Tampere University

Raazia Sultan

TOOLS, METHODS AND FRAMEWORKS OF CYBERSECURITY VISUALIZATION

Faculty of Information Technology and Communication Sciences (ITC)
Master's thesis
Supervisors:Bilhanan Silverajan and Hanning Zhao
November 2023

Abstract

Raazia Sultan: TOOLS, METHODS AND FRAMEWORKS OF CYBERSECURITY VISUALIZATION
Master's thesis
Tampere University
Master's Degree Programme in Information Security
November 2023

This thesis is dedicated to the investigation of contemporary tools, methodologies, and frameworks utilized in the ever-evolving realm of cybersecurity. The main goal of this study was to find out the most common things in this field. We did this by carefully looking at more than 50 research papers. We chose these papers from well-known sources and only kept the ones that matched our specific research criteria.

The structure of this work encompasses an introduction, offering an overview of research questions and the thesis's scope. The background section elucidates the critical context of cybersecurity visualization and reviews existing literature. Methodology is detailed, encompassing research question formulation, the chosen research methodology, and the process of data extraction.

The heart of the thesis is the analysis, which delves into data sources, visualization techniques, implementation, end-users, design, and evaluation methodologies. Results are presented categorically, exploring security scanning tools, behavior anomaly analysis, encryption tools, and runtime protection tools.

Subsequently, a comprehensive discussion reflects upon the research questions, offering insights and interpretations. Finally, a conclusion wraps up the findings and their implications. This scholarly endeavor culminates with a bibliography of the sources referenced throughout the thesis, providing a valuable resource for further research. This thorough analysis in the thesis not only adds to what we already know about cybersecurity visualization but also helps point the way for future research in this ever-changing field.

Keywords: Visualization, cyber security, tools of cybersecurity

Contents

1 Preface

When I started writing my thesis, I was doing a part-time job at the same time; therefore, it was a challenge for me to do both things at the same time. After a while, I even switched to a full-time job. All in all, I learned a lot during the process and managed to multitask effectively. My supervisors helped a lot with my time management. First and foremost, I would like to thank Bilhanan Silverajan for providing me with this awesome topic. I remember emailing professors of my university that I wanted to do a theoretical thesis. And thus, Mr. Bilhanan Silverajan proposed this topic for me. He helped me with my thesis a lot and even assigned me a research room so that I can study on campus as well. I would also like to thank Hanning Zhao for being the main examiner of the thesis. She provided me with enough analytical help and listened to my research proposals. I genuinely thank both of my supervisors for making this journey a lot easier for me. I would also like to thank my parents as well, who have always been my support system throughout. I also want to acknowledge that the support of ChatGPT was instrumental in ensuring that this thesis meet the highest standards of readability and linguistic precision. I am immensely appreciative of this technological aid.

2 Introduction

Cybersecurity is a field of study and practice dedicated to safeguarding computer systems, networks, programs, and digital data on the internet. The inception of cybersecurity dates back to the early 1970s. In the past, the necessity for cybersecurity in everyday internet use and computer systems was minimal. However, over the years, the volume of digital data has exponentially grown, making cybersecurity tools and processes imperative.

There are numerous ways in which cybersecurity tools, methods, and frameworks contribute to the detection of malware, breaches, or any malicious activities. One such approach is through cybersecurity visualization.

Cybersecurity visualization is a subset of data visualization that employs charts, graphs, dashboards, and various visualization techniques to present data to a diverse audience, including developers, analysts, security experts, visualization specialists, and novice users.

This thesis aims to analyze the contemporary tools, methods, and frameworks utilized in the visualization of cybersecurity data. The investigation will also focus on elucidating the similarities and differences among these tools and their classification. This comprehensive examination will facilitate the identification of the most commonly used and beneficial tools within this domain, offering insights for potential future modifications and enhancements.

2.1 Research questions

This thesis poses two main research questions, which will be described in detail below:

1. What are cybersecurity visualization's tools, methods and frameworks being used in today's world?

2. How can cybersecurity visualization tools, methods, and frameworks be classified??

These two questions are further addressed in sub-sections that cover the main components of the thesis.The sub-sections for each question are detailed as follows:

1. Tools, methods, and frameworks currently in use.
   - Defining tools, methods, and frameworks?
   - Identifying the types of tools, methods, and frameworks used in cybersecurity?
2. Analysis and evaluation between tools,methods and frameworks
   - Identifying the most common types of tools, methods, and frameworks?
   - Classification of tools, methods and frameworks

2.2 Scope

This paper adheres to specific parameters to define its scope. Firstly, it focuses exclusively on recent research papers for analysis, as the primary objective is to identify contemporary tools, methods, and frameworks within the current landscape. Consequently, research papers published prior to 2014 were excluded from the analysis.

Furthermore, this study strictly conducts a literature review to gather results and perform a comprehensive analysis. It refrains from direct interaction with any of the tools proposed in the research papers, maintaining an observational and analytical approach

2.3 Timeline of Thesis

The composition of this thesis adhered to a meticulously planned timeline. Commencing on March 1, 2022, the preliminary stage involved acquiring foundational knowledge in the subject matter. Subsequently, the research phase commenced on April 15, 2022, wherein an extensive examination of past papers was conducted.

Upon the comprehensive review and assimilation of pertinent research materials, the data analysis phase commenced on June 1, 2022. Following the completion of data analysis, the thesis writing process commenced on August 1, 2022, subsequent to the collection of essential research findings. The writing phase continued until the year 2023 and finally after reviews the thesis was submitted on October 15, 2023 for final inspection.

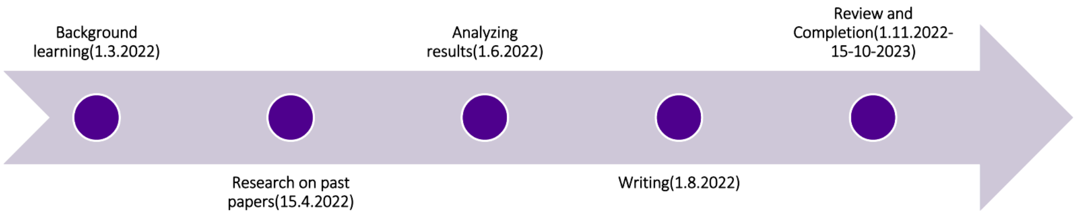
Background learning(1.3.2022)
Research on past papers(15.4.2022)
Analyzing results(1.6.2022)
Writing(1.8.2022)
Review and Completion(1.11.2022-15-10-2023)

Figure* *2.1 *Timeline of Thesis.*

Throughout the thesis development process, dual supervision was provided by a primary and secondary supervisor. Regular weekly meetings were conducted to oversee and guide the progression of the thesis. These meetings featured the creation of meeting notes, the establishment of weekly or monthly tasks and deadlines, and monthly progress discussions.

The chronological progression of the thesis is visually represented in Figure 2.1, which illustrates the timeline of thesis development using a Gantt chart.

2.4 Structure of the thesis

The thesis is structured into distinct sections, each serving a specific purpose:

1. Introduction:

   - Research Questions: This segment delineates the primary research questions guiding the study.
   - Scope: Here, the scope of the research is outlined, including any defined limitations or boundaries.
   - Timeline of Thesis Writing: A detailed chronology of the thesis development process is presented, offering insights into the project's progression.
   - Thesis Supervision Plan: This subsection elucidates the supervisory framework, featuring both primary and secondary supervisors, along with a description of the regular meetings and task-oriented approach.
   - Structure of Thesis: The overall structure of the thesis is provided to give readers an overview of what to expect.

2. Methodology: This section provides a comprehensive account of the research methodology employed throughout the study, offering a clear explanation of how the research was conducted.

3. Theory (Evaluation): As this thesis primarily consists of a literature review, this section serves as the core of the evaluation process. It directly addresses the research questions by critically assessing and synthesizing the relevant theoretical frameworks and existing literature.

4. Results and Summary: This segment presents the outcomes of the evaluation and synthesizes the findings. Additionally, it encapsulates the essence of the thesis in a concise summary.

5. References: The thesis concludes with a comprehensive list of references, acknowledging the sources and studies that contributed to the research.

