Utilisation of OSINT: Empirical Study of CTI Practices in Pakistan

By

Fizza Shafiq

2019-MS-IS 317909 SEECS

Supervisor

Dr Sana Qadir

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Security (MS IS)

In

School of Electrical Engineering & Computer Science (SEECS) ,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(June 2023)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Utilisation of OSINT - Empirical Study of CTI Practices in Pakistan " written by FIZZA SHAFIQ, (Registration No 00000317909), of SEECS has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: 

Name of Advisor: Dr. Sana Qadir

Date: 15-Jun-2023

HoD/Associate Dean: _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

Approval

It is certified that the contents and form of the thesis entitled "Utilisation of OSINT - Empirical Study of CTI Practices in Pakistan " submitted by FIZZA SHAFIQ have been found satisfactory for the requirement of the degree

Advisor : Dr. Sana Qadir

Signature: _____

Date: 15-Jun-2023

Committee Member 1:Dr. Hasan Tahir

Signature: _____

15-Jun-2023

Committee Member 2:Dr. Razi Arshad

Signature: _____

Date: 16-Jun-2023

Signature: _____

Date: _____

Dedication

This thesis is dedicated to everyone who helped me along the way to accomplish this daunting task. It takes a village to raise a child, and the same is true for this thesis.

Certificate of Originality

I hereby declare that this submission titled "Utilisation of OSINT - Empirical Study of CTI Practices in Pakistan " is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: FIZZA SHAFIQ

Student Signature: 

Acknowledgments

All praise and thanks go to Allah who gave me the energy to carry out this thesis. His blessings were the sole reason for this work to exist. I am thankful for my husband and my family who have helped and encouraged me to work. I would also like to mention my son, without his efforts, this would have been completed a lot sooner. I am extremely grateful for my advisor Dr. Sana whose endless patience and support made the completion of this thesis possible. Her valuable time and guidance was my motivation for working on this project. I am also grateful and thankful to committee members Dr Razi Arshad and Dr Hasan Tahir for their cooperation towards the completion of this research work.

Fizza Shafiq

Contents

List of Figures

List of Tables

Abstract

With the observed increase in Internet users, the volume of available data is increasing as well. Public platforms such as social media, news sources, and open data repositories present a vast potential that remains largely untapped. Open Source Intelligence (OSINT) holds unparalleled utility, particularly in the realm of Cyber Threat Intelligence (CTI). Although there has been significant progress in the IT infrastructure in Pakistan, it lags behind in terms of cyber security implementations. To address this gap, a comprehensive empirical study was conducted over a period of seven months, employing a mixed methods approach. Data were collected from general employees and security specialists through surveys and interviews. These resources are often utilized without proper awareness of the corresponding terminology of "OSINT". This paradigm indicates a suitable environment in Pakistan for progress and improvement in the utility of open source data and tools. A framework is also proposed to facilitate the integration of Open Source Intelligence (OSINT) into the routine IT operations of organizations and maximize the effectiveness of their endeavors.

Keywords: Cyber Threat Intelligence (CTI), Open Source Intelligence (OSINT), Security practices, Information security, Framework

Chapter 1

Introduction

1.1 Background

Statistically, it may seem that organizations will always be at a disadvantage in terms of security[4]. This fact is explained by the statistic that in 2023 cybercrime is expected to cost $8 trillion annually[5]. Due to these circumstances, security professionals often find themselves in a position where they can only examine the aftermath of cyber attacks. Left with trails of information that serve as the remnants of an attacker's past actions, putting them at a significant disadvantage. According to the Check Point 2023 cyber security report, 32% of the organizations were affected by multi-purpose malware in 2022[6]. This underscores the critical importance of organizations to prioritize robust cyber security measures, including proactive threat detection.

By prioritizing timely and effective communication of information, organizations can transform potential threats into preventable problems. A crucial aspect of achieving this is through the use of relevant threat intelligence. This valuable resource enables collaboration and information sharing among stakeholders, fostering the development of targeted mitigation measures. By integrating robust intelligence processes into their operations, organizations can tailor their approach to align with their unique needs and risk profiles.

The traditional method of reactive security needs to be updated with a model that accommodates the ever-changing cyber-security environment. Proactive security measures can help organizations maintain compliance with rules and standards and adapting to changes in the threat landscape.

Traditional security controls, while important, may not be sufficient in defending against advanced tactics such as social engineering. These sophisticated and ever-changing attack techniques have the potential to bypass traditional security measures, making it crucial for organizations to adopt solutions that take advantage of threat intelligence. Moreover, the value of threat intelligence extends beyond individual organizations. When an organization falls victim to an attack, the information gathered during the incident response process can be shared with other organizations, helping to identify and prevent similar attacks. This collective intelligence strengthens the overall security posture of the community by enabling a proactive and collaborative approach to threat detection and mitigation.

1.2 Cyber Threat Intelligence (CTI)

Cyber threat intelligence refers to the application of traditional intelligence methodologies in the field of cyber security, with a specific focus on identifying and mitigating threats[7]. In the literature, it can be addressed as Cyber Threat Intelligence (CTI), technical threat intelligence [8], or cyber intelligence [9]. Though not exactly the same, the context in which they are mentioned is similar, hence allowing the liberty of using them alternatively.

1.2.1 Sources of CTI

There are three types of CTI sources based on how the information is gathered, as classified by [10]:

1. **Internally Sourced:** CTI derived from internal sources consists of observable events that occur within an organization's internal network and systems. It offers indications of security breaches, violations of internal access control rules, system infections, or unauthorized attempts to access restricted systems.

2. **Externally Sourced Observables:** CTI obtained from external sources outside the organization. These observables are typically related to cyber security and are used to identify and analyze potential threats or malicious activities. Common examples of externally sourced observables include IP addresses, domains, URLs, file names, and hashes. These observables are typically obtained from feeds

that adhere to formal standards such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII). These standards facilitate the structured and standardized sharing of cyber threat intelligence. Additionally, observables can also be obtained in common file formats such as CSV (Comma-Separated Values), JSON (JavaScript Object Notation), or simple plain text.

3. **External Open Source Intelligence:** This source of CTI refers to the collection and analysis of information from publicly available sources, such as websites, social media platforms, online forums, news articles, and public databases.

1.3 Open Source Intelligence (OSINT)

Definition 1.1 (Open Source Intelligence)**.** *Information processing from open source data and tools including the search, collection and analysis of raw data[11].*

Open source information, which has found applications in various domains such as medicine [12] [13], business decision making[14], and city planning[15], has immense potential for cyber security, particularly in the realm of Cyber Threat Intelligence (CTI). The use of open source information in cyber security enables organizations to exploit a wide range of data sources, including public websites, social media platforms, forums, and other publicly available resources. Additionally, Open Source Intelligence (OSINT) allows organizations to stay informed about the latest trends and developments in the cyber security landscape. By monitoring publicly available information, organizations can proactively detect indicators of compromise, emerging vulnerabilities, or potential attacks targeting their infrastructure or industry. This early warning system empowers organizations to take preventive measures to prevent or mitigate potential threats.

Open source intelligence (OSINT) is not limited to large organizations and can offer significant benefits to smaller organizations as well. While larger organizations may have dedicated resources and cyber security teams, smaller organizations often face resource constraints and may not have the same level of expertise or infrastructure. However, OSINT can level the playing field by providing valuable information and insights that can improve the security posture of smaller organizations.

One of the key advantages of OSINT for smaller organizations is its accessibility. Un-

like proprietary or expensive intelligence sources, OSINT is typically freely available or accessible at a lower cost. This allows smaller organizations with limited budgets to tap into a wide array of open source data and intelligence, allowing them to gain insight into potential threats, vulnerabilities, and malicious activities.

1.3.1 OSINT Structure

The structure and processing of Open Source Intelligence (OSINT) can vary between organizations based on their specific requirements. However, there are generally five main steps as shown in Figure 1.1 involved in the OSINT process [16], which are as follows:

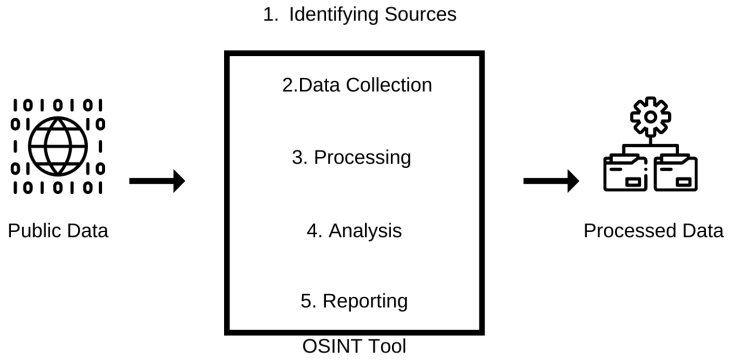

Figure 1.1: OSINT Structure

1. Identifying the Source: This initial step involves identifying and selecting relevant sources of open information. These sources can include websites, social media platforms, news outlets, public records, blogs, forums, and other publicly available information.

2. Data Collection: Once the sources have been identified, the next step is to collect the necessary data. This can be done by manual searching, web scraping, data mining, or using automated tools designed for OSINT collection.

3. Processing: After data collection, the information obtained needs to be processed to make it usable and more manageable. This involves tasks such as data cleans-

ing, data normalization, and structuring the information in a way that facilitates further analysis. Processing may also include categorizing or tagging the data to enable efficient retrieval and organization.

4. Analysis: Once the data is processed, the analysis phase begins. Analysts examine and interpret the information collected to extract information and identify patterns, trends, relationships, or potential risks. This can involve various techniques, such as data mining, text analysis, sentiment analysis, or other analytical methods specific to the organization's needs.

5. Reporting: The final step involves reporting the findings and insights derived from the analysis. This includes summarizing relevant information in a clear and concise manner, often in the form of reports, briefings, or alerts. Reports should be tailored to the target audience, providing actionable intelligence and recommendations based on the analysis carried out.

1.3.2 OSINT Tools and Techniques

Open Source Intelligence (OSINT) plays a crucial role in gathering and analyzing of information from publicly available sources using various tools and techniques. The following are a selection of OSINT tools and techniques that are provided as examples to illustrate their capabilities.

MITRE ATT&CK

MITRE ATT&CK [17] stands as one of the prominent and substantial Open Source Intelligence (OSINT) resources available. Developed by MITRE Corporation, the MITRE ATT&CK framework provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) observed in real-world cyber attacks. It offers a structured and organized repository of information that helps organizations understand the behavior of threat actors and improve their cyber defense strategies. The framework classifies various attack techniques into a matrix, allowing organizations to map and analyze adversary behavior against their own security controls. It covers a wide range of tactics, including initial access, execution, persistence, privilege escalation, and exfiltration, among others.

Search Engines

The largest and most common tools used on a daily basis to search the Internet are search engines. Even untrained individuals can use search engines to gather information. In the hands of a professional, the results produced can be elaborate and precise., if they make use of advanced search options and filters[18].

Social Media

OSINT professionals use tools specifically designed to monitor and analyze social media platforms. These tools can track keywords, hashtags, and user activities to identify trends, sentiments, and potential threats. Tools such as SL Professional [19] can help automate the OSINT process, creating connections in a web-like way for better visualization.

Web Scraping

For traversing multiple online sources simultaneously, web scraping tools can help collect data much more efficiently than manual search. Some examples of tools are Photon-Scanner[20], TG-API, and instant data scraper[21].

Data Visualization Tools

Visualizing OSINT data can help identify patterns, connections, and trends. Tools such as data visualization software and graph databases provide interactive and intuitive representations of complex data, enhancing understanding and analysis of information. One such example is Maltego [22], which is a powerful tool to help OSINT investigations.

Open Data Platforms

Open data platforms provide access to publicly available data sets from various government, research, and institutional sources. These platforms allow users to explore and analyze large datasets for research, analysis, and intelligence purposes. An example of such a platform is "Open Data Pakistan"[23].

Geo-location

Geo-location techniques help identify the physical location associated with digital information. Mapping tools and geospatial analysis software enable visualization and analysis of geolocation data, contributing to investigations and intelligence gathering.

A significant disadvantage of OSINT tools and techniques that one should consider is their inconsistency with respect to their availability. A resource available one day can be withdrawn or unavailable the next, as is the example of social networks, as tech giants such as Facebook and Instagram are known to regularly change their source code to make use of OSINT techniques difficult.

1.3.3 Advantages of OSINT:

Open Source Intelligence (OSINT) offers several advantages, particularly for non-technical and untrained individuals. Some of the key benefits include:

- **Accessibility:** OSINT is derived from publicly available sources, which makes it accessible to anyone with an Internet connection. There is no need for specialized access or technical skills to collect OSINT.
- **User-Friendly:** OSINT tools and platforms have evolved to be user-friendly with intuitive interfaces, allowing nontechnical users to perform searches, analyze data, and extract relevant information.
- **Broad Range of Information:** The variety of sources included in OSINT allows users to gather diverse and comprehensive information about individuals, organizations, events, or topics of interest. Sources such as news articles, social media platforms, online forums, blogs, and various websites contribute to a vast pool of information available for gathering open source intelligence (OSINT)
- **Cost-Effectiveness:** OSINT sources and tools are cost effective eliminating the need for expensive subscriptions or specialized software.
- **Real-Time Updates:** OSINT sources often provide real-time updates, allowing users to stay informed about current events, trends, or developments. This is particularly valuable for nontechnical users who rely on up-to-date information for decision-making, increasing their situational awareness.

- **Versatility:** OSINT can be applied in numerous domains and industries. It provides valuable insights and data to support research, research projects, or daily decision-making.

1.4 Motivation

The motivation behind this thesis was to address the existing gap in awareness and adoption of current security trends and developments in Pakistani organizations. Cyber Threat Intelligence (CTI), particularly through the use of free Open Source Intelligence (OSINT) tools and data, can play a crucial role in bridging this gap. The world is moving toward the use of OSINT with AI [18], but Pakistan is yet to explore OSINT itself. The primary objective of the study was to gain insight into the current state and attitudes of both the general public and security professionals about OSINT, free tools, and data.

1.5 Problem Statement

Limited research on security practices in Pakistani organizations, coupled with a lack of understanding of the extent to which OSINT sources are used for CTI, creates a significant knowledge gap. This gap makes it difficult to identify areas for improvement and propose solutions to improve CTI practices. The study seeks to investigate the landscape of cyber security with an emphasis on OSINT sources and CTI practices, seeking to identify the common challenges faced by organizations in adopting and implementing OSINT sources.

1.5.1 Objectives

- Assess the current state and attitudes of Pakistani organizations, both general public and security professionals, towards Open Source Intelligence (OSINT), free tools, and data in the context of cyber security.
- Investigate the CTI programs and the use of OSINT in security companies operating in Pakistan, including their observations on the security attitudes and trends of organizations within the country.

- Propose an updated framework for Pakistani organizations to add Open Source Intelligence (OSINT) and Cyber Threat Intelligence (CTI) to their existing IT infrastructure.

1.6 Methodology

The following research methodology has been used to answer the above questions:

1. **Literature Review:** A comprehensive literature review was conducted to determine the current state of Cyber Threat Intelligence (CTI) and Open Source Intelligence (OSINT). Special attention was paid to literature pertaining to Pakistan and Cyber Security. Google Scholar and Semantic Scholar were used to examine the relevant literature. This involved analyzing academic papers, relevant articles, and studies focused on cyber security.

2. **Data collection:** This study employed a mixed methods research approach, using surveys and semi-structured interviews, to collect information on the use of Open Source Intelligence (OSINT) for Cyber Threat Intelligence (CTI) purposes in organizations in Pakistan. The data was collected though three main components:

   (a) A preliminary survey of sample size 151 was disseminated among employees working in Pakistani organizations. The survey aimed to gather a broader perspective on the use and awareness of OSINT sources, free tools, and open data among various industries in Pakistan.

   (b) Semi-structured interviews were conducted with participants who volunteered to elaborate on the results of the surveys. The interviews were conducted with individuals who were **Security Professionals** or **IT Team Leaders** of their respective companies. The results of the interviews highlighted the differences in the perception of the usefulness of OSINT in the two groups.

   (c) A targeted survey was created specifically for the leading cyber security companies in Pakistan. The survey was designed to collect information about their experience in the field, the CTI services they offered, and their observations of trends related to cyber security in Pakistan.

3. **Data Analysis:** The research used a mixed-method approach, combining quantitative and qualitative analysis techniques. Surveys included open-ended and closed-ended questions, allowing for a multifaceted examination of the research objectives. Inferential statistic tests, such as t-tests and chi-square test, were applied on closed-ended questions using online statistics software Stats.Blue [24]. Open-ended questions from the surveys were subjected to thematic analysis, conducted on Google Sheets, where the responses were cleaned, categorized and assessed to identify common themes and draw meaningful conclusions. The interview data also underwent thematic analysis, following a similar process in Google Sheets.

4. **Framework Proposal:** Following data collection and analysis, a framework was proposed to accumulate the knowledge gained from surveys and interviews.

1.7 Structure

This document is organized as follows:

- **Section 2** is a review of the existing research and publications on the topic of Open Source Intelligence (OSINT) and Cyber Threat Intelligence (CTI).
- **Section 3** outlines the research design and approach used in the study.
- **Section 4** presents the study findings and provides a detailed analysis and interpretation of the data collected.
- **Section 5** Discusses the baseline framework and proposes a workflow framework.
- **Section 6** provides a concise summary of the main findings and conclusions of the study, as well as a description of potential avenues for future research.

Chapter 2

Literature Review

Cyber threat intelligence (CTI) is a critical component in understanding and mitigating the risks posed by adversaries in the digital landscape. It involves analyzing the intent, opportunity, and ability of an adversary to inflict harm on the assets and operations of an organization[25]. Unlike a mere data feed or a tool, intelligence provides actionable information that addresses specific knowledge gaps, pain points, or requirements of an organization.

