UNIVERSITY OF SOUTHAMPTON

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES

School of Electronics and Computer Science

***EEVi*: A Model Developed to Aid the Design and Evaluation Process of Cyber-Security Visualisation for Cyber-Security Analysts**

by

Aneesha Sethi

Thesis for the degree of Doctor of Philosophy

June 2019

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES
School of Electronics and Computer Science

Doctor of Philosophy

EEVI: A MODEL DEVELOPED TO AID THE DESIGN AND EVALUATION PROCESS OF CYBER-SECURITY VISUALISATION FOR CYBER-SECURITY ANALYSTS

by Aneesha Sethi

The area of visualisation in cyber-security is advancing quickly. At present, there are no standardised guidelines for designing and evaluating visualisations. There is limited end-user involvement in the design process, which leads to visualisations that are generic and often ineffective for cyber-security analysts. This contributes to low adoption of the resulting cyber-security visualisation solutions, highlighting a major research need. This research presents ***EEVi*** (**E**ffective **E**xecution of **Vi**sualisation), a model developed to aid in the design and evaluation of cyber-security visualisations for cyber-security analysts. 'Thematic Analysis', a qualitative data analysis technique, was used to develop *EEVi*. 13 experts were interviewed (seven cyber-security analysts and six visualisation designers) to validate this model. Their feedback guided revisions to the model and was subsequently used to perform statistical analyses. This demonstrated that there were no statistically significant differences between visualisation designers and cyber-security analysts. Neither was there statistically significant agreement. The individual responses led to modification of the component tasks of the model. The modified model was confirmed by 30 respondents, primarily from cyber-security, through an online questionnaire. This confirmed the model's relevance, and validity, guiding the revision of the component tasks. The confirmed model, were used to create a work-domain analysis (abstraction hierarchy) diagram and mockups to demonstrate a possible real-world utilisation of *EEVi*. These were evaluated by 10 experts (five cyber-security analysts and five visualisation designers) and their feedback validated the notion that, with a common structure the disparity of understanding between cyber-security analysts and visualisation designers can be minimised. The questionnaire responses were also used to formulate a quantitative value calculator called *C-EEVi* (Calculator for *EEVi*) using the 'Analytical Hierarchy Process'. *C-EEVi* can be used to score cyber-security visualisation solutions for a performed task.

This work has developed a model, *EEVi*, to help design cyber-security visualisations for cyber-security analysts to perform a specific task. The abstraction hierarchy diagram of *EEVi* provides a basis for communication between cyber-security analysts and visualisation designers. Lastly, *C-EEVi* evaluates cyber-security visualisation solutions for a task, by allocating them a quantitative value score. These address the major research gaps identified in this thesis.

Contents

List of Figures

List of Tables

Declaration of Authorship

I, Aneesha Sethi, declare that the thesis entitled *EEVi: A Model Developed to Aid the Design and Evaluation Process of Cyber-Security Visualisation for Cyber-Security Analysts* and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a research degree at this University;
- where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- parts of this work have been published as: (Sethi, Paci, & Wills, 2016a), (Sethi, Paci, & Wills, 2016b) and (Sethi & Wills, 2017)

Signed:...

Date:..

Acknowledgements

I would like to express my deepest gratitude to **Prof. Gary Wills** - my supervisor - for his relentless support, useful advice and encouraging meetings. With the oversight of my main supervisor, editorial advice has been sought. No changes of intellectual content were made as a result of this advice.

I also want to thank my family, friends and colleagues, especially my parents, who have constantly supported me in all my endeavours. They have always motivated me to strive for the best with their constant encouragement and friendly advice.

I want to dedicate this thesis to my parents, **Gopika and Rohit Sethi**, and my dog, **Taurus**, for their role in making me the person I am today.

I would also like to dedicate this thesis to my grandparents, **Sudesh and Baldev Raj Sethi**, and **Neena and Lalit Kumar Kohli**.

Finally, this thesis would not have been possible without my support system in Southampton and New Delhi. A big thank you to – Daniel Fay, Paul Nicholas, Dr. Aneesha Haryal, Ricardo De La Garza-Cano, Elena Demarchou, Lauren Johnstone, Anna Hurley-Wallace, Sunayana Sahni, Alankrita Narang, Saanya Ashra, Gabriella Schneider, Nikita Karra, Nikitta Shepherd, Iris Kramer, Robert Chan Seem, Madelene Orderud, Elise Rasmussen, Iren Nuthaya Engan, Dr. Nawfal Al Hashimy, Jo C Axtell, Osheen Jain, Malevi Chyrstostomou, Antigoni Kritioti, Dr. Enrique Marquez, Eryx Paredes, Dr. Shre Chatterjee, Supriya Ambwani and Dr. Vanissa Wanick.

Chapter 1

Introduction

1.1 Research Context

In the field of cyber-security, cyber attacks and threats are increasing day-by-day and so is the dependence of people on cyber-networks. According to a survey by United Kingdom's Department for Digital, Culture, Media and Sport (2018), 56% of businesses and 44% of charities hold personal data electronically. Of these, 47% of businesses and 30% of charities have identified at least one cyber-security breach or attack. The survey also found that cyber-security is a high priority for senior management for 74% of businesses and 53% of charities. Both public and private sectors rely on the expertise of cyber-security analysts to protect their assets and resources connected across cyber-networks.

Investment in cyber-security is growing[1] as data becomes one of the most important and vulnerable of resources. In May 2018, Forbes[2] reported that 90% of the data in the world had been generated in the previous two years by more than 3.7 billion internet users. This enormous quantity of data, quoted as 2.5 quintillion bytes, is bound to contain much private and sensitive information, creating an impetus to protect it. In November 2016, the UK government announced £1.9 billion funding for cyber-security for 2016–2021[3]. The World Economic Forum (2018)'s Global Risks Report estimated the cost of cybercrime to businesses over the next five years to be US$8 trillion (∼£6.3 trillion). World Economic Forum (2019)'s Global Risks Report warns of an increase in data fraud and disruption to operations by cyber-attacks this year. The United Kingdom's Department of Health and Social Care published a review of the 2017 cyber-attack on the National Health Service, which affected patient

[1] http://fortune.com/2015/09/23/cyber-security-investing/ [Accessed: 5 May, 2017]

[2] https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5556a76c60ba [Accessed: 8 March, 2019]

[3] https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy [Accessed: 5 May, 2017]

healthcare (Smart, 2018). This highlights the inherent dependence of critical infrastructure on the IT that underpins modern society, making a proactive, rather than a reactive, approach to cyber-security of paramount importance.

1.1.1 Cyber-Security Visualisation

One area within cyber-security is that of cyber-security visualisation, which provides cyber-security analysts with visual data rather than textual data. It represents an opportunity for developing solutions (Fink, North, Endert, & Rose, 2009) that help detect, monitor and mitigate technical and social attacks in a timely manner. However, these solutions focus on the technological aspects of the tools rather than considering the critical roles played by people that affect cyber operations (Vieane et al., 2016). Some industries are turning towards cyber-security analysts to mitigate the cyber threats, as automated defences are not seen as adequate protection in isolation (Gutzwiller, Hunt, & Lange, 2016), due to the increasing scope and criticality of attacks in new and creative ways. This makes it important to provide cyber-security analysts with efficient cyber defence solutions against potential cyber attacks. Investment in cyber-security visualisation solutions are increasing as well; in January 2017, IBM acquired Agile3 for an unspecified amount, a cyber-security visualisation solution, to be integrated with its own data security services[4].

1.2 Research Rationale

Cyber-security visualisation solutions are being intensively researched (Adams & Snider, 2018), but the solutions being developed are rarely evaluated against the task they aid in performing (Staheli et al., 2014). Moreover, most such visualisations have been developed, and sometimes evaluated, without any involvement of end-users. This has led to a low rate of adoption of such tools (Best, Endert, & Kidwell, 2014). In April 2015, The Wall Street Journal[5] claimed that only 15% of cyber-security analysts are using cyber-security visualisations to help with their analyses. The interview with Shawn Wiora[6] revealed that cyber-security visualisations have not caught up with the fast-growing field of cyber-security, and still reflect the 1990s.

The biggest challenge is the lack of user involvement in the design and evaluation of cyber-security visualisation solutions, which has led to the low adoption rate. Visualisation designers often focus on Human-Computer Interaction (HCI) elements such as dashboards or widgets, rather than trying to understand the tasks performed

[4] http://fortune.com/2017/01/23/ibm-cybersecurity-agile-3-acquisition/ [Accessed: 5 May, 2017]

[5] https://blogs.wsj.com/cio/2015/04/20/security-professionals-stymied-by-outdated-visualization-tools/ [Accessed: 5 May, 2017]

[6] Chief information officer and chief information security officer at Creative Solutions in Healthcare

by cyber-security analysts and building for them (Shiravi, Shiravi, & Ghorbani, 2012; Zhao, Tang, Zou, Wang, & Zu, 2019). These solutions do not always present the characteristics of visualisations that would be the most beneficial for the job required. Visualisation designers also do not understand the application environment or the needs of the cyber-security analysts (Adams & Snider, 2018; Gates & Engle, 2013). The lack of user involvement is often limited to having restricted, or even no, access to cyber-security experts (Mckenna, Staheli, & Meyer, 2015).

Guidelines for understanding the requirements of the task, which could lead to effective visualisation, have not been widely researched and is a limitation of the field (Staheli et al., 2014). Another limitation arises from the lack of a standardised evaluation technique for cyber-security visualisations. As a result, guidelines aiding the design process including the requirements of cyber-security analysts would be an immensely useful resource for this field, and a common model to evaluate these cyber-security visualisation solutions, keeping the end-user's requirements in mind.

1.3 Research Questions

The aims of this research are to address research gaps in the literature, around how to design visualisation for cyber-security analysts for a given task. This research aims to answer the following questions:

RQ_1 *What suitable method would help design cyber-security visualisation solutions for cyber-security analysts for a given task?*

SRQ_1 *What is an appropriate model to help visualisation designers create cyber-security visualisation solutions for cyber-security analysts?*

SRQ_2 *What are the characteristics that enable visualisation to support a cyber-security analyst in performing a given task?*

RQ_2 *What instrument can be used to promote communication between cyber-security analysts and visualisation designers who build cyber-security visualisations?*

RQ_3 *What quantitative metrics can be proposed that will score cyber-security visualisation solutions?*

These research questions led to the identification of the following objectives:

- Develop a model that can be used for designing cyber-security visualisation solutions for a performed task;
- Develop guidelines stating which characteristics of visualisation aid in performing which tasks;

- Investigate the existence of disparity of domain-knowledge between cyber-security analysts and visualisation designers;
- Identify an instrument that could alleviate this disparity, if it exists;
- Propose a quantitative measure that can be used to score cyber-security visualisation solutions.

1.4 Thesis Structure

This thesis consists of eight chapters with eight appendixes. A diagrammatic representation of the research plan followed is presented in Figure 1.1. The chapters, as follows, are laid out to facilitate the research plan.

Chapter 2 reviews the literature on visualisation and on cyber-security. This is followed by an overview of cyber-security visualisation and the current solutions. It discusses the challenges of designing and evaluating cyber-security visualisations. The chapter demonstrates the requirement, and the gap for a design and evaluation model for cyber-security visualisation.

Chapter 3 presents the research for developing *EEVi*, a model to help design cyber-security visualisations. The chapter discusses the techniques used in the development of *EEVi* followed by an overview of the 'Thematic Analysis' and how it led to structure of the model. The constituent component tasks and their development process, are reviewed.

