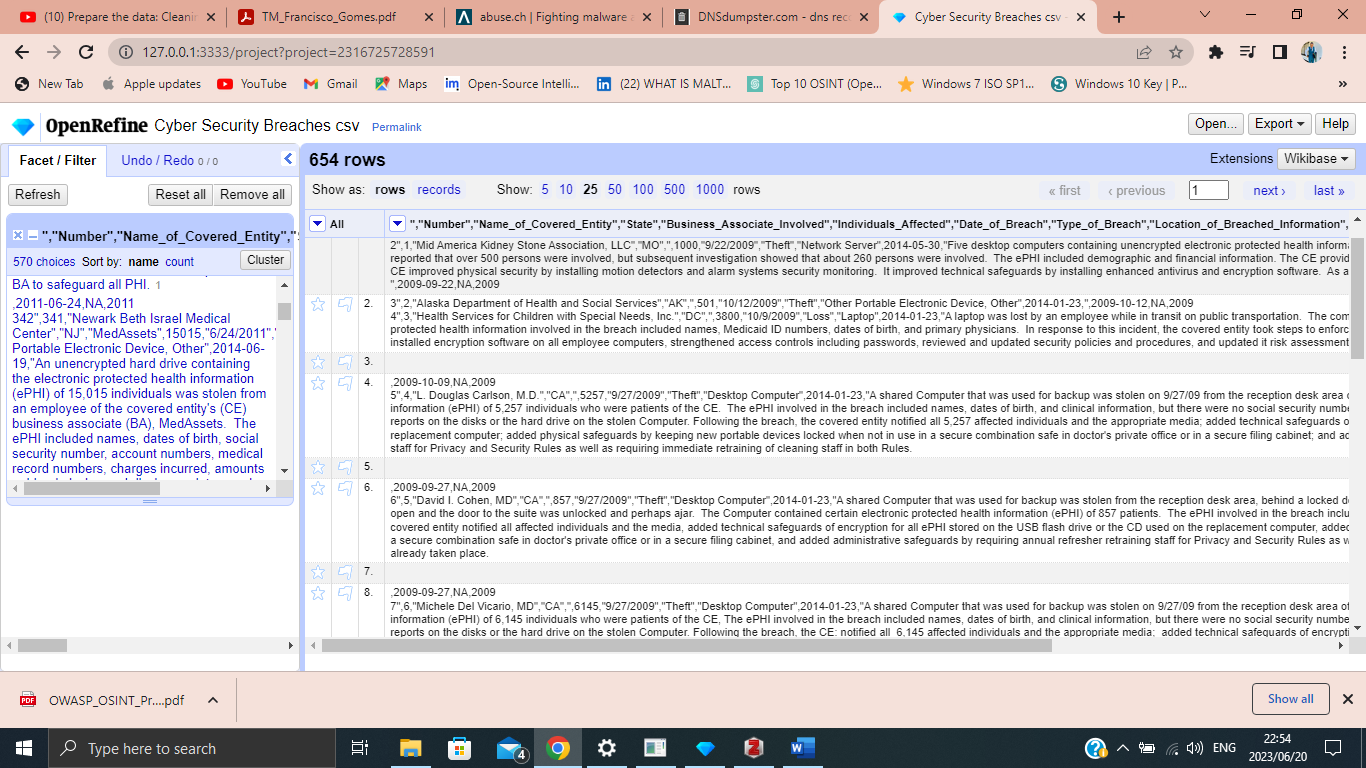


Figure 2 Removing duplicates with Open refinement

A screenshot of a computer

Description automatically generated

Figure 3 Cleaning malicious phishing data

A computer screen with a computer screen

Description automatically generated

# DATA ANALYSIS

Analysing data includes evaluating, assessing, and interpreting the information, in terms of confidence, relevance, likelihood, risk, and impact, to get valuable recommendations on how to minimise the spread of cybersecurity crimes against the security of e-Commerce and online shopping for both businesses and their customers.

# NETWORK MAPPING

Network mapping is the practise of creating a visual depiction of a network and all the elements connected to it. It encompasses both physical and virtual components, offering a comprehensive view of an organisation's IT infrastructure. Network mapping solutions are designed to provide detailed insights into a company's network setup.

These solutions often come integrated with network performance monitors (NPMs), which allow users to generate or view network maps. These maps typically consist of straightforward images or diagrams that illustrate the performance status of devices within the network. They serve as a valuable tool for understanding how various network elements operate.

Network mapping technologies are used by organisations to simplify the task of monitoring their networks and quickly identifying any network issues. Network mapping involves the creation of a visual representation of a network that helps IT teams uncover and visualise how devices and components are connected within the network. This map typically includes network diagrams, devices list, flowcharts, and the detection of network topology. These visual aids are highly beneficial for various purposes, including network maintenance and improving network security measures(Digital, 2023).

The OSINT tools can be used to map the network infrastructure of an e-Commerce website, including servers, routers, and other network devices, to identify vulnerabilities that could be exploited by cybercriminals(Tabatabaei & Wells, 2016a).

Lampyre also provides a range of other features, such as the ability to perform social media monitoring, dark web monitoring, threat modelling and malware analysis(Semenishchev et al., 2020).

* Social media monitoring: This can provide early warning of potential cyberattacks or data breaches, as well as insight into the sentiment of customers and other stakeholders.
* Threat modelling: This involves identifying potential attack vectors and mapping out the likely actions of an attacker. This can help prioritize security measures and allocate resources effectively.
* Malware analysis: This can help identify the specific type of malware and determine its capabilities, such as stealing payment card information or personal customer data.
* Dark Web Monitoring: An OSINT tool can be used to keep an eye on underground online marketplaces on the dark web where cybercriminals may be selling stolen payment card details, customer data or other confidential information. This proactive monitoring can assist in the early detection of potential data breaches and take steps to reduce their consequences.