This well-structured framework ensures clarity and coherence throughout the thesis, allowing readers to navigate and comprehend the research process and outcomes effectively.

3 Background

3.1 Cybersecurity visualization

Cybersecurity has emerged as a critical term in today's modern world. Awareness of cybersecurity extends to individuals and organizations alike, whether they are managing large-scale systems with a focus on data protection or simply engaging with social media for leisure.

Cybersecurity visualization is a concept intricately connected to various related terms. To comprehend this concept better, it can be initially described as a subset of data visualization. In the digital realm, vast amounts of data are constantly generated, comprising log files and other valuable information. However, the sheer volume of this data makes it challenging to discern common patterns or trends. To address this challenge, the concept of visualization was introduced.

Visualization is a technique that encompasses the creation of images, animations, graphs, diagrams, and other methods to effectively convey specific messages or information. Data visualization, therefore, represents the methodology of employing these techniques to illustrate data.

In scenarios where data security is paramount, such as within enterprises and for other critical purposes, the data in question is referred to as secure data. The process of visualizing this secure data is termed as cybersecurity visualization.

Cybersecurity visualization has proven to be a valuable means of analyzing anomalies, detecting emerging attack trends, and employing various security-related techniques.

In the contemporary landscape, a plethora of tools, methods, and frameworks are utilized. Ascertaining the superiority of one over another can be a daunting task. This paper aims to address this challenge by presenting a curated selection of significant research papers encompassing diverse visualization tools. These papers are categorized to facilitate further research and advancement within this specialized field.

3.2 Existing literature reviews

In this paper, we distinguish the difference between our analysis and three other researches. In this analysis, we present an extensive examination of network security visualization, offering a categorization consisting of five distinct use-case categories that cover the majority of recent research in this domain. We delineate the visualization methods and data resources employed and present a descriptive table to present our discoveries. Through the assessment of these systems, we investigate challenges in network security visualization. After assessing those we then offer recommendations for researchers and developers of visual systems.

As Shiravi, Shiravi and Ghorbani(2011)[42] the study examines have current cybersecurity visualization projects from the viewpoint of a use-case. Five sorts of use cases, each a distinct application area, were identified and each category's most works focused were extensively examined described. The primary data sources for the visualization of network security and provided some instances of all categories.The research goes into detail about the benefits and flaws of all use-case types and clarifying routes it should be the area of inquiry.As Shiravi, compiled the results of our research into a useful table for the future. references.

According to Staheli et al.(2014)[44], the Visualization for Cyber Security research community (VizSec) addresses persistent issues with cyber security by modifying and assessing information visualization methods for use in the field. This also differs from the argument made by Crouser, Erina, and Subashini in their paper, which claims that The VizSec research community has adopted various information visualization techniques to assist cyber analysts in their core responsibilities, there remains a lack of a cohesive approach within the community for designing and implementing these system applications.

The analysis is also distinct from Crouser, Erina, and Subashini's (2017)[18] research because it offers a retrospective analysis of the previous ten years' worth of VizSec papers with the goal of creating a more comprehensive knowledge of the new design trends at play in our community. The researchers find similar subject clusters within the body of work as well as a number of intriguing design trends centered on the use of different visual encodings. Additionally, they examine the gaps that still need to be filled in the application of information visualization techniques to cybersecurity applications and suggest possible directions for further study. My research diverges from Staheli's work, which led to the creation of multiple tools and techniques aimed at improving cybersecurity. However, there are currently no unified standards within the community to assess these methods and ascertain their operational validity.

In this work, the researchers review and classify the assessment metrics, elements, and methods applied in the VizSec research literature during the last ten years. In order to provide an agenda for advancing the state-of-the-art in assessing cyber security visualizations, the research also explore the methodological gaps that currently exist in the field and identify prospective directions for future study. In order to identify gaps in the present state of the practice in assessment and suggest future research paths, Staheli, performed a study of evaluation procedures used in VizSec publications using already established methodology from recent information visualization research.

Staheli conducted a comprehensive survey and categorization of evaluation metrics, components, and approaches used in the VizSec research literature over the past decade. This effort also provided an overview of the current landscape of visualization assessment in this study. We have highlighted methodological limitations that currently exist in the evaluation of visualization in cyber security and have made recommended directions for further investigation.

In addition to increasing the state-of-the-art in evaluating cyber security visualization, we expect that this work will stimulate more discussion on operational utility evaluation. While Crouser, Erina, and Subashini offer a retrospective survey and analysis of VizSec papers over the previous ten years with the goal of gaining a more comprehensive knowledge of the new design trends at work in our community. The study employs a variety of techniques, from text mining to the use of pre-existing task analysis frameworks, in order to give a thorough perspective on the state of VizSec research today.

The researchers find similar subject clusters within the body of work as well as some intriguing design trends centered on the usage of different visual encodings. Additionally, they address current shortcomings in the use of information visualization technologies for use in cybersecurity applications and suggest directions for the creation of new systems in their study.

4 Methodology

This thesis paper represents a comprehensive literature review encompassing past research papers in the field of cybersecurity visualization. The analysis and evaluation conducted in this thesis involved a meticulous review of approximately 50 papers, which were sourced from various academic databases, including Vizsec, Google Scholar, and ResearchGate.

To identify pertinent research papers, a set of key research phrases was employed, including:

1. Cybersecurity Visualization
2. Visualization Tools
3. Visualization Methods
4. Visualization Frameworks
5. Modern Cybersecurity Visualization Tools
6. Visualization Techniques in Cybersecurity

Every document identified through this research underwent a rigorous examination to determine its relevance within the scope of the thesis. Only papers that directly contributed to the thesis's analysis and targeted research objectives were selected for inclusion. A structured approach was employed to review each paper systematically, with the creation of a list of key attributes. This approach enabled the extraction of valuable information from each paper, enhancing the depth and quality of the analysis. While numerous methodologies exist for conducting research, this thesis adopted a straightforward approach that considered four fundamental elements.

4.1 Deciding research Questions

The first step in the methodology was to select the research questions that would best address the core objectives of this thesis. Initially, five research questions were shortlisted, which were subsequently refined to three, and finally, two research questions. These research questions are intentionally concise yet comprehensive, aligning perfectly with the scope of the research presented in this paper. The motivation behind these research questions has been previously elucidated in the ”Research Questions” section.

4.2 Research methodology

This section delineates the research methodology employed in the analysis of the literature. The objective was to systematically review a substantial number of research papers to categorize them and elucidate overarching trends across these papers. Furthermore, this thesis aimed to provide insights into the prevalence of specific tools, methods, and frameworks in the contemporary landscape of cybersecurity visualization.

Initially, the decision was made to source research papers exclusively from Vizsec, a reputable IEEE conference that comprehensively covers research papers pertaining to visualization within this specific domain. Subsequently, we expanded our sources to include papers from diverse platforms such as ResearchGate and digital libraries.

The primary search engine utilized for this endeavor was Google Scholar. To obtain the desired results, specific queries were meticulously crafted. The initial queries included fundamental keywords such as ’Cyber,’ ’Visualization,’ and ’Data,’ among others. These basic queries were later augmented with more precisely defined terms as outlined in the ’Methodology’ section. The amalgamation of these queries yielded a corpus of relevant research papers that served as the foundation for this research.

The process of study selection entailed rigorous scrutiny of each paper to determine its suitability for inclusion in the thesis, ensuring alignment with the research questions. Preference was given to papers that were recent, particularly those sourced from Vizsec and other reputable resources.

A total of 50 research papers were selected for comprehensive evaluation, drawn from various research categories within the domain. These selections were subject to review and discussion with the thesis supervisors during weekly meetings. The inclusion of papers was guided by adherence to specific criteria, as delineated by

L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi, and M. A. Babar in their work titled 'Systematic Literature Review on Cyber Situational Awareness Visualizations,' published in IEEE Access, Volume 10 [27].

1-	Paper should include or introduce a specific tool,method or framework for cybersecurity visualization.
2-	Paper should not be too short or too long.
3-	Paper should be published in english language
4-	Most of the papers should be taken from VIZsec since it is a prestigious conference in this field.
5-	Papers that were somewhat similar were also dropped.