Chapter 4 presents the process of expert-review used to validate the model. The chapter discusses the techniques used, followed by the arrangements for the expert-review and the demographics of the experts. The results of the review are given and a revised version of *EEVi* examined. Statistical analyses address the responses of the experts.

Chapter 5 presents the questionnaire results and findings used to confirm the model. The background of the technique used is discussed, followed by the arrangements for the questionnaire. The results are addressed, which led to confirmation of the *EEVi* and revision of its component tasks.

Chapter 6 presents the work domain analysis (abstraction hierarchy) diagrams, user interface mockups and the interview findings used to determine the real world utilisation of *EEVi*. The techniques used are discussed, followed by the arrangements for and findings from the interviews, confirming the real world utilisation of *EEVi* through work domain analysis diagrams or user interface mockups. The work domain analysis diagrams for all the component tasks of *EEVi* are also illustrated.

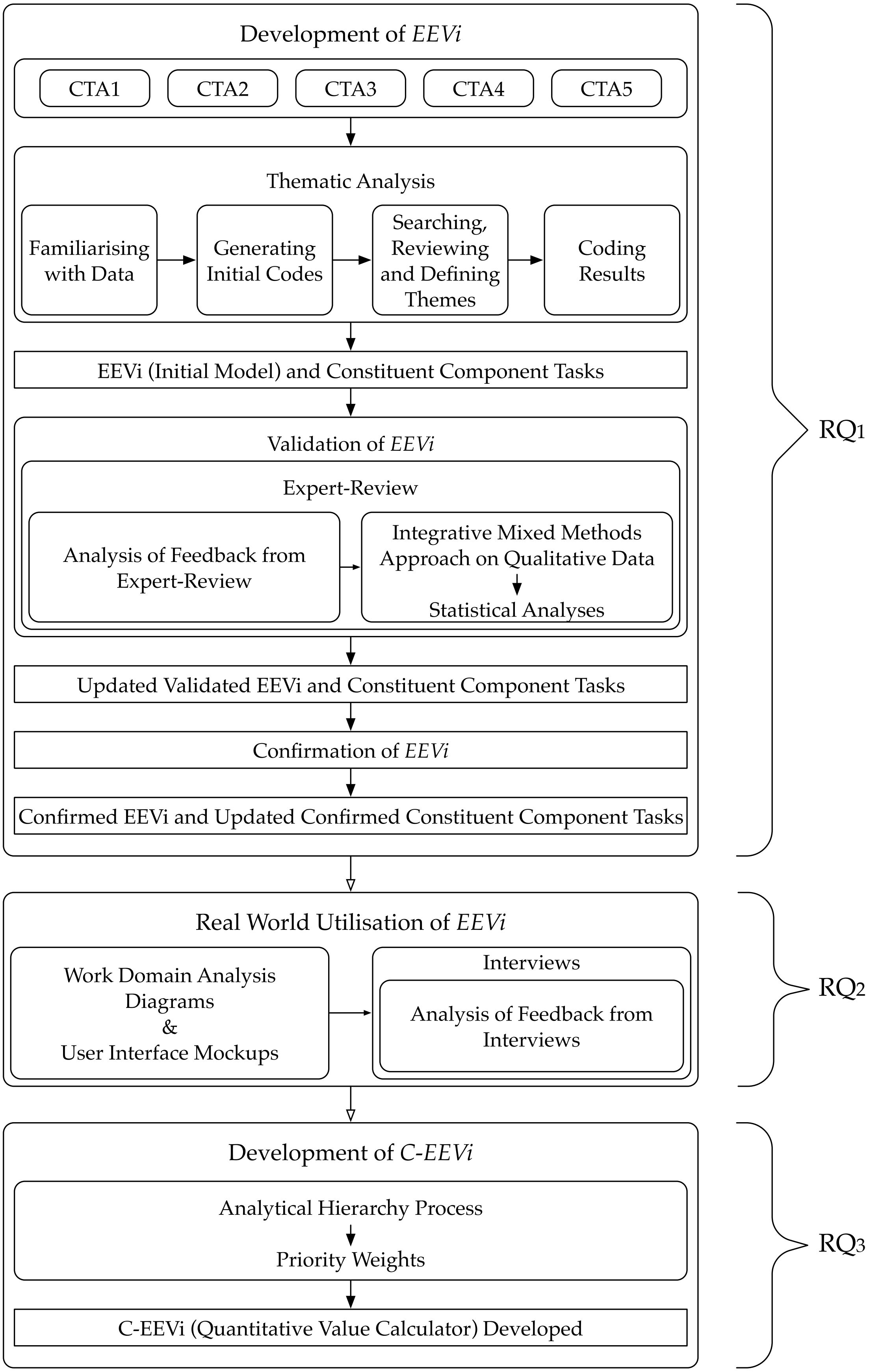

Development of *EEVi*
CTA1
CTA2
CTA3
CTA4
CTA5
Thematic Analysis
Familiarising with Data
Generating Initial Codes
Searching, Reviewing and Defining Themes
Coding Results
EEVi (Initial Model) and Constituent Component Tasks
Validation of *EEVi*
Expert-Review
Analysis of Feedback from Expert-Review
Integrative Mixed Methods Approach on Qualitative Data
Statistical Analyses
Updated Validated EEVi and Constituent Component Tasks
Confirmation of *EEVi*
Confirmed EEVi and Updated Confirmed Constituent Component Tasks
RQ1
Real World Utilisation of *EEVi*
Work Domain Analysis Diagrams & User Interface Mockups
Interviews
Analysis of Feedback from Interviews
RQ2
Development of *C-EEVi*
Analytical Hierarchy Process
Priority Weights
C-EEVi (Quantitative Value Calculator) Developed
RQ3

Figure 1.1: Diagrammatic representation of the research plan followed in this thesis, following the development process and outputs for each research question.

Chapter 7 presents the development process of *C-EEVi*, and a quantitive value calculator for *EEVi*. The development process of priority weights for *C-EEVi* is discussed using the 'Analytical Hierarchy Process' with a running example. Finally, priority weights of all component tasks and wireframe examples of *C-EEVi* are presented.

Chapter 8 concludes this work with the contributions, limitations and recommendations for future work.

Appendix A presents the associations of all tasks with other codes, defined in Chapter 3.

Appendix B presents the documents which state the conditions on which ethical approval was received for the expert-review (Section 4.2.1), questionnaire (Section 5.2.1) and interviews (Section 6.2.1).

Appendix C presents the format of the semi-structured interviews conducted for the expert-review, in Chapter 4, for validation of *EEVi*.

Appendix D presents the format of the questionnaire used for the confirmation of *EEVi*, in Chapter 5.

Appendix E presents the results of the questionnaire in Chapter 5 for the ratings of characteristics of visualisation for each component task, on a Likert scale.

Appendix F presents the format of the semi-structured interviews conducted in Chapter 6, to determine the real-world utilisation of *EEVi*.

Appendix G presents the calculation of comparison matrices for each component task for development of *C-EEVi* in Chapter 7.

Appendix H presents the calculation of priority weights ratios for all component task used in the development of *C-EEVi* in Chapter 7.

Chapter 2

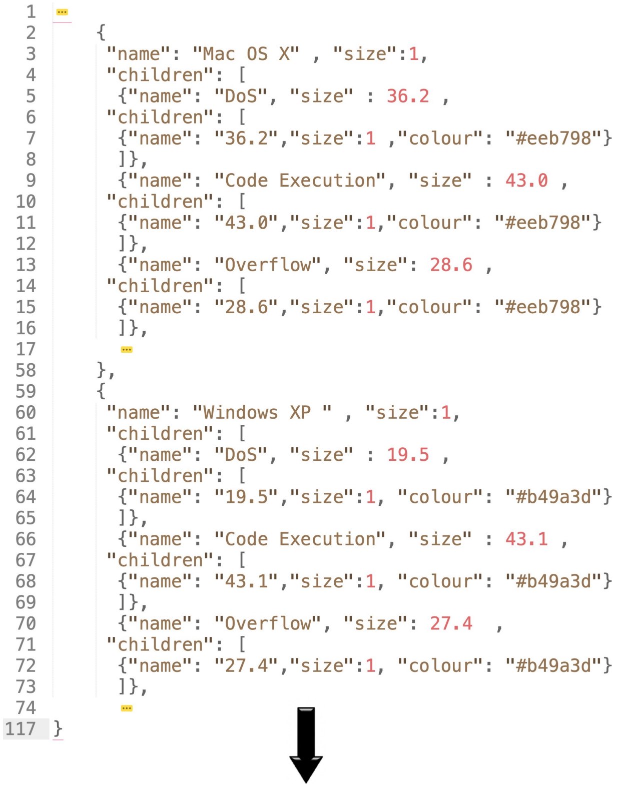
Literature Review

Visualisation theory is not a new science; many applications in the past have used visual analysis to reveal hidden patterns and improve understanding (Card, Mackinlay, & Shneiderman, 1999). However, its application to cyber-security and the challenges it faces are still being explored, as highlighted below. Cyber-security visualisation is an interdisciplinary field and a comprehensive understanding is founded in the two disciplines it arose from: visualisation and cyber-security. The review starts with an overview of these. Subsequently an analysis of the current cyber-security visualisation solutions will be presented, along with the challenges faced during the design and evaluation processes to identify research gaps.

2.1 Visualisation

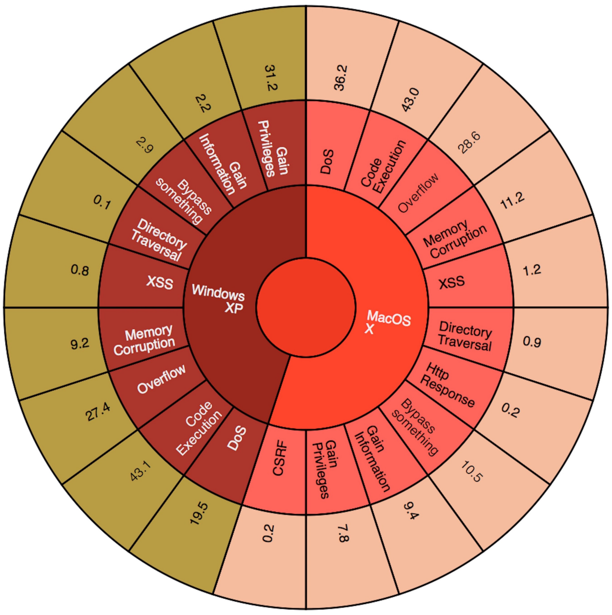
The field of visualisation can be generically defined as the communication of data through interactive computer-supported visual representation to enhance cognition (Card, 2012; Keim, Mansmann, Schneidewind, & Ziegler, 2006). Card (2012) argues that the purpose of visualisation should be to amplify cognition rather than just create pretty pictures, and would allow for a fast-paced medium to assimilate information in a world of data overload.