# RESPONSE PLANNING

Response planning is the final stage in OSINT in which we deliver the results after testing.

Based on the identified potential threats, the final stage is to develop a response plan to minimise the threats risks against e-Commerce security. This involves implementing OSINT security measures such as firewalls, cybercriminals detection systems, and authentication system for organisations or businesses to always validate and protect their customer’s information when doing online transactions(Charles, 2022).

# CHAPTER SUMMARY

This chapter clearly explains in detail the methodology of the study. The open source intelligence tools that are to be used to test and find the results to improve and minimise the cybercrimes to defend businesses and individuals.

# CHAPTER 4 RESULTS AND ANALYSIS

# 4.1. INTRODUCTION

In this chapter, the results are analysed and visualised. The results obtained were obtained independently using different pieces of codes, and an open source tool Jupyter Notebook was deployed to get data visualisation and results.

# DATA MANAGEMENT AND ANALYSIS

Figure Pie chart

The data collected show that individuals experience a 54.3% higher theft breach, indicating a higher rate of cybercrimes involving the setup of fake retailers' websites to steal from individuals and sell fake products. This theft occurs frequently when individuals engage with these fake websites.

About 23.8% of losses occurred in online shopping that affects e-Commerce individuals, these losses occur most when cybercriminals pose or send messages pretending to be trusted people, their goal is to steal sensitive information such as credit card information, password, and login details of individuals or install viruses on victim’s computers (Phishing attacks)

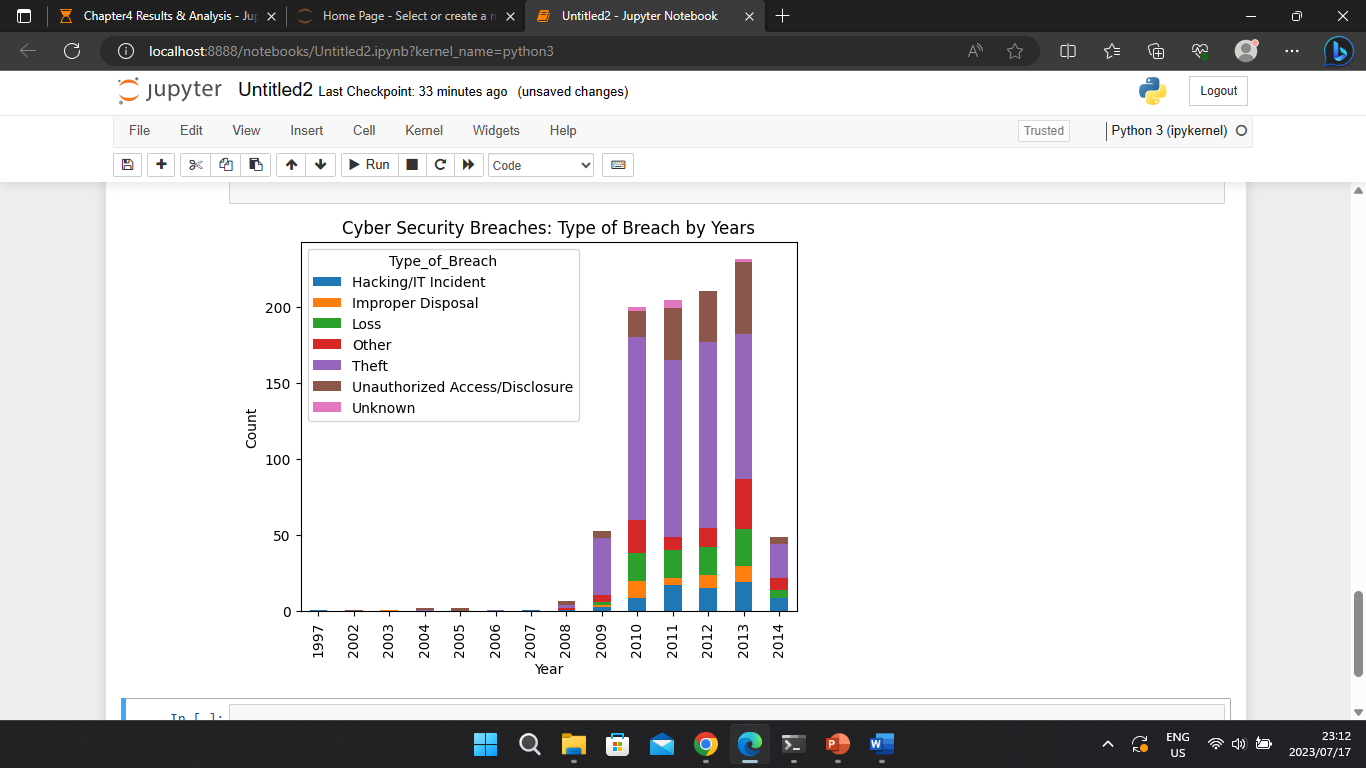
The results from the pie chart show that organisations or businesses need to improve their security more in order to minimise phishing attacks against their customers.

Figure Bar Chart

The chart clearly shows that attackers mainly abuse the e-Commerce system and its consumers through theft, phishing, and spoofing. These attacks exploit vulnerabilities in the online shopping ecosystem to steal sensitive information or manipulate E-commerce customers into taking actions that are consequential to their interests.