Initially, a total of 67 papers were gathered for consideration. However, after a comprehensive evaluation, this number was subsequently reduced to 50 papers, ultimately chosen for inclusion in this thesis. The rationale behind this reduction primarily hinged upon the papers' pertinence to the domain of cybersecurity visualization and their capacity to elucidate specific tools, methodologies, and frameworks from a user-centric perspective.

4.3 Data extraction

The data was extracted according to a pre-defined table that was created before. The table include following classifications.

The importance of this table was evaluated by discussing with supervisors and by comparing the specific criterias by comparing these with other pre-defined research data extraction methods.

Table 4.1 *Data extraction pre-defined sources.*

Data Sources	Data sources of the visualization system, e.g., network packets, intrusion detection system, log files.
Visualization Techniques (what)	The techniques used in the system, e.g., node-link, scatter plot, 3D interface.
End Users	The targeted users of visualization systems, e.g., security analysts, non-expert users.
Design Methodology	What is the methodology of designing visualization? e.g., user centred design method? Interviews with users? Or not mentioned at all.
Evaluation Methodology	What is the methodology of evaluating visualization? e.g., user testing? Or the visualization is not evaluated by end users.

5 Analysis

This thesis was supposed to present an analysis of tools,methods and frameworks in cybersecurity visualization according to the research question. For that purpose 5 tables were proposed to evaluate 50 papers As shown in figure 6.1 to 6.6.

5.1 Data source

Data is called the information that has been created,collected or observed during a research. Data source simply means the source of data from where the data has been collected. It can be in different forms. The data sources that came across while doing analysis of the research papers. Different type of data sources were found which are as follow:

1. Log files
2. Intrusion detection system
3. Network packets
4. Binary SELinux and SEAndroid policies
5. Standards and Frameworks
6. User inputs
7. Firewall configuration data
8. Selected privacy parameters
9. System log files
10. GDPR data from Facebook and Google users
11. Dalvik Executable (DEX) file
12. Risk-scoring Model data
13. Android code

14. Deep learning models

All these data sources were often repeated in some papers. The most popular data source is log files , network packets and intrusion detection system. Since it might be a bit lengthy to describe all data sources in detail only three most common data sources will be described here.

Log files:

Log file is simply the type of file that is generated by computer. It contains information about patterns and trends of usage and activities in an operating system.

Network packets:

Packet means a smaller part of a longer thing such as a message ,file or data. Network packets means the smaller part of network data. The network data can be internet.

Intrusion detection system:

It could be a network device or application that monitors traffic and reports any violation of privacy and security.

		Software code	Log Files	Intrusion detection system	Network traffic	Deep learning models	Malware codes	Network Traffic log	Network packets	Network logs	Log files	Wikipedia data	System log files	Risk-scoring Model data	GDPR data from Facebook	Selected privacy parameters	User sessions	Android code	Dalvic Executable (DEX) file	Cyber-threat data	Firewall configuration data	Internet download	User requests	Binary SELinux and SEAndroid	Standards and Frameworks	Literature materials	User inputs	Network data
Provence-driven Automated Security Board	[1]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An interactive visualization system for developers	[2]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
VulnEx	[3]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Automatic Narrative Summarization	[4]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
File System Metadata Analysis Tool (Beran et al.)	[5]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A Visual Analytics Framework for Adversarial	[6]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Malware Battle Visualization (Gotta Evade 'em)	[7]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Eventpad	[8]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Intrusion Alert-driven Attack Graph Extractor	[9]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Interpretable Visualizations of Neural Networks	[10]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Image-based Malware Classification	[11]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
NetCapVis	[12]	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Three-Dimensional Visualization Network Intrusion	[13]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Anomalous IP-Block Behavior Using Geo-IP Data	[14]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
The RiskID application	[15]	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
AI Total – a web-based visualization system	[16]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Wikipedia behavior analysis tool	[17]	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
BUCEPHALUS	[18]	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Visual Decision Support for Live Digital Forensics	[19]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Focus and Context Visualizations	[20]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
The web interface TransparencyVis	[21]	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
A visual uncertainty model	[22]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Sharing Data Using Differential Privacy	[23]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Insider Threat Visualization Product	[24]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
User Behavior Map	[25]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Android Malicious Flow Visualization Toolbox	[26]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
Android Malware Familial Classification method	[27]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
STARLORD	[28]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PCA an GCPA Methodology	[29]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Network Data Curation Toolkit (NDCT)	[30]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Hyperion	[31]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Trogdor (Yuen and Turnbull)	[32]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.)	[33]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○
HSViz	[34]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PERCIVAL	[35]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
SDN Data Analysis Tool	[36]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Ocelot	[37]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Method and Tool to Visualize Network Traffic	[38]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Bigfoot	[39]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
CyberPetri	[40]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Web Download Analysis Tool	[41]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
ADVERS ARIAL PLAYGROUND (Norton and Qi)	[42]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
IMap	[43]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
Zone-based vulnerability visualization	[44]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
CVSS score Vulnerability scanning tool	[45]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
MITRE ATT&CK Matrix	[46]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Guidelines for Cybersecurity Visualization Design	[47]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Cybersecurity Awareness on IoT context	[48]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
CRUMBS	[49]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
V3SPA	[50]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○

Figure 5.1 *Data-resources used in each research paper*

5.2 Visualization technique

To analyse visualization techniques was the main part of the thesis. While doing analysis many types of visualization techniques were discovered which are as follows:

1. Bar Charts
2. 3D Interface
3. Scatter Plot
4. Graphs
5. 2D interface
6. Trees
7. node link
8. Clusters
9. Histogram
10. Line graph
11. Pie chart

The visual representation of some of these visualization techniques are as follows:

Out of all these visualization techniques the most common ones that were found are Bar graph , 3D interface and scatter plot.

Bar graph:

A bar chart or bar graph utilizes rectangular bars with heights or lengths that correspond to the values they represent to visualize categorical data. Both vertical and horizontal bar plots can be employed. Another term for a vertical bar graph is a column chart.

3D Interface:

The term ”3D interfaces” refers to interfaces used for 3D interaction.It incorporates two-way communication between users and the system, like other kinds of user interfaces, but it also enables users to do actions in three dimensions.

Scatter plot:

A scatter plot, alternatively termed a scatter chart or scatter graph, visually conveys numerical values for two separate variables through the use of dots. The positioning of each dot on both the horizontal and vertical axes signifies the values associated with a particular data point.

		Bar Charts	3D Interface	Graphs	List view, histogram, and clusters	Line chart, event log, and scatterplot	Tree	Node-link and histogram	Node-link, bar charts, and scatter plot	Cluster chart, bar and pie charts	Scatter plot	Charts	Bar Charts, Scatter plot and node-link	Line graph and bar charts	Histogram, line graph, and bar graph	Web interface	Relation martrix, node link, and histogram	Node link, line graph, and scatter plot	Scatter plot, charts	Node link and pie chart	Node link and line graph	Tree and node link	2D interface	Scatter Plot and Line graph	Scatter plot, histogram, and bar charts	Scatter plot on maps	None	Network data
Provence-driven Automated Security Board	[1]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An interactive visualization system for developers	[2]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
VulnEx	[3]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Automatic Narrative Summarization	[4]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
File System Metadata Analysis Tool (Beran et al.)	[5]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A Visual Analytics Framework for Adversarial	[6]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Malware Battle Visualization (Gotta Evade 'em)	[7]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Eventpad	[8]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Intrusion Alert-driven Attack Graph Extractor	[9]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Interpretable Visualizations of Neural Networks	[10]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Image-based Malware Classification	[11]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
NetCapVis	[12]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Three-Dimensional Visualization Network Intrusion	[13]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Anomalous IP-Block Behavior Using Geo-IP Data	[14]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
The RiskID application	[15]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
AI Total – a web-based visualization system	[16]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Wikipedia behavior analysis tool	[17]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
BUCEPHALUS	[18]	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Visual Decision Support for Live Digital Forensics	[19]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Focus and Context Visualizations	[20]	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
The web interface TransparencyVis	[21]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A visual uncertainty model	[22]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Sharing Data Using Differential Privacy	[23]	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Insider Threat Visualization Product	[24]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
User Behavior Map	[25]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Android Malicious Flow Visualization Toolbox	[26]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Android Malware Familial Classification method	[27]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
STARLORD	[28]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PCA an GCPA Methodology	[29]	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Network Data Curation Toolkit (NDCT)	[30]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Hyperion	[31]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Trogdor (Yuen and Turnbull)	[32]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.)	[33]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
HSViz	[34]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PERCIVAL	[35]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○
SDN Data Analysis Tool	[36]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Ocelot	[37]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
Method and Tool to Visualize Network Traffic	[38]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Bigfoot	[39]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
CyberPetri	[40]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
Web Download Analysis Tool	[41]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
ADVERS ARIAL PLAYGROUND (Norton and Qi)	[42]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
IMap	[43]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
Zone-based vulnerability visualization	[44]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
CVSS score Vulnerability scanning tool	[45]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
MITRE ATT&CK Matrix	[46]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Guidelines for Cybersecurity Visualization Design	[47]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Cybersecurity Awareness on IoT context	[48]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
CRUMBS	[49]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
V3SPA	[50]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 5.2 *Visualization-technique used in each research paper*