Visualisations are powerful tools that allow people to analyse, discover insights, extract meaning and communicate knowledge from data using their visual (eyes) and cognitive (brain) systems at a glance (Szafir, 2018). Visualisations present a high volume of visual information at a given time, which enhances the potential to uncover trends, patterns, gaps or outliers in data (Shneiderman, 1996). Ben Shneiderman (1996) also introduced the "Visual Information Seeking Mantra" that reveals the best way to gain insight from data is by starting from an overview, that can be filtered or zoomed in, providing more details on demand. This allows the user to view the full picture before digging in to the parts of the visualisation that look interesting (Marty, 2008). They also spark the viewers' interest and allow information to be assimilated easily and quickly (Figueiras, 2014).



```
…
  {
   "name": "Mac OS X" , "size":1,
   "children": [
    {"name": "DoS", "size" : 36.2 ,
   "children": [
    {"name": "36.2","size":1 ,"colour": "#eeb798"}
    ]},
    {"name": "Code Execution", "size" : 43.0 ,
   "children": [
    {"name": "43.0","size":1,"colour": "#eeb798"}
    ]},
    {"name": "Overflow", "size": 28.6 ,
   "children": [
    {"name": "28.6","size":1,"colour": "#eeb798"}
    ]},
     …
  },
  {
   "name": "Windows XP " , "size":1,
   "children": [
    {"name": "DoS", "size" : 19.5 ,
   "children": [
    {"name": "19.5","size":1, "colour": "#b49a3d"}
    ]},
    {"name": "Code Execution", "size" : 43.1 ,
   "children": [
    {"name": "43.1","size":1, "colour": "#b49a3d"}
    ]},
    {"name": "Overflow", "size": 27.4  ,
   "children": [
    {"name": "27.4","size":1, "colour": "#b49a3d"}
    ]},
     …
}
```

(a) Textual data



(b) Visualised presentation of textual data

Figure 2.1: Example of a visual presentation of textual data, showing the vulnerabilities and their risks for two operating systems (Sethi, 2015).

An example by Sethi (2015), demonstrating the use of visualisation, is presented in Figure 2.1. The figure shows vulnerabilities and risk in two operating systems: Windows XP[1] and MacOS X[2] in both textual and visual representations. The data, in Figure 2.1(a), was generated from CVE[3] and CVE Details[4] datasets into a JSON[5] file. The visual representation in Figure 2.1(b) is a zoomable sunburst diagram[6] made with D3.js[7]. It is difficult to assimilate the textual data in Figure 2.1(a) however, the visual representation (Figure 2.1(b)) presents a high value of information. At one glance of the visualisation, it appears that Windows XP has less risk to known vulnerabilities than MacOSX. On further examination, it appears that there are no known reported cases of CSRF[8] in Windows XP. The benefit of using visualisation over textual data becomes apparent in this example.

Visualisations offer a number of benefits. It is easier for a human brain to detect changes in size, colour, shape or movement than in textual representations of such data, as outlined by (Gatto, 2015; Gonzalez & Kobsa, 2003; Kemal, 2019; Marty, 2008; Ware, 2013). The benefits are that, visualisations:

- allow users to **answer questions** quickly and concisely, without wading through textual data. They can facilitate representation of theories, or hypotheses, which may or may not be clear from textual data. As a result, users can discover previously unknown relationships which enhances their understanding of the data;
- increase **accessibility** by providing comprehensible ways for users to absorb and process the abundance of available data. They also allow different audiences, especially non-technical ones, to assimilate and interpret complicated information;
- allow users to find emergent relationships, patterns or trends that were not anticipated, which could lead to **new questions and discoveries** in the data;
- can help with **quality control** as problems with data or previously assumed relationships become apparent immediately;
- support rich **investigations** that help detect hidden properties or new insights from the data, especially using interactivity;

[1] Windows XP is a personal computer operating system produced by Microsoft

[2] macOS X is a graphical operating systems developed and marketed by Apple Inc

[3] Common Vulnerabilities and Exposures contains a list of publicly known cyber-security vulnerabilities - https://cve.mitre.org [Accessed: 29 May, 2019]

[4] Provides an easy to use web interface to view vulnerability data from CVE - https://www.cvedetails.com [Accessed: 29 May, 2019]

[5] JavaScript Object Notation - https://www.json.org [Accessed: 29 May, 2019]

[6] Radial space-filling visualisation - https://www.jasondavies.com/coffee-wheel/ [Accessed 29 May, 2019]

[7] Data Driven Documentation is a JavaScript Library for visualisation - https://d3js.org [Accessed: 29 May, 2019]

[8] Cross-site request forgery is a known vulnerability where users are forced to execute unwanted actions unwittingly

- **support decision making** by improving the understanding of data. They can distil a large amount of data into meaningful visualisations that are easier to interpret and can support decisions made by users;
- **communicate** information by showing a complete picture of the data, through stories or graphical representations;
- **increase efficiency** as users spend less time wading through textual data, as it is easier to see trends or outliers in a visual presentation.

Visualisations enable problem-solving by improving human cognition through visual data exploration and analysis (Borland, Wang, Gotz, & Rhyne, 2018). They help convey a large amount of information by using engaging visual outputs (McInerny et al., 2014). Additionally, visualisation solutions are not just about the "passive act of displaying information" (Lugmayr, Stockleben, Scheib, & A. Mailaparampil, 2017) like charts or histograms, but the complete process of "conceptual representation ... [and making] ... data perceptible" (Lugmayr et al., 2017) inclusive of communication and actions that deliver more understanding and knowledge to the end-user.

Many data visualisation libraries and tools are available to use in creating generic visual (or graphical) representations of data that suit the users' exact requirements or use-cases. These libraries and tools can be used to create visualisations for any kind of data that is provided and related to any field.

Data visualisation libraries are dependent on the programming language, whereas data visualisation tools are dependent only on the platform. Some examples of these are presented in Table 2.1, along with their dependence (programming languages or platforms) and nature of visualisations that can be produced. Some can be used to create static data graphs whereas others can create stand-alone interactive or animated visualisations.

Data visualisation tools and libraries (Table 2.1) can be used to design generic or specific purpose visual (or graphical) representations of data. However, as with programming languages, they do not have any inbuilt information on visualisation development or end-users'. The visualisation designers need to understand the end-user requirements before they can employ these resources to develop any visualisation solution. These resources can also be used to develop cyber-security visualisation solutions, but without understanding the tasks and end-user requirements, such solutions would only focus on the HCI elements, which are not useful for end-users (cyber-security analysts).

Table 2.1: Common libraries and tools used to design data visualisation, along with their dependences on programming languages or platforms, and the nature of visualisation they can produce.

Name	**Dependence**	**Interactive or Animated or Static**
Data Visualisation Libraries		
Vega[9]	Higher Level Cross Platform	Interactive
Boost Graph Library[10]	C++	Interactive & Animated
Data-Driven Documents[11]	Javascript	Interactive
Dygraphs[12]	Javascript	Interactive
InfoVis Toolkit[13]	Javascript	Interactive
Open Graphics Library[14]	Cross-Platform	Interactive & Animated
VisPy[15]	Python	Interactive
Data Visualisation Tools		
Cytoscape[16]	UNIX, LINUX, OS X, Windows	Interactive
Gephi[17]	LINUX, OS X, Windows	Interactive
Graphvis[18]	UNIX, LINUX, OS X, Windows	Static
R[19]	UNIX, LINUX, OS X, Windows	Limited Interactivity
Tulip[20]	UNIX, LINUX, OS X, Windows	Interactive

2.2 Cyber-Security

Pfleeger and Pfleeger (2006) defined cyber-security as an approach to protect computer systems from attacks. In over a decade, the definition of cyber-security has been updated to the protection of systems, devices, networks, and services - and the data they hold - against unintended or unauthorised attacks, theft or damage, as defined by The National

[9] https://vega.github.io/vega/ [Accessed: 25 April, 2017]
[10] https://www.ibm.com/developerworks/aix/library/au-aix-boost-graph/ [Accessed: 25 April, 2017]
[11] https://d3js.org [Accessed: 25 April, 2017]
[12] http://dygraphs.com [Accessed: 25 April, 2017]
[13] http://philogb.github.io/jit/ [Accessed: 25 April, 2017]
[14] https://www.opengl.org [Accessed: 25 April, 2017]
[15] http://vispy.org [Accessed: 25 April, 2017]
[16] http://www.cytoscape.org [Accessed: 25 April, 2017]
[17] https://gephi.org [Accessed: 25 April, 2017]
[18] http://www.graphviz.org [Accessed: 25 April, 2017]
[19] https://www.r-project.org/about.html [Accessed: 25 April, 2017]
[20] http://tulip.labri.fr/TulipDrupal/ [Accessed: 25 April, 2017]

Cyber Security Centre (2018). According to von Solms and van Niekerk (2013), cyber-security is more than just protecting systems and services; it is also about protecting the people using the systems and their assets, both tangible or intangible.

However, with the advance of technology and the increase in malicious cyber attacks, the task of protecting resources has become extremely important and challenging. Many different approaches have been utilised to monitor and mitigate the sophisticated technical and social attacks on networks and data. One such approach is cyber-security visualisation.

2.3 Cyber-Security Visualisation

In the field of cyber-security, public and private sectors rely on the expertise and capabilities of cyber-security analysts to protect assets and resources in cyberspace. An area under the umbrella of cyber-security is cyber-security visualisation, which provides these analysts with visual data, rather than textual data, for better analysis, pattern recognition, anomaly detection and communication of findings (Goodall, 2008). The main goal of cyber-security visualisation is to provide effective tools (Fink et al., 2009) that help to detect, monitor and mitigate attacks in a timely manner. To quote Marty (2008), “A picture is worth a thousand log records”.

Visualisation approaches have helped cyber-security analysts raise their level of awareness to an all-inclusive approach and help to identify problems and find solutions visually (Fink et al., 2009). These approaches should be developed to aid cyber-security analysts to fulfil their tasks and keep their needs in mind (Sharafaldin, Lashkari, & Ghorbani, 2019; Shiravi et al., 2012; Zhao et al., 2019) The vast amount of data to be processed, along with the need for new methods and tools, has made visualisation a new and popular approach in the domain of cyber-security (Marty, 2008). Cyber-security analysts are unable to go through terabytes of textual log records to extract useful summaries rapidly; however, visualisation can help summarise all that information in a single picture (Sharafaldin et al., 2019).Visualisations focus on providing cyber-security analysts with a tool to prevent and defend against these attacks. But, there is a major research gap in the development of cyber-security visualisation solutions, which should become clear further on in this chapter in Section 2.4.

A number of cyber-security visualisation solutions focus on different aspects of cyber-security, ranging from a high-level view to a technical low-level one. This increase in cyber-security visualisation, over the last decade, has led to different types of analysis performed by different solutions. Most can be broadly classified into; Network Analysis (Section 2.3.1), Malware and Threat Analysis (Section 2.3.2), and Situational Awareness (Section 2.3.3).

2.3.1 Cyber-Security Visualisation Solutions for Network Analysis

Network Analysis solutions focus on mapping the physical system network to detect possibilities of attacks. The need for network security has risen with the growth of network-based security events (Shiravi et al., 2012). Many different types of cyber-security visualisation solutions analyse network activities to detect threats. The following categories present solutions within the broad domain of Network Analysis.

2.3.1.1 Active Network Defence Management and Traffic Monitoring

Some cyber-security visualisation *(secVis)* solutions provide real-time management of a network. They create explorative models for investigations and monitoring of traffic to/from a network to detect the possibility of attacks or suspicious activities.

Zhong et al. (2018) introduced a solution that can be used for daily network operations and maintenance, using a collaborative visual analysis system. The network is visualised as a dashboard viewing a real-time alert with a list of alerts or queries, a 2-D map to represent the physical connections, a node-link diagram[1] visualising the network topological space for exploring activity patterns, and graphs to show the real-time state of devices, such as memory utilisation rate or transmission rate.

Coudriau, Lahmadi, and François (2016) introduced a solution that focused on network monitoring of the dark-net to extract similar groups of packets, especially malicious ones. Their approach uses topological analysis of network packets to cope with the high volume of traffic and identify malicious packets. Topological graphs in a colour-coded 3D coordinate system help identify the packets.