### RESEARCH RESULTS

1. Credit Card Fraud: Cybercriminals can steal credit card information stored on e-Commerce websites or intercept it during transactions. They can then use this information for fraudulent purchases, leading to financial losses for both consumers and the e-Commerce platform.
2. Identity Theft: Attackers can use stolen personal information to create fake accounts, make unauthorised purchases. This can result in reputational damage and financial damage to consumers.

## Phishing in e-Commerce

1. Credential Theft: Phishing emails often trick users into clicking on malicious links or providing their login credentials on fake websites that resemble legitimate e-Commerce platforms. Once the attacker has these credentials, they can gain unauthorised access to user accounts.
2. Financial loss: Phishing attacks can cause consumers unknowingly to making purchases on fraudulent websites or to disclose sensitive financial information. As a result, they may suffer financial losses.
3. Reputation damage: E-Commerce platforms can suffer reputational damage if their customers are targeted by phishing attacks through emails or messages that appear to come from the platform itself.

## Spoofing in e-Commerce

1. Fake Websites: Spoofing attacks involve creating counterfeit websites that mimic legitimate e-Commerce platforms. These fake sites deceive unsuspecting consumers who may make purchases on them, resulting in financial loss and potential data exposure.
2. Brand Impersonation: Spoofing can damage the reputation of e-Commerce businesses if attackers impersonate their brand, send fraudulent emails, or create fake social media accounts. Customers may lose trust in the legitimate brand.

To protect e-Commerce systems and consumers from these threats, OSINT is deployed to minimise and monitor all the fraudulent activities of cybercriminals.

### OVERVIEW OF RESEARCH FINDINGS

Using Maltego for attack surface assessments to help organisation find their vulnerabilities or entry points of attacks.

Step 1: Define the scope of the Assessment.

Step 2: Identify potential data sources.

Step 3: Network mapping.

Step 4: Analyse the information.

Step 5: Response planning

## Define the Scope of the Assessment

The first step in any attack surface assessment is to define its scope. This includes identifying the target systems or networks and determining the objectives. Our aim is to monitor, litigate, and or minimise the spread of cybercrime against online shopping, and its abuse on people, organisation, and businesses and to understand the threat landscape and help defend businesses and individuals from known risks of online shopping by identifying all publicly accessible domains and IP addresses associated with your organisation.

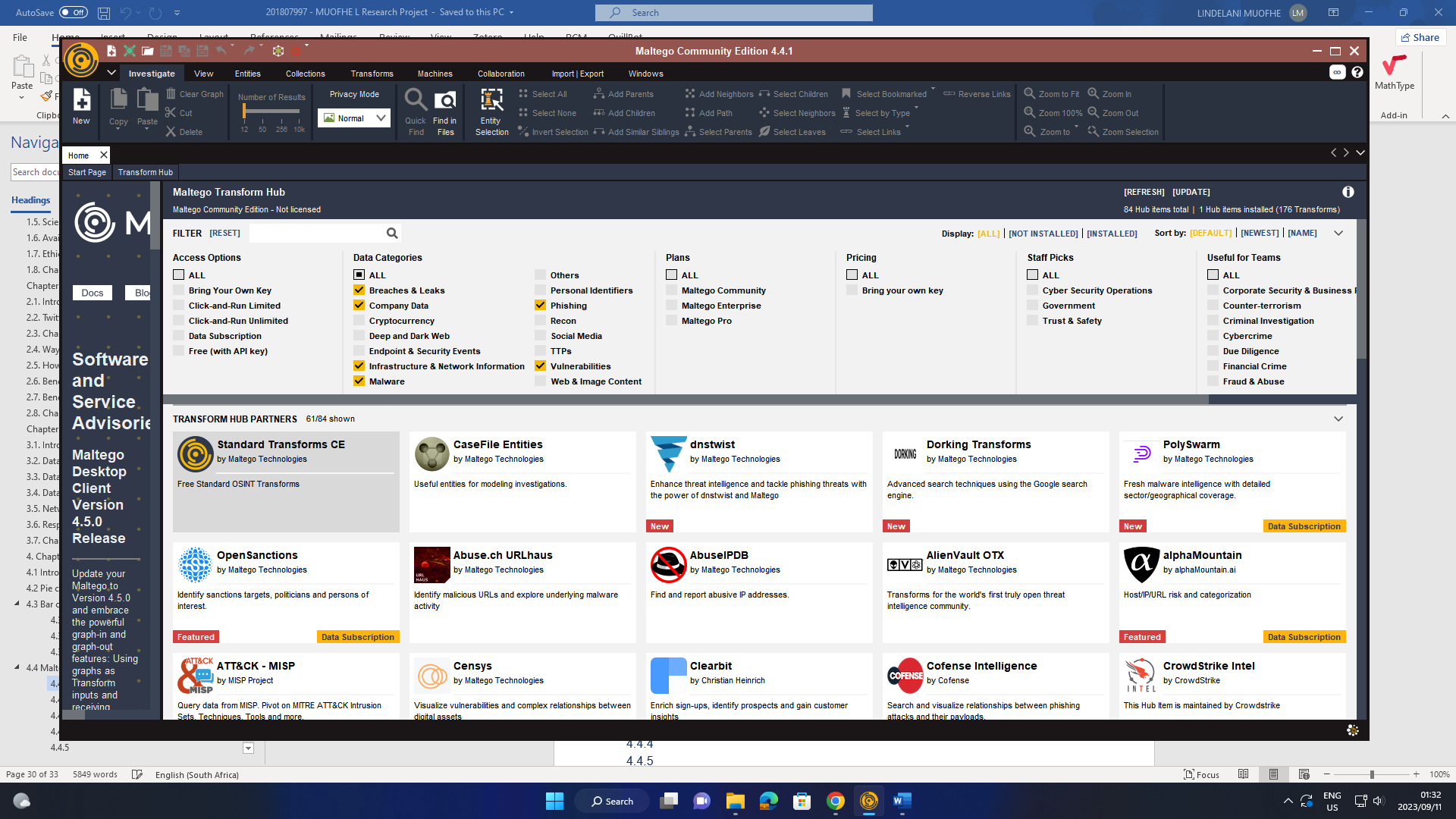
We explore the on-premises infrastructure of a large international organisation. We will look to identify any potential security vulnerabilities, including open ports, legacy systems, exposed security solutions, and critical vulnerabilities such as unpatched software.