5.3 Implementation

In implementation we studied as to how different visualization techniques have been implemented. The most common types of implementation that were analysed are:

1. Desktop application
2. Open-source platform
3. Web-based
4. JS Library
5. Open platforms
6. AR Application
7. Implemented using a recommendation algorithm and a semi-supervised learning algorithm etc

The most common type of implementation that were found in the analysed papers are: Desktop application, Web based and Open source platform.

Desktop application:

A desktop application is a software program designed for use by an end user to perform specific tasks on an individual, standalone computer.

Web based:

A web-based application is any software that can be accessed through a network connection using HTTP, as opposed to being stored in the memory of a device.

Open source platform:

Code that is meant to be publicly accessible is termed open source software, allowing anyone to inspect, modify, and distribute the code as they wish. The decentralized, collaborative development of open source software often involves peer review and community production.

		Web-based,open platform	Desktop application,open platform	Desktop application,open-source	Desktop application on D3.js library	AR app. machine learnings algorithms	Desktop app, machine learnings algorithms	AR application,Supervised learning algorithms	Web-based app,JS library	Desktop application,Python and C#	Web-based, using JS library	Web-based, semi-supervised algorithm	Web-based, machine -learning algorithm	Web-based,AI algorithm	AR Application, open platforms	Mobile application,open platforms	AR Application,JS Library	Literature review
Provence-driven Automated Security Board	[1]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An interactive visualization system for developers	[2]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
VulnEx	[3]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Automatic Narrative Summarization	[4]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
File System Metadata Analysis Tool (Beran et al.)	[5]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
A Visual Analytics Framework for Adversarial	[6]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Malware Battle Visualization (Gotta Evade 'em)	[7]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Eventpad	[8]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Intrusion Alert-driven Attack Graph Extractor	[9]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Interpretable Visualizations of Neural Networks	[10]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Image-based Malware Classification	[11]	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
NetCapVis	[12]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
Three-Dimensional Visualization Network Intrusion	[13]	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○
Anomalous IP-Block Behavior Using Geo-IP Data	[14]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
The RiskID application	[15]	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
AI Total – a web-based visualization system	[16]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
Wikipedia behavior analysis tool	[17]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
BUCEPHALUS	[18]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Visual Decision Support for Live Digital Forensics	[19]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Focus and Context Visualizations	[20]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
The web interface TransparencyVis	[21]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A visual uncertainty model	[22]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Sharing Data Using Differential Privacy	[23]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Insider Threat Visualization Product	[24]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
User Behavior Map	[25]	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
Android Malicious Flow Visualization Toolbox	[26]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
Android Malware Familial Classification method	[27]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
STARLORD	[28]	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
PCA an GCPA Methodology	[29]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Network Data Curation Toolkit (NDCT)	[30]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Hyperion	[31]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
Trogdor (Yuen and Turnbull)	[32]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.)	[33]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
HSViz	[34]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
PERCIVAL	[35]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
SDN Data Analysis Tool	[36]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Ocelot	[37]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Method and Tool to Visualize Network Traffic	[38]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
Bigfoot	[39]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
CyberPetri	[40]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Web Download Analysis Tool	[41]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
ADVERS ARIAL PLAYGROUND (Norton and Qi)	[42]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
IMap	[43]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Zone-based vulnerability visualization	[44]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
CVSS score Vulnerability scanning tool	[45]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
MITRE ATT&CK Matrix	[46]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Guidelines for Cybersecurity Visualization Design	[47]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Cybersecurity Awareness on IoT context	[48]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
CRUMBS	[49]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
V3SPA	[50]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○

Figure 5.3 *Implementation used in each research paper*

5.4 End Users

End user is the individual for whom a hardware or software product is designed. While reviewing the papers for the analysis of this thesis it was seen that some papers did not specify any type of end users However most of the papers were designed for or targeted different type of end users for example:

1. Vulnerability remediation teams
2. Cyber-security analysts
3. System administrators
4. Senior or middle management
5. Cyber forensics experts
6. Security professionals
7. Business owners
8. Developers
9. Non-expert users
10. Executive leadership etc

The most common type of end users found in those papers were: Cyber-security analysts , Network administrator and developers.

Cybersecurity analyst:

A cybersecurity analyst is an expert in the field of cybersecurity, specializing in network and IT infrastructure security.

The cybersecurity analyst diligently strives to anticipate and remove cyberattacks by possessing a deep understanding of malware, cyber threats, and the tactics employed by cybercriminals.

Network administrator:

The daily oversight of these networks falls under the purview of network and computer system administrators. Their role entails the planning, configuration, and ongoing maintenance of a company's computer systems, encompassing LANs, WANs, network segments, intranets, and other data transmission systems.

Developers:

Software developers leverage a range of technologies and skills to conceptualize, code, develop, distribute, and oversee software.

The end users can be defined into three major categories such as:

1-Security analysts

2-Non-security experts such as (data scientists, data engineers and business stakeholders, Visualization experts, software developers)

3- And even Ordinary users

- **Security analysts:**
  Security analysts are people who are closely working with security. They have enough knowledge of security and if given certain amount if data or files for them to analyze then they know which piece of information is important for them and how they think will help them in their analysis.

- **Non security experts:**
  Non security experts are people who are not working close to security however they do have know how of how computer systems work and how data is being transferred. Non security experts have different types of experts in this area e.g, data scientists, data engineers and business stakeholders, Visualization experts, software developers.

- **Ordinary users:**
  Third and last type of people that can use cybersecurity visualization to visualize data are ordinary users or in short naive users. These naive users have little or no expertise in security or operating systems.

		Developers	Developers and Security Analysts	Developers, Project Managers Analysts	Cyber-security Analysts	Cyber-security analyst,non-expert users	Cyber-security analysts,System administrators	System designers and Security Analysts	Security Analysts,Cybersecurity Researchers	Domain Experts, Network Administrators	Network Administrators,Cybersecurity Analysts	Internet service provider, Internet authorities	Administrators, Cybersecurity Analysts	Cybersecurity Analysts and System Testers	Cybersecurity Analysts,non-experts	Cyber forensics experts, security professionals	Cyber forensics experts,business owners	Cybersecurity team	Developers, Security,Software Testers	Internet Service Providers	Cybersecurity Analyst,Policy analyst	Cybersecurity Analyst,Policy designer
Provence-driven Automated Security Board	[1]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An interactive visualization system for developers	[2]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
VulnEx	[3]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Automatic Narrative Summarization	[4]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
File System Metadata Analysis Tool (Beran et al.)	[5]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A Visual Analytics Framework for Adversarial	[6]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Malware Battle Visualization (Gotta Evade 'em)	[7]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Eventpad	[8]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Intrusion Alert-driven Attack Graph Extractor	[9]	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Interpretable Visualizations of Neural Networks	[10]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Image-based Malware Classification	[11]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
NetCapVis	[12]	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Three-Dimensional Visualization Network Intrusion	[13]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Anomalous IP-Block Behavior Using Geo-IP Data	[14]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
The RiskID application	[15]	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
AI Total – a web-based visualization system	[16]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
Wikipedia behavior analysis tool	[17]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○
BUCEPHALUS	[18]	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Visual Decision Support for Live Digital Forensics	[19]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
Focus and Context Visualizations	[20]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
The web interface TransparencyVis	[21]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
A visual uncertainty model	[22]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
Sharing Data Using Differential Privacy	[23]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
Insider Threat Visualization Product	[24]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
User Behavior Map	[25]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
Android Malicious Flow Visualization Toolbox	[26]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
Android Malware Familial Classification method	[27]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
STARLORD	[28]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PCA an GCPA Methodology	[29]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Network Data Curation Toolkit (NDCT)	[30]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Hyperion	[31]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Trogdor (Yuen and Turnbull)	[32]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.)	[33]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
HSViz	[34]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
PERCIVAL	[35]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
SDN Data Analysis Tool	[36]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Ocelot	[37]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Method and Tool to Visualize Network Traffic	[38]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
Bigfoot	[39]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
CyberPetri	[40]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Web Download Analysis Tool	[41]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
ADVERS ARIAL PLAYGROUND (Norton and Qi)	[42]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
IMap	[43]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Zone-based vulnerability visualization	[44]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
CVSS score Vulnerability scanning tool	[45]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
MITRE ATT&CK Matrix	[46]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Guidelines for Cybersecurity Visualization Design	[47]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Cybersecurity Awareness on IoT context	[48]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	●	○	○	○	○
CRUMBS	[49]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
V3SPA	[50]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●