Ocelot by Arendt et al. (2015) presented visualisation for active network defence by quarantining dynamic network management. This improves security by better real-time monitoring of the network and providing effective decision support for cyber analysts. *Ocelot* centres around a multi-faceted graph visualisation which uses petri dishes[2] and sunburst plots[3]. The internal nodes are displayed within petri dish groups and external nodes in an outer ring; the sunburst view can be used to display the hierarchical layout. *Ocelot* allows for filtering and has an alert panel to interact with the visualisations for exploration of the information.

Creese, Goldsmith, Moffat, Happa, and Agrafiotis (2013) introduced *CyberVis*, which builds on existing intrusion detection systems and supports alerts from existing tools such as Snort[4], Nagios[5] and ClamAV[6]. The network is visualised in a scalable format

[1] https://datavizcatalogue.com/methods/network_diagram.html [Accessed: 8 March, 2019]

[2] Circle packing - hybrid hierarchical/node-link visualisation

[3] http://www.datavizcatalogue.com/methods/sunburst_diagram.html [Accessed: 1 May, 2017]

[4] https://www.snort.org [Accessed: 1 May, 2017]

[5] https://www.nagios.org [Accessed: 1 May, 2017]

[6] http://www.clamav.net [Accessed: 1 May, 2017]

using a presentation that has an overlay of an abstrac of the business processes to convey the relevant information, which represents potential consequences of network attacks to the business as a whole.

2.3.1.2 Analyse Network Vulnerabilities

Another type of *secVis* solution investigates the current status of the network to assess possible vulnerabilities or threats and provides details of those detected and possible mitigation strategies.

Watson and Lipford (2017) presented solution for network security with a zone-based vulnerability visualisation. A directed node-link visualisation is developed to represent each unique device on the network, along with the flow of network traffic. A colour-coded approach presents the nodes according to vulnerability severity. The zone locations of the nodes also help determine which nodes require remediation first, depending on which assets need to be protected the most.

An example of such a solution is *Nv* by Harrison, Spahn, Iannacone, Downing, and Goodall (2012). This web-based tool visualises tree-maps[7] which analyse open ports, holes and nodes of a LAN to find the versions they run, for detection of potential threats. It uses online sources like the CVE database[8] to calculate the CVSS score[9], and BugTraq[10] to provide vulnerability descriptions and possible mitigation strategies. *Nv* uses zoomable tree-maps to easily identify the most vulnerable devices, and histograms to give an overview of the state of the data. It also provides filtering abilities to analysts. It uses data acquired from Nessus[11] scan results and is implemented using D3.js[12].

2.3.1.3 Analyse Routing Anomalies

SecVis solutions also span the area of visually analysing the difference between legitimate routing changes and spam.

Ulmer, Schufrin, Sessler, and Kohlhamme (2018) presented a solution[13] that helps detect suspicious behaviour of IP-blocks, through a visual and interactive web interface. It allows the analysis of Geo-IP[14] data over time, on a 2D geographical

[7] http://ornl-sava.github.io/nv/ [Accessed: 1 May, 2017]

[8] Common Vulnerabilities and Exposures - https://cve.mitre.org [Accessed: 1 May, 2017]

[9] Common Vulnerability Scoring System which measures the harmfulness of a threat - https://www.first.org/cvss [Accessed: 1 May, 2017]

[10] http://www.securityfocus.com/archive/1 [Accessed: 1 May, 2017]

[11] A vulnerability scanner - https://www.tenable.com/products/nessus-vulnerability-scanner [Accessed: 1 May, 2017]

[12] Data Driven Documentation - JavaScript Library - https://d3js.org [Accessed: 25 April, 2017]

[13] http://crisp.igd.fraunhofer.de [Accessed: 8 March, 2019]

[14] GeoIP refers to the method of locating a computer's geographic location by identifying the IP address - https://docs.nexcess.net/article/what-is-geoip.html [Accessed: 8 March, 2019]

world map, to recognise anomalous route changes. It also supports a timeline view to represent the changes between two points over a period of time, a statistics view showing information about IP-block owners and changes to the IP-block, a search view to search by organisation or IP blocks, and a pop-up view showing detailed information about the IP-block when a point on the map is chosen.

Fischer, Fuchs, Vervier, Mansmann, and Thonnard (2012) presented *VisTracer*, a solution that helps to analyse routing anomalies on large trace-route data. It allows analysts to explore, identify and analyse suspicious events by combining different types of visual representation. It adopts a pixel-based visualisation technique to give an overview of anomalous events. It uses graph-based summary presentations with a combination of temporal glyph presentations to give an overview of route changes to specific destinations over time.

2.3.1.4 Determine Attack Patterns

This category presents proactive *secVis* solutions that create attack graphs[15] to assess potential attacks to a system.

PERCIVAL (Proactive and rEactive attack and Response assessment for Cyber Incidents using Visual AnaLytics), by Angelini, Prigent, and Santucci (2015), assesses the static and dynamic risk levels of a system, to increase situational awareness. It highlights potential attack vectors based on the state of the network using attack-graphs. Along with colour-coded attack graphs, it uses a donut chart[16] to display the composition of the network topology displayed by the attack graph, which displays mitigation barriers in the dynamic mode.

Trogdor (Yuen, Turnbull, & Hernandez, 2015) automates planning techniques to determine and assess complex potential attacks on an organisation. It is a data-driven solution which visualises data into different types of attack graphs, to provide an overview of the network, and for easy detection of failure points of a potential attack to reach the target machine.

2.3.2 Cyber-Security Visualisation Solutions for Malware and Threat Analysis

Malware and Threat Analysis focus on detecting, analysing and eliminating malware and threats. The different categories of cyber-security visualisation solutions within the broad domain of Malware and Threat Analysis are discussed below.

[15] http://www.idart.sandia.gov/methodology/RT4PM.html [Accessed: 1 May, 2017]
[16] http://www.datavizcatalogue.com/methods/donut_chart.html [Accessed: 1 May, 2017]

2.3.2.1 Intrusion Detection Support

Some *secVis* solutions support intrusion detection by providing additional analysis capabilities to understand intrusion attacks and their effects.

Karami (2018) presented an anomaly-based intrusion detection system using a modified self-organised map[1] to detect attacks and anomalies, and also provide insights to end-users. It enables the end-users to analyse large amounts of data more efficiently with easy-to-use interactive 2D visualisations.

OwlSight by Carvalho, Polidoro, and es (2016) focused on real-time detection of cyber-attacks using maps and graphs. It uses dashboards to allow prompt detection of threats by pinpointing their origin using geographical maps and graphs.

Wüchner, Pretschner, and Ochoa (2014) introducd *DAVAST*, which visualises system activities through data-flow graphs, using pattern-matching to correspond to understand potentially malign activities in a system. It has four distinct views: project the activity model to visualise hierarchical relationships between different activities; an overview of the system state over a period of time; a statistical view of all activities over a period of time; and a data-flow graph of all system interactions.

2.3.2.2 Malware Detection

Some *secVis* solutions support malware detection by providing analysts with capabilities of detecting existing malware in the system or potential malware originating from various sources.

Angelini, Aniello, Lenti, Santucci, and Ucci (2017) presented a solution to detect malware in uncertain live web traffic and files downloaded from the web. The tool supports malware monitoring to keep track of the origins of downloaded files, and analysis the malware by allowing the user to inspect parts of the file to check for malicious data. It has three main views: the current decisions view allows the analyst to see colour-coded files in benign, malicious, and dubious categories; the classification explanation view provides explanations for decisions made in the previous view using a tree; and feature space analysis view allows analysis of files using a radial visualisation to make a decision on the files being malicious or benign.

Santhanam, Holland, Kothari, and Mathews (2017) presented a solution to detect zero-day malware for Android applications using interactive visualisations of program artefacts that help understand the semantics of Android applications. The tool uses smart views (interactive visual models) to demonstrate the interaction of applications

[1] A type of unsupervised artificial neural network - https://en.wikipedia.org/wiki/Self-organizing_map [Accessed: 8 March, 2019]

with Android subsystems. It visualises throw and catch events and conditional paths in the code, where the integrity of critical variables may be at risk, and can be analysed to check for zero-day malware.

2.3.2.3 Insider Threat Analysis

Insider Threat Analysis focuses on analysing attacks by malicious insiders, people who intentionally try to misuse the legitimate information and systems they have access to. The amount of data to be analysed, for insider threat detection, is huge and dynamic (Marty, 2008; Zeadally, Yu, Jeong, & Liang, 2012).

Agrafiotis et al. (2015) developed a framework to identify attack patterns[2] for insider threat detection using machine learning to check for anomalous behaviour and increase the analyst's understanding and detection capabilities. The attack trees are used to detect which resources are available and which require human intervention to gain access to, or privileged resources to detect potential insider threat attacks.

Another graph-based approach was presented by Nance and Marty (2011), which focuses on visualising insider behaviour to establish acceptable action patterns based on workgroup classification. Bipartite graphs[3] are used to detect patterns or behaviour that are not normal, highlighting areas and individuals for further investigation.

2.3.3 Cyber-Security Visualisation Solutions for Situational Awareness

In the study of *secVis* solutions, one of the most common characteristics of cyber-security visualisation is the presence of a view that provides Situational Awareness (SA) capabilities. According to Franke and Brynielsson (2014), visualisation is a very important characteristic in attaining situational awareness for cyber-security.

Erbacher, Frincke, Wong, Moody, and Fink (2010) stated that SA is a higher-level abstract view that represents the underlying data for immediate comprehension. Adam (1993) simply puts it as "...[SA is] knowing what's going on so you can figure out what to do". Most *secVis* solutions have SA capabilities that provide an overview and awareness of the system and current activities (Franke & Brynielsson, 2014). This helps collect, disseminate, and present information (Varga, Brynielsson, & Franke, 2018) about attacks and their impacts for technical and non-technical people, as it aims to bridge the knowledge gap between the two.

For the purpose of *secVis*, SA is achieved in three stages; *Perception*, *Comprehension* and *Projection*. According to Endsley (2016), *Perception* is a presentation of the current

[2] https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns [Accessed: 1 May, 2017]

[3] http://mathworld.wolfram.com/BipartiteGraph.html [Accessed: 1 May, 2017]

state of a situation attained by perceiving the related status, attributes and dynamics, like mental models; *Comprehension* is a higher-level understanding of the data attained by understatinging the data and what the perceived cues mean; and *Projection* is the ability to predict future actions of the elements by combining the knowledge gained in the previous two steps.

CyberVis by Creese et al. (2013) visualises an overlay of an abstraction of the business processes on the network view, and impact of security threats in the 'Business Process Layout' view. This allows cyber-security analysts to be aware of and understand the crucial tasks and interdependencies of an organisation or business.

Dagger by Peterson (2016) is a modelling and visualisation framework to present knowledge and information for decision-makers by using layering and sunbursts.

ePSA by Legg (2016) focuses on mapping internet data for novice users to enhance their SA using a timeline, scatterplot and fixed-ring layout visualisations.

OwlSight by Carvalho et al. (2016) visualises threats and their origin points, using geographical maps, along with information about the attack, to increase situational awareness. It also allows users to share information within the application by sharing the dashboard.

PERCIVAL by Angelini et al. (2015) has two modes: Proactive and Reactive. Proactive mode displays a precomputed attack path on the network, where the system is most prone or likely to be attacked. Reactive mode gets automatically selected when an attack is detected and displays the state of the network and attack in colour. It keeps the analyst aware of the state of the system at all times.