## Define the Scope of the Assessment

Once we have defined the scope of the assessment, the next step is to identify potential data sources that can be used to gather information about the target. The pie and bar charts show that the most common attacks that target the e-Commerce system are Theft, phishing and or spoofing attacks.

To configure Maltego for attack surface assessments, we select the appropriate, relevant data sources using the Filters available on the Start Page of your Maltego Client.

Figure 6 Maltego scope assessment

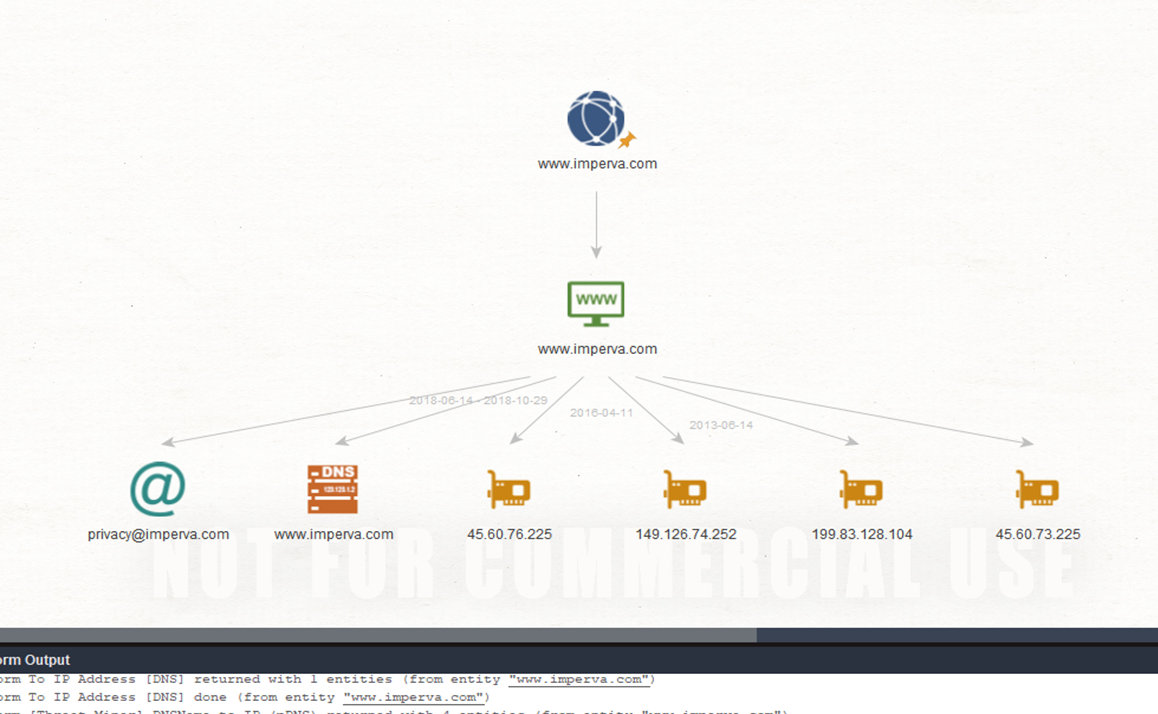


## Network mapping

The process of collecting data on a specific system or network, often referred to as reconnaissance or information gathering, involves obtaining various details related to the target. This information can encompass a range of elements, such as domain names linked to your organisation, currently active IP addresses, accessible ports, software versions in use, and any other publicly accessible data that can aid in identifying potential weaknesses or vulnerabilities.

* Domain name associated with the Organisation.
* IP addresses, open ports, and Software versions in use.
* Trace the origin of threats that infiltrate the company’s data or network.