Organizations currently utilize Open Source Intelligence (OSINT) and Cyber Threat Intelligence (CTI) in an ad hoc manner. This means that their usage of OSINT and CTI is not systematic or structured, but rather sporadic and based on immediate needs or circumstances. This ad hoc approach often leads to inefficiencies and missed opportunities for organizations to fully leverage the benefits. A survey of 338 CTI practitioners [26] revealed that even in the CTI community about 85% of the respondents had no formal training in OSINT, although 83% of the analysts used search engines as their main tool for conducting research.

Previously, it was commonly believed that only large organizations with established cyber security teams could utilize Cyber Threat Intelligence (CTI). However, recent trends show that more organizations, including those with fewer than 1,000 employees, are adopting CTI capabilities [27]. In the SANS Cyber Threat Intelligence Survey [27], more than half of the respondents (51%) indicated that their organization follows a hybrid model, using internal capabilities as well as external support for Cyber Threat Intelligence (CTI). This finding suggests that organizations recognize the benefits of leveraging a combination of internal and external CTI resources to enhance their cyber

security defenses.

2.1 Empirical Studies

Various empirical studies have been carried out in multiple domains to explore the perception and significance of Cyber Threat Intelligence (CTI) and Open Source Intelligence (OSINT). These studies encompass a range of fields and research areas.

Berndt and Ophoff [28] conducted a qualitative research study published in 2020 to explore the value of a Cyber Threat Intelligence (CTI) function within an organization. The study used a non-probability sampling method and collected empirical data through semi-structured interviews with South African employees who work in cyber security teams for at least six months. Using the Socio-Technical Framework as a lens, the findings revealed that implementing a CTI function can bring significant value to an organization. However, it requires skilled resources, a process to integrate the CTI function into existing cyber security teams, and sufficient budget for tools to maximize its benefits for the organization.

Another study by Kassim, Li, and Arief [29] provides detailed information on the utilization and perception of Open Source Intelligence (OSINT) and free tools among Computer Security Incident Response Teams (CSIRT) staff from multiple continents. The survey and interviews involved a total of 25 participants. The findings revealed three key results: first, all participants actively used public data, OSINT, and free tools for incident investigation; second, most (92%) perceived these resources as useful in their operational practices; and third, various operational challenges were identified, including the lack of standardized approaches and processes to utilize and validate these resources in different national CSIRTs.

A research study by Zibak and Simpson [30] developed an anonymous Web-based survey to assess the understanding and attitudes of stakeholders towards the sharing of Cyber Threat Intelligence (CTI). The survey consisted of 17 questions covering four main areas, participants' definitions and their attitudes concerning cyber security information sharing, as well as their organizations' information sharing maturity levels and efficacy. They proposed a categorizing framework on various types of terms used for CTI sharing. The study also shed light on how to evaluate the quality and effectiveness of CTI sharing.

Research on perception and the motivation behind the adoption of any technology such as OSINT can help policy makers and regulators provide evidence-based insight into the impact of that technology on individuals and society.

To understand the social dynamics of the OSINT community, including the motivations behind collaboration and competition, Belghith, Venkatagiri, and Luther [31] conducted semi-structured interviews with 14 OSINT investigators who were affiliated with nine different organizations. The main objective was to understand the patterns of collaboration and competition within this community of investigators and to gain insight into their investigative processes. The paper also examines the use of existing OSINT tools by investigators and highlights the challenges they face while using these tools. The article draws implications that are significant for enhancing the effectiveness and impact of OSINT investigations, that address a variety of issues, such as uncovering human rights violations and combating child trafficking and exploitation.

A study by Oxford University [30] examined the attitudes of stakeholders toward the sharing of CTI. Using a triangulated mixed-methods research design, the authors also aimed to investigate the advantages and disadvantages of sharing and how it impacted the productivity and performance of cyber security analysts. The methodology made use of a non-experimental survey design and semi-structured interviews. From the survey results, it was evident that the majority of respondents recognized the positive effect of sharing CTI. Another interesting statement on which most of the subjects agreed was that there is a skill shortage of required qualifications to handle CTI. This highlights the need for further research to understand the skills required, technical or otherwise, for CTI handling.

2.2 Pakistan and Cyber Threat Intelligence

Security programs across organizations in Pakistan *lack depth*, are *understaffed* and rely on *cosmetic solutions* to satisfy some on-paper requirement[32]. Rafique[33] emphasizes the importance of OSINT for National Security, suggesting the use of OSINT to complement traditional intelligence methodologies. The lack of standardized methodologies and ad hoc approaches used by Pakistani organizations to implement cyber security measures or develop software can pose significant challenges and risks. This problem highlights the lack of structured frameworks and processes, leading to inconsistencies

and the potential for vulnerabilities and inefficiencies. Pakistan is currently facing a rapid increase in cyber threats, which poses significant challenges to its cyber security landscape. The country's vulnerability to such threats is notably high, mainly due to its heavy reliance on external entities for security measures and support [34].

According to a white paper published by Delta Tech Global [32], the slow progress of standardization in Pakistan can be attributed to several barriers and issues. The article emphasizes that time and budget constraints, along with cultural factors, are the primary reasons for this slow progress. These constraints make it challenging for organizations and stakeholders to allocate sufficient resources and invest in the standardization process. Furthermore, the white paper highlights that Pakistan has witnessed significant advances in its IT infrastructure over the past ten years. However, during this period, the importance of cyber security has been neglected, resulting in a significant delay of approximately 10 years. This neglect has led to a gap between the growth of the IT infrastructure and the corresponding development of robust cyber security measures.

The development of a robust CTI and OSINT strategy in Pakistan is still in its early stages, with limited policies and laws in place. While organizations such as banks [35] and the military [36], [37] are researching and using CTI frameworks, there is a lack of comprehensive policies and regulations, especially in the corporate sector.

2.3 Open Source Tools and Resources

Although OSINT has gained significant popularity in the fields of journalism [38] and fact checking [39], its official use in the corporate sector may be limited or less explored in the existing literature. Pakistan can explore both proprietary and open source tools and platforms. There are proprietary frameworks, such as Cisco Talos and IBM X-Force, that offer comprehensive threat intelligence solutions with advanced analytics and research capabilities. These tools can provide real-time threat data, vulnerability information, and actionable intelligence for timely decision making. Furthermore, open-source OSINT tools can also be beneficial for Pakistan's CTI efforts. Platforms such as AlienVault OTX enable access to a global community of threat researchers and security professionals, facilitating the exchange of threat intelligence. MITRE ATT&CK[17] provides a comprehensive enterprise matrix that IT professionals can use to map their security threats with their own security controls. Another resource, Threat Crowd[40]

provides search and investigation capabilities for malicious IPs, websites, and organizations. Websites such as virusshare.com[41] and openphish.com offer detailed analysis and real-time threat intelligence on malicious domains, phishing pages, and other cyber threats[42].

2.4 Maturity Models and Frameworks

An empirical study conducted at MIT [43] focused on the incentives that drive organizations to participate in CTI sharing through a framework. Survey responses consisted of 25 individuals who had knowledge of their firm's membership in the CTI sharing organizations. The survey was divided into three parts. The first part of the survey focused on the membership of CTI sharing organizations and its reasoning. The second part was concerned with the type of information that is shared and received. The last part gauged the firm's behavior and what incentives and barriers effected their decisions to share CTI. The study showed that large firms are more often members of CTI-sharing organizations. Furthermore, some of the main incentives to remain involved in CTI sharing are access to high-level expertise and knowledge on cyber threats, as well as situational awareness of the current state of cyber security. One of the barriers identified in the study was privacy concerns about their personal data.

Ryan Stillions' DML model [44] has been modified to integrate OSINT into cyberattack investigations in this IEEE publication [1]. The maturity model can help gauge the level an organization has achieved when detecting cyber attacks, as shown in Figure 2.1.

First is the collection phase in which DML-1 focuses on atomic indicators of compromise, while DML-2 involves the collection of host and network artifacts that contribute as the starting point for any investigation. Then the information obtained from the DML-3 to DML-6 analysis levels significantly helps in identifying patterns, correlations with previously stored cases, and analyzing execution details; thus, a more intelligent and comprehensive analysis can be conducted. The highest levels of DML-7 to DML-9 include understanding the strategy used, identifying specific goals, and ultimately attributing the actions to a responsible entity.

The research carried out by Sillaber et al. [2] used the case study approach, using an exploratory survey and two focus group discussions that involved 17 stakeholders who

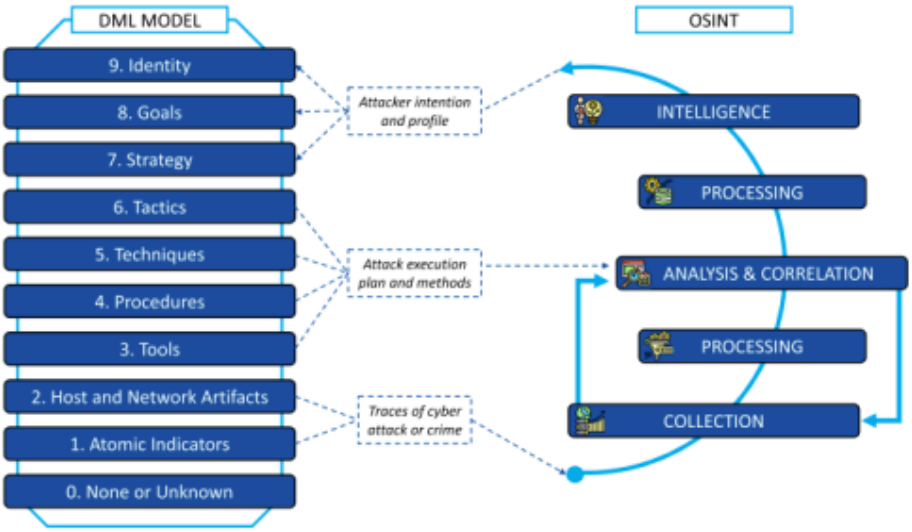

Figure 2.1: Integration of OSINT in DML [1]

participated in the implementation of a Cyber Threat Intelligence (CTI) sharing platform. The primary objective of the research was to determine the main expectations of the stakeholders and the types of information they are willing to share on a possible CTI sharing platform. Based on the findings derived from the investigation, the researchers propose the development of a maturity model specifically tailored for CTI sharing platforms. The maturity model used in the study consisted of six levels to assess the usage

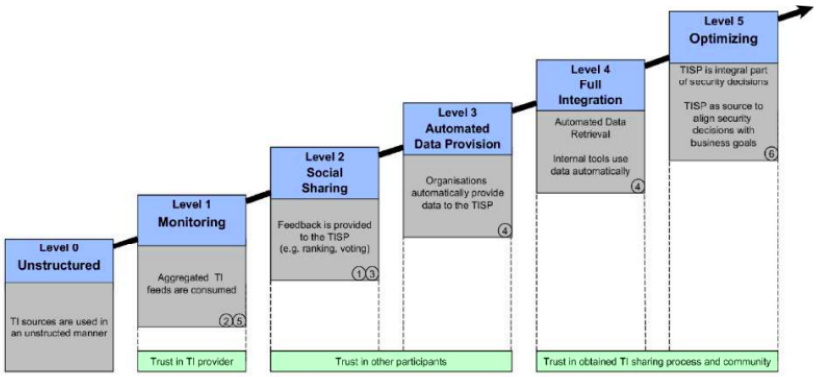

Figure 1: Maturity model for inter-organizational CTI (TI) sharing. (Remark: The numbers in the circles are referencing the respective expectations.)

Figure 2.2: Maturity Model for inter-organizational CTI (TI) sharing [2]

of Cyber Threat Intelligence (CTI) sources. Level 0 represented an ad hoc approach to CTI utilization, indicating a basic and informal usage of CTI without a structured process. As maturity levels progress, the participation of stakeholders and the complex-

ity of CTI usage increase. The maturity model used in this study signifies that as the system becomes more automated and formalized, the maturity level increases. Level 5 represents the highest level of maturity, characterized by optimization and real-time CTI sharing.

The empirical study conducted by Zibak and Simpson [45] used surveys and thematic analysis to examine CTI programs and their sharing capabilities and proposed a maturity model. The maturity model focused on evaluating the level of maturity based on three key factors:

1. The degree to which the sharing of CTI was formalized within the organization.
2. The integration of CTI sharing processes with other security practices within the organization.
3. The allocation of resources and the skill set of the staff involved in the threat intelligence sharing process.

In summary, most of the empirical studies in the literature review focused on perceptions surrounding CTI sharing. Given that sharing is the next step after CTI adoption, the focus of our research is more on understanding the current picture of Open Source Intelligence (OSINT) in Pakistan. With a clear understanding that Pakistan lags behind in terms of technology, as is evident from the existing literature, our empirical study focused primarily on gauging the receptiveness and familiarity of the general population, particularly IT leads, with Cyber Threat Intelligence (CTI) and Open Source Intelligence (OSINT). Through the use of surveys and interviews, we sought to gain insight into their level of awareness and understanding regarding these concepts. By conducting this research, our aim was to provide valuable recommendations to help bridge the knowledge gap and facilitate the adoption of CTI. The aim is to at least increase the level of awareness, which can help prime organizations for implementation of CTI and OSINT functions.

Chapter 3

Research Methodology

3.1 Research Design

The study used a mixed method approach to obtain empirical data on Open Source Intelligence (OSINT) in the context of cyber security. The primary objective of the exploratory research is to improve the comprehension of a population, as well as investigate the theoretical and methodological aspects associated with a study [46]. This design allowed for in-depth exploration, hypothesis generation, and a comprehensive understanding of the research topic.

3.2 Data Collection

The data collection for this study involved a mixed-method approach. The preliminary survey was distributed through emails, in-person visits, and telephone calls. For interviews, security professionals or IT team leads from the respective companies were selected as candidates. Similarly, for the targeted survey, the top cyber security companies were shortlisted, and contact was made through online channels such as phone and email. In some cases, in-person visits were also made to gather the necessary data.

3.2.1 Preliminary Survey

A survey consisting of quantitative and qualitative questions was used to collect data on security practices and OSINT awareness among participants. The survey consisted of structured questions designed to assess various aspects, such as the participants'

familiarity with OSINT, their usage patterns, and their perceptions of its effectiveness.

Sampling

The sample size of the study participants was determined based on exploratory research recommendations that generally involve a range of 20 to 150[46]. This sample size was chosen to ensure an adequate representation of the population under investigation and to facilitate a comprehensive exploration of the research objectives. Snowball or referral sampling was the primary distribution method. This approach facilitated data collection from a wider range of industries beyond the immediate circle. In total, 151 completed questionnaires were collected for analysis. The selection criteria was employment in a Pakistani organization.

Design

The design of the questionnaire was influenced by the survey design presented by Kassim, Li, and Arief [29] as well as questions asked in the SANS survey[27]. The questionnaire was divided into four sections to gather complete information from the respondents.

1. **Respondent Information:** The first section aimed to collect general information about the respondents, including their demographic details, job title, organization size, and duration of the experience. This section provided context for understanding the background of the participants and allowed for further analysis based on their characteristics.

2. **OSINT Knowledge:** This section aimed to explore their familiarity with the terminology of OSINT, their use of open source data and tools for official work, and their participation in social networks. The objective was to gain information about the level of awareness and utilization of OSINT in their professional activities.

3. **Experience with Security Issues:** The third section of the survey was designed to investigate the security practices and culture within the organizations where the respondents worked. This section aimed to explore their organization's experience in dealing with cyber security issues, the presence of protocols or guidelines for such incidents, and the perception of the top cyber security challenges faced by their organization.

4. **Open Source Data and Tools Usage:** The fourth section of the survey was subdivided into two subsections, focusing on open source data and open source tools, respectively. Both subsections followed a similar format and aimed to assess the respondents' perceptions and usage patterns. This section also aimed to determine the percentage of tasks that were completed using open source.

3.2.2 Interview Design

In addition to the survey, qualitative interviews were conducted with a subset of participants who had worked on cyber security issues in their respective organizations, cyber security professionals, or IT team leaders. The interviews aimed to delve deeper into the responses of the survey participants and explore their cyber security experiences. The interview questions were designed to obtain detailed information about knowledge, challenges, and best practices regarding cyber security and OSINT usage. The interviews were conducted in person or online via whatsapp or zoom calls.

Sampling

Out of the 11 participants who volunteered for interviews, 4 of them held official positions specifically related to cyber security. These individuals were responsible for overseeing and managing cyber security measures within their respective organizations. The remaining participants consisted of IT department heads or IT team leaders who held key roles in managing and implementing IT strategies and operations.

Design

The interview phase of the study used a mixed approach through closed and open-ended questions to obtain detailed responses from the participants. The interview design was developed with the objective of generating detailed narratives that would add to the questions answered in the survey. Through open-ended questions, participants were given the freedom to express their thoughts, share examples, and provide recommendations. The interview was divided into three sections to ensure cohesiveness and facilitate comprehension:

1. **Assessing Connection to Cyber Security:** In this section, the interview aimed

to gather insights into the participants' background, experience, and their organization's experience in the realm of cyber security.

2. **State of CTI:** The focus of this section was to explore the current state of Cyber Threat Intelligence (CTI) within the organizations of the participants. Questions were asked to assess the methodologies employed by the organizations in relation to CTI.

3. **Adoption and Perspective on OSINT:** The objective of this section was to examine the adoption and perspective of the participants on Open Source Intelligence (OSINT). Participants were asked about their use of OSINT and its impact within their organizations. In addition, they were encouraged to provide examples of specific use cases where OSINT had proven beneficial.