A solution by Watson and Lipford (2017) provides the ability to visualise network traffic within and between systems or zones, providing decision makers with environmental information to support real world decision-making.

Trogdor by Yuen et al. (2015) provides an overview of the network in 'Situation View'. This allows the analyst to be greatly involved in the decision-making processes of assessing complex attacks on the system.

2.4 Challenges for Cyber-Security Visualisation Solutions

The following sections discuss the challenges faced in designing and evaluating cyber-security visualisation solutions, as shown in Figure 2.2.

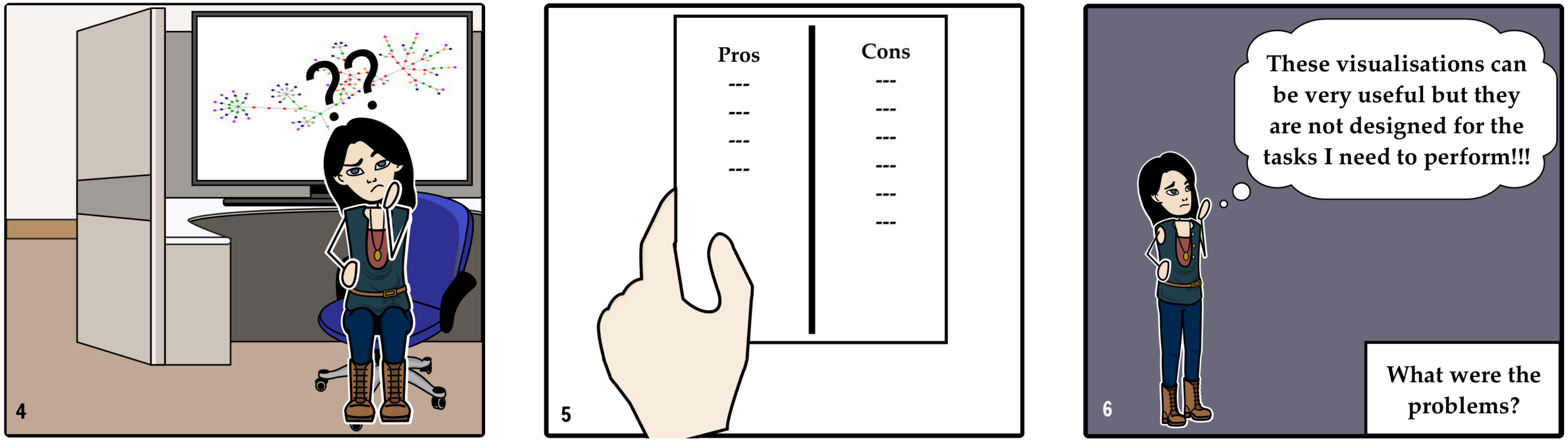
(a) Ari is a cyber-security analyst. Their job requires them to spend all day checking textual log records. They are tired and exhausted performing time-critical monotonous tasks of checking log records to find anomalies.

(b) Ari is in luck, because there is a better and easier way. Cyber-security visualisations can help detect, monitor and mitigate attacks in a timely manner. Now instead of textual log records, Ari gets to analyse visualised graphs.

(c) Ari is happy and excited now to have been introduced to cyber-security visualisations. The visualisations provide analysts, like Ari, with a competent tool to prevent and defend against attacks.

Figure 2.2: A comic[1]representing the need of cyber-security visualisation solutions to make a cyber-security analyst's task easier. This is followed by an introduction to the challenges of these solutions that ultimately lead to low adoption rate of these solutions.

[1] © Created with Strroryboard That (https://www.storyboardthat.com)
Sublime-text Text Editor (https://www.flickr.com/photos/xmodulo/14391734181/) by xmodulo License: Attribution (http://creativecommons.org/licenses/by/2.0/)
fon graph (https://www.flickr.com/photos/cromo/185028548/) by Cromo License: Attribution, Non Commercial (http://creativecommons.org/licenses/by-nc/2.0/)
2-core graph of #rstats people (https://www.flickr.com/photos/hjl/4094315135/) by hjl License: Attribution (http://creativecommons.org/licenses/by/2.0/)
indica-website-graph (https://www.flickr.com/photos/indi/271647921/) by indi.ca License: Attribution (http://creativecommons.org/licenses/by/2.0/)


4
??
5
Pros

Cons

6
These visualisations can be very useful but they are not designed for the tasks I need to perform!!!
What were the problems?

(a) Unfortunately, Ari's excitement was short-lived. Using these visualisation solutions for their day-to-day tasks turned out to be more complicated than they first thought.

(b) Ari makes a list of the benefits of using these visualisations instead of the textual records and finally comes to a conclusion…

(c) Ari is at a crossroads now. On one hand, the visualisations make their job easier but on the other hand, the visualisations do not have the functionality to support the tasks they needs to perform.

Figure 2.2: A comic representing the need of cyber-security visualisation solutions to make a cyber-security analyst's task easier. This is followed by an introduction to the challenges of these solutions that ultimately lead to low adoption rate of these solutions.

Although a number of cyber-security visualisation solutions exist, many lack the ability to directly support cyber-security analysts' goals and activities with the analytical capabilities of the solution (Franke & Brynielsson, 2014; Franklin, Pirrung, Blaha, Dowling, & Feng, 2017). The following highlights the problems with current cyber-security visualisation solutions, :

1. Most cyber-security visualisation solutions are designed without any end-user involvement.
2. Solutions are rarely evaluated for effectiveness in terms of the task they aid in performing and the needs of the analysts. Solutions that were evaluated did not have or use any standardised evaluation techniques.
3. There is disparity of domain-knowledge between cyber-security analysts and visualisation designers.

2.4.1 Challenges for Designing Cyber-Security Visualisation Solution

Even with an abundance of cyber-security visualisation solutions, there are numerous challenges to their successful design and execution. Following the aforementioned solutions, this section looks at the main difficulties that hinder the development of cyber-security visualisation solutions that can be effective for cyber-security analysts.

2.4.1.1 Access to Experts

Adams and Snider (2018) noted that there exists an overwhelming lack of access to relevant experts across many research papers. Due to the fast-paced nature of cyber-security analysts' work and the sensitivity of their field, experts have very limited time to spare (Mckenna et al., 2015). As a consequence, alternative resources must be found to understand the requirements of the analysts, and the tasks they perform, to create effective and useful cyber-security visualisations.

2.4.1.2 Source Data

Data on its own is a very broad term, but it forms the very basis of visualisation as there is no visualisation without the underlying data that it presents. In January 2018, an article in Software Development Times[2] discussed the overwhelming amount of data and recognised the lack of visualisation in security operation tools.

[2] https://sdtimes.com/data/cybersecurity-operations-and-the-role-of-visualization-design-and-usability/ [Accessed: 19 Dec, 2018]

Best et al. (2014); D'Amico, Whitley, Tesone, O'Brien, and Roth (2005); Erbacher et al. (2010); Fink et al. (2009); Marty (2008) recognised many challenges associated with source data, which are presented below:

Access to Real-Data: There is limited and restricted access to real data due to the confidentiality and sensitivity of the field of cyber-security. This often prevents analysts sharing real data cases.

Varied Data Sources: There is an abundance of potential heterogeneous data-sources that are not joined together due to discrepancies and a lack of common information.

Volume of Data: The amount of incoming data to be processed is huge and will increase by several magnitudes in the future.

Terminology Used: There is no standardised lexicon for the complex data in different data sources.

Consistency of Data: Data from different sources may or may not always be homogeneous which leads to different presentations of the same data.

Quality of Data: The data sources may not always be reliable, correct, maintained or up-to-date.

Completeness of Data: Data from the various sources may not always be complete; there could be possibilities of missing elements or elements containing incomplete data.

Unclear Data Formatting: Unclear formatting of data can lead to multiple nodes in a visualisation presenting the same information, which leads to confusion.

Data Minimisation using Aggregation or Filtering: Aggregation of data is performed by combining different data-sets in a visualisation node, and presenting them on demand. However, filtering of data removes it permanently from the visualisation. As a result, there is a tradeoff of either saving screen space, which increases the speed of access, or the possibility of losing critical data.

2.4.1.3 Representation of Visualisation

The Representation of Visualisation is one of the major challenges for cyber-security to create effective and usable visualisations for cyber-security analysts. The challenges of representation of visualisation, as recognised by Adams and Snider (2018); Best et al. (2014); Fink et al. (2009); Gates and Engle (2013); Marty (2008), are presented below:

Perspective of End-Users: It is important to keep the perspective of end-users (cyber-security analysts) in mind to understand what characteristics they require to perform specific tasks.

Flexible Manipulation of Data: Ease of data exploration is important as analysts need to move between high-level analytical processes to low-level investigation of datasets.

Refresh Rate: The refresh rate of the visualisation should be quick and in real-time, especially for dynamic presentations.

presentation of Useful Information: Only information that is useful for the particular task should be presented in the visualisation to avoid cluttering it. Overly complex and 'busy' visualisations can lead to frustration or misinterpretation of the data.

Aesthetics of Visualisation: Aesthetics should be secondary to the ability of the solution to support data analysis. Visualisations should be built to perform a task or achieve a goal and not to present 'pretty pictures'.

Size of Visualisation: The visualisation should be presented keeping in mind the average screen size In case of overload of information, data minimisation should be performed.

Interaction or Animation: Interaction enables the end-user to explore the data by interacting with static images, while animation displays a dynamic view of how information changes over time. The right presentation must be selected on the basis of the data and task at hand.

When to Use Visualisations: Visualisation may not help in every scenario. If the problem is too simple, then a visualisation may not add anything as they would be overly simplistic visualisations. If it is too complex, then visualising without understanding the problem may lead to polluted results that fail to quickly communicate information to the analysts.

2.4.2 Challenges for Evaluating Cyber-Security Visualisation Solution

Evaluation is used to determine if the outlined goals and objectives of a tool have been achieved. It provides an overview of improvements or corrections required to achieve the objective. Specifically, user evaluation measures the benefits of the tool and the impact and effectiveness of the tool, on the basis of the goal (Staheli et al., 2014). There are many techniques to conduct evaluations, but only with appropriate (purpose-made) evaluation techniques can a tool be correctly validated. However, evaluating the effectiveness of any visualisation is a challenge in itself, even more so in the field of cyber-security, as most evaluation techniques address the visualisation in isolation rather than the related analysis process of the solution (Gates & Engle, 2013; Plaisant, 2004).

2.4.2.1 Evaluation Techniques for Data Visualisation

Ellis and Dix (2006) fount that of 65 visualisation papers, only 12 described any kind of evaluation for the tool they were presenting. One of the reasons for not using evaluation techniques was found to be the lack of clear guidelines for conducting an evaluation. Another reason could be the lack of a performance measure for comparing visualisation solutions (Battle et al., 2018). There also seems to be a dearth of specialised evaluation techniques for different fields within data visualisation. The techniques most commonly used to validate data visualisation solutions by Lam, Bertini, Isenberg, Plaisant, and Carpendale (2012); Plaisant (2004); Staheli et al. (2014) are summarised below:

Field Observations: Observational method that elicits information in an uncontrolled environment.

Laboratory Observation: Observational studies in laboratories to allow for more control.

Controlled Experiments: Abstraction of real-life tasks to scoped and defined tasks, performed by participants in a controlled environment.

Interviews: Participants are asked a series of questions to elicit information regarding a topic.

Case Studies: Studies on participants interacting with the visualisation in a pre-defined case.