***Figure* 5.4** *End-users used in each research paper*

5.5 Design methodology

Design methodology means the creation of a method. It is the study of practices and procedures of designing. Through the analysis of research papers we got to know different type of design methodologies being used today. They are as follows:

1. User-centered design
2. Human-centered design
3. User interviews
4. Interview of representative domain experts Etc

The most common type of design methodologies that was found is user-centered designs and interviews with partners or users. User centered designs: User centered designs are the type of designs that focus on the user's needs on every step of design methodology. Interviews with partners or users: A user interview is a technique where a researcher questions one user about an interest issue.

		User-centered design	Interviews with domain experts	Not mentioned	Interview of participants	Interview of human factors professionals	Interview of representative domain experts	Interview network operators,security specialists	Interviews with user	User Interviews	Web-based Design	Human-centered design
Provence-driven Automated Security Board	[1]	●	○	○	○	○	○	○	○	○	○	○
An interactive visualization system for developers	[2]	●	○	○	○	○	○	○	○	○	○	○
VulnEx	[3]	○	●	○	○	○	○	○	○	○	○	○
Automatic Narrative Summarization	[4]	●	○	○	○	○	○	○	○	○	○	○
File System Metadata Analysis Tool (Beran et al.)	[5]	●	○	○	○	○	○	○	○	○	○	○
A Visual Analytics Framework for Adversarial	[6]	●	○	○	○	○	○	○	○	○	○	○
Malware Battle Visualization (Gotta Evade 'em)	[7]	○	○	●	○	○	○	○	○	○	○	○
Eventpad	[8]	●	○	○	○	○	○	○	○	○	○	○
Intrusion Alert-driven Attack Graph Extractor	[9]	○	○	●	○	○	○	○	○	○	○	○
Interpretable Visualizations of Neural Networks	[10]	●	○	○	○	○	○	○	○	○	○	○
Image-based Malware Classification	[11]	●	○	○	○	○	○	○	○	○	○	○
NetCapVis	[12]	●	○	○	○	○	○	○	○	○	○	○
Three-Dimensional Visualization Network Intrusion	[13]	●	○	○	○	○	○	○	○	○	○	○
Anomalous IP-Block Behavior Using Geo-IP Data	[14]	●	○	○	○	○	○	○	○	○	○	○
The RiskID application	[15]	●	○	○	○	○	○	○	○	○	○	○
AI Total – a web-based visualization system	[16]	●	○	○	○	○	○	○	○	○	○	○
Wikipedia behavior analysis tool	[17]	●	○	○	○	○	○	○	○	○	○	○
BUCEPHALUS	[18]	●	○	○	○	○	○	○	○	○	○	○
Visual Decision Support for Live Digital Forensics	[19]	●	○	○	○	○	○	○	○	○	○	○
Focus and Context Visualizations	[20]	●	○	○	○	○	○	○	○	○	○	○
The web interface TransparencyVis	[21]	○	○	○	●	○	○	○	○	○	○	○
A visual uncertainty model	[22]	○	○	●	○	○	○	○	○	○	○	○
Sharing Data Using Differential Privacy	[23]	○	○	○	○	●	○	○	○	○	○	○
Insider Threat Visualization Product	[24]	○	○	○	○	○	●	○	○	○	○	○
User Behavior Map	[25]	●	○	○	○	○	○	○	○	○	○	○
Android Malicious Flow Visualization Toolbox	[26]	○	○	●	○	○	○	○	○	○	○	○
Android Malware Familial Classification method	[27]	○	○	●	○	○	○	○	○	○	○	○
STARLORD	[28]	●	○	○	○	○	○	○	○	○	○	○
PCA an GCPA Methodology	[29]	●	○	○	○	○	○	○	○	○	○	○
Network Data Curation Toolkit (NDCT)	[30]	○	○	○	●	○	○	○	○	○	○	○
Hyperion	[31]	○	●	○	○	○	○	○	○	○	○	○
Trogdor (Yuen and Turnbull)	[32]	○	○	○	○	○	○	●	○	○	○	○
An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.)	[33]	●	○	○	○	○	○	○	○	○	○	○
HSViz	[34]	●	○	○	○	○	○	○	○	○	○	○
PERCIVAL	[35]	○	○	○	○	○	○	○	●	○	○	○
SDN Data Analysis Tool	[36]	●	○	○	○	○	○	○	○	○	○	○
Ocelot	[37]	●	○	○	○	○	○	○	○	○	○	○
Method and Tool to Visualize Network Traffic	[38]	●	○	○	○	○	○	○	○	○	○	○
Bigfoot	[39]	●	○	○	○	○	○	○	○	○	○	○
CyberPetri	[40]	○	○	○	○	○	○	○	○	●	○	○
Web Download Analysis Tool	[41]	●	○	○	○	○	○	○	○	○	○	○
ADVERS ARIAL PLAYGROUND (Norton and Qi)	[42]	○	○	●	○	○	○	○	○	○	○	○
IMap	[43]	○	○	○	○	○	○	○	○	○	●	○
Zone-based vulnerability visualization	[44]	●	○	○	○	○	○	○	○	○	○	○
CVSS score Vulnerability scanning tool	[45]	●	○	○	○	○	○	○	○	○	○	○
MITRE ATT&CK Matrix	[46]	●	○	○	○	○	○	○	○	○	○	○
Guidelines for Cybersecurity Visualization Design	[47]	○	○	○	○	○	○	○	○	○	○	●
Cybersecurity Awareness on IoT context	[48]	○	○	○	○	○	○	○	○	○	○	●
CRUMBS	[49]	●	○	○	○	○	○	○	○	○	○	○
V3SPA	[50]	●	○	○	○	○	○	○	○	○	○	○

Figure 5.5 *Design-methodology used in each research paper*

5.6 Evaluation methodology

The evaluation methodology serves as a tool for elucidating the steps necessary to conduct a comprehensive examination.There were different type of evaluation methodology in the papers that were analysed:

1. Testing by participants
2. User testing
3. Testing using trained data by the developers
4. Testing by Security analysts
5. Evaluated by Domain Experts Etc

Along the way it was noticed that most of the tools, methods and frameworks were not evaluated by anyone.