3.2.3 Targeted Survey

In order to address the existing knowledge gap and provide a more complete understanding of the state of Open Source Intelligence (OSINT) in Pakistan, a supplementary survey was conducted. This subsequent survey specifically targeted security companies operating within Pakistan, with the objective of capturing their experience on Cyber Threat Intelligence (CTI) and prevalent security trends. Additionally, the survey aimed to gather information on the utilization of OSINT within the CTI services offered by these companies.

Sampling

Out of the initial pool of 20 companies contacted, a total of 11 companies voluntarily participated in the survey by completing the survey form provided. The sample size of the survey included companies that were actively engaged in providing cyber security services to organizations and companies within Pakistan. Companies included in the survey were contacted through the contact details available on their respective websites. Initially, communication was initiated electronically and survey forms were shared with the companies for their participation. However, in cases where there was a lack of response or limited engagement, additional efforts were made to encourage participation. This involved physically visiting the offices of companies that did not respond to the

survey to further discuss the survey and encourage their participation.

Design

The supplementary survey was structured into three main sections, in addition to the section collecting basic information from the respondents. Each section aimed to explore specific aspects related to CTI services, the use of OSINT, and observations on security trends in Pakistani organizations based on the experience of the participating cyber security service providers.

1. **CTI Services:** This section included questions regarding the existence and provision of CTI services by participating companies. It sought to gain insight into the types of CTI services offered, their methodologies, and the extent of their implementation within organizations.

2. **Use of OSINT:** The second section focused on the utilization of OSINT by companies. It explored the channels and methodologies employed to collect OSINT data, along with the level of integration of OSINT into their overall CTI processes. The aim was to understand the significance and effectiveness of OSINT as a source of information for cyber-security activities.

3. **Cyber Security Trends in Pakistan:** The final section aimed to gather perspectives on the security trends observed by participating companies while providing cyber security services to Pakistani organizations. It sought to capture their insights on the security habits and awareness of organizations regarding cyber security.

3.3 Data Analysis

Section 4 of the document provides an in-depth analysis of the collected data and presents the findings obtained from the mixed-method approach employed in the study. The analysis involved both quantitative and qualitative techniques to gain a comprehensive understanding of the perspectives of the companies surveyed on CTI services, the use of OSINT, and the cyber security trends in Pakistan.

3.3.1 Quantitative Analysis

In the quantitative analysis phase of the study, Google Sheets and Google Forms were used as tools to clean and organize the data. Google Sheets facilitated the creation of cohesive data sets, and data visualization techniques such as charts and comparisons were employed to enhance data understanding. Formulas and pivot tables within Google Sheets were used to perform calculations and explore the relationships between variables. To further investigate the relationship between specific factors, two statistical tests were used: the two-proportion test and the chi-square test.

3.3.2 Qualitative Analysis

The qualitative interview data were transcribed and analyzed using thematic analysis. The transcripts were carefully read, reread, reviewed, coded, and categorized to identify key themes, patterns, and recurring concepts related to security practices and OSINT usage. The analysis involved a systematic process of organizing and interpreting the qualitative data to derive meaningful insights and generate hypotheses.

3.4 Ethical Considerations

Ethical guidelines, including informed consent and data confidentiality, were followed throughout the study. Participants received clear information about the purpose of the study, their rights, and the voluntary nature of their participation. The anonymity and confidentiality of the responses of the participants was ensured during data collection, analysis, and reporting.

3.5 Limitations

The study recognizes several limitations that should be taken into account. First, the reliance on self-reported data from employees introduces the possibility of response biases and subjective perceptions. This may impact the accuracy and comprehensiveness of the information gathered.

Secondly, the small study sample of employees from various companies in Pakistan may limit the generalizability of the findings. The results may not fully represent the diversity

of organizational contexts, industry sectors, and geographical regions within the country.

Lastly, the study's seven-month data collection period may impose temporal limitations. The rapidly evolving nature of cyber threats and security practices means that changes that occur after the study period might not be captured.

To mitigate potential biases, ethical considerations were carefully addressed and robust research methods were used, including mixed-method data collection that involved surveys and interviews. Limitations were acknowledged to ensure transparency and provide a comprehensive understanding of potential constraints and implications.

Chapter 4

Analysis and Results

This section delves into the methodology used, covering data collection methods and the analysis of survey and interview data. To streamline the data collection and compilation process, Google Forms was used to design and administer the survey, while a connected Google Sheet was used to automatically compile the survey results into a spreadsheet, thus eliminating the need for manual entry. To ensure data consistency and ease of analysis, a data cleaning process was conducted. This involved aggregating the results and organizing the data into relevant categories. For open-ended questions, where respondents provided diverse answers, similar responses were grouped under common themes or categories.

4.1 Preliminary Survey

4.1.1 Respondent Information

In the first section, respondents were asked to provide general information about themselves.

1. **Email Address:** The respondent was asked to provide their email address for possible follow-up communication.

2. **Industrial Sector:** Respondents were asked to specify the industrial sector in which their organization operates. 65% of the respondents belonged to the technology sector, while the rest belong to academic, government, finance, service provision, and telecommunications.

Total Number of Questions	27
Employees from Small Organizations	33
Employees from Mid Organizations	29
Employees from Large Organizations	89
Respondent's Experience (<1 year)	30
Respondent's Experience (1 - 5 year/s)	94
Respondent's Experience (6 - 10 years)	13
Respondent's Experience (10+ years)	8
Respondents with Technical Jobs	104
Respondents with Non-Technical Jobs	47
Total Number of Responses Collected	151

Table 4.1: Key Aggregate Statistics - Preliminary Survey

3. **Geographical Location of Company:** All the respondents were employed in Pakistani organizations, some of whom had multi-national operations in other areas such as the United States, the UK, Europe, and the Gulf.

4. **Job Title:** Based on an analysis of the job titles and industry sectors of the respondents, it was observed that 69% of the participants held technical positions, such as scientists, engineers, analysts, and similar roles. The remaining 31% consisted of individuals with job titles such as lecturers, managers, human resource personnel, and other non-technical positions. This distribution indicated that the majority of participants came from technical backgrounds, suggesting a significant representation of individuals with expertise and experience in the field of interest (Figure 4.1). The technical jobs were evaluated on the basis of whether the position required hands-on experience with technology.

Figure 4.1: Job Type (Technical/Non-Technical)

5. **Work Experience:** The aggregated results of years of experience in the current

job of the employee are shown in Figure 4.2

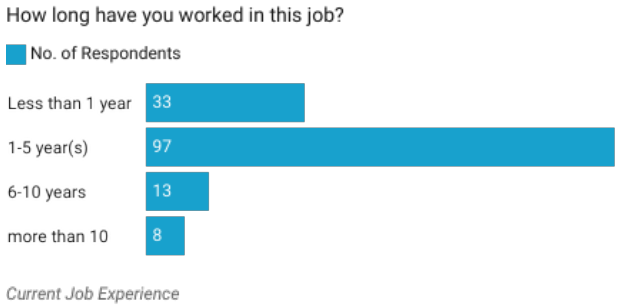

Figure 4.2: Work Experience

6. **Organization Size:** Most of the employees belonged to organizations with more than 250+ employees. Figure 4.3 shows the rest of the distributions.

Figure 4.3: Organizations Size

4.1.2 Open Source Intelligence (OSINT) Knowledge

The second section focused on assessing the respondents' knowledge and usage of Open Source Intelligence (OSINT) and related tools.

1. **Awareness of Open Source Intelligence (OSINT):** 54% of the respondents answered "no" when asked if they know what Open Source Intelligence (OSINT) is. This indicates that most of the participants do not have knowledge or experience with OSINT. On the other hand, 30% of the respondents answered "yes," indicating that they understand OSINT. The remaining 15% responded with "maybe," suggesting some level of uncertainty or lack of clarity regarding their knowledge of OSINT.

   One-sample hypothesis t-test was performed to examine whether there is a significant difference between the proportion of individuals who possess knowledge and

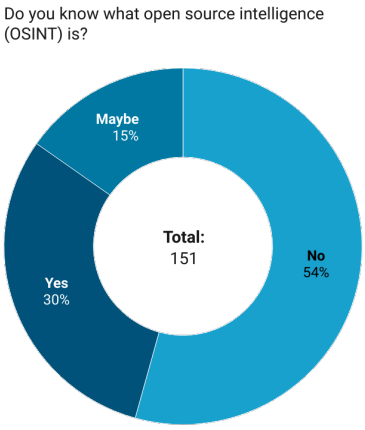

Figure 4.4: Awareness of Terminology of Open Source Intelligence (OSINT)

those who do not possess knowledge on OSINT.

Null Hypothesis (H0): There is no difference in the proportion of people who know about OSINT and those who do not.

Alternate Hypothesis (H1): There is a significant difference in the proportion of people who know about OSINT and those who do not.

To ensure consistency in the data analysis process, the responses that indicated "no" and "maybe" were merged together. This decision was made based on the understanding that "maybe" leans closer to a negative response rather than an affirmative one, facilitating a better interpretation of the data. The sample size (n) used in the analysis was 151, and the proportion of people who did not know OSINT ($\hat{p}$) was found to be 0.7. The significance level for the test was set at 0.05.

Based on the analysis carried out with a statistical tool, *Stats.Blue* [24], the p-value obtained was 0, which is less than the significance level of 0.05. As a result, the null hypothesis is rejected, indicating that there is a significant difference in the proportion of individuals who possess knowledge and those who do not. The t-test is a commonly used statistical test in research and analysis, used to determine if there is a significant difference between the means of two groups or to compare a sample mean to a known or hypothesized value. It is particularly useful when the sample size is small or the population standard deviation is unknown, allowing us to make inferences about the population based on the sample data.

The interpretation indicates that most of the people surveyed do not know what

OSINT is, which is consistent with the initial expectation.

2. **Use of Open Resources for Official Work:** Despite the majority of respondents (54%) indicated that they were not familiar with OSINT, a significant portion of them (75%) reported using open source data and tools from the Internet, for their official work, as shown in Figure 4.5.

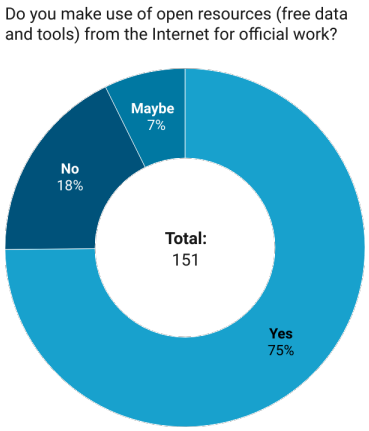

Figure 4.5: Use of Open Resources (Free Data and Tools)

This suggests that, although they may not be explicitly aware of the term "OSINT," they are still using open source data and tools to support their work. Furthermore, 18% of the respondents stated that they do not use open source data and tools, while 7% responded with "maybe". This indicates that there is a portion of the surveyed population who choose not to use open source data and tools or are uncertain about their usage for official tasks.

In general, the findings suggest that the utilization of open source data and tools for official work is prevalent among respondents, regardless of their knowledge or familiarity with the specific term "OSINT."

3. **Social Media Sites:** Among the options provided, YouTube, LinkedIn, and Facebook were the most used by respondents to obtain information for official tasks, including security-related purposes, as shown in Figure 4.6. Specifically, 74% of the respondents marked at least one website from the options provided, indicating their use of social media platforms to gather information. On the other hand, 26% of the respondents did not select any of the websites given, suggesting

that they do not use social networks for official tasks or prefer other sources for obtaining information (Figure 4.7).

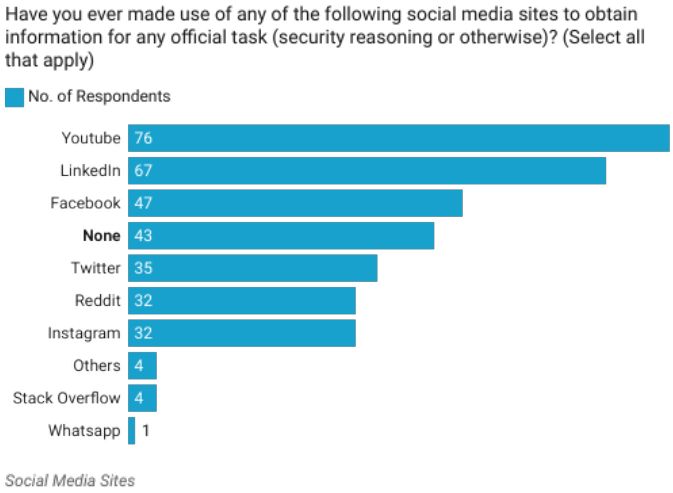

Figure 4.6: Social Media Sites Selected

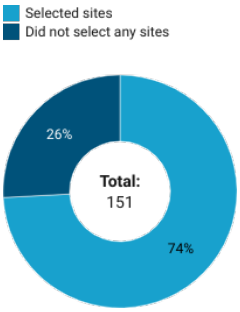

Figure 4.7: Percentage Visual of Social Media Usage

This finding is further proof of the fact that most of the respondents (54%) are unaware of the terminology of Open Source Intelligence (OSINT), but use open source data and tools for official tasks. Despite their lack of awareness of OSINT, a significant proportion (74%) still reported using social media sites to obtain information for official tasks, highlighting the relevance and popularity of these platforms in their work.

Approximately 74% of the respondents indicated their use of at least one social media platform for work-related tasks. (Figure 4.7)

4. **Open Source Tools and Data:**

The vast majority of respondents (83%) indicated that they have used open source tools or data in an official capacity for work. This suggests a significant adoption and utilization of open source resources in their professional endeavors. Only a minority (17%) did not mark any open source tool or data resource, indicating a smaller proportion who may not have explored or used these resources for their work (Figure 4.9).

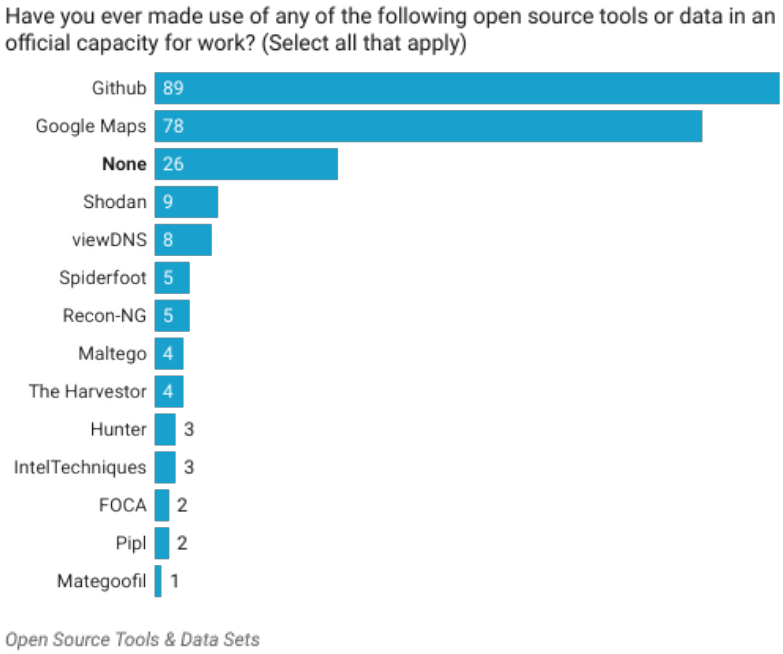

Figure 4.8: Open Source Tools Selected

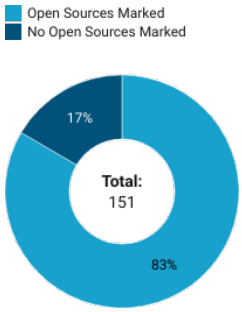

Figure 4.9: Percentage Visual of Open Source Tools and Data

5. **Purpose of Using Open Source Tools and Data:** Thematic analysis was used using Excel to examine the responses provided by participants regarding their use of tools and data. Notably, the analysis revealed that the tag "Cod-

ing/Programming" was the most commonly mentioned, with 59 participants referencing it. Furthermore, discussions related to research and analysis were mentioned 28 times, while only 10 responses were directly related to security considerations. These interpretations shed light on the participants' preferences and priorities, highlighting the prominence of technical skills and research-oriented approaches in their practices.

4.1.3 Experience with Cyber Security Issues

1. **Organizational Experience in Dealing with Cyber Security Issues:** According to the survey responses (Figure 4.10), 50% of the employees indicated that their respective organizations have experienced and dealt with security issues.

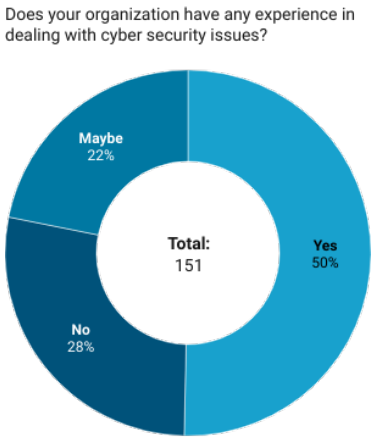

Figure 4.10: Organizational Experience in Dealing with Cyber Security Issues

This finding highlights the prevalence of security incidents within the organizations surveyed, suggesting that a significant portion of the workforce has first-hand experience dealing with these challenges. The response rate indicates a considerable level of exposure to security issues, emphasizing the importance of effective security measures and practices in the organizational context.

2. **Protocols/Guidelines for Cyber Security Issues:** As in Figure 4.11, 62% believed that their organizations had protocols or guidelines in place to handle cyber security issues.

   This suggests that most of the participants perceive that their organizations have specific measures in place to handle such security concerns.