Usage Scenarios: Navigation and usage of the visualisation behaviour, defined by the evaluator, in a pre-constructed scenario.

Field Logs: Analysis of automatically captured logs and user traces using the visualisation in an uncontrolled environment.

Informal Evaluation: Gathering informal user feedback by letting experts play with the visualisation and comment on it.

Usability Test: Observing the performance of users on a set of pre-defined tasks.

Laboratory Questionnaire: Participants complete a questionnaire to give opinions and reactions to the tool being tested.

2.4.2.2 Evaluation Techniques for Cyber-Security Visualisation

A survey by Staheli et al. (2014) showed that little research has gone into finding aspects that make a visualisation effective for analysts using cyber-security visualisation solutions. They also found that 46% of cyber-security visualisation tools have no user involvement in the evaluation process. Another survey of cyber-security visualisation papers by Mckenna et al. (2015) found that 40% of 51 papers involved user evaluation and only 7 of those included an iterative evaluation process, which involved end-users in both, the design and evaluation processes.

To reinforce the results from these surveys, Table 2.2 presents an overview of evaluation techniques for some of the solutions discussed in earlier sections. It includes evaluation goals (common evaluation techniques), research strategies used to evaluate the solution, information on the nature of the evaluation - being summative or formative, the dataset used, and type of user-involvement, if any.

The different evaluation techniques for cyber-security visualisation solutions, summarised in Table 2.2, are described below:

Laboratory Observations, Usability Test, Controlled Experiments and Interview: Used by Zhong et al. (2018) to evaluate their solution. Laboratory observations were used to verify the validity of the systems. This was followed by a usability test for the user-friendliness of the system. Lastly, a controlled experiment, along with interviews with experts, was conducted to evaluate the use of the system. This solution had a formative design process.

Field Observation and Interview: Used by Angelini et al. (2015) and Yuen et al. (2015) to evaluate *PERCIVAL* and *Trogdor*, respectively. Case studies or scenarios were developed to demonstrate the working of both the solutions. This was followed by interviews with cyber-security experts. *PERCIVAL* had a summative development process whereas *Trogdor* had a formative one.

Controlled Experiment and Informal Evaluation: Used by Arendt et al. (2015) to evaluate *Ocelot*. Participants, MSc students, and cyber-security experts, used the tool on a modified data-set from VAST[3] and commented on the effectiveness of the solution. *Ocelot* had a formative design process.

Usage Scenarios: Used to evaluate *VisTracer* (Fischer et al., 2012), *Nv* (Harrison et al., 2012), *BURN* (Roveta et al., 2011), solution by Angelini et al. (2017) and solution by Santhanam et al. (2017). For all three solutions, usage scenarios were mistakenly presented as a case study, without any user involvement to comment on the tools. There was no user-involvement in the development of the tools as all three solutions were developed in a summative way. Also used by Carvalho et al. (2016) to evaluate *OwlSight* for a formative development. However, there was no information about the users involved in the evaluation and feedback process.

[3] Visual Analytics Science and Technology - http://www.vacommunity.org/About+the+VAST+Challenge [Accessed: 4 May, 2017]

Table 2.2: Overview of evaluation techniques for Cyber-Security Visualisation, detailing the goals and strategies of the way evaluation was performed and recorded

Evaluation Goals	**Research Strategies**	**Summative/ Formative**	**Dataset**	**User Involvement**	**Reference**
Laboratory Observations, Usability Test, Controlled Experiments and Interview	Participants reviewed the prototype by answering pre-set requests on real scenarios and then reviewed the usability of the system. Finally, experts evaluated the system at a forum.	Formative	Data from the University	18 participants consisting of network administrators and student assistants. 44 experts, 12 from the university and rest from other organisations.	Zhong et al. (2018)
Field Observation and Interview	Experts reviewed the tool by using a synthetic case study	Summative	Synthetic data-set, similar to ACEA architecture	Seven Network Security Experts	Angelini et al. (2015)
	Modelled two scenarios and presented to experts	Formative	Synthetic data set; created from network, policy and process captures of experts	16 groups of potential users (Five were Network Security Experts)	Yuen et al. (2015)
Controlled Experiment and Informal Evaluation	Participants were presented with a dataset and had to use the tool as a mechanism to achieve the final goal, then they commented on the use of the tool	Formative	Modified data set from VAST 2013	17 MSc Cyber-Security University Students; Four Cyber Defence Engineers	Arendt et al. (2015)
Usage Scenarios (Defined as Case Studies)	Demonstrated the tool in two different suspicious routing events	Summative	SpamTracer data-set collected from April to August, 2011	None	Fischer et al. (2012)
	Demonstrated the tool in two different vulnerability scenarios	Summative	VAST Challenge 2011	None	Harrison et al. (2012)
	Demonstrated the tool using three different scenarios to find malicious ASes, tracing attacks or finding migrations in a system.	Summative	FIRE data-set collected from January to December, 2010	None	Roveta et al. (2011)

Table 2.2: Overview of evaluation techniques for Cyber-Security Visualisation, detailing the goals and strategies of the way evaluation was performed and recorded

Evaluation Goals	**Research Strategies**	**Summative/ Formative**	**Dataset**	**User Involvement**	**Reference**
	Demonstrated the tool by presenting results using real world data.	Summative	242,678 files downloaded from November 2014 to August 2015 on a server in Sapienza University of Rome	None	Angelini et al. (2017)
	Demonstrated the tool by presenting results provided by real world data	Summative	77 Android Apps provided by DARPA	None	Santhanam et al. (2017)
Usage Scenarios	Demonstrated real-word scenarios for cyber-defence (situational awareness) and organisational security operations	Formative	DNS results from Internet Service Providers and feeds based on external domain sink-holing	Yes; No Information	Carvalho et al. (2016)
Usability Test	Participants performed a usability test to measure the learnability and satisfaction parameters	Summative	None	Yes; No Information	Karami (2018)
	Participants performed a cognitive walkthrough of pre-defined tasks.	Formative	None	29 students	Ulmer et al. (2018)

Usability Test: Used by Karami (2018) and Ulmer et al. (2018) to evaluate their solutions. Participants used the tools to determine their usability. Karami (2018) used a summative approach whereas Ulmer et al. (2018) used a formative approach in the design process.

While the solutions in Table 2.2 had some kind of evaluation, other solutions had no details about evaluation at all. These solutions were:

Solution by Coudriau et al. (2016) presented experimental results to demonstrate the capabilities of the solution and an overview of performance analysis from the testing.

CyberVis by Creese et al. (2013) presented 'Concept of Operations and Workflow' to demonstrate the navigation of the tool.

Solution by Watson and Lipford (2017) presented a sample result to demonstrate the resulting visualisation.

This survey of 15 solutions revealed:

- Three solutions had no form of evaluation.
- Five tools had no user-involvement.
- Ten tools had a summative development process.
- One tool allowed complete and unguided interaction with the tool.
- A lack of standardisation of evaluation techniques currently used.

To summarise, there exists a need to involve users and their requirements in the development and evaluation of cyber-security visualisation tools. Additionally, the technique should evaluate the goal of the solution (Gates & Engle, 2013). The lack of a common model for standardised evaluation methods (Staheli et al., 2014) has been identified many times, but there is currently no model to evaluate cyber-security visualisation solutions based on user requirements. This highlights a need for a common model to standardise design and evaluation of cyber-security visualisations.

2.4.3 Dichotomy of Cyber-Security Visualisation

Cyber-security visualisation solutions are either designed by cyber-security analysts who do not know much about visualisation theory or Human-Computer Interaction (HCI), or they are designed by visualisation designers who do not have much knowledge about cyber-security and related fields (Marty, 2008). Consequently, the resultant solutions suffer from lack of expert domain-knowledge in one of the areas (D. Zage & Zage, 2010). There is a need to ameliorate this disparity to create cyber-security visualisation solutions which are technically accurate and easy-to-use (W. Zage, Zage, Gaw, & Mast, 2011), combining the knowledge and understanding from both domains. Section 4.4.3.2 attempts to illustrate the existence of this disparity of domain-knowledge using the findings from the experts in Chapter 4.

2.5 Discussion

This literature review focused on the research already conducted. There is no shortage of cyber-security visualisations solutions. However, the research shows a lack of experience and general consensus on how to model these solutions effectively (Adams & Snider, 2018). The low adoption of solutions developed for cyber-security visualisation results from not taking the needs of the end-users into account or involving them in the design and evaluation process. Common tasks routinely performed by cyber-security analysts are often not addressed by the cyber-security visualisation solution (Franklin et al., 2017). An assessment of user requirements must be included in early design phases and in later evaluation phases. Also, the evaluation techniques used to measure most tools are not effective, nor is the evaluation standardised. Thus, there is a need to construct guidelines and standardise design and evaluation techniques for cyber-security visualisation, which will be discussed in Chapter 3.

Chapter 3

Initial Model of *EEVi* and Guidelines

This chapter describes the development process of ***EEVi*** (**E**ffective **E**xecution of **Vi**sualisation), a model, from Thematic Analysis on Cognitive Task Analysis papers to address RQ_1, arising from the research gaps found in the literature (Chapter 2). *EEVi* has been developed to address the needs of cyber-security analysts by providing a model of characteristics of visualisation for cyber-security visualisation solutions. As Franklin et al. (2017) concluded, a system should be built that provides the baseline visualisations required by cyber-security analysts to support the desired workflow.

3.1 Background of Techniques Used

The main challenge faced in conducting research to develop a model in the area of cyber-security visualisation is the lack of access to experts. Vessey's theory of cognitive fit includes a classification of spatial tasks, which requires problems to be looked at as a whole and requires "*...making associations or perceiving relationships in the data*" (Vessey, 2015) to find solutions for the problems (Teets, Tegarden, & Russell, 2010). To perceive the use of cyber-security visualisation solutions by analysts, Cognitive Task Analysis (CTA) papers were found which described studies with cyber-security analysts. Thematic analysis was performed on these CTA papers, so that *EEVi* could be built by forming relationships from the themes that arose.

3.1.1 Existing Models

A model is defined as "an abstraction of a system, aimed at understanding, communicating, explaining, or designing aspects of interest of that system" (Dori, 2002). The Department of Defense, USA (1998) identifies three main forms of model:

- *Physical Models* represent the physical characteristics of an actual system through instruments such as mockups for physical security for any resource;
- *Mathematical Models* encode information and properties so that they are represented purely by mathematical symbols and relationships, such as the generation of ciphers;
- *Logical Models* represent relationships of how system components interconnect, such as the topological map of a network in an organisation.

Models are representations of a system that help design, analyse and communicate concepts (SEBoK, 2019). They also provide a concise way of capturing and retaining knowledge about the system they are used to develop. According to Stanton, Roberts, and Fay (2017); Stanton, Salmon, Jenkins, and Walker (2009), models help overcome major challenges for designers, namely, the complex nature of a system's design, how optimisation might be achieved, and documenting implicit understanding of a system. Models provide a standard mechanism through which knowledge can be documented, updated and shared by operators, manufacturers, and researchers, to enhance understanding for all stakeholders.

Models which describe a domain underpin crucial understanding required to inform software design, using modelling languages such as UML[1]. This stems from The Software Engineering Body Of Knowledge recommending building a model of the context of the potential software before development, to understand the operational environment and to identify the interfaces within the system's environment (ISO/IEC TR 19759:2015, 2015).