		Not evaluated by end users	Evaluated by Domain Experts	Testing by Security analysts	Testing by SOC analyst	System Usability Scale (SUS)	Testing use case by the developers	Testing in real-world office by the developers	Testing using trained data by the developers	Testing using training,class label of malware	Visualization is not evaluated by end users	Reviews by students for 19 and 26 years old	Testing by Participants, filled questionnaires	User testing	Testing by human factors professionals	Testing by users(representative domain expert)	User testing (participants)	Testing by participants
Provence-driven Automated Security Board	[1]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
An interactive visualization system for developers	[2]	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
VulnEx	[3]	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Automatic Narrative Summarization	[4]	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○
File System Metadata Analysis Tool (Beran et al.)	[5]	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
A Visual Analytics Framework for Adversarial	[6]	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
Malware Battle Visualization (Gotta Evade 'em)	[7]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Eventpad	[8]	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
Intrusion Alert-driven Attack Graph Extractor	[9]	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Interpretable Visualizations of Neural Networks	[10]	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○
Image-based Malware Classification	[11]	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○
NetCapVis	[12]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Three-Dimensional Visualization Network Intrusion	[13]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Anomalous IP-Block Behavior Using Geo-IP Data	[14]	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
The RiskID application	[15]	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○
AI Total – a web-based visualization system	[16]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Wikipedia behavior analysis tool	[17]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
BUCEPHALUS	[18]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Visual Decision Support for Live Digital Forensics	[19]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Focus and Context Visualizations	[20]	○	○	○	○	○	○	○	○	○	●	○	○	●	○	○	○	○
The web interface TransparencyVis	[21]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
A visual uncertainty model	[22]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Sharing Data Using Differential Privacy	[23]	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○
Insider Threat Visualization Product	[24]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○
User Behavior Map	[25]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Android Malicious Flow Visualization Toolbox	[26]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Android Malware Familial Classification method	[27]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
STARLORD	[28]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
PCA an GCPA Methodology	[29]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Network Data Curation Toolkit (NDCT)	[30]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Hyperion	[31]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
Trogdor (Yuen and Turnbull)	[32]	○	●	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.)	[33]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
HSViz	[34]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
PERCIVAL	[35]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●
SDN Data Analysis Tool	[36]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Ocelot	[37]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Method and Tool to Visualize Network Traffic	[38]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Bigfoot	[39]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
CyberPetri	[40]	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
Web Download Analysis Tool	[41]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
ADVERS ARIAL PLAYGROUND (Norton and Qi)	[42]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
IMap	[43]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Zone-based vulnerability visualization	[44]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
CVSS score Vulnerability scanning tool	[45]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
MITRE ATT&CK Matrix	[46]	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○
Guidelines for Cybersecurity Visualization Design	[47]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
Cybersecurity Awareness on IoT context	[48]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
CRUMBS	[49]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○
V3SPA	[50]	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○

Figure 5.6 *evaluation-methodolgy used in each research paper*

6 Results

The papers that were evaluated were also divided into different categories. These categories were formed after skimming through all the papers included in analysis carefully. The reason of making these categories was to have an insight about which type of tools,methods and frameworks are being used in today's world. The categories will be able to help future analysis in the field too. Below is a taxonomy for categories.

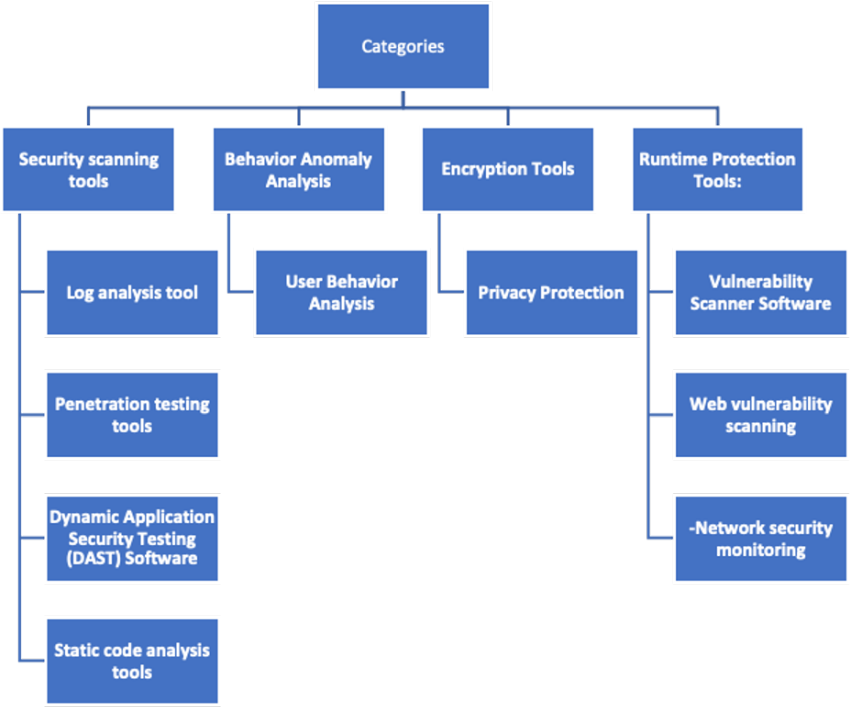
Categories
Security scanning tools
Behavior Anomaly Analysis
Encryption Tools
Runtime Protection Tools:
Log analysis tool
Penetration testing tools
Dynamic Application Security Testing (DAST) Software
Static code analysis tools
User Behavior Analysis
Privacy Protection
Vulnerability Scanner Software
Web vulnerability scanning
-Network security monitoring

***Figure* 6.1** *Taxonomy of categories*

All the research paper were later categorized in four main categories such as:

- Security Scanning Tools
- Behavior Anomaly Analysis
- Encryption Tools

- Runtime Protection Tools

6.1 Security scanning tools

Vulnerability scanning can encompass various activities, but it is commonly defined as the process of assessing the security of a website, web-based software, network, or file system to identify potential weaknesses or unauthorized file alterations. The analysis showed that there are in total 22 research papers in the analysis that belonged to this category. This category can be divided into sub categories as well such as:

1. **Static code analysis tools**
   These type of tools examine the code of Software, while it is not being executed as a whole. This has in total 5 papers in this sub category.

   - Provence-driven Automated Security Board (Schreiber et al., 2021) [39]
   - An interactive visualization system for developers (Reynolds et a., 2021) [38]
   - VulnEx (Dennig, Cakmak, Plate and Keim, 2021) [20]
   - Android Malicious Flow Visualization Toolbox (Santhanam et al.) [20]
   - Android Malware Familial Classification method (Fang et al.) [21]

2. **Log analysis tool**
   Extract meaningful data from logs to help users find trends and patterns for quick analysis and investigations. This has in total 6 papers in this sub category.

   - Automatic Narrative Summarization (Gove, 2021) [24]
   - File System Metadata Analysis Tool (Beran et al., 2020) [12]
   - STARLORD (Leichtnam et al.) [31]
   - PCA an GCPA Methodology (Theron and Magan-Carrion) [47]
   - Network Data Curation Toolkit (NDCT) (Acosta et al.) [2]
   - Hyperion (Yoo et al.) [50]

3. **Penetration testing tools**
   Tools/methods/frameworks are used to check network or system security threats and present graphical analysis to improve testing efficiency and discovery of issues. This has in total 6 papers in this sub category.

   - A Visual Analytics Framework for Adversarial Text Generation (Laughlin et al., 2019) [29]
   - Malware Battle Visualization (Chaffey and Sgandurra, 2020) [15]
   - Eventpad (Cappers et al., 2018) [14]
   - Trogdor (Yuen and Turnbull) [37]
   - An eight-step cyber threat intelligence framework and timeline visualization tool (Amaro et al.) [4]
   - HSViz (Lee et al.) [30]

4. **Dynamic Application Security Testing (DAST) Software**
   Checks whether the a software system is vulnerable, by simulation of attacks towards it. This has in total 5 papers in this sub category.

   - Intrusion Alert-driven Attack Graph Extractor (Nadeem et al., 2021) [32]
   - Interpretable Visualizations of Deep Neural Networks (Becker et al.,2021) [11]
   - Image-based Malware Classification (O'Shaughnessy, 2019) [34]
   - PERCIVAL (Angelini et al., "PERCIVAL") [5]
   - SDN Data Analysis Tool (Post et al.) [36]

6.2 Behavior Anomaly Analysis

There are in total 5 papers that were in this category. This category also has a sub category:

1. **User Behavior Analysis** Automated tools that aid understanding user behavior by monitoring activities on websites and applications to provide insights for improving security.

- Insider Threat Visualization Product(Graham et al., 2021) [25]
- User Behavior Map (Chen et al., 2018) [16]
- MITRE ATTaCK Matrix (Franklin et al.) [23]
- Guidelines for Cybersecurity Visualization Design (Seong et al.) [41]
- Cybersecurity Awareness on IoT context (Corallo et al.) [17]

6.3 Encryption Tools

There are in total 3 papers in this category. It also has a sub category:

1. **Privacy Protection** Framework/Method/Tool used to automate the classification of private data and avoid release to third parties.