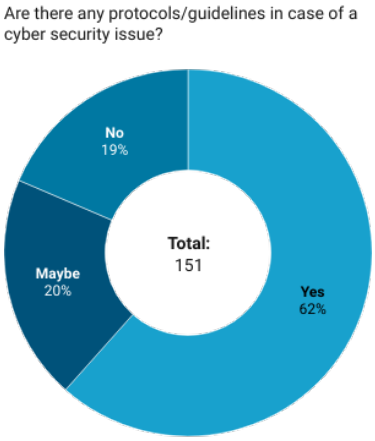

Figure 4.11: Protocols/Guidelines for Cyber Security Issues

3. **Cyber Security Issues Faced by the Organization:** Based on the responses to the survey, the two main cyber security issues encountered by organizations are data leaks/breaches, mentioned by 70% of the participants, and phishing attacks, mentioned by 43% of the participants. These findings highlight the significant challenges organizations face in protecting their sensitive data and protecting themselves against unauthorized access or disclosure. Furthermore, the mention of phishing attacks indicates the increasing sophistication of cyber threats targeting organizations through deceptive online tactics.

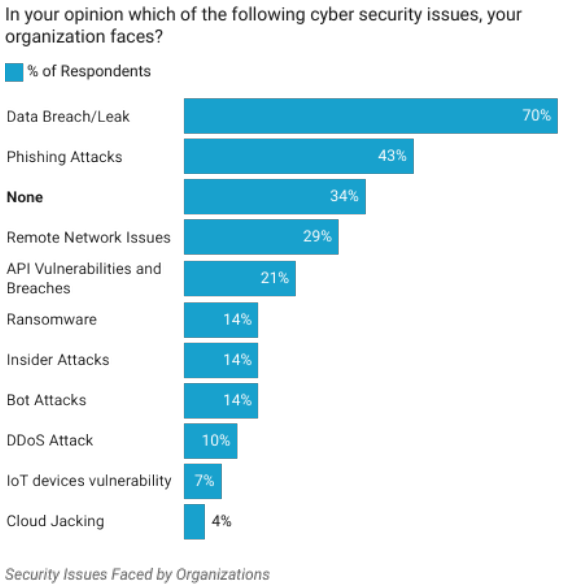

Figure 4.12: Cyber Security Issues Faced by the Organization

It should be noted that a significant proportion (34%) of the participants expressed the belief that their organization does not face any cyber security issues. This perception can be influenced by various factors, including lack of awareness or a possible underestimation of existing threats.

4. **Presence of Dedicated Personnel:** The findings reveal that 60% of the respondents reported that their organizations have dedicated personnel or teams responsible for handling security issues. This indicates that most organizations have recognized the importance of having specialized resources to address security concerns. Interestingly, when comparing this with the response of the employ-

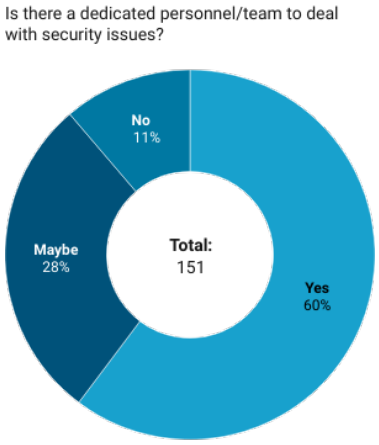

Figure 4.13: Presence of Dedicated Personnel

ees, 50% of them stated that their respective organizations have experienced and dealt with security incidents, as shown in Figure 4.10. This suggests that, while some organizations have dedicated personnel or teams, there are still a significant number of organizations that have experienced security incidents without having a specific focus on security resources (Figure 4.13).

5. **Involvement in Cyber Security Issues or Incidents:** Among the respondents, 13 confirmed that they directly deal with cyber security issues or incidents and 11 respondents stated that they are part of a dedicated security team that handles such matters.

   On the other hand, 121 participants reported that they do not deal with cyber security issues, as there is a separate team or personnel responsible for it (Figure 4.14).

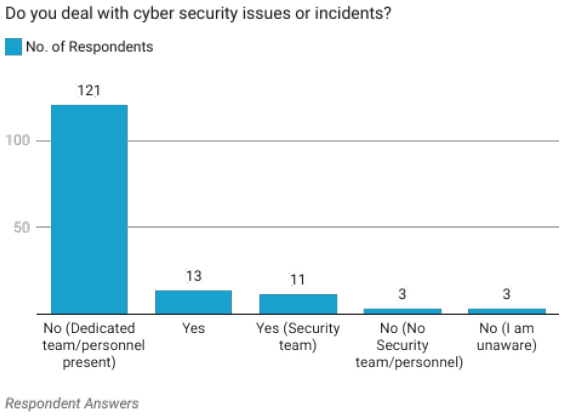

Figure 4.14: Involvement in Cyber Security Issues/Incidents

4.1.4 Open Source Data and Tools Usage

1. **Sources of Data Used for Processing and Analysis:** When asked about the sources of data they used, 53% of the respondents indicated that they rely on closed source data provided by their organization for processing and analysis. This shows the dependence on proprietary sources. 33% of the participants use public data, suggesting that they leverage publicly available information for their tasks. Furthermore, 14% of the respondents use open source data that have been vetted. Figure 4.15

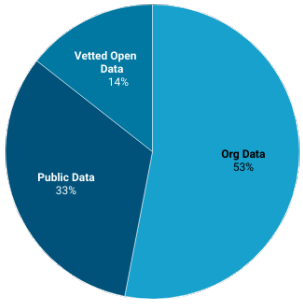

Figure 4.15: Sources of Data Used for Processing and Analysis

2. **Reliance on Close Sourced Data** The survey results indicate that 60% of the respondents find the close sourced data they have access to sufficient for their daily tasks (Figure 4.16). This suggests that most participants believe that the internal data sources provided by their organization adequately meet their needs.

   On the other hand, 22% of the respondents indicated that data sourced from

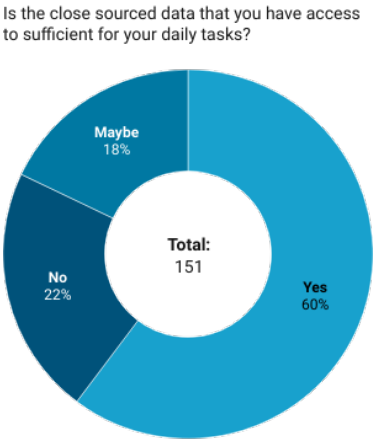

Figure 4.16: Sufficiency of Close Sourced Data

close sources are not sufficient for their daily tasks. This could imply that these individuals may require additional or alternative data sources to effectively perform their tasks. Furthermore, 18% of the participants responded with "maybe" when asked about the sufficiency of the data from the close source. This suggests that there may be some uncertainty or variability among the respondents about the adequacy of the internal data sources.

3. **Sources of Public Data:** The survey results indicate that the respondents collect public data from various sources. Most of the respondents reported using search engines as a primary means of collecting public data. Additionally, 66 respondents marked social media platforms and 80 respondents indicated using public data sets and feeds as a source of public data (Figure 4.17).

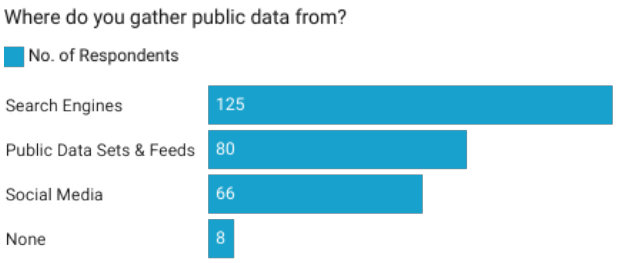

Figure 4.17: Sources of Public Data

This suggests that structured datasets and curated feeds play a role in gathering relevant information for analysis and decision making. In addition, the importance

of search engines as a popular tool for accessing publicly available information is also highlighted.

4. **Percentage of Tasks Utilizing Open-Sourced Data:** The survey results indicate that most of the respondents do not rely on open source data for their tasks (62%), (Figure 4.18).

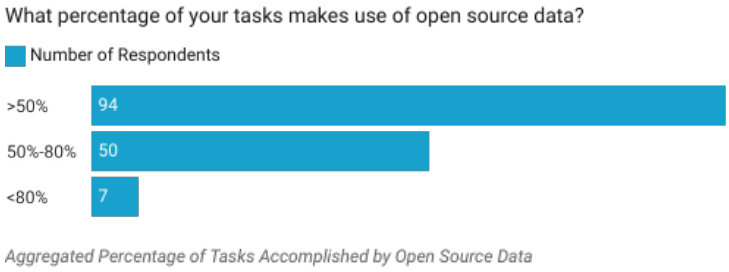

Figure 4.18: Percentage of Tasks Utilizing Open-Sourced Data

This suggests that there is a significant reliance on proprietary sources for information in their work, while only a small fraction of the respondents rely on open source data. This reinforces the notion that a combination of open source and proprietary data sources may be necessary to meet the specific demands of different contexts, industries, and tasks.

5. **Perceived Usefulness of Open-Sourced Data for Tasks:** Based on survey responses, it can be inferred that a significant portion of respondents find open source data to be useful for their tasks (approximately 84%). 46 respondents marked a score of 3, indicating moderate usefulness, while 35 respondents marked a score of 4, indicating high usefulness. Additionally, 45 respondents marked a score of 5, indicating the highest level of usefulness (Figure 4.19).

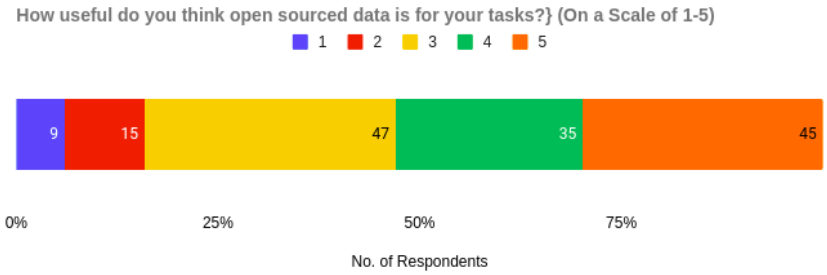

Figure 4.19: Perceived Usefulness of Open Sourced Data

Combining these answers, approximately 84% of the 151 respondents considered open source data useful (rated 3, 4, or 5) for their day-to-day tasks.

6. **Software Tools Used:** According to the responses, the distribution of software tools used is as follows (Figure 4.20):

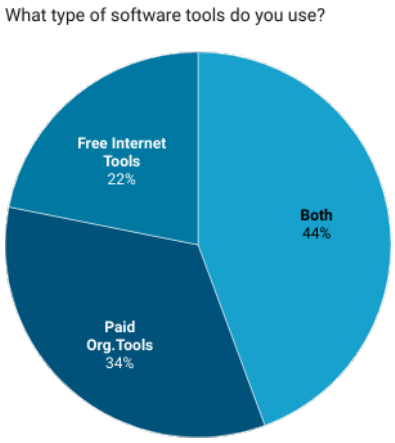

Figure 4.20: Types of Software Tools Utilized

- 34% of the respondents use commercial tools provided by their organization.
- 22% of the respondents use only free tools obtained from the Internet.
- 44% of the respondents use both commercial tools provided by their organization and free tools from the Internet.

This indicates that a significant portion of the respondents rely on a combination of commercial and free tools for their tasks.

7. **Tasks Accomplished Using the Tools:** Thematic analysis was conducted in Google Sheets utilizing conditional formatting as a methodological approach. The use of conditional formatting allowed for the identification and categorization of themes within the data. By applying specific formatting rules based on predefined criteria, patterns and clusters of responses related to particular themes were visually highlighted in the spreadsheet. This facilitated the process of organizing and interpreting the data, enabling the identification of recurring themes and patterns across the dataset. Then, deductive reasoning was employed in the thematic analysis to create codes for the data. The analysis revealed several key findings. First, most of the tools were reported to be used for **programming**

and coding-related tasks, indicating their significance in software development and coding projects. Second, **research and data analysis** emerged as the second most common reason for tool use, highlighting the importance of these tools in conducting research and performing data analysis tasks. Furthermore, **general management tasks** were identified as the third most mentioned reason for tool usage, suggesting that tools have utility beyond technical functions. Lastly, some respondents mentioned the use of tools for **security purposes**, indicating their potential relevance in supporting cyber security efforts.

8. **Percentage of Tasks Accomplished by Free Tools:**

   A significant proportion of the respondents, approximately 56.3% (85 respondents), indicated that less than 50% of their tasks are accomplished with free tools, with only a smaller percentage of the respondents, approximately 9.3% (14 respondents), indicated significant use of free tools (Figure 4.21).

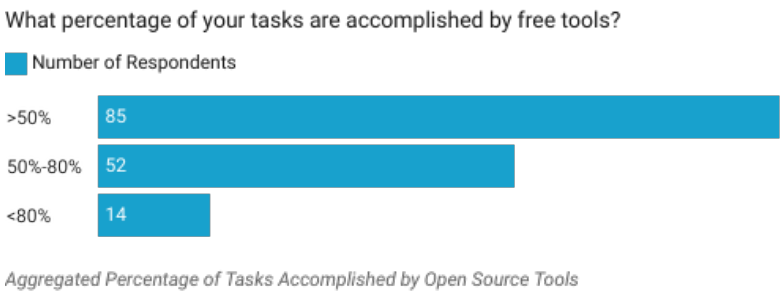

Figure 4.21: Percentage of Tasks Accomplished by Open Source Tools

   This suggests that the majority of respondents rely on a combination of free and commercial tools to perform their tasks.

9. **Perceived Usefulness of Open-Sourced Tools for Tasks and Investigations:** Based on the responses, the percentage distribution of the perceived usefulness of open-source tools for day-to-day tasks and cyber security investigations is as follows.

   Combining these answers, approximately 87% of the 151 respondents considered open source tools useful (rated 3, 4, or 5) for their day-to-day tasks and cyber security investigations.

   This indicates a positive perception among the majority of respondents about the

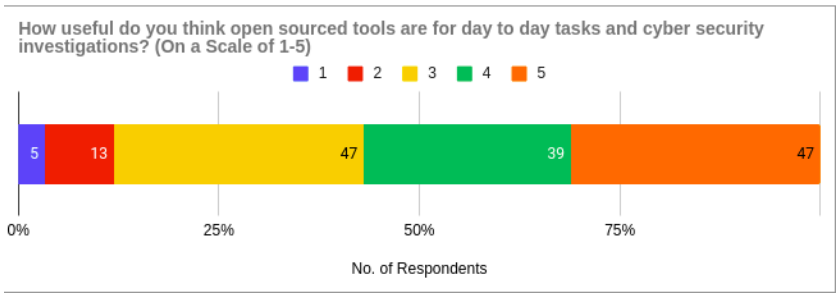

Figure 4.22: Perceived Usefulness of Open Sourced Tools

usefulness of open-source tools in their work.

4.1.5 Key Findings

Discrepancy Between Self-Reported Knowledge and Usage of OSINT:

The findings reveal an interesting discrepancy between the self-reported knowledge of the respondents about OSINT and their actual use of open source resources. While most of the respondents (54%) indicated that they were not aware of OSINT, a significantly higher percentage (76%) reported making use of open source data and tools for their official work.

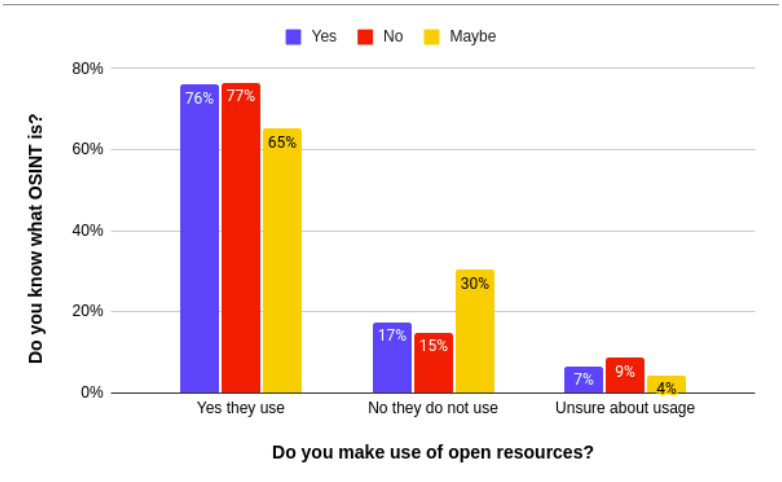

Figure 4.23: Discrepancy between Self-Reported Knowledge and Usage of OSINT

As indicated in the Figure 4.23, there is a disparity between respondents' awareness of the term "OSINT" and their practical utilization of open source data and tools. It suggests that individuals may be using OSINT without necessarily being familiar with

the specific term or concept.

Two-sample proportion test was carried out to assess the discrepancy between OSINT knowledge and the use of open source data and tools among the respondents. The significance level was established at 0.05. This test is appropriate for working with categorical data and allows for comparison of proportions between two groups. Other tests, such as the chi-square test or Fisher's exact test, are more suitable for analyzing the association between two categorical variables rather than comparing proportions directly.

Null hypothesis (H0): There is no significant difference between knowledge of OSINT and the use of open source data and tools.

Alternate hypothesis (H1): There is a significant difference between OSINT knowledge and the use of open source data and tools.

The test was carried out using sample proportions, where p1 represented the proportion of respondents with knowledge of OSINT and p2 represented the proportion of respondents who reported using open source data and tools. The calculated p-value was found to be zero.

$$p_1 = \frac{\text{Number of respondents with knowledge of OSINT}}{\text{Total number of respondents}} = \frac{46}{151} = 0.305$$

$$p_2 = \frac{\text{Number of respondents who use open source data and tools}}{\text{Total number of respondents}} = \frac{113}{151} = 0.748$$

$$\text{p-value} = 0.000$$

Based on the obtained p-value, which is less than the significance level of 0.05, there is sufficient evidence to reject the null hypothesis. Calculated by *Stats.Blue*[24], the results indicate that there is a significant difference between OSINT knowledge and the use of open source data and tools among respondents. The observed discrepancy suggests that OSINT is being used without a comprehensive understanding. This implies that open source is being utilized in an ad hoc manner without a formalized approach and lack of awareness of OSINT principles and techniques.