These modelling languages can express any conceptual relationship provided they are informed by a domain-specific model. The domain-specific models provide the required content to populate the diagrams built from the modelling languages, in order to develop software (Gray & Rumpe, 2018). This means that the quality of the domain model would make one model better than the other. To develop a domain-specific model to inform cyber-security visualisation, the following section provides the background of using cognitive task analysis to model cognitive behaviours of cyber-security analysts using visualisation.

3.1.2 What are CTA papers?

CTA (Cognitive Task Analysis), which comes from the field of applied psychology (Machuca, Miller, & Colombi, 2012), attempts to follow an inductive approach instead of trying to identify predefined data (Albar & Jetter, 2013). It has

[1] Unified Modelling Language

been used in many studies to describe the cognition (the way the mind works) necessary for task performance and to extract mental models. In this case, mental models refer to the way analysts achieve situational awareness for cyber-security (Crandall, Klein, & Hoffman, 2006). Most studies generally yield interviews, observations, and hypothetical scenarios (D'Amico & Whitley, 2007).

Mckenna et al. (2015) introduced the technique of qualitatively coding CTA papers to form requirements for the cyber-security visualisation tool they were developing. One of the main goals of CTA analysis conducted by D'Amico and Whitley (2007) was using the results as foundation material for studies which lacked access to cyber-security experts or analysts. Qualitative coding was also used by Lam et al. (2012) to describe different evaluation techniques for visualisations. This led to a need for CTA papers for cyber-security visualisation in order to develop *EEVi*.

3.1.3 Thematic Analysis

The development of the *EEVi* model used a qualitative *bottom-up* approach, called *Thematic Analysis*, to define the aspects within *EEVi*. A *bottom-up* approach involves going through the data without any pre-conceived notions, in order to completely develop themes and codes. Thematic Analysis is used to identify, examine, and report patterns (or themes) within data, as explained by Braun and Clarke (2006). They recognised six major phases of Thematic Analysis:

Phase 1 ***Familiarising with Data:*** The first phase begins by collecting the data for the analysis, and reading it multiple times. This allows the researcher to reach an overall understanding of the data and form a list of initial notes and ideas for analysis in the next phase.

Phase 2 ***Generating Initial Codes:*** This phase began with further analysis of the initial list of ideas. The process of coding involves identifying interesting features and reducing the amount of raw data by aggregating it into manageable high-level abstractions, called codes. This stage involves the production of an initial set of codes, which represent the most basic meaningful excerpts of data and are used to intuitively identify the aspects of the data they represent. These codes are represented by a codebook, which includes a collated list of all the initially generated codes. At this stage, an idea of the themes was not fully formed.

Phase 3 ***Searching for Themes:*** This phase is to search for themes, based on the codebook that has been generated in the previous phase. A theme captures the significance of the data and represents a patterned response, which is reflected by the group of codes it defines. This phase focuses on organising the codes and comparing them to find the similarities and differences between them. A potential candidate theme is attached to each cluster of similar codes. At this stage, the relationships between the potential candidate themes and codes starts to form.

Phase 4 ***Reviewing Themes:*** This phase begins with the refinement of the list of potential candidate themes. Data represented by themes should cohere meaningfully, but there should be clear distinctions amongst the different themes. The potential themes are then reviewed against the constituent codes to find the common denominator and make sure that these are representative of the codes they represent. The potential themes are reviewed against the literature and research questions to validate their representation of the data.

Phase 5 ***Defining Themes:*** By this point, there is a map of the themes and codes. The finalised themes are named and defined in accordance with the codes they represent, and how they fit within the literature. The names need to be concise and should immediately give the reader an idea of what the theme represents. The themes are defined according to the literature they represent and how they fit in relation to the research questions.

Phase 6 ***Producing the Final Report:*** The last phase begins with a set of refined themes and codes, along with the cognitive relationships identified as a result of thematic analysis of the dataset. The cognitive relationships lead to a storyline which presents the narrative of a coherent story through which themes can be described and cognitively linked. At this stage, these cognitive relationships have been identified on the basis of the study being conducted (Braun & Clarke, 2006; Vaismoradi, Jones, Turunen, & Snelgrove, 2016).

3.2 Process of Thematic Analysis

The development of the model was an iterative process using Thematic Analysis. There were four major milestones in the creation of the themes and codes for the qualitative aspect of the model. Figure 3.1 represents these milestones and how they relate to the phases of Thematic Analysis. This section explains the steps that were followed to develop the model.

3.2.1 Familiarising with Data

The research papers that were used for the development of *EEVi* were selected because of the data they presented. A search was made on the Web of Science[2] (WoS) and Scopus[3] databases for the keywords “cyber”, “security”, “visualisation”, and “visualization”.

[2] https://wok.mimas.ac.uk [Accessed: 22 May, 2019]

[3] https://www.scopus.com/ [Accessed: 22 May, 2019]

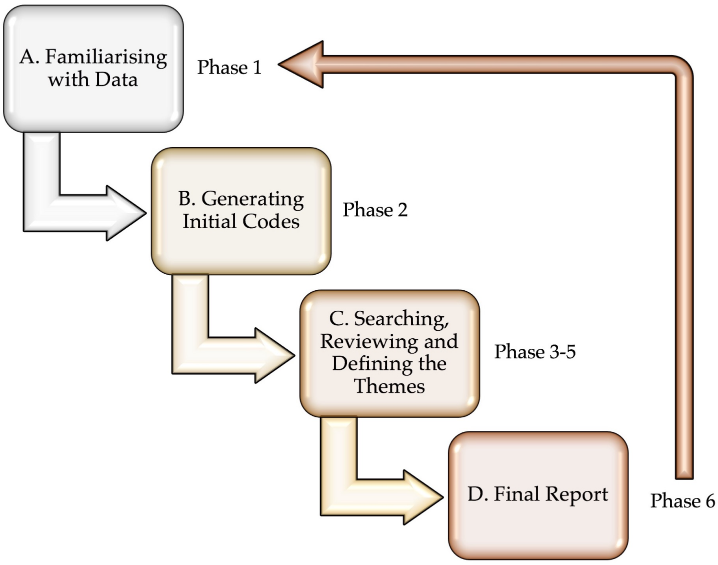

A. Familiarising with Data
Phase 1
B. Generating Initial Codes
Phase 2
C. Searching, Reviewing and Defining the Themes
Phase 3-5
D. Final Report
Phase 6

Figure 3.1: Overview of Thematic Analysis, the methodology followed for the development of *EEVi* in four stages.

WoS yielded 101 results and Scopus yielded 211. The results were scoured for relevant CTA research papers for cyber-security visualisation. This resulted in five relevant research papers being selected (Table 3.1). Despite an extensive search using cross-disciplinary literature research tools and relevant keywords, literature about the use of cyber-security visualisation solutions by cyber-security analysts is still underreported. A limitation for the development of *EEVi*, at the time of this research, was the lack of relevant literature in the area. It was recognised that the number of papers found limited the generalisability at this stage. However, it was also recognised that many cyber-security analysts would not publish sensitive findings, which could have been useful for this research. To address this, the future chapters present findings of validation of *EEVi* (Chapter 4) with seven expert cyber-security analysts, followed by a confirmation of *EEVi* (Chapter 5) with analysts, mostly from cyber-security domain. This would make the generalisability of *EEVi* robust.

Together, the collated information from these papers covered the breadth and depth of the field, precisely detailing cyber-security analyst roles, type of data the analysts used, how the analyses were conducted, what the analysts thought about visualisation approaches, and their experiences, if any, with visualisation solutions. D'Amico and Whitley (2007) and D'Amico et al. (2005) gave insight into the roles of cyber-security analysts and the tasks they perform in organisations. Erbacher et al. (2010) presented interviews with cyber-security analysts for the specific purpose of cyber-security visualisation. Fink et al. (2009) presented a variety of information about how to make visualisations effective for cyber-security analysts (who were the end-users), while Mckenna et al. (2015) reflected on how to research the CTA papers, by taking the relevant elements from them, for designing cyber-security visualisation solutions. Table

3.1 presents a summary of the relevance of these research papers for developing a model to help visualisation designers build better cyber-security visualisation solutions.

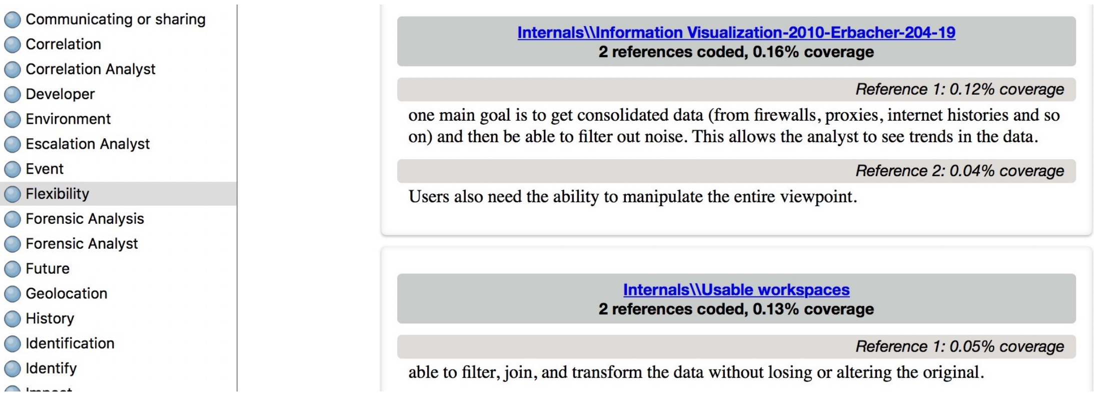
Table 3.1: Summary of the relevance of research papers selected for this research

Title of Research Paper	Authors	Research Relevance
Unlocking User-Centered Design Methods for Building Cyber Security Visualizations	Sean McKenna, Diane Staheli, Miriah Meyer (Mckenna et al., 2015)	Presents information about user-centred design to help visualisation designers build visualisation solutions that can meet the needs of cyber-security analysts.
A Multi-Phase Network Situational Awareness Cognitive Task Analysis	Robert Erbacher, Deborah Frincke, Pak Chung Wong, Sarah Moody and Glenn Fink (Erbacher et al., 2010)	Presents CTA of cyber-security analysts about their goals, concerns and data they analyse, to build visualisation solutions for them.
Visualizing Cyber Security: Usable Workspaces	Glenn Fink, Christopher North, Alex Endert and Stuart Rose (Fink et al., 2009)	Presents a study of cyber-security analysts views and concerns of using visualisation solutions for the tasks they perform.
The Real Work of Computer Network Defense Analysts	Anita D'Amico and Kirsten Whitley (D'Amico & Whitley, 2007)	Presents CTA of cyber-security analysts about their day-to-day operations and cognitive requirements for designing visualisations for them.
Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts.	Anita D'Amico, Kirsten Whitley, Daniel Tesone, Brianne O'Brien and Emilie Roth (D'Amico et al., 2005)	Presents CTA of cyber-security analysts which gave insight into the roles, goals, obstacles and activities of the analysts in an organisation.

3.2.2 Generating Initial Codes

The initial list of codes was manually generated by the author, by attaching names to excerpts of data. These codes were collated in a codebook. Figure 3.2 displays an extract of the initial list of codes, along with the excerpts of data it refers to. Tables 3.2, 3.3, 3.4 and 3.5 present all the codes, along with the frequency of occurrence in the data.

[4] https://www.qsrinternational.com/product/nvivo-mac



Internals\\Information Visualization-2010-Erbacher-204-19
2 references coded, 0.16% coverage

Reference 1: 0.12% coverage

one main goal is to get consolidated data (from firewalls, proxies, internet histories and so on) and then be able to filter out noise. This allows the analyst to see trends in the data.