    - The web interface TransparencyVis (Schufrin et al., 2020) [40]
    - A visual uncertainty model (Dasgupta et al., 2019) [19]
    - Sharing Data Using Differential Privacy (Pankova et al., 2021) [28]

6.4 Runtime Protection Tools

There are in total 19 papers in this category.

1. **Network security monitoring** Tools/Framework/Method designed to catch anomalous behaviors missed by security systems on the computer network and analyze indicators of potential security threats. There are in total 8 papers in this sub category.

    - NetCapVis (Ulmer et al., 2019) [48]
    - Interactive Three-Dimensional Visualization of Network Intrusion (Zong et al., 2020) [51]
    - Anomalous IP-Block Behavior Using Geo-IP Data (Ulmer et al., 2018) [49]
    - The RiskID application (Guerra et al., 2019) [26]
    - Ocelot (Arendt et al, “Ocelot”) [9]
    - Method and Tool to Visualize Network Traffic (Aupetit et al.) [10]

  - Bigfoot (Syamkumar et al.) [46]
  - CyberPetri (Arendt et al., “CyberPetri”) [8]

2. **Web vulnerability scanning** Automated tools that scan web applications to identify security vulnerabilities and present them in a graphical format. There are in total 6 papers in this sub category.

   - AI Total – a web-based visualization system (Sopan and Berlin, 2021) [43]
   - Wikipedia behavior analysis tool (Subramanian et al., 2019) [45]
   - Web Download Analysis Tool (Angelini et al., “The Goods”) [7]
   - ADVERSARIAL PLAYGROUND (Norton and Qi) [33]
   - IMap (Fowler et al.) [22]

3. **Vulnerability Scanner Software** Automated tools that allow the detection of vulnerabilities in applications by analyzing code bugs, inspecting potential exploit areas, and classifying system weaknesses. There are in total 5 papers in this sub category.

   - BUCEPHALUS (Angelini et al., 2021) [6]
   - Visual Decision Support for Live Digital Forensics (Bohm et al., 2021) [13]
   - Focus and Context Visualizations (Alperin et al., 2020) [3]
   - Zone-based vulnerability visualization (Watson and Lipford) [1]
   - CVSS score Vulnerability scanning tool (Painter) [35]

7 Discussion

The primary research question initially posed in this study was, ’What are the methods, tools, and frameworks in contemporary use?’ To enhance clarity and comprehensiveness, this question was subsequently deconstructed into sub-parts.

Firstly, it was imperative to establish the definitions of ’methods,’ ’tools,’ and ’frameworks.’ ’Tools’ were defined as specific devices or implementations designed for the execution of particular functions. ’Methods’ were characterized as procedural approaches or sets of guidelines utilized to address specific situations, while ’frameworks’ were identified as fundamental structural underpinnings.

The latter component of the question revolved around identifying the types of tools, methods, and frameworks prevalent in the field of cybersecurity. To address this inquiry, a comprehensive table was compiled, incorporating data from 50 recent research papers. These papers were predominantly sourced from contemporary conferences, chosen to isolate and elucidate the most current tools, methods, and frameworks within the realm of cybersecurity visualization.

The second research question posed was, ’What is the analysis or evaluation of these tools, methods, and frameworks?’ This question, too, was subdivided into two distinct facets for in-depth exploration. The first facet aimed to identify the most prevalent types of tools, methods, and frameworks. This analysis was undertaken by revisiting the previously mentioned table, generated following the scrutiny of 50 research papers. This table facilitated the identification of tools, methods, or frameworks recurrently featured across multiple papers.

The second facet of this research question centered on the classification of tools, methods, and frameworks. To address this aspect, a comprehensive table was crafted, cataloging the major categories and subcategories within the diverse array of research papers considered in the analysis. This categorization facilitated the systematic classification of papers according to their respective criteria.

8 Conclusion

Cybersecurity visualization is a sprawling domain replete with a myriad of tools, methods, and frameworks. This thesis undertakes a theoretical investigation within the confines of its title, focusing on the analysis of tools, methods, and frameworks in the contemporary landscape.

The thesis is structured into five principal sections: Introduction, Background, Analysis/Results, Discussion, and Conclusion.

This research paper offers a comprehensive examination of contemporary visualization techniques, evaluation methodologies, and the delineation of target user demographics.

The intention is to furnish developers with insights into the existing landscape of cybersecurity visualization, identifying areas where tools may be lacking and highlighting opportunities for the creation of new tools. Such endeavors are expected to enhance our understanding of cybersecurity threats and fortify defense mechanisms.

Bibliography

[1] "A Proposed Visualization for Vulnerability Scan Data". In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, July 2017. URL: `https://www.usenix.org/conference/soups2017/workshop-program/wsiw2017/watson`.

[2] Jaime Acosta et al. "Network Data Curation Toolkit: Cybersecurity Data Collection, Aided-Labeling, and Rule Generation". In: Nov. 2021, pp. 849–854. DOI: `10.1109/MILCOM52596.2021.9653049`.

[3] Kenneth Alperin, Allan Wollaber, and Steven Gomez. "Improving Interpretability for Cyber Vulnerability Assessment Using Focus and Context Visualizations". In: Oct. 2020, pp. 30–39. DOI: `10.1109/VizSec51108.2020.00011`.

[4] Lucas Amaro et al. "Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data". In: *Applied Sciences* 12 (Jan. 2022), p. 1205. DOI: `10.3390/app12031205`.

[5] Marco Angelini, Nicolas Prigent, and Giuseppe Santucci. "PERCIVAL: Proactive and rEactive attack and Response assessment for Cyber Incidents using Visual AnaLytics". In: Oct. 2015. DOI: `10.1109/VIZSEC.2015.7312764`.

[6] Marco Angelini et al. "BUCEPHALUS: a BUsiness CEntric cybersecurity Platform for proActive anaLysis Using visual analyticS". In: *2021 IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2021, pp. 15–25. DOI: `10.1109/VizSec53666.2021.00007`.

[7] Marco Angelini et al. "The Goods, the Bads and the Uglies: Supporting Decisions in Malware Detection through Visual Analytics". In: Oct. 2017. DOI: `10.1109/VIZSEC.2017.8062199`.

[8] Dustin Arendt et al. "CyberPetri at CDX 2016: Real-time network situation awareness". In: Oct. 2016, pp. 1–4. DOI: `10.1109/VIZSEC.2016.7739584`.

[9] Dustin Arendt et al. "Ocelot: User-Centered Design of a Decision Support Visualization for Network Quarantine". In: Oct. 2015. DOI: `10.1109/VIZSEC.2015.7312763`.

[10] Michael Aupetit et al. "Visualization of actionable knowledge to mitigate DRDoS attacks". In: Oct. 2016, pp. 1–8. DOI: 10.1109/VIZSEC.2016.7739577.

[11] Becker et al. *Becker, Franziska.* Jan. 1970. URL: https://publications.rwth-aachen.de/record/813881.

[12] Michal Beran et al. "Exploratory Analysis of File System Metadata for Rapid Investigation of Security Incidents". In: Oct. 2020, pp. 11–20. DOI: 10.1109/VizSec51108.2020.00008.

[13] Fabian Böhm et al. "Visual Decision-Support for Live Digital Forensics". In: *2021 IEEE Symposium on Visualization for Cyber Security (VizSec).* 2021, pp. 58–67. DOI: 10.1109/VizSec53666.2021.00012.

[14] Bram C.M. Cappers et al. "Eventpad: Rapid Malware Analysis and Reverse Engineering using Visual Analytics". In: *2018 IEEE Symposium on Visualization for Cyber Security (VizSec).* 2018, pp. 1–8. DOI: 10.1109/VIZSEC.2018.8709230.

[15] Emily J. Chaffey and Daniele Sgandurra. "Malware vs Anti-Malware Battle - Gotta Evade 'em All!" In: *2020 IEEE Symposium on Visualization for Cyber Security (VizSec).* 2020, pp. 40–44. DOI: 10.1109/VizSec51108.2020.00012.