Organization Size and OSINT Knowledge

Statistical tests such as the t-test or ANOVA are more appropriate to analyze continuous variables or compare means between groups. Since we are interested in examining the relationship between two categorical variables, the chi-square test provides a suitable method to assess the association.

Organization Size	Yes	No	Maybe	Total
Small Org	13	16	4	33
Medium Org	7	18	4	29
Large Org	26	47	15	88
Total	46	81	23	150

Table 4.2: Organization Size and Answers to "Do you know what OSINT is?"

Data analysis using a *Chi-square test* yielded a significant relationship between organization size and OSINT knowledge, as evidenced by a Chi-Square statistic of 20.867 with 4 degrees of freedom (DF) and a p-value of 0.0003 that is significantly less than 0.05.

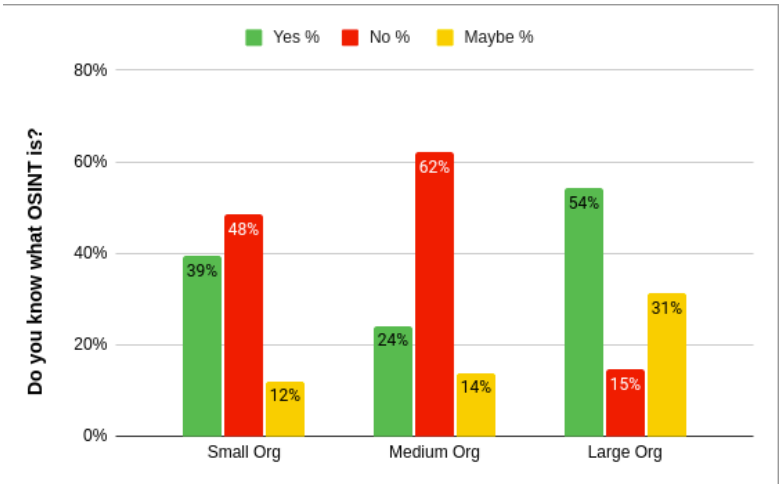

Figure 4.24: Effect of Organization Size on OSINT Knowledge

The results indicate that employees in larger organizations have a higher level of awareness of the terminology associated with OSINT. This observation is supported by the findings shown in the graph, Figure 4.24, where 54% of employees in large organizations reported having knowledge of OSINT, in contrast to 39% of the employees of smaller organizations who marked 'yes'.

In contrast, a larger proportion of employees from smaller organizations (48%) indicated a lack of knowledge of OSINT, while only 15% of employees from larger organizations provided the same response.

The statistically significant relationship between the size of the organization and OSINT knowledge suggests that larger organizations tend to foster a higher level of familiarity with OSINT terminologies among their employees. The discrepancy in awareness between smaller and larger organizations provides valuable information for further investigation and highlights the importance of addressing OSINT awareness and training in different organizational contexts.

Organization Size and Use of Open Resources

To examine the association between organization size and the utilization of open source data and tools, a *Chi-Square Test* was conducted. This statistical analysis aimed to assess the relationship between these two variables and determine if there was a significant association.

Organization Size	Yes	No	Maybe	Total
Small Org	29	3	1	33
Medium Org	20	5	4	29
Large Org	63	19	6	88
Total	112	27	11	150

Table 4.3: Organization Size and Use of Open Source

The results of the *Chi-Square test* revealed a non-significant relationship between organization size and open source usage, with a Chi-Square statistic of 1.7955 and 1 degree of freedom (DF), resulting in a p-value of 0.1803.

Despite the lack of statistical significance, an examination of the observed data indicates notable differences in proportions between small and large organizations. Specifically, 88% of the employees of small organizations reported using open source data and tools, compared to 71% of the employees of large organizations. On the contrary, 9% of the employees of small organizations reported that they did not use open source data and tools, while 26% of the employees of large organizations fell into this category.

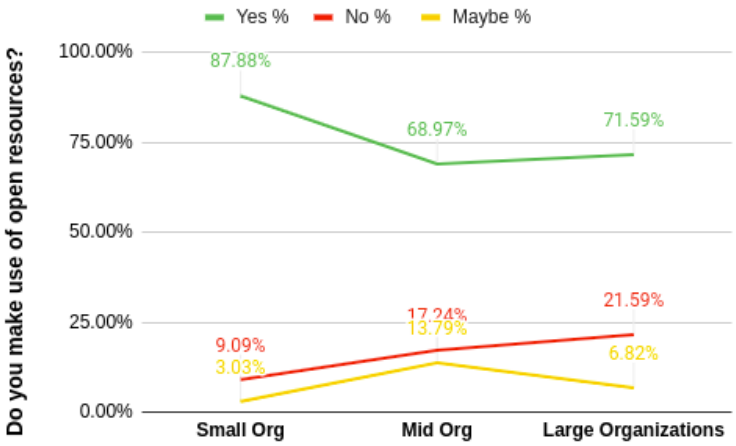

Figure 4.25: Effect of Organization Size on Open Source usage

Although the statistical test did not demonstrate a significant association, the differences observed in Figure 4.25 suggest the possible existence of a relationship between the size of the organization and the use of open source data and tools. Further exploration of this topic is recommended, particularly with a larger sample size that specifically focuses on different organizational sizes.

Organization Size and Experience with Cyber Security Issues

To analyze the relationship between organization size and the cyber security issues faced by them, a *Chi-Square Test* was conducted to determine if there is a significant association. The purpose of this analysis was to examine whether the size of an organization influences the types and severity of the issues encountered.

Organization Size	Yes	No	Maybe	Total
Small Org	10	16	7	33
Medium Org	10	10	9	29
Large Org	56	15	17	88
Total	76	41	33	150

Table 4.4: Organization Size and Experience with Cyber Security Issues"

A chi-square test was performed to assess the relationship between the size of the or-

ganization and the level of experience with cyber issues, producing a significant result with a Chi-Square Statistic of 17.8458 and a value of p of 0.0013. The findings indicate a strong association between organization size and the incidence of cyber incidents, suggesting that larger organizations are more likely to encounter such issues and possess a higher level of experience dealing with them. The analysis reveals that 64% of the em-

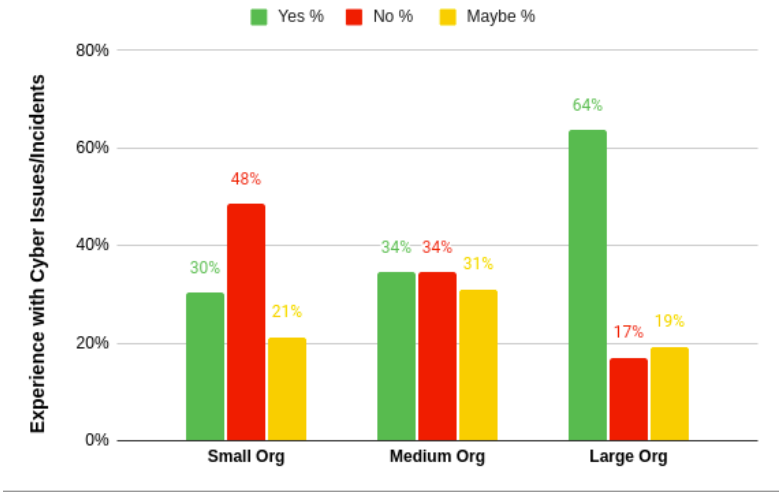

Figure 4.26: Organization Size and Experience with Cyber issues

ployees of the larger organizations reported first-hand experience with cyber incidents, compared to 30% of the employees of the smaller organizations, as shown in Figure 4.26. Conclusively, the significant relationship observed between organization size and experience with cyber issues implies that Open Source Intelligence (OSINT) solutions can be particularly valuable for larger organizations. As larger organizations tend to encounter a higher frequency of cyber incidents, using OSINT tools and techniques can help to improve their cyber security posture.

Proprietary Sources and Open Sources

Participants were asked to indicate their use of open source data and tools, and the response options included "yes," "no," and "maybe." Interestingly, upon analyzing the data, it became apparent that participants' perceptions regarding the sufficiency of closed source data were not aligned with their actual behavior. Although 60% of the participants, in Section 4.1.4, indicated that closed-source data was sufficient for their daily tasks, further examination revealed that a substantial majority of the participants

in all response categories used open source data and tools in their work (Figure 4.27). This discrepancy suggests that participants' subjective beliefs about the sufficiency of

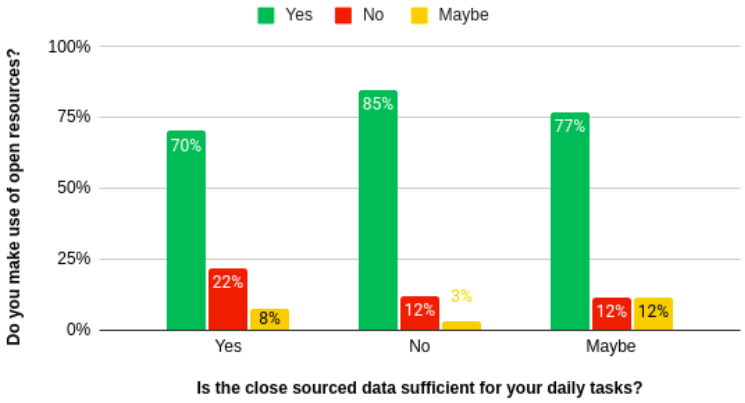

Figure 4.27: Discrepancy in Sufficiency of Closed Sources

closed source data may not accurately reflect their actual reliance on open source data and tools for carrying out their daily tasks. The shift towards utilizing open-source data could be attributed to factors such as the increasing availability and accessibility of such information, the potential cost-effectiveness compared to proprietary sources, or the recognition of the diverse and comprehensive nature of open source data.

Moreover, these findings highlight the importance of considering the actions and behavior of individuals in addition to their self-reported perceptions when studying the use of open source data and tools in professional settings.

4.2 Interviews

As part of the research methodology, semi-structured interviews were conducted to gather qualitative data and supplement the insights obtained from the survey. The interviews aimed to obtain in-depth information on participants' experiences, challenges, and perspectives related to security and Open Source Intelligence (OSINT).

The process of obtaining interviews with security professionals presented some challenges. Despite reaching out to more than 20 organizations, we were only able to secure interviews with 10 individuals who were involved in security-related roles. This lower response rate can be attributed to apprehension about data confidentiality and the sensitive nature of security. It is important to recognize that the field of security requires

Total Number of Questions	22
Employees from Small Organizations (<50)	4
Employees from Mid Organizations (50 - 500)	3
Employees from Large Organizations (>500)	3
Respondent's Experience (<5 years)	4
Respondent's Experience (5 - 10 year/s)	3
Respondent's Experience (10+ years)	3
Total Number of Responses Collected	10

Table 4.5: Key Aggregate Statistics - Interview

a high level of trust and discretion, which can be an understandable reason why people were unwilling to openly discuss their experiences. Despite these challenges, the interviews we conducted still provided valuable insight and perspectives from a diverse group of security professionals. Their willingness to share their knowledge and experience contributes to a deeper understanding of the topic and enhances the overall robustness of our research findings.

The respondents were classified into two groups according to their professional background and experience. The first group consisted of four individuals who were experienced security professionals with substantial knowledge and experience in the field. The second group consisted of six IT professionals who were relatively new to the security domain. During the interviews, participants were asked about their organization's security protocols and procedures, OSINT usage, and any specific examples of OSINT usage. In addition, participants were asked to provide a rating that indicated their perception of the usefulness of OSINT. By categorizing the respondents in this way, the objective was to capture insights and perspectives from both experienced security professionals and individuals who were transitioning or expanding their roles in the security domain.

4.2.1 Security Professionals

Respondent Information

Among the respondents, four organizations had a dedicated security team or personnel. The individuals we interviewed were part of these security teams. To maintain

anonymity, the respondents are referred to as A, B, C, and D. Respondents A and B had more than 20 years of experience in the field, holding the positions of Senior Manager of Cyber Security and External Auditor, respectively. Meanwhile, respondent C had 7 years of experience and held the position of Senior Penetration Tester. Respondent D had 2 years of experience and held the position of Head of Security.

Cyber Security Insights

All of the interviewed individuals mentioned that their respective organizations had experienced an increase in the size of their security teams through new hires in recent years. Furthermore, they also noted an increase in security incidents within their organizations. These insights suggest a growing recognition of the importance of robust security measures and the need for skilled professionals to address emerging threats.

Use of Cyber Threat Intelligence (CTI)

- Of the 4 security professionals, three subjects reported that their companies were **members of CTI sharing organizations** such as Microsoft Azure, Symantec, and CyberArk. These organizations were actively involved on a daily basis, indicating a close working relationship between the respondents' firms and these CTI sharing organizations.

- When asked about the **production of Cyber Threat Intelligence (CTI)**, only Respondent B indicated that their organization has a dedicated CTI team that actively participated in the creation, analysis and dissemination of threat reports. This suggests that most of the organizations surveyed were not involved in the production of CTI. The reasons for this disparity could be attributed to various factors, such as limited resources, lack of expertise, or reliance on external sources for CTI.

- The **sources of Cyber Threat Intelligence (CTI)** mentioned by the security professionals in the survey mainly included paid subscription services and government agencies. However, it is worth noting that these professionals expressed a preference for their own detection processes. This indicates that they relied on their organization's internal methods and expertise to gather and analyze threat

intelligence. Interestingly, two respondents (C and D) also mentioned making use of open source as a source of CTI.

- During the interviews, respondents A, C, and D indicated that their organizations had established **internal processes** to convert CTI into actionable intelligence. Once converted, this intelligence is then disseminated to the relevant teams within their organizations, who are responsible for taking necessary actions based on the received information. This highlights the importance of effective knowledge transfer and collaboration within the organization, ensuring that CTI is shared with the appropriate teams in a timely manner. Respondent B highlighted that their organization has an internal department dedicated to handling CTI. This department is responsible for generating reports and sharing them as needed. Their main collaboration is with Information Systems (IS) engineers, who are involved in addressing any identified vulnerabilities or threats. The organization's intelligence system is described as robust, as it automatically alerts the Network Operations Center (NOC) and Security Operations Center (SOC) teams. This indicates a well-coordinated and proactive approach to CTI, where the CTI department works closely with other teams to ensure a timely response and remediation of any identified security issues.

- During the interviews, the respondents mentioned various **features that are incorporated into their CTI systems** to improve their capabilities. These features include Security Information and Event Management (SIEM) systems, dynamic threat feeds, smart visualization tools, and analysis tools. These tools and technologies are instrumental in collecting, analyzing, and visualizing CTI data, allowing organizations to identify, and respond to potential threats effectively. It is worth noting that respondent A specifically mentioned the use of open source tools for CTI, indicating the utilization of freely available resources to augment their CTI capabilities. This demonstrates the flexibility and adaptability of organizations in leveraging different tools and technologies, including open source solutions, to meet their CTI requirements.

Open Source Intelligence (OSINT) Usage

Respondents A and C shared their experiences related to a ransomware situation where OSINT was used. Respondents B and D mentioned the use of Open Source Intelligence (OSINT) after vetting the data for penetration testing purposes. Respondent C specifically mentioned that their penetration testers use OSINT. These responses demonstrate the diverse applications of OSINT in the context of cyber security, ranging from **incident response to proactive testing and assessment**.

4.2.2 Lead IT Managers

Respondent Information

The interviews included six leads from the IT team of startups or small organizations, serving as a comparison group with security professionals. This helps to understand the security needs of smaller organizations and to assess their awareness and knowledge of Cyber Threat Intelligence (CTI) and Open Source Intelligence (OSINT). The average years of experience among IT team leaders were 5.7, with a maximum of 11 years and a minimum of 3 years. When asked about their experience with security issues, the majority rated it as 3 on a scale of 1 to 5, indicating limited experience. The scale ranged from 1 (no experience) to 5 (extensive experience). To ensure confidentiality, the IT team leads will be referred to as E, F, G, H, I, and J in the subsequent analysis.

Cyber Security Insights

None of the organizations represented by the six IT team leaders had dedicated teams or personnel specifically assigned to deal with cyber security issues. Only respondent E mentioned their intention to hire someone for this purpose in the future. Interestingly, the respondents F and J highlighted that their organizations had experienced security issues in the past year and still did not express a proactive approach toward adopting official security measures.

Use of Cyber Threat Intelligence (CTI)

As anticipated, the organizations represented by the six IT respondents did not use formalized Cyber Threat Intelligence (CTI) methodologies in their operations. Additionally, the respondents themselves displayed limited awareness and knowledge of the CTI terminology. This is in line with the context of smaller organizations where resources and expertise dedicated to cyber security may be limited.

Open Source Intelligence (OSINT) Usage

In contrast to their limited knowledge of cyber-threat intelligence (CTI), all respondents acknowledged the use of crowd-sourced and open source data and tools in their security practices. Respondent H specifically mentioned manual web searches for security concerns and potential solutions, which are then shared with the team lead for approval. This information was corroborated by the other IT respondents. For example, respondent F mentioned the use of web scrapers to gather information on emerging cyber security issues that the company had faced in the previous year. These findings highlight the need to rely on open source data and tools, such as web-based information, to address security concerns in the absence of formal CTI practices.

Most of the respondents mentioned that individual software developers within their organizations perform Google searches and utilize search engines to gather information related to security. Respondents G and J further added that the information collected is then shared with the IT team lead, who disseminates it to other teams within the organization. This practice highlights the *informal and decentralized nature* of collecting security-related information, where individual developers take the initiative to stay informed and contribute to overall security efforts.

During the interviews, respondents were asked to provide examples of instances in which they used OSINT. Respondent F shared an example where their organization encountered problems related to a PHP-based Trojan malware that affected similar companies. Through their search efforts, they discovered that this particular Trojan did not pose a threat to Python applications, which allowed them to mitigate the risk and ensure the security of their systems. This, in turn, encouraged software developers to be proactive and look for similar problems before they arise. Similarly, respondent J shared a case involving a social engineering issue. They were able to resolve the issue by obtaining

valuable information from the Reddit website, which helped them effectively address the security issue.

4.2.3 Key Findings

Consumption of CTI

A notable difference was observed in responses when participants were asked about their consumption of raw data versus finished reports. Security professionals indicated that their organizations used raw data and finished reports, suggesting a comprehensive approach to information use. On the other hand, IT leaders mentioned that their organizations primarily consumed finished reports, which implies a dependence on pre-analyzed and summarized information.

When asked to elaborate on the discrepancy between the consumption of raw data and the final reports, the participants identified multiple factors that contribute to this difference. However, the main reason IT leaders highlighted was the *lack of resources, manpower and the set of skills required to process and analyze raw data effectively.* Due to the limited capabilities and expertise within their teams, IT leaders relied on completed reports that provided a more concise and easily understandable presentation of information. This limitation in processing capacity hindered their ability to leverage raw data for deeper analysis and decision-making.

Perceived Usefulness of OSINT

All interviewees, including security professionals and IT professionals from smaller companies, were asked to rate the usefulness of OSINT sources for their respective organizations on a scale of 1 to 5. Responses from security professionals consistently indicated high scores, suggesting a strong belief in the value and utility of OSINT sources for their company's cyber security efforts. On the other hand, the responses from IT professionals in smaller organizations varied, with ratings ranging from 2 to 4.

This discrepancy in ratings may reflect a difference in awareness, exposure, or understanding of the potential benefits and applications of OSINT sources among IT professionals in smaller companies compared to their counterparts in the security field.

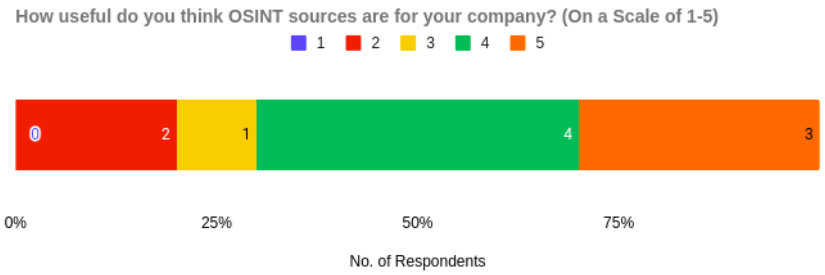

Figure 4.28: Usefulness of OSINT Sources

Hindrances to Formalization of OSINT

The responses obtained from the interviewees highlighted several barriers to the formal use of Open Source Intelligence (OSINT) for security. These barriers included the presence of vulnerabilities in open source software and tools, lack of awareness and understanding of security among individuals in Pakistan, concerns about the validity and reliability of OSINT sources, cost considerations, and the perception that security is a low-level priority for many companies. Respondent A emphasized the presence of vulnerabilities in open source software and tools and the lack of comprehensive documentation and support. Additionally, they also mentioned that open source solutions often provide limited coverage of various areas within a security problem.

Another significant insight provided by respondent A is the lack of awareness of security among individuals in Pakistan. This insight was also corroborated by the other interviewees. Respondent F highlighted that one of the effects of lack of awareness is that *"security becomes a low-level priority for most companies"*.

Respondent D shared their perspective on the challenges associated with validating Open Source Intelligence (OSINT) sources (OSINT). According to their experience, many companies find it difficult to validate the credibility and reliability of OSINT information. This process often requires additional resources, including time and financial investments, which can pose challenges for organizations with limited budgets or tight project timelines. They also highlighted that sorting through the overwhelming amount of OSINT data can be a daunting task for companies, further complicating the process of utilizing OSINT effectively.

Respondent E shed light on the significant impact that limited budgets and resources have on organizational decision making about security prioritization. They highlighted

that many organizations face financial constraints, which often lead to difficult choices about resource allocation.

4.3 Targeted Survey

The preliminary survey and interviews targeted a broad range of Pakistani organizations in various fields to gather information on their security practices. However, to gain further insight into some of the answered questions, a follow-up questionnaire was created and distributed to targeted cyber security companies. The questionnaire was designed to gather information on the prevailing trends in the cyber security landscape in Pakistan, through the eyes of the most experienced entities in this field, people whose bread and butter was information security. Respondents, representing various cyber security organizations, were asked to provide detailed information on their observations and experiences.

To gather responses for the survey, a total of 20 Pakistani cyber security companies, including prominent organizations such as Pak CERT, Trilium and Tier3, were approached through various means such as emails, phone calls and in-person office visits. The objective was to encourage these companies to participate in the survey and provide their valuable insights.

Of the 20 companies contacted, a total of 11 companies responded to the survey, demonstrating their willingness to contribute to the research. It should be noted that the response rate of 55% reflects the voluntary participation of companies in the survey. The survey included questions that explored various aspects, such as the expertise of cyber security companies, the specific CTI services they provided, and their insights into the evolving landscape of cyber security in the country. The objective was to capture the experiences and perspectives of these leading companies to gain valuable insights into the current state of cyber security and the trends shaping the industry in Pakistan.

4.3.1 Respondent Information

1. **Organization Name:** The organization name refers to the official name or title of the cyber security company or organization participating in the survey. It serves as a unique identifier for each participating entity but will remain anonymous for

Total Number of Questions	24
Employees from Small Organizations (1-49)	6
Employees from Mid Organizations (50-250+)	3
Employees from Large Organizations (250+)	3
Respondents with Executive Level Jobs	9
Total Number of Responses Collected	12

Table 4.6: Key Aggregate Statistics - Targeted Survey

the purpose of identity protection.

2. **Position or Job Title:** The position or job title indicates the specific role or position held by the respondent within the participating organization and helps to understand the rank from which we received responses. The 11 participants who responded to the survey on behalf of their respective companies held leadership positions in the field of security, including security leads, directors, and managers.

3. **Organization Size:** The size of the organization is measured in terms of the total number of employees working within the entity. (Figure 4.29)

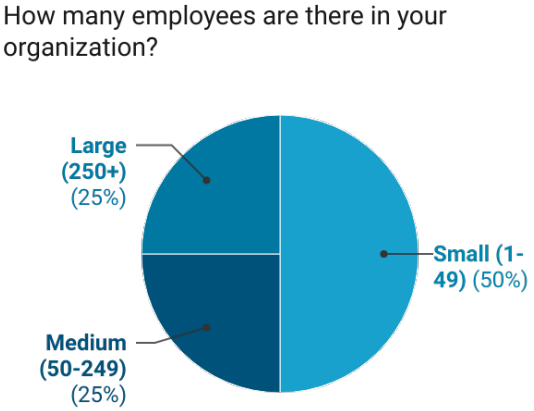

Figure 4.29: Size of organization (Interviews)

4. **Provision of CTI Service:** According to the data, 55% of security companies reported providing Cyber Threat Intelligence (CTI) services (Figure 4.30). This suggests that CTI is still a relatively new technology/service in the industry. The fact that nearly half of security companies offer CTI services indicates that it is gaining recognition and adoption. However, it also implies that there is still a

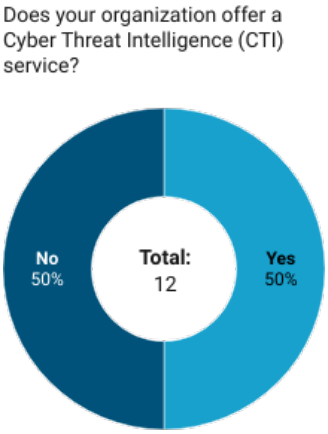

Figure 4.30: Provision of CTI Service

learning curve for security experts, and they need to fully familiarize themselves with this emerging field.

4.3.2 Cyber Threat Intelligence

Organization's CTI Experience

In the survey, participants were asked about the duration of their organization's provision of Cyber Threat Intelligence (CTI) services. It sheds light on their experience and expertise in the field of CTI. The responses obtained ranged from 2 years to more than 20 years, with only one response indicating a duration greater than 10 years. It can be deduced that most organizations providing CTI services have relatively shorter experience in this domain.

Reason for CTI Hesitancy

Upon being asked about the primary factors that hinder the adoption of CTI as a service, a significant number of respondents expressed a lack of awareness as the key reason. Furthermore, several respondents emphasized the impact of budget constraints, while one respondent specifically pointed out concerns related to compliance and regulatory requirements.

CTI Awareness

According to responses received from survey participants, awareness of IT threats (CTI) has seen a slight increase in organizations in recent years. All respondents indicated that the level of awareness has increased, although to a modest extent.

This suggests that organizations are gradually becoming more aware of the importance and benefits of CTI in addressing cyber security threats. The slight increase in awareness could be attributed to various factors, such as the increasing incidence of cyber attacks, the increased media coverage of cyber security issues, and the emphasis placed on cyber security measures by industry standards and regulations.

Primary Focus of CTI Service

The respondents were asked to select the primary focus of the Cyber Threat Intelligence (CTI) service they provide. This category explores the main areas of focus or specialization within the CTI services offered by participating organizations. According to survey responses (Figure 4.31), security risk assessments emerged as the main focus of Cyber Threat Intelligence (CTI) services.

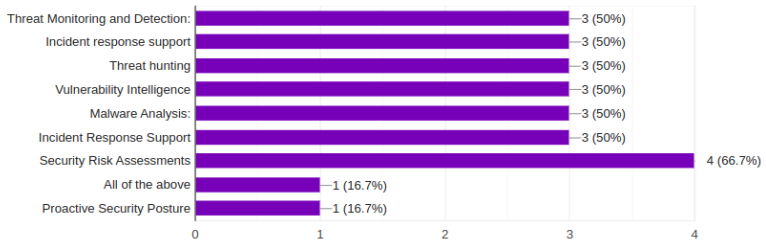

Figure 4.31: Primary Focus of Cyber Threat Intelligence (CTI) Service

Average Number of Clients Served with CTI

Among the organizations that responded to the survey, the number of clients who used CTI services varied. The reported numbers ranged from 3, 4, 5, and 10 clients, to an organization with 100 or more clients. Additionally, one organization was unable to disclose the exact number of clients due to privacy concerns.

Types of Organizations Using CTI Service

The participants were requested to categorize the organizations that predominantly use their CTI services. Of the six participants, four mentioned government entities along with others such as financial sector and healthcare companies. One participant was unable to disclose their clients.

Criteria for CTI Service

When inquired about the participants' organizations having selection criteria for clients receiving CTI services, the responses varied. Two participants stated that their organizations did not have any specific criteria. One participant mentioned that they had their own "Know Your Client" verification process in place. Another participant stated that they offer CTI services based on the sensitivity of the client's information. Furthermore, a participant provided a detailed response, stating that their organization had three requirements. These requirements included the client's level of awareness, their ability to share information, and their openness to ideas and methods proposed by the organization.

Key Components of CTI Service

The survey responses indicate that CTI services offered by organizations primarily focus on vulnerability assessment and intelligence reports. This aligns with the previous finding of the importance of the assessment of security risks within the CTI domain offered by the firms. By conducting comprehensive vulnerability assessments, organizations can identify potential weaknesses in their systems, networks, and applications, allowing them to address and mitigate risks proactively (Figure 4.32).

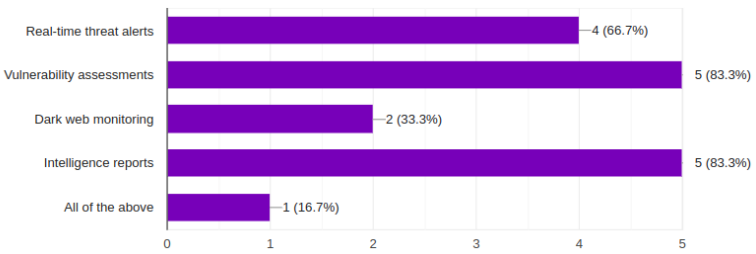

Figure 4.32: Key Components of Cyber Threat Intelligence (CTI) Service

Subscription Plans or Tiers for CTI Clients

When inquired about CTI packages, one organization revealed a monthly subscription model with different tiers based on the services offered. This indicates that clients can select a package that fits their specific needs and budget, providing flexibility in accessing CTI services. Another organization provided the option of billing on an hourly or monthly basis, with the pricing structure depending on factors such as the complexity of infrastructure or the scope of the CTI engagement. This suggests that the cost of CTI services can be tailored to the specific needs of the organization. Furthermore, another organization mentioned tiers in its packages based on the types of alert received, distinguishing between government alerts and public information. This highlights the customization of CTI packages to meet the specific intelligence needs of the organization.

4.3.3 Use of OSINT in CTI Service

To investigate the extent to which participating organizations utilize Open Source Intelligence (OSINT) in their CTI operations, respondent's were asked if and how do they integrate public sources into their CTI program.

Utilization of OSINT in CTI

Among the participants, the majority of the organizations used Open Source Intelligence (OSINT) for Cyber Threat Intelligence (CTI) purposes, as visible in Figure 4.33. The fact that only one participant's organization did not use OSINT emphasizes the value and relevance of gathering intelligence from open source data and tools in the field of cyber threat analysis.

Primary Sources of OSINT

When queried about their primary sources of Open Source Intelligence (OSINT), the responses were consistent among the participants. Additionally, a participant mentioned the inclusion of OSINT-specific feeds or scripts as part of their primary sources. These responses indicate a consensus among participants on the commonly used channels for gathering OSINT for their CTI activities.

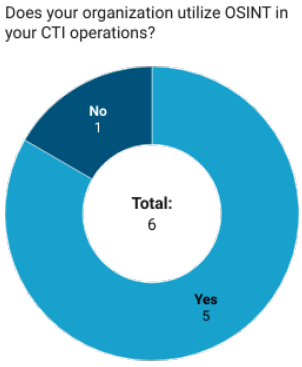

Figure 4.33: Use of OSINT in CTI Operations

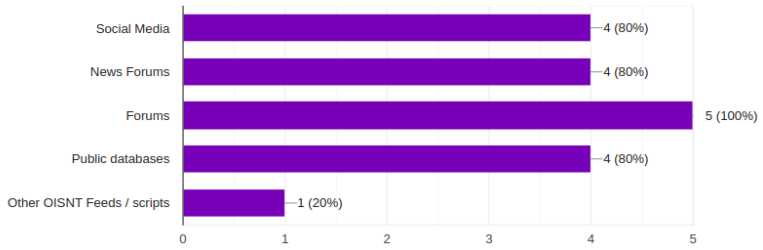

Figure 4.34: Primary Sources of OSINT

Assessment of Credibility and Reliability of OSINT

When asked about how they evaluate the credibility and reliability of the OSINT information they gather, two subjects refrained from providing detailed explanations due to confidentiality reasoning. However, two participants mentioned using the multiple feed comparison method to validate the information they collect. Additionally, a participant indicated that their organization follows a risk assessment process to assess the credibility and reliability of OSINT data. These approaches demonstrate a variety of strategies used by participants to ensure the accuracy and reliability of OSINT information that they rely on for their CTI activities.

Integration of OSINT into CTI Service and Analysis

One participant mentioned that the OSINT information gathered is added to their CTI reports and cyber alerts. This suggests that OSINT plays a role in enhancing the intelligence and insights provided to clients through regular reports and real-time alerts. Two participants mentioned the use of risk registers in the integration of OSINT in-

formation. Risk registers are tools that are used to identify, assess, and manage risks within an organization. In the context of CTI, risk registers can serve as repositories where OSINT information is logged and evaluated for potential threats and vulnerabilities. This enables organizations to prioritize and address cyber security risks based on the insights gained from OSINT sources. 2 participants did not elaborate due to confidentiality reasoning.

4.3.4 Evaluation of Services Provided

To evaluate the success or effectiveness of a Cyber Threat Intelligence (CTI) service, participants shared similar methodologies. They used various key performance indicators (KPIs) to measure the results and impact of their services. Here are the KPIs mentioned:

1. Feedback from clients - Regular contact, surveys and meetings
2. Reduction in risk and impact
3. Return on investment (ROI) and value to cost
4. Number of threats predicted

4.3.5 Security Trends in Pakistan

1. **Awareness of Cyber Security:** All participants unanimously indicated an increase in cyber security awareness as shown in Figure 4.35. This consensus suggests that there is a growing recognition and understanding of the importance of cyber security across the board.
2. **Factors Influencing Security Outsourcing:** When asked about the primary factors that influence an organization's decision to outsource security services, the participants highlighted two main perks: **cost-effectiveness** and **access to specialized expertise** (Figure 4.36. Of the 11 participants, 9 specifically mentioned these factors.
3. **Security Updates:** According to the majority (72%) of the observations of the subjects, organizations update their security measures occasionally (Figure 4.37).

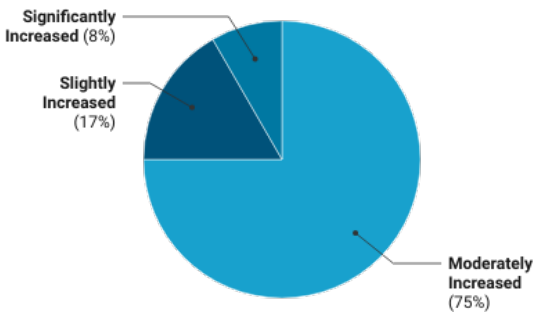

Figure 4.35: Answers to the "If Cyber Security has Increased in Organizations?"

Figure 4.36: Primary Factors that Affect the Decision to Outsource Security

This implies that, while organizations recognize the importance of security, they may not consistently prioritize or actively maintain their security systems. The term "occasionally" suggests that security updates are implemented periodically or in response to specific events or incidents. It highlights the need for organizations to adopt a more vigilant and regular security update schedule to effectively mitigate emerging threats and vulnerabilities.

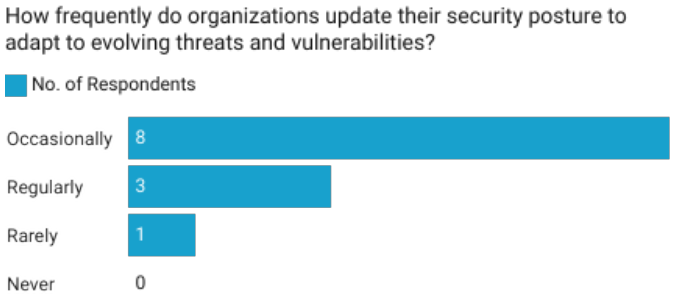

Figure 4.37: Frequency of Security Updates Observed by Organizations

4. **Factors Affecting Updates:** According to the responses of 10 out of 11 participants, security incidents/breaches are the primary reason for organizations to

update their security posture (Figure 4.38). This finding confirms the observation that organizations tend to update their security measures "occasionally". The second reason cited by the participants is compliance requirements, which serve as an external driving force that forces organizations to improve their security measures to meet the standards and regulations established by governing bodies or industry-specific guidelines.

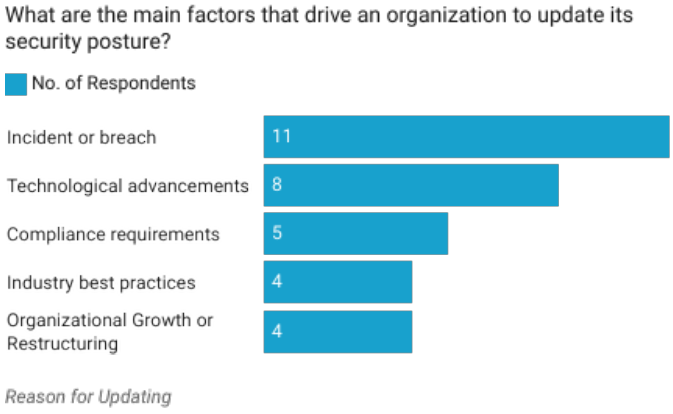

Figure 4.38: Factor that Motivate Organizations to Update Security Posture

4.3.6 Key Findings

General State of CTI in Pakistan

Based on the survey findings, it is evident that Cyber Threat Intelligence (CTI) is still considered a relatively new field for the corporate sector. Their participation in CTI is primarily based on security experts, suggesting that organizations are increasingly recognizing the need to invest in security solutions to protect their digital assets. The fact that many companies have entered the CTI market in the past decade, indicated by the survey finding that a significant majority (90%) of the companies surveyed possess less than 10 years of experience in the field of CTI. However, organizations can only request features and services of CTI that they are aware of, highlighting the crucial need to raise awareness about CTI within the industry.

The CTI services provided by the security companies were found to be comprehensive, employing formal workflows and methodologies. These companies emphasized the importance of getting constant feedback from clients and measuring their success through

key performance indicators (KPIs). In particular, security risk assessment emerged as a main focus for most CTI providers, with vulnerability assessments and intelligence reports ranking as top priorities.

Furthermore, the integration of Open Source Intelligence (OSINT) is a significant component of the CTI services offered. Approximately 83% of the security companies surveyed acknowledged using public feeds and data as part of their OSINT practices.

Based on survey data, it was determined that at least 122 organizations use Cyber Threat Intelligence (CTI) services from the companies included in the survey. It is important to note that this number could potentially be higher, as one of the respondents was unable to disclose the exact number of their clientele. The significant presence of 122 organizations employing CTI services is indicative of the growing demand for the adoption of these services in the industry.

Reactive Security

The participants' responses highlight the reactive nature of security updates, where incidents or breaches serve as triggers for organizations to review and strengthen their security. Compliance requirements act as additional motivators, reinforcing the need for organizations to maintain a robust and up-to-date security posture.

There is a recognized need to transition from reactive security to proactive security practices. Reactive security refers to responding to security incidents or breaches after they occur, whereas proactive security involves taking preemptive measures to prevent or minimize the impact of potential threats. Although reactive security has its merits in incident response and mitigation, it also carries certain disadvantages.

By solely relying on reactive security, organizations may find themselves constantly playing catch-up with evolving cyber threats. They may be more susceptible to significant financial losses, reputational damage, and disruptions to their operations. Reactive measures may also lead to increased downtime, increased recovery costs, and potential legal and compliance issues. To achieve a more proactive approach, organizations should prioritize continuous security updates and consider compliance requirements as essential components of their overall security strategy.

Chapter 5

Proposed OSINT Framework

Based on the findings derived from our preliminary surveys and interviews, it is evident that a significant number of organizations tend to employ ad hoc Open source Intelligence (OSINT) methodologies as part of their routine IT tasks. This approach involves using open source available on the Internet to support their security practices. On the other hand, a considerable portion of organizations opt to outsource their security services to external providers, thereby relying on specialized expertise to protect their systems and data.

There is a recognized need for a middle ground approach that empowers organizations to make decisions about security practices in a structured and formal manner. This involves establishing a well-defined workflow for decision-making processes, allowing organizations to effectively evaluate and implement OSINT strategies within their operational frameworks.

In this chapter, we discuss the baseline framework that served as the initial foundation and source of inspiration. This framework provides a starting point for understanding existing practices and processes related to the use of OSINT in security operations.

Subsequently, we will delve into the additions proposed for this framework, which are based on the insights and discoveries obtained through the survey and interview data. These additions aim to address the identified gaps, challenges, and opportunities revealed during the research process.

5.1 Baseline Framework

The OSINT workflow proposed in [1] has been used as a basis for further investigation. The workflow outlined in the paper by Pastor-Galindo et al. focuses primarily on OSINT investigations and the identification of adversarial targets. However, for the purpose of this study, our objective is to focus on an OSINT framework that can be easily embraced by diverse organizations and effectively integrated into their existing IT practices. This framework will provide a starting point for organizations to take advantage of the potential of open source data and tools available on the Internet in a systematic and integrated manner.

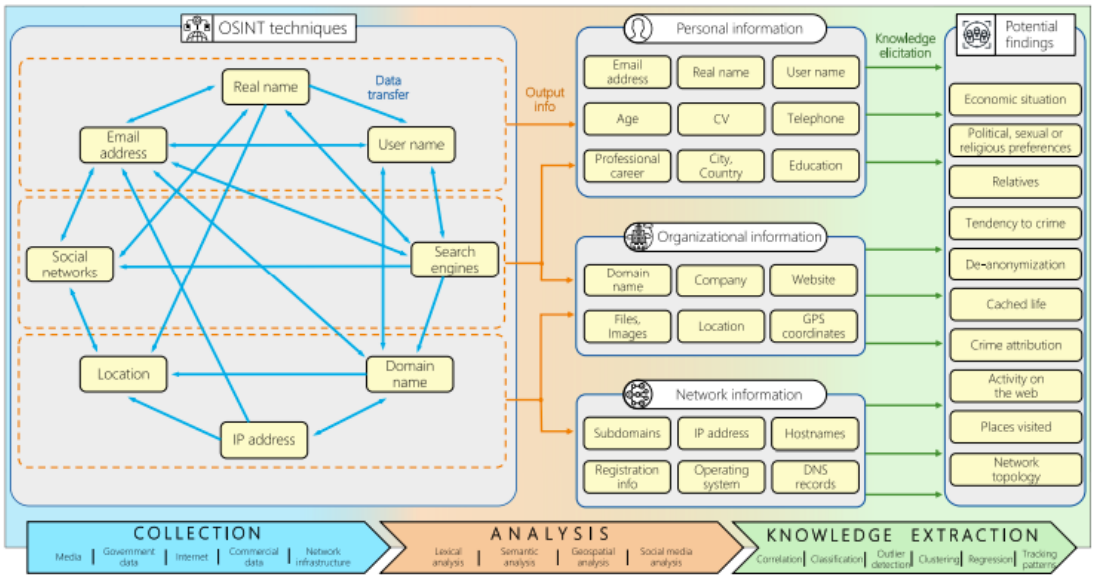

Figure 5.1: OSINT Workflow [1]

There are three main sections of the OSINT model workflow:

5.1.1 Data Collection:

[1] proposes a range of collection techniques as the initial step in an OSINT investigation. Beginning with an initial piece of information, the selection of the most appropriate technique is determined, and the results obtained from that technique serve as input for subsequent techniques in the investigation process. The investigative process often begins with an initial piece of information, such as an email address, name, or username. Various sources can be explored during the initial data gathering phase. These sources

include government databases, public records, media outlets, internet resources, social media platforms, and other publicly available information. On the basis of the nature of the information and the specific objective, the selection of the most suitable technique is determined. Various techniques can be used, including the use of search engines equipped with advanced filtering options or social media sites, to collect additional details such as locations, IP addresses, or domain names. The results obtained from these initial techniques can then serve as input for subsequent investigative techniques, creating a reiterative process that ensures systematic gathering of information.

5.1.2 Data Analysis

Once the sequential processes have been conducted, the gathered information is categorized into three distinct groups: personal information, organizational information, and network information. To derive valuable insights and achieve the defined goals, various procedures are applied to these categorized datasets. These procedures cover a variety of analytical techniques, including lexical analysis, social media analysis, geo-spatial analysis, and semantic analysis. The selection of a specific procedure depends on the type of data collected and the defined objectives of the investigation. Using appropriate analytical methods, meaningful patterns and insights can be extracted from the collected information, enabling a comprehensive understanding of the target subjects or entities.

5.1.3 Knowledge Extraction:

[1] proceeds to define several knowledge extraction techniques, some of which use artificial intelligence (AI) methodologies. These techniques include correlation analysis, classification algorithms, outlier detection methods, clustering algorithms, regression analysis, and pattern tracking approaches. By employing these AI-based techniques, researchers and analysts can effectively extract valuable knowledge and insights from the collected data.

5.2 Proposed Additions

Based on the evaluation conducted through surveys and interviews with IT teams in Pakistani organizations, the main framework can be adapted to meet their specific re-

quirements. To enhance and complement the main baseline framework, the traditional intelligence cycle [3] can be incorporated.

Figure 5.2: Traditional Intelligence Cycle [3]

We propose the following additions to improve the effectiveness of the framework (Figure 5.3).

5.2.1 Developing a Clear Strategy

Before proceeding with data collection and implementing OSINT within security operations, it is crucial to determine the specific use cases where OSINT can contribute effectively to achieve the goals and objectives. By defining these use cases, organizations can ensure that the use of OSINT is in line with their security requirements. In the context of Pakistan, three main use cases emerge for organizations: **threat intelligence, vulnerability assessment,** and **incident response**.

5.2.2 Provide Training and Education

Based on the preliminary survey and interviews, it is glaringly evident that there was a lack of awareness about OSINT. Therefore, organizations must offer comprehensive training programs to enhance the skills of your IT team members in OSINT techniques and tools. This can include **workshops, seminars, online courses, or the participation of external experts**. These training programs can include workshops,

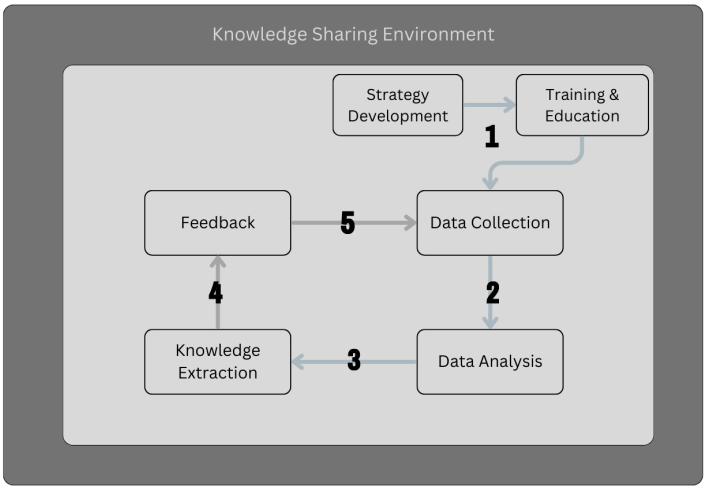

Figure 5.3: Proposed OSINT Cycle

seminars, online courses, or the participation of external experts who can provide specialized OSINT training. Update training materials regularly to stay up to date with the evolving nature of OSINT.

5.2.3 Promote Collaboration and Knowledge Sharing

Based on the interviews conducted, it became apparent that there is an informal approach to communicating security patches within organizations. The predominant mode of communication within IT teams relies on verbal discussions, without a written trail. Therefore, as a third addition, we propose the promotion of collaboration and knowledge sharing through formalized communication channels. This approach aims to facilitate effective information exchange and support joint investigations, particularly in the context of cross-functional projects. There needs to be an environment of knowledge sharing throughout the OSINT workflow. To effectively implement the proposed addition, several key strategies can be employed, including the use of **knowledge sharing platforms and incident documentation**.

5.2.4 Feedback

Feedback is a crucial step in any process, including the intelligence cycle. By incorporating feedback into the framework, organizations can ensure continuous improvement and adaptation based on the insights gained from previous experiences.

5.3 Implementation

In light of the insights gathered, we propose some suggestions for smooth implementation of the above framework.

- **Avoid Over Documentation:** When considering the adoption of a framework in Pakistan, it is important to take into account cultural considerations that can influence the implementation process. One such consideration is the tendency to over-document procedures in Pakistani organizations [32]. To address this, it is recommended to streamline the documentation process and focus only on preparing essential documentation. This can help avoid excessive paperwork and ensure that documentation remains concise, relevant, and effective.
- **Stakeholder Communication:** Another cultural consideration is the preference to minimize unnecessary meetings. To accommodate this preference, it is advisable to limit the number of meetings and ensure that they are purposeful and focused. Providing stakeholders with only the necessary and relevant information related to their roles and responsibilities can help avoid overwhelming them with extraneous details. Respecting the value placed on efficiency and minimalism in communication, the adoption of the framework can align with the cultural context and facilitate a smoother implementation.
- **Regulatory Compliance:** Emphasize compliance with relevant regulatory frameworks and industry standards specific to Pakistan, such as data protection and privacy regulations [47]. Ensure that the framework is aligned with these requirements to support organizations in maintaining legal and regulatory compliance.
- **Continuous Improvement:** Following the implementation of the framework, it is crucial to prioritize regular evaluations and updates on the security posture of Pakistani organizations. The results of the targeted survey have indicated that

many organizations do not consistently update their security measures, discussed in Section 4.3.5. Incorporating ongoing monitoring and leveraging open source intelligence (OSINT) can play a vital role in ensuring the effectiveness and relevance of the implemented framework.

Chapter 6

Conclusions

6.1 Perception of OSINT

Based on the results of the surveys and interviews, it is apparent that a significant portion of the population uses open source data and tools. Respondents generally rated the usefulness of OSINT and the tools positively, with an average response of 83% rating 3 or higher on the Likert scale. However, it was also observed that the actual usage of OSINT is relatively low, as discussed in detail in the analysis section. This discrepancy suggests that, while there is recognition of the potential benefits of OSINT, there is a lack of formal adoption and use. However, familiarity with the use of tools and data in an informal manner indicates that Pakistani organizations can potentially transition to formal usage relatively easily, building on the existing foundation. To address the observed gap in the formal adoption and use of OSINT in Pakistani organizations, we have proposed the addition of training and education programs. Based on the survey and interview findings, it is evident that there is a lack of awareness and familiarity with the proper terminology and techniques of OSINT. Therefore, comprehensive training and education initiatives are recommended to improve the skills and knowledge of IT team members to use OSINT tools and methodologies effectively.

6.2 Identified Barriers

1. **Presence of vulnerabilities in open source software**: Open-source software may have inherent vulnerabilities that can pose security risks if not properly ad-

dressed. Organizations need to ensure regular software updates and patches to mitigate these vulnerabilities.

2. **Limited documentation and support for open source solutions**: Open-source software often lacks comprehensive documentation and dedicated support, making it challenging for organizations to troubleshoot issues and seek assistance when needed. This can hinder the effective utilization of OSINT tools.

3. **Lack of security awareness among individuals and organizations**: Many individuals and organizations in Pakistan have limited knowledge and awareness of security practices and the importance of OSINT. This hampers their ability to recognize and utilize OSINT effectively for threat intelligence.

4. **Challenges in validating the credibility and reliability of OSINT sources**: Verifying the credibility and reliability of OSINT sources can be a complex task. It requires careful evaluation and validation of information obtained from various sources to ensure its accuracy and relevance to specific security needs.

5. **Limited budgets and resources allocated to security**: Organizations often prioritize their budgets and resources for other business areas, neglecting adequate investments in security measures. Insufficient funding and resources can restrict the implementation of robust OSINT strategies and hinder effective threat detection and mitigation.

6.3 Limitations of OSINT Tools

It is important to recognize that there are some challenges associated with OSINT, particularly its inconsistency in terms of source availability. This inconsistency stems from the dynamic nature of the Internet, where sources can become inaccessible or modified over time. For example, popular social networks like Facebook and Instagram frequently update their source code [18], making it difficult for OSINT practitioners to effectively use these techniques.

The evolving nature of online platforms and technologies poses a significant obstacle for OSINT practitioners, as the availability and accessibility of certain sources can change rapidly. This inconsistency can affect the reliability and accuracy of the gathered infor-

mation, as well as the effectiveness of OSINT tools and techniques. It requires practitioners to continually adapt and refine their methods to keep up with the ever-changing online landscape.

6.4 Contributions

1. Detailed insights on how open source data and tools and OSINT are used in operational practices across different organizations.
2. Empirical evidence confirming that employees consider open source data and tools and OSINT useful for facilitating daily tasks.
3. Identification of barriers and challenges faced by organizations, the knowledge of which can help guide future research and development in this area.
4. Proposed OSINT framework for Pakistani organizations that can be integrated into existing organizational workflow.

6.5 Future Work

The generalizability of the results in this study is limited due to several factors. First, there is the challenge of verifying self-reported data, as participants may provide inaccurate or biased information. Additionally, the sample size in this study was relatively small, which may have affected the accuracy and representativeness of the findings. A larger sample size in future studies would allow for more precise results and the possibility of uncovering statistically significant relationships.

Furthermore, the sample in this study was predominantly composed of large organizations, which could have introduced bias in the results. Certain industries, such as information and communication, were over represented, while other sectors may have been under-represented or not included in the survey at all.

Given these limitations, it is important to interpret the findings with caution. They provide valuable information, but further research is needed to validate and expand on the results. This study serves as a starting point for a long-term research plan on the role of OSINT in Pakistan's cyber security, raising important questions that require

further investigation. Future studies with larger and more diverse samples, along with rigorous methodologies, can contribute to a more comprehensive understanding of the topic.

Bibliography

[1] Javier Pastor-Galindo et al. "The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends". In: *IEEE Access* 8 (2020), pp. 10282–10304.

[2] Christian Sillaber et al. "Towards a maturity model for inter-organizational cyber threat intelligence sharing: A case study of stakeholders' expectations and willingness to share". In: *Proceedings of Multikonferenz Wirtschaftsinformatik (MKWI 2018)* (2018), pp. 6–9.

[3] B Kime. "Cyber Threat Intelligence Support to Incident Handling". In: *SANS Institute Information Security Reading Room* (2017).

[4] CyberProof. *Managed threat intelligence - CyberProof*. Feb. 27, 2023. URL: https://www.cyberproof.com/cyber-101/managed-threat-intelligence/.

[5] Cybersecurity Ventures and Steven C. Morgan. *2022 Official Cybercrime Report*. URL: www.esentire.com/resources/library/2022-official-cybercrime-report-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf (visited on 05/08/2023).

[6] Check Point Research Team. *2023 Cyber Security Report*. Feb. 8, 2023. URL: https://blog.checkpoint.com/2023/02/08/check-point-2023-security-report-cyberattacks-reach-an-all-time-high-in-response-to-geo-political-conflict-and-the-rise-of-disruption-and-destruction-malware/ (visited on 05/12/2023).

[7] Stjepan Groš. "Research Directions in Cyber Threat Intelligence". In: *arXiv preprint arXiv:2001.06616* (2020).

[8] Wiem Tounsi and Helmi Rais. "A survey on technical threat intelligence in the age of sophisticated cyber attacks". In: *Computers & security* 72 (2018), pp. 212–233.

[9] Matteo E Bonfanti. "Cyber Intelligence: In pursuit of a better understanding for an emerging practice". In: *Cyber, Intelligence, and Security* 2.1 (2018), pp. 105–121.

[10] Andrew Ramsdale, Stavros Shiaeles, and Nicholas Kolokotronis. "A comparative analysis of cyber-threat intelligence sources, formats and languages". In: *Electronics* 9.5 (2020), p. 824.

[11] João Rafael Gonçalves Evangelista et al. "Systematic literature review to investigate the application of open source intelligence (osint) with artificial intelligence". In: *Journal of Applied Security Research* 16.3 (2021), pp. 345–369.

[12] Haley Stone et al. "Using open source data to estimate the global epidemiology of pertussis". In: *Global Biosecurity* 2.1 (2020).

[13] Michael N Cantor, Rajan Chandras, and Claudia Pulgarin. "FACETS: using open data to measure community social determinants of health". In: *Journal of the American Medical Informatics Association* 25.4 (2018), pp. 419–422.

[14] Craig S Fleisher. "Using open source data in developing competitive and marketing intelligence". In: *European journal of marketing* 42.7/8 (2008), pp. 852–866.

[15] Shiqin Liu et al. "A generalized framework for measuring pedestrian accessibility around the world using open data". In: *Geographical Analysis* 54.3 (2022), pp. 559–582.

[16] Yong-Woon Hwang et al. "Current status and security trend of OSINT". In: *Wireless Communications and Mobile Computing* 2022 (2022).

[17] *MITRE ATT&CK®*. URL: https://attack.mitre.org/.

[18] Isabelle Böhm and Samuel Lolagar. "Open source intelligence: Introduction, legal, and ethical considerations". In: *International Cybersecurity Law Review* 2 (2021), pp. 317–337.

[19] Social Links. *OSINT in Social Media Investigations | Blog | Social Links*. Mar. 2023. URL: https://blog.sociallinks.io/osint-and-social-media-investigations-the-perfect-combination/.

[20] Talha Hussain. *Photon Scanner | Web Scraping OSINT Tool*. June 2021. URL: https://www.geeksforgeeks.org/photon-scanner-web-scraping-osint-tool/.

[21] Joseph Jones. *Scraping social media data, analysing disinformation, and batch scraping from Telegram*. May 2022. URL: https://os2int.com/toolbox/scraping-social-media-data-analysing-disinformation-and-batch-scraping-from-telegram/.

[22] Klaus Schwarz and Reiner Creutzburg. "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools-Part 3: Maltego". In: *Electronic Imaging* 2021.3 (2021), pp. 45–1.

[23] *Open Data Pakistan*. URL: https://opendata.com.pk/.

[24] *Online Statistics Suite*. URL: https://stats.blue/index.html.

[25] *FOR578: Cyber Threat Intelligence Training | SANS Institute*. URL: https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/.

[26] Cybersecurity Insiders. *Cyber Threat Intelligence Report*. Tech. rep. Mar. 2020. URL: https://www.cybersecurity-insiders.com/webinar/cyber-threat-intelligence-in-2020/.

[27] Rebekah Brown and Pasquale Stirparo. *SANS 2022 Cyber Threat Intelligence Survey | SANS Institute*. Feb. 2022. URL: https://www.sans.org/white-papers/sans-2022-cyber-threat-intelligence-survey/.

[28] Anzel Berndt and Jacques Ophoff. "Exploring the value of a cyber threat intelligence function in an organization". In: *Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13*. Springer. 2020, pp. 96–109.

[29] Sharifah Roziah Binti Mohd Kassim, Shujun Li, and Budi Arief. "How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study". In: *Cyber Security: A Peer-Reviewed Journal* 5.3 (2022), pp. 251–276.

[30] Adam Zibak and Andrew Simpson. "Cyber threat information sharing: Perceived benefits and barriers". In: *Proceedings of the 14th international conference on availability, reliability and security*. 2019, pp. 1–9.

[31] Yasmine Belghith, Sukrit Venkatagiri, and Kurt Luther. "Compete, collaborate, investigate: Exploring the social structures of open source intelligence investiga-

tions". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 2022, pp. 1–18.

[32] Nahil Mahmood. *Pakistan's Cyber Security Challenges & Solutions [Whitepaper]*. July 2019. URL: http://www.deltatechglobal.com/pakistans-cyber-security-challenges-solutions/.

[33] Tanveer Rafique. "Open-Source Intelligence (Osint) For National Security ". In: *THE BEACON JOURNAL 2021-22* 2.1 (2022), pp. 135–156. URL: https://pnwc.paknavy.gov.pk/thebeaconjournal/crs/Vol2No1_2022/8.Open-Source%5C%20Intelligence%5C%20(Osint)%5C%20For%5C%20National%5C%20Security%5C%20A%5C%20Counter%5C%20%5C%20by%5C%20Lt%5C%20Cdr%5C%20Tanveer%5C%20Rafiq.pdf.

[34] Faayed Al Faisal, Syed Ali Saif Kazmi, and Haider Abbas. "Growing Digital Vulnerability: A Case Study of Threats to Pakistans National Assets". In: *2021 International Conference on Communication Technologies (ComTech)*. IEEE. 2021, pp. 79–84.

[35] *Cyber Threat Intelligence Platform (1TIP) - 1LINK*. July 2021. URL: https://1link.net.pk/products-services/1tip/.

[36] Haris Bilal Malik. *OSINT in Current and Future Military Operations by Haris Bilal Malik - CASS Publications, Opinion Articles*. Feb. 2023. URL: https://casstt.com/osint-in-current-and-future-military-operations/.

[37] AsianLion. *Pakistan needs it's own OSINT Organization | Satellite Imagery Analysis & Tools*. July 2021. URL: https://defence.pk/pdf/threads/pakistan-needs-its-own-osint-organization-satellite-imagery-analysis-tools.669647/.

[38] Khawaja Khalid Farooq. "Using OSINT". In: (Mar. 2023). URL: https://www.thenews.com.pk/print/1050411-using-osint.

[39] *Project Baseerat – Open Source Intelligence (OSINT) in Pakistan*. URL: https://www.projectbaseerat.com/.

[40] *Threat Crowd | A Search Engine for Threats*. URL: http://ci-www.threatcrowd.org/.

[41] *VirusShare.com*. URL: https://virusshare.com/.

[42] Jawad Khalid Mirza. "Cyber Threat Intelligence - Where Pakistan Stands". In: *www.linkedin.com* (). URL: https://www.linkedin.com/pulse/cyber-threat-intelligence-where-pakistan-stands-jawad-khalid-mirza.

[43] Priscilla Koepke. "Cybersecurity information sharing incentives and barriers". In: *Sloan School of Management at MIT University: Cambridge, MA, USA* (2017).

[44] Ryan Stillions. *The DML model*. Aug. 2014. URL: http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html.

[45] Adam Zibak and Andrew Simpson. "Towards better understanding of cyber security information sharing". In: *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE. 2019, pp. 1–8.

[46] Johnnie Daniel. *Sampling Essentials: Practical Guidelines for Making Sampling Choices*. Jan. 2012. DOI: 10.4135/9781452272047. URL: https://doi.org/10.4135/9781452272047.

[47] Ministry of Information Technology and Telecommunication. *NATIONAL CYBER SECURITY POLICY 2021*. Tech. rep. July 2021. URL: https://moitt.gov.pk/SiteImage/Misc/files/National%5C%20Cyber%5C%20Security%5C%20Policy%5C%202021%5C%20Final.pdf.

Appendix A

Preliminary Survey

The survey is created to understand the data and security practices in Pakistan at corporate level. The information provided in this survey will only be used for research purposes. Your answers will remain anonymous.

1. Can you please provide us with your email address?
2. What sector do you belong to?
    - Academic
    - Telecom
    - Armed Forces
    - Technology
    - Finance
    - Service providers
    - Government
    - Other
3. In which country is your company based?
4. What is your job title?
5. How long have you worked in this job?
6. How many employees are there in your organization?
    - 0 - 9

- 10 - 49
- 50 - 249
- 250+

7. Do you know what Open Source Intelligence (OSINT) is?
   - Yes
   - No
   - Maybe
8. Do you make use of open source (free data and tools) from the Internet for official work?
   - Yes
   - No
   - Maybe
9. Have you ever made use of any of the following social media sites to obtain information for any official task (security reasoning or otherwise)?
   - Facebook
   - Twitter
   - Instagram
   - Reddit
   - Youtube
   - LinkedIn
   - None
   - Other...
10. Have you ever made use of any of the following open source tools or data in an official capacity for work? (Please mention any other similar to these)
    - Github
    - Google Maps
    - FOCA

- Mategoofil
- Maltego
- Shodan
- Hunter
- Pipl
- viewDNS
- Spiderfoot
- The Harvester
- IntelTechniques
- Recon-NG
- None

11. For what task(s) do you use the above mentioned (or similar) data and tool(s)? If you don't use them, please mention the reason why?

12. Does your organization have any experience in dealing with cyber security issues?

    - Yes
    - No
    - Maybe

13. Are there any protocols/guidelines in case of a cyber security issue?

    - Yes
    - No
    - Maybe

14. In your opinion, which of the following cyber security issues does your organization face?

    - Insider Attacks
    - Ransomware
    - Data Leak
    - Data Breach

- Remote work issues (Network Perimeter and Endpoint Security)
- DDoS (Distributed Denial of Service)
- Phishing Attacks
- Bot attacks
- Cloud jacking
- IoT devices vulnerability
- API Vulnerabilities and Breaches
- None
- Other...

15. What are the top 3 cyber security issues of your organization?
16. Is there a dedicated personnel/team to deal with security issues?
    - Yes
    - No
    - Maybe
17. Do you deal with cyber security issues or incidents?
    - Yes (I deal with it on my own)
    - Yes (I am part of a security team)
    - No (A dedicated security team/personnel deals with it)
    - Other...
18. What sources of data do you use for processing and analysis in your daily tasks?
    - Close Sourced Data (Provided by the organization)
    - Public Data (Through search engines, public forums, etc)
    - Open data that has been vetted
    - Other...
19. Is the close sourced data that you have access to sufficient for your daily tasks?
    - Yes

- No
- Maybe

20. Where do you gather public data from? (Select all that apply)
    - Search Engines
    - Social Media
    - Public data sets and feeds
    - Other...
21. What percentage of your tasks make use of open sourced data?
22. How useful do you think open sourced data is for your tasks? (Scale of 1-5), 1 being Not useful at all and 5 being very useful)
23. What type of software tools do you use?
    - Commercial tools (paid tools provided by your organization)
    - Free tools (From the Internet)
    - Other...
24. What task(s) do you use the tool(s) for? (Mention all that apply)
25. What percentage of your tasks are accomplished by free tools?
26. How useful do you think open sourced tools are for day to day tasks and cyber security investigations?(Scale of 1-5), 1 being Not useful at all and 5 being very useful)
27. Would you be willing to be contacted for a short interview?
    - Yes
    - No
    - Maybe

Appendix B

Interview Questions

1. What is your organization?
2. How many employees are there in your organization?
3. What is your job title?
4. Please state your work experience?
5. Can you give your job description?
6. How closely are you related to security?
7. Does your organization have a dedicated security team?
8. Would you say in the last 2 years, your security team has increased/decreased?
9. Would you say there has been an increase/decrease in security incidents?
10. Is your firm/organization a member of any cyber security information sharing organization?
11. Are you or your organization a consumer/producer of TI?
12. Indicate whether your organization produces or consumes Cyber Threat Intelligence (CTI) in terms of raw data and/or finished threat intelligence reports.
13. Does your organization have resources that focus on CTI?
14. What sources of threat intelligence do you rely on? (Select all that apply)
    - Our own detection processes

- Trusted peers
- Paid subscription service
- Government/government agencies
- Crowdsourced/Open Source
- Blogs/online forums
- We do not use threat intelligence

15. Does threat intelligence make it easier to respond to security incidents?
16. Do you have any of the following features in the CTI system?
    - Dynamic intelligence feed
    - Automated workflows
    - Integrated with the IT system
    - Smart data visualization
    - Analysis tools, built-in or external
17. How does your organization currently gather and analyze information from publicly available sources?
18. Can you give a real-life example of the usage of OSINT sources for CTI?
19. How has the use of OSINT sources improved your security and response?
20. How useful do you think OSINT sources can be for your company? Rate from 1-5.
21. What do you consider the biggest reasons behind the hesitation to usage of OSINT sources for CTI?
22. How willing would you be to make use of OSINT sources for CTI purposes?

Appendix C

Targeted Survey

1. Organization Name
2. Please provide your position or job title within the organization.
3. Size of your organization (Number of Employees)
   - 1-49
   - 50-249
   - 250+
4. Does your organization offer a Cyber Threat Intelligence (CTI) service?
   - Yes
   - No
5. How long has your organization been providing CTI services?
6. What do you think is the biggest reason for hesitancy among organizations to employ Cyber Threat Intelligence?
7. To what extent has awareness of Cyber Threat Intelligence increased in organizations over the past few years?
   - Significantly increased
   - Moderately Increased
   - Slightly Increased
   - No change

- Decreased

8. How would you describe the primary focus of your CTI service?
   - Threat Monitoring and Detection:
   - Incident response support
   - Threat hunting
   - Vulnerability Intelligence
   - Malware Analysis:
   - Incident Response Support
   - Security Risk Assessments
   - Other...
9. On average, how many clients does your organization serve with CTI?
10. Could you provide an estimate or breakdown of the types of organizations that typically use your CTI service? (e.g., government, financial institutions, healthcare, technology, etc.)
11. Do you have any specific requirements or criteria for organizations to be eligible for your CTI service? If yes, please specify.
12. What are the key features or components of your CTI service offering?
    - Real-time threat alerts
    - Vulnerability assessments
    - Dark web monitoring
    - Intelligence reports
    - Other...
13. Is there a range of subscription plans or tiers available for clients to choose from? If yes, please provide a brief overview.
14. Does your organization utilize Open Source Intelligence (OSINT) in your Cyber Threat Intelligence operations?
    - Yes

- No

15. What are the primary sources or channels of OSINT that your organization leverages?
    - Social Media
    - News Forums
    - Forums
    - Public databases
    - Other...
16. How does your organization assess the credibility and reliability of the OSINT information gathered?
17. How is the OSINT information integrated into your CTI service and analysis?
18. How do you measure the success or effectiveness of your CTI service for your clients?
19. Do you regularly collect feedback from clients regarding the quality and usefulness of the CTI service? If yes, how do you gather and utilize this feedback?
20. To what extent has awareness of Cyber Security increased in organizations over the past few years?
    - Significantly increased
    - Moderately Increased
    - Slightly Increased
    - No change
    - Decreased
21. What are the primary factors that influence an organization's decision to outsource security services?
    - Cost-effectiveness
    - Access to specialized expertise
    - Scalability

- Compliance requirements
- Other...

22. How frequently do organizations update their security posture to adapt to evolving threats and vulnerabilities?
    - Regularly
    - Occasionally
    - Rarely
    - Never
23. What are the main factors that drive an organization to update its security posture?
    - Incident or breach
    - Compliance requirements
    - Industry best practices
    - Technological advancements
    - Organizational Growth or Restructuring
    - Other...
24. Thank you for filling the form. Would you be willing to be contacted for follow-up questions, if any? If yes please leave your contact details.