Reference 2: 0.04% coverage

Users also need the ability to manipulate the entire viewpoint.

Internals\\Usable workspaces
2 references coded, 0.13% coverage

Reference 1: 0.05% coverage

able to filter, join, and transform the data without losing or altering the original.

Figure 3.2: Extract of initial codes (on the left), with excerpt of data (on the right), generated in NVivo 11 Software [4].

3.2.3 Searching, Reviewing and Defining the Themes

The codebook was searched to find potential themes represented by the codes. The potential themes were reviewed and refined on the basis of the literature and the research questions. The potential themes were finalised, according to the data they represent.

Four themes were identified during this process:

1. ***Analysis of Data:*** Task performed by cyber-security analysts;
2. ***Data:*** Type of data used to perform the task;
3. ***Features of Visualisation:*** Features required to perform the task;
4. ***Role of Analyst:*** The cyber-security analyst that performs the task.

Note: In Chapter 4, *EEVi* is validated and updated according to the feedback from the expert-review. As part of this review the terminology of the themes is updated to the following, which is explained in Section 4.4.1.1:

1. Analysis of Data is replaced by ***Goal***
2. Data is replaced by ***Type of Data***
3. Features of Visualisation is replaced by ***Characteristics of Visualisation***
4. Role of Analyst is replaced by ***Role of End-User***

For ease of reading, the themes will be referred to, by the updated terminology and not the ones initially identified in the Thematic Analysis.

3.2.4 Final Report

The process of thematic analysis led to the identification of a set of themes, codes and cognitive relationships. The descriptions of all the codes originated purely from the data. The list and description of all identified codes and themes is displayed in Tables 3.2, 3.3, 3.4 and 3.5.

Table 3.2: Results of Thematic Analysis for the theme 'Goal', detailing the name of the code, their descriptions and number of occurrences in data.

Code	Description	Frequency
Triage Analysis (TA)	The first look at data. False positives are weeded out for further analysis within the order of a few minutes.	35 occurrences
Escalation Analysis (EA)	The investigation of suspicious activities and production of reports.	26 occurrences
Correlation Analysis (CA)	Data being searched for previously unrecognised patterns and trends.	14 occurrences
Threat Analysis (ThA)	An intelligent analysis to profile attackers and their motivations using additional sources.	25 occurrences
Impact Assessment (IA)	Identify impact, damage, and critical nodes that may be compromised or potentially reachable after a breach caused by malicious users or external source of attacks.	8 occurrences
Incident Response Analysis (IRA)	A recommendation or implementation of action against a confirmed incident.	27 occurrences
Forensic Analysis (FA)	When an analyst gathers and preserves data to inform and support law enforcement agencies.	13 occurrences
Security Quality Management (SQM)	The task related to services, such as tutorials or training, that maintain the quality of information security in an organisation.	5 occurrences

Table 3.3: Results of Thematic Analysis for the theme 'Type of Data', detailing the name of the code, their descriptions and number of occurrences in data.

Code	Description	Frequency
Raw Data	Most elemental data, usually in a very large quantity, which is passed through an automated process to filter.	21 occurrences
Interesting Activity	Data flagged by automated processes and inspected by an analyst, usually consists of a large number of false positives.	12 occurrences
Suspicious Activity	Data that is anomalous after the initial *TA* and needs to be monitored;	11 occurrences
Incident	The point when the occurrence and seriousness of activity is confirmed and formally reported.	20 occurrences
Intrusion Set	Sets of related *Incidents* that are given increased attention and resources to detect, understand and respond to.	6 occurrences
Source Data	Data gathered from an intrusion used for further analysis or reporting.	5 occurrences
Security Regulations ***(Security Policies)***	Regulations defined by the government or organisations relating to cyber-security; also includes cyber law.	5 occurrences

Table 3.4: Results of Thematic Analysis for the theme 'Role of End-User', detailing the name of the code, their descriptions and number of occurrences in data.

Code	Description	Frequency
Real-Time Analyst	Performs *Triage Analysis.*	1 occurrence
Lead Analyst	Performs *Escalation Analysis.*	3 occurrences
Tactical Defender	Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems.	4 occurrences
Site-Specific Analyst	Performs *Correlation Analysis.*	3 occurrences
Threat Analyst	Performs *Threat Analysis.*	1 occurrence
Strategic Analyst	Works at the community level to understand implications of an attack and categorise it.	4 occurrences
Incident Handler/ Responder	Performs *Incident Response Analysis.*	2 occurrences
Forensic Analyst	Performs *Forensic Analysis.*	1 occurrence
IT Manager ***(Network Manager)***	Identifies impact damage after intrusion and arranges training and development.	9 occurrences

Table 3.5: Results of Thematic Analysis for the theme 'Characteristics of Visualisation', detailing the name of the code, their descriptions and number of occurrences in data.

Code	Description	Frequency
Alerts	A system to alert the user of the status of activity being investigated.	28 occurrences
Case-Building Capabilities ***(Investigation)***	Provides support to the user for the purpose of building a case.	20 occurrences
Chain of Custody	Maintains a log of users who have analysed data or had access to data from an incident.	3 occurrences
Collaboration ***(Communication)***	Enable users to communicate and collaborate with other analysts by sharing findings.	32 occurrences
Colour Highlighting	Using colour to highlight the risk level of activity to bring it to the user's attention.	11 occurrences
Correlation	Displays relationships between different data dimensions.	3 occurrences
Feedback ***(Communication)***	Provides feedback (to the manager) for tasks performed, which could be quantitative or qualitative.	32 occurrences
Filter	Allows the data to be easily filtered, joined or transformed without changing the original. Also allows the analyst to filter noise to be able to see trends.	20 occurrences
Flexibility	The ability to manipulate the focal point of the visualisation and support the analytical process.	18 occurrences
Impact Identification	The identification of vulnerabilities, malicious users or external source of attacks, the intended target of attacks or main resources of the system affected.	22 occurrences

Table 3.5: Results of Thematic Analysis for the theme 'Characteristics of Visualisation', detailing the name of the code, their descriptions and number of occurrences in data.

Code	Description	Frequency
Interoperation	The ability of a tool to work efficiently with other tools, applications, utilities or datasets.	5 occurrences
Investigatory Capabilities (Investigation)	Allow the investigation of data by providing a platform for rapid and open-ended foraging activities.	20 occurrences
Mitigation	Performs clean-up and containment and provides support for mitigation activities.	5 occurrences
Priorities	Use of a priority system to inform the user of the severity of attack.	2 occurrences
Real-Time Access (Speed)	Viewing real-time data within seconds to minutes of an event.	7 occurrences
Reporting (Communication)	Providing support for report building.	32 occurrences
Situational Awareness	An accurate picture of external and internal information to understand the state of all resources.	17 occurrences
Timeline	Order of events and activities that took place over a period of time to coordinate all views.	8 occurrences

The cognitive relationships influenced the development of *EEVi* by linking the themes to the model. The cognitive relationships formed between different codes led to a similar generic storyline of themes. This storyline was defined and formed the structure of *EEVi*, which is explained in greater detail in the next section.

3.2.5 Secondary Coder

To confirm the appropriate identification of codes and themes, an academic from the University of Southampton, who was consulted throughout the coding process, also performed coding on the same data to check for consistency.

3.3 Development of *EEVi* from the Thematic Analysis

The codes identified in the previous section were cognitively linked and led to the development of *EEVi*, which can be used to help design cyber-security visualisation solutions. The structure of the model can be seen in Figure 3.3.

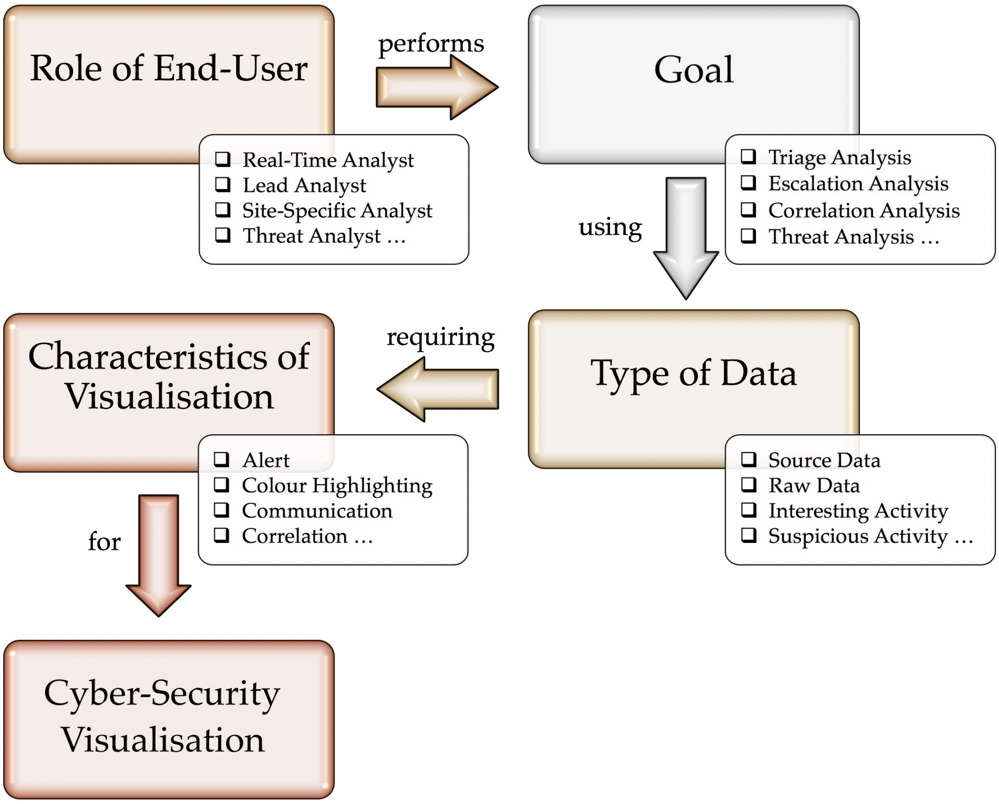


Figure 3.3: Structure of *EEVi*, a model to help design cyber-security visualisation for a task, developed from the results of the Thematic Analysis.

The model shows the conceptual relationships between the themes to help design cyber-security visualisation. These themes are defined by the set of codes, as shown in Tables 3.2, 3.3, 3.4 and 3.5. When codes from one theme are cognitively linked with codes from other themes, they form a cognitive relationship, which is represented by the flow through the themes. These relationships identify relevant codes from themes that would be imperative for a cyber-security visualisation of the performed task, as defined in the data. The generic structure of the model was defined as the *Role of End-User* performs *Goal* using *Type of Data* and requires *Characteristics of Visualisation* to help create a cyber-security visualisation solution.

EEVi represents cognitive relationships for each constituent component task of *EEVi* to determine the critical characteristics of visualisation that are required by cyber-security analysts. These cognitive relationships represent the guidelines to help design cyber-security visualisation for cyber-security analysts for each task identified.

These characteristics of visualisation represent the resources required by a cyber-security analyst to perform a task and not the aesthetics (i.e. the type or colour of graphs) that would be preferred by cyber-security analysts. The characteristics corresponding to each task can be identified in the guidelines of the component tasks.

The results of the thematic analysis led to the identification of eight component tasks, represented by the *Goal* theme. These eight tasks were identified from the data gathered from the CTA papers, as they were the most commonly conducted tasks by cyber-security analysts. These tasks are identified by different names in different organisations (D'Amico & Whitley, 2007