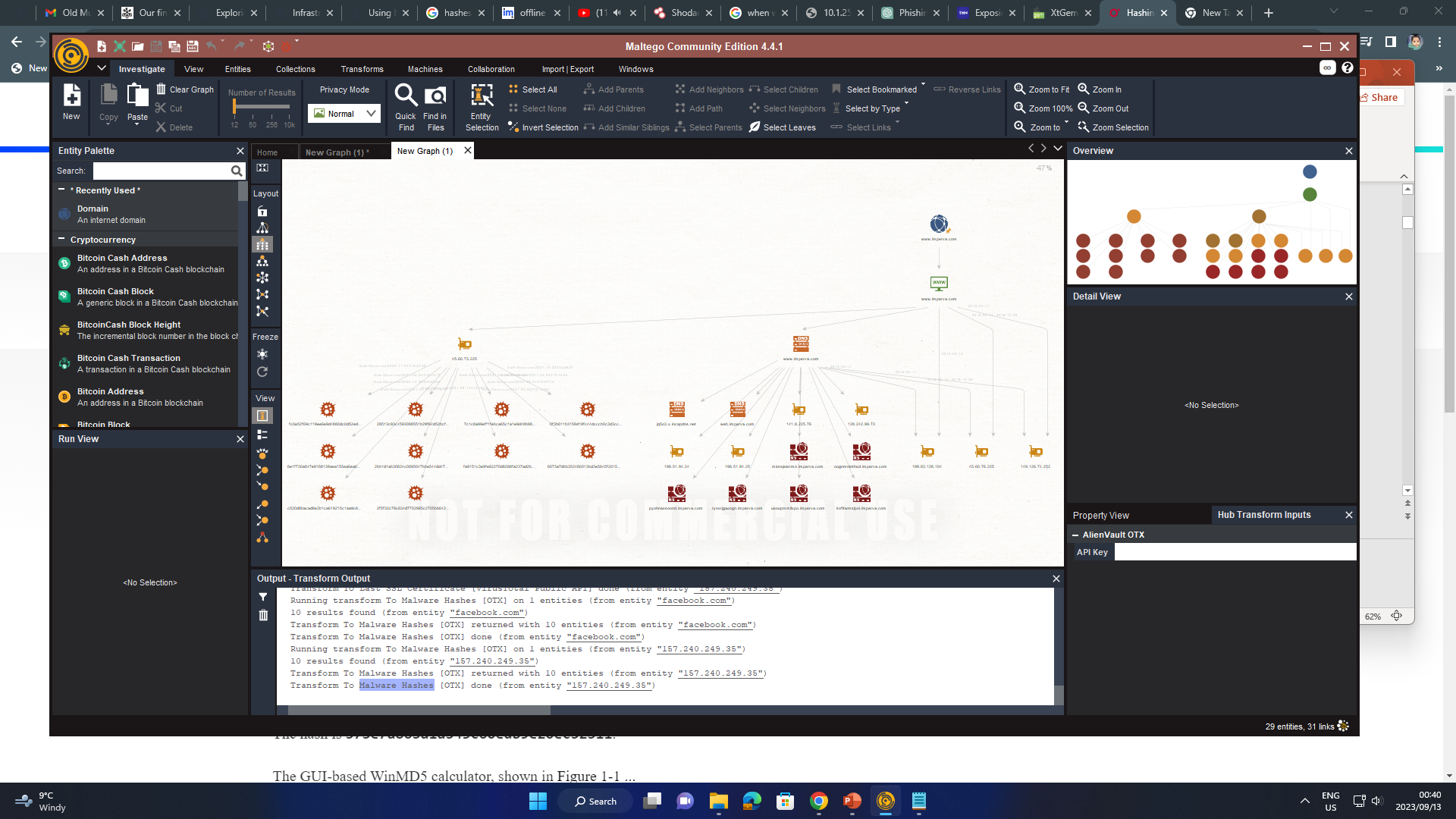
Figure 7 Network mapping



## Response planning

* Virus Total Transformation: This service is designed to examine files and web links, checking for viruses, trojans, and various forms of malicious content.
* Investigators can return information on association IP addresses, hashes, domains, and URLs.
* Hashing is a common method that is used to uniquely identify malware.

Figure 8 Monitoring infrastructure network



The findings indicate instances related to testing and email activities. To ascertain whether these instances are associated with live hashes or potential attacks, we can take the following steps.

1. We can resolve the IP addresses linked to each entity to validate its existence or detect potential attacks. This can be accomplished by selecting the newly identified entities and executing the "To IP Address [DNS] Transform." Any instance that yields a matching IP address can be considered potentially active or live.
2. Additionally, we identified other vulnerabilities by selecting all the IP addresses and running the "To Vulnerabilities [Shodan] Transform." This process helps us to uncover potential weaknesses or security concerns associated with these IP addresses.

That is, we can use these transformations to confirm the activity status of entities and uncover vulnerabilities that may require further investigation or mitigation measures.

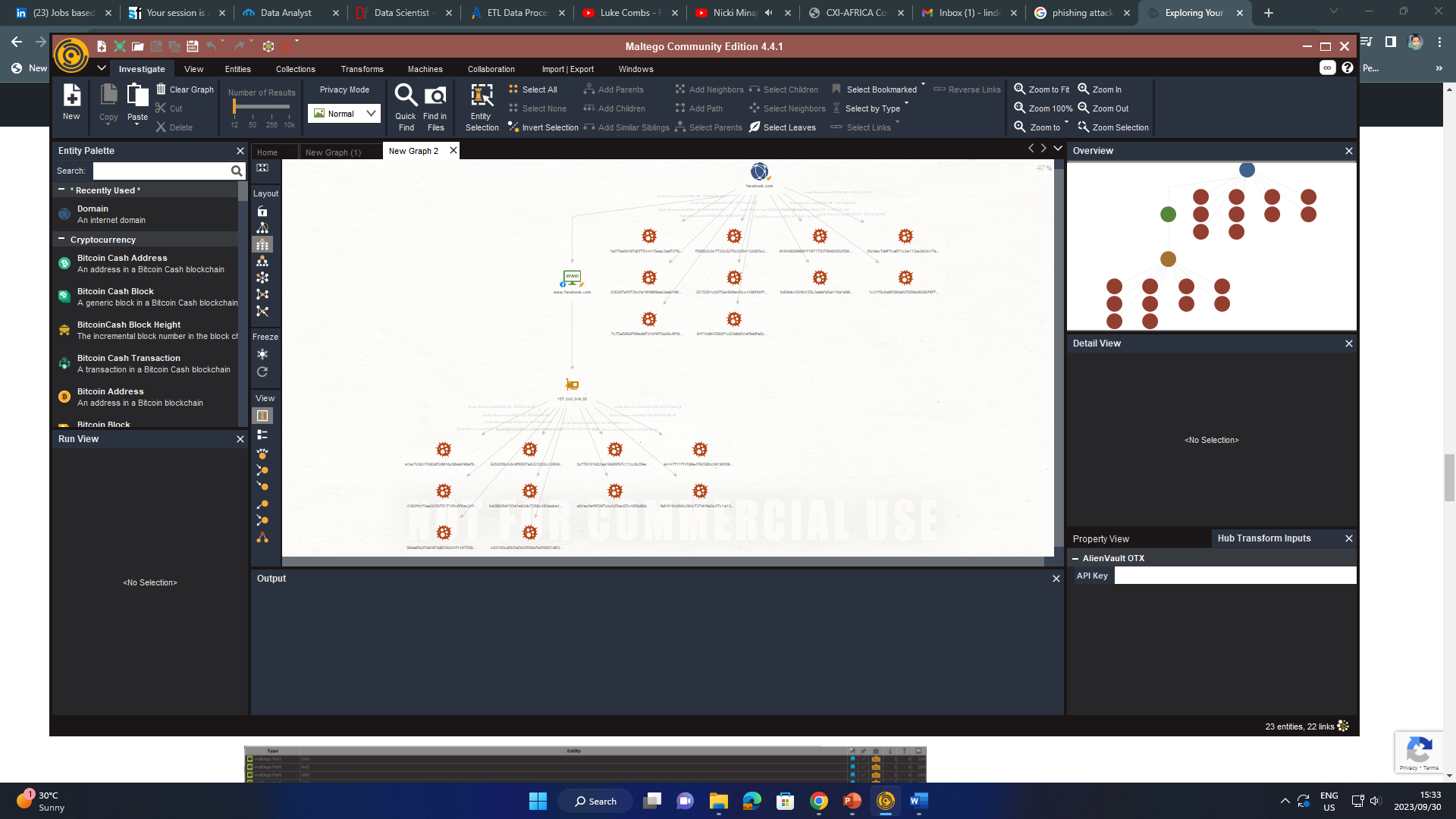


Figure Monitoring for information leaks entry points

The results of the attack surface assessment can serve as a basis for crafting a comprehensive plan aimed at improving security and network integrity. This plan encompasses various strategic actions, including:

1. Implementing Security Patches: Addressing vulnerabilities and potential threats by applying the necessary security patches to systems and software. This proactive measure helps fortify the organisation's defences against potential exploits.
2. Closing Unsecured Ports: Identifying and shutting down any open or unsecured network ports that could serve as potential entry points for malicious actors. By doing so, the organisation minimizes its exposure to external threats.
3. Establishing a Request for Change (RFC): Creating a structured RFC process that outlines the steps and protocols for decommissioning test instances and other non-essential systems. This ensures that unnecessary access points are removed, reducing the attack surface.
4. Implementing Additional Security Measures: Implementing additional security measures and best practises as deemed necessary to safeguard the organisation's infrastructure and customer data. These measures can include firewall configurations, intrusion detection systems, and enhanced authentication protocols.

By executing these steps, the E-Commerce organisation can significantly decrease its attack surface, thereby bolstering its defences against potential security breaches. This not only enhances the security of the organisation's systems and data but also reinforces the protection of its valued e-Commerce customers.

* 1. CONCLUSION

In this chapter, the primary focus was on Maltego's role in conducting attack surface assessment. Maltego is a valuable tool that assists security teams in pinpointing potential vulnerabilities and weaknesses within an organisation's network and assets. Its purpose is to help companies evaluate their own security vulnerabilities by actively monitoring for various security red flags. These red flags may include leaked customer credentials, the use of weak passwords, and other indicators of inadequate security practises that could potentially impact e-Commerce systems and overall security.

# CHAPTER 5 CONCLUSION & FUTURE WORK:

# 5.1. INTRODUCTION

This chapter aims to discuss the summary of the research findings. These are the results of Phishing, Spoofing, and theft on the E-Commerce network system affecting both consumers and E-Commerce organisations. This chapter will refer to all the objectives that have been achieved; it will also show future work, conclusions, and as well as limitations.

# 5.2. RESEARCH DESIGN AND METHOD

## Objective 1

To investigate previous e-Commerce security incidents using OSINT tools by gathering data on how to monitor, litigate, and minimise their spread against e-commerce security or online shopping.

The data that we obtained after cleaning and processing we analysed it, both the bar and pie chart clearly shows that the most common attack targeting the e-Commerce platform is theft, this includes phishing and spoofing, so from these analysis companies can easily be aware of this threat and always monitor their infrastructure and provide early warning to their customers and protect themselves from these possible threats.

## Objective 2

To identify possible potential threats and detect fraudulent activities such as fake reviews, phishing attacks, and scams targeting e-Commerce customers, and provide early warning of potential cyberattacks to businesses.

Figure 8, the findings indicate instances related to testing and email activities. To ascertain whether these instances are associated with live hashes or potential attacks that resemble the company websites and domains.

Taking the following steps, we achieved objective 2 and identified phishing attacks, scams and their fraudulent activities to harm the e-Commerce system.

We can resolve the IP addresses linked to each entity to validate its existence or detect potential attacks. This can be accomplished by selecting the newly identified entities and executing the "To IP Address [DNS] Transform." Any instance that yields a matching IP address can be considered potentially active or live to unmask all the fake revies and any related phishing attack.

Additionally, we identified other vulnerabilities by selecting all the IP addresses and running the "To Vulnerabilities [Shodan] Transform." This process helps us to uncover potential weaknesses or security concerns associated with these IP addresses to uncover all fake websites pretending to be original.

That is, we can use these transformations to confirm the activity status of entities and uncover vulnerabilities that may require further investigation or mitigation measures.

## Objective 3

To help businesses investigate the source of the attack and entry points by identifying hashes that are appended to the company domain or IP addresses by attackers and also trace their origin.

Figure 7 shows that using Maltego, a powerful OSINT tool, we could assess company vulnerabilities by monitoring for poor security practises that are affecting the e-Commerce system such as identifying hashes that are appended to the company domain or IP addresses by attackers and also trace their origin by collecting data on a specific system or network, this is the process of reconnaissance or information gathering, involves obtaining various details related to the target.

This information can encompass a range of elements, such as domain names linked to the organisation, currently active IP addresses, accessible ports, software versions in use, and any other publicly accessible data that can help in identifying potential weaknesses or vulnerabilities.

## Objective 4

Using Open source intelligent we can also achieve objective 4 which is to gather intelligence to prevent future attacks by providing early warning of potential cyberattacks to businesses by monitoring leaked customer credentials, weak passwords, and other indicators of poor security practises affecting the e-Commerce systems.

The results on figure 9 clearly show that the attack surface assessment can serve as a basis for crafting a comprehensive plan aimed at improving security and network integrity making sure that customers data and company network are not tempered with.

Addressing vulnerabilities and potential threats by applying the necessary security patches to systems and software. This proactive measure helps fortify the organisation's defences against potential exploits.

Identifying and shutting down any open or unsecured network ports that could serve as potential entry points for malicious actors. By doing so, the organisation minimizes its exposure to external threats.

Implementing additional security measures and best practises as deemed necessary to protect the organisation's infrastructure and customer data.

# 5.3. SUMMARY AND INTERPRETATION OF THE RESEARCH FINDINGS

The data collected indicates a significant 54.3% higher rate of theft breaches, highlighting a strong issue of cybercrimes involving fake retailer websites aimed at stealing from individuals and selling counterfeit products. These thefts occur frequently when individuals engage with fraudulent websites.

Approximately 23.8% of losses in the realm of online shopping, primarily affecting e-Commerce individuals, are posed by cybercriminal activities. These losses are most commonly associated with phishing attacks where cybercriminals impersonate trusted entities to steal sensitive information, including credit card details, passwords, login credentials and attempt to install viruses on victim’s computers.

The findings suggest that there is a considerable risk associated with cybercrimes, particularly in the context of e-Commerce. Cybercriminals use various tactics such as setting up fake retailer websites, engaging in phishing attacks, and employing spoofing techniques to exploit vulnerabilities within the online shopping ecosystem. As a result, individuals and businesses through the use of OSINT tools can take measures to enhance their cybersecurity efforts. The data underscores the importance of improving security measures to reduce the incidence of phishing attacks that can be achieved by monitoring for information leaks, scanning for viruses and malicious sites appended to the domain of e-Commerce platforms, as these attacks pose a significant threat to both individual consumers and e-Commerce organisations. It is important for businesses to prioritise the protection of sensitive customer information and maintain the integrity of their online platforms to ensure a safe and trustworthy e-Commerce environment.

# 5.4. CONCLUSION

This review paper offers an in-depth exploration of open source intelligence (OSINT) and its applications within the field of cybersecurity against the security of E-Commerce. It covers the various stages of OSINT, highlighting widely used methodologies and tools. By harnessing the appropriate technology, expertise, and analytical skills, OSINT has demonstrated its ability to predict events well in advance. This predictive power extends beyond early warnings to organisation to provide proper defence against their data and customers; OSINT can also be employed for root cause analysis and forensic investigations, particularly in incidents such as civil disturbances.

# 5.5. RECOMMENDATIONS

The proposed OSINT solution aims to streamline investigations, making them stress-free and business-friendly. By adopting this advanced digital platform, we can improve national security and investigation efficiency using more OSINT tools. This platform ensures that investigations maintain a high success rate by optimising time and resources.

OSINT proves invaluable for data extraction and processing, enabling access to high-quality data from publicly available legal sources. Once implemented, this solution could revolutionise real-time search capabilities, offering significant benefits to the nation.

# 5.6. CONTRIBUTIONS OF THE STUDY

The research successfully achieves its objective by identifying potential threats and fraudulent activities, including fake reviews, phishing attacks, and scams targeting e-Commerce customers. The process of linking IP addresses to entities and using transformations helps to uncover potential vulnerabilities and security concerns, further contributing to the understanding of threats and the development of mitigation strategies.

The study employs OSINT tools, such as Maltego, to assess company vulnerabilities and investigate the source of attacks. It successfully identifies hashes appended to company domains or IP addresses by attackers, tracing their origins. This reconnaissance approach helps in gathering essential information related to potential weaknesses or vulnerabilities, contributing to a proactive security stance.

The study's results offer insights into preventing future cyberattacks by monitoring leaked customer credentials, weak passwords, and indicators of poor security practices. The attack surface assessment enables businesses to craft comprehensive plans to improve security and network integrity through open source intelligence. This includes addressing vulnerabilities, applying security patches, closing unsecured network ports, and implementing additional security measures to protect customer data and network infrastructure. These contributions help in strengthening the organisation's cybersecurity posture.

# 5.7. LIMITATIONS OF THE STUDY

During the paper review, it was identified that some areas within OSINT do not extensively monitor the threat landscape for cybersecurity events. Notable research gaps include:

* Lack of Intelligent Analysis: OSINT currently lacks intelligent analysis mechanisms, relying on tools for basic data collection and straightforward connections. Incorporating semantic analysis, pattern analysis, and event correlation could reduce dependence on human analysts.
* Need for Machine Learning and Automated Reasoning: OSINT should incorporate machine learning and automated reasoning to intelligently address various problems and open questions.
* Automated Detection of Misleading Information: Rather than relying solely on human intervention, OSINT should implement automated processes to identify misleading or false information, considering the inherently unverified nature of Internet content.

# 5.8. CONCLUDING REMARK

This paper underscores the important role of open source intelligence (OSINT) in cybersecurity within the realm of e-Commerce. Through its comprehensive exploration of OSINT stages, methodologies, and tools. OSINT serves as a valuable early warning system for organisations and also empowers them to put in place effective defences against cyberthreats to their data and customers. As cybersecurity continues to grow, OSINT stands as a formidable ally, offering a proactive and insightful approach to protecting e-Commerce in an ever-changing digital landscape.

# REFERENCE

Bhandari, P. (2021, October 18). *Ethical Considerations in Research | Types & Examples*. Scribbr. https://www.scribbr.com/methodology/research-ethics/

Charles, K. (2022, September 19). The Open-Source Intelligence (OSINT) Cycle. *Security Boulevard*. https://securityboulevard.com/2022/09/the-open-source-intelligence-osint-cycle/

Dastres, R., & Soori, M. (2020). Secure Socket Layer (SSL) in the Network and Web Security. *International Journal of Computer and Information Engineering*, *14*(10), 330–333.

Digital, S. T. L. (2023, February 1). Network Mapping: How it Works and Best Practices. *STL Digital*. https://stldigital.tech/blog/network-mapping-how-it-works-and-best-practices/

Gottschalk, P., Filstad, C., Glomseth, R., & Solli-Sæther, H. (2011). Information management for investigation and prevention of white-collar crime. *International Journal of Information Management*, *31*, 226–233. https://doi.org/10.1016/j.ijinfomgt.2010.07.002

Hayes, D., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, *61*. https://doi.org/10.1016/j.bushor.2018.02.001

Kaur, C., & Sharma, Dr. Y. (2020). *The vital role of VPN in making secure connection over internet world*. *8*, 2336–2339. https://doi.org/10.35940/ijrte.F8335.038620

Khan, D. S. W. (2019). *Cyber Security Issues and Challenges in E-Commerce* (SSRN Scholarly Paper 3323741). https://doi.org/10.2139/ssrn.3323741

Lande, D., & Shnurko-Tabakova, E. (2019). OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, *1*(1). https://www.academia.edu/41391165/OSINT\_as\_a\_part\_of\_cyber\_defense\_system

Marinho, R., & Filho, R. (2023). Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing. *IEEE Access*, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2023.3260020

Mittal, S., Das, P., Mulwad, V., Joshi, A., & Finin, T. (2016a, August 1). *CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities*. https://doi.org/10.1109/ASONAM.2016.7752338

Mittal, S., Das, P., Mulwad, V., Joshi, A., & Finin, T. (2016b, August 1). *CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities*. https://doi.org/10.1109/ASONAM.2016.7752338

Nguyen, D. (2010, December 30). *Chapter 1. Using Google Refine to Clean Messy Data*. ProPublica. https://www.propublica.org/nerds/using-google-refine-for-data-cleaning

Santarcangelo, V., Oddo, G., Pilato, M., Valenti, F., & Fornaro, C. (2015, August 24). *Social Opinion Mining: An Approach for Italian Language*. https://doi.org/10.1109/FiCloud.2015.52

Semenishchev, I., Sinadskiy, A., Sinadsky, M., Sinadsky, N., & Sushkov, P. (2020). *Method for Forming the Dynamic Components of Conditionally Real Data Arrays Based on Color Petri Net Algorithms for Organizing a Computer Training Platform for Investigating Information Security Incidents*. 582–585. https://doi.org/10.1109/USBEREIT48449.2020.9117652

Tabatabaei, F., & Wells, D. (2016a). *OSINT in the Context of Cyber-Security* (pp. 213–231). https://doi.org/10.1007/978-3-319-47671-1\_14

Tabatabaei, F., & Wells, D. (2016b). *OSINT in the Context of Cyber-Security* (pp. 213–231). https://doi.org/10.1007/978-3-319-47671-1\_14

Tabatabaei, F., & Wells, D. (2016c). OSINT in the Context of Cyber-Security. In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation* (pp. 213–231). Springer International Publishing. https://doi.org/10.1007/978-3-319-47671-1\_14

U., Y., & Karani, K. P. (2021). Open Source Intelligence and its Applications in Next Generation Cyber Security—A Literature Review. *International Journal of Applied Engineering and Management Letters*, 1–25. https://doi.org/10.47992/IJAEML.2581.7000.0100

Wiradarma, A., & Sasmita, G. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*, 17–29. https://doi.org/10.5815/ijcnis.2019.12.03

Yamin, M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Muhammad, K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics*, *10*, 2054. https://doi.org/10.3390/math10122054

Yeboah-Ofori, A. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*, *7*, 87–98. https://doi.org/10.17781/P002378

Zhang, Y. (Cicilia), Frank, R., Warkentin, N., & Zakimi, N. (2022). Accessible from the open web: A qualitative analysis of the available open-source information involving cyber security and critical infrastructure. *Journal of Cybersecurity*, *8*(1), tyac003. https://doi.org/10.1093/cybsec/tyac003