[16] Siming Chen et al. "User Behavior Map: Visual Exploration for Cyber Security Session Data". In: *2018 IEEE Symposium on Visualization for Cyber Security (VizSec).* 2018, pp. 1–4. DOI: 10.1109/VIZSEC.2018.8709223.

[17] Angelo Corallo et al. "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review". In: *Computers in Industry* 137 (Jan. 2022), pp. 1–16. DOI: 10.1016/j.compind.2022.103614.

[18] R. Jordan Crouser, Erina Fukuda, and Subashini Sridhar. "Retrospective on a decade of research in visualization for cybersecurity". In: *2017 IEEE International Symposium on Technologies for Homeland Security (HST).* 2017, pp. 1–5. DOI: 10.1109/THS.2017.7943494.

[19] Aritra Dasgupta, Robert Kosara, and Min Chen. “Guess Me If You Can: A Visual Uncertainty Model for Transparent Evaluation of Disclosure Risks in Privacy-Preserving Data Visualization”. In: Aug. 2019. DOI: 10.1109/VizSec48167.2019.9161608.

[20] Frederik Dennig et al. “VulnEx: Exploring Open-Source Software Vulnerabilities in Large Development Organizations to Understand Risk Exposure”. In: Oct. 2021, pp. 79–83. DOI: 10.1109/VizSec53666.2021.00014.

[21] Yong Fang et al. “Android Malware Familial Classification Based on DEX File Section Features”. In: *IEEE Access* PP (Jan. 2020), pp. 1–1. DOI: 10.1109/ACCESS.2020.2965646.

[22] J. Fowler et al. “IMap: Visualizing network activity over internet maps”. In: Nov. 2014, pp. 80–87. DOI: 10.1145/2671491.2671501.

[23] Lyndsey Franklin et al. “Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design”. In: *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2017, pp. 1–8. DOI: 10.1109/VIZSEC.2017.8062200.

[24] Robert Gove. “Automatic Narrative Summarization for Visualizing Cyber Security Logs and Incident Reports”. In: Oct. 2021, pp. 1–9. DOI: 10.1109/VizSec53666.2021.00005.

[25] Martin Graham et al. “Developing Visualisations to Enhance an Insider Threat Product: A Case Study”. In: Oct. 2021, pp. 47–57. DOI: 10.1109/VizSec53666.2021.00011.

[26] Jorge Guerra, Eduardo Veas, and Carlos Catania. “A Study on Labeling Network Hostile Behavior with Intelligent Interactive Tools”. In: Oct. 2019, pp. 1–10. DOI: 10.1109/VizSec48167.2019.9161489.

[27] L. Jiang et al. “Systematic Literature Review on Cyber Situational Awareness Visualizations”. In: *IEEE Access* 10 (2022). DOI: 10.1109/ACCESS.2022.3147227.

[28] Mark F. St. John et al. “Decision Support for Sharing Data using Differential Privacy”. In: *2021 IEEE Symposium on Visualization for Cyber Security (VizSec)*. 2021, pp. 26–35. DOI: 10.1109/VizSec53666.2021.00008.

[29] Brandon Laughlin et al. "A Visual Analytics Framework for Adversarial Text Generation". In: *2019 IEEE Symposium on Visualization for Cyber Security (VizSec)* (2019), pp. 1–10.

[30] Hyunjung Lee et al. "HSViz: Hierarchy Simplified Visualizations for Firewall Policy Analysis". In: *IEEE Access* PP (May 2021), pp. 1–1. DOI: 10.1109/ACCESS.2021.3077146.

[31] Laetitia Leichtnam et al. "STARLORD: Linked security data exploration in a 3D graph". In: Oct. 2017, pp. 1–4. DOI: 10.1109/VIZSEC.2017.8062203.

[32] Azqa Nadeem et al. *SAGE: Intrusion Alert-driven Attack Graph Extractor.* Aug. 2021.

[33] Andrew Norton and Yanjun Qi. "Adversarial-Playground: A Visualization Suite for Adversarial Sample Generation". In: (June 2017).

[34] Stephen O'Shaughnessy and Stephen Sheridan. "Image-Based Malware Classification Hybrid Framework Based on Space-Filling Curves". In: *Comput. Secur.* 116.C (May 2022). ISSN: 0167-4048. DOI: 10.1016/j.cose.2022.102660. URL: https://doi.org/10.1016/j.cose.2022.102660.

[35] Ryan Painter. "Targeted Data Visualization and Reporting Approaches for Vulnerability Management at Enterprise Organizations". In: Nov. 2021.

[36] Tobias Post et al. "Visually guided flow tracking in software-defined networking". In: Oct. 2016, pp. 1–4. DOI: 10.1109/VIZSEC.2016.7739586.

[37] Suneel Randhawa et al. "Mission-Centric Automated Cyber Red Teaming". In: Aug. 2018, pp. 1–11. DOI: 10.1145/3230833.3234688.

[38] Steven Lamarr Reynolds et al. "User-Centered Design of Visualizations for Software Vulnerability Reports". In: *2021 IEEE Symposium on Visualization for Cyber Security (VizSec).* 2021, pp. 68–78. DOI: 10.1109/VizSec53666.2021.00013.

[39] Andreas Schreiber, Tim Sonnekalb, and Lynn Kurnatowski. "Towards Visual Analytics Dashboards for Provenance-driven Static Application Security Testing". In: Oct. 2021, pp. 42–46. DOI: 10.1109/VizSec53666.2021.00010.

[40] Marija Schufrin et al. “A Visualization Interface to Improve the Transparency of Collected Personal Data on the Internet”. In: *IEEE Transactions on Visualization and Computer Graphics* PP (Nov. 2020), pp. 1–1. DOI: 10.1109/TVCG.2020.3028946.

[41] Younho Seong, Joseph Nuamah, and Sun Yi. “Guidelines for cybersecurity visualization design”. In: Aug. 2020, pp. 1–6. DOI: 10.1145/3410566.3410606.

[42] Hadi Shiravi, Ali Shiravi, and Ali A. Ghorbani. “A Survey of Visualization Systems for Network Security”. In: *IEEE Transactions on Visualization and Computer Graphics* 18.8 (2012), pp. 1313–1329. DOI: 10.1109/TVCG.2011.144.

[43] Awalin Sopan and Konstantin Berlin. “AI Total: Analyzing Security ML Models with Imperfect Data in Production”. In: Oct. 2021.

[44] Diane Staheli et al. “Visualization Evaluation for Cyber Security: Trends and Future Directions”. In: *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*. 2014, pp. 49–56. DOI: 10.1145/2671491.2671492.

[45] Siva Subramanian et al. “Explainable Visualization of Collaborative Vandal Behaviors in Wikipedia”. In: Oct. 2019, pp. 1–5. DOI: 10.1109/VizSec48167.2019.9161504.

[46] Meenakshi Syamkumar, Ramakrishnan Durairajan, and Paul Barford. “Bigfoot: A geo-based visualization methodology for detecting BGP threats”. In: Oct. 2016, pp. 1–8. DOI: 10.1109/VIZSEC.2016.7739583.

[47] Roberto Therón et al. “Network-wide intrusion detection supported by multivariate analysis and interactive visualization”. In: Oct. 2017, pp. 1–8. DOI: 10.1109/VIZSEC.2017.8062198.

[48] Alex Ulmer, David Sessler, and Jorn Kohlhammer. “NetCapVis: Web-based Progressive Visual Analytics for Network Packet Captures”. In: Oct. 2019, pp. 1–10. DOI: 10.1109/VizSec48167.2019.9161633.

[49] Alex Ulmer et al. “Visual-Interactive Identification of Anomalous IP-Block Behavior Using Geo-IP Data”. In: Oct. 2018, pp. 1–8. DOI: 10.1109/VIZSEC.2018.8709182.

[50] Seunghoon Yoo et al. “Hyperion: A Visual Analytics Tool for an Intrusion Detection and Prevention System”. In: *IEEE Access* PP (July 2020), pp. 1–1. DOI: 10.1109/ACCESS.2020.3010789.

[51] Wei Zong, Yang-Wai Chow, and Willy Susilo. “Interactive three-dimensional visualization of network intrusion detection data for machine learning”. In: *Future Generation Computer Systems* 102 (Aug. 2019). DOI: 10.1016/j.future.2019.07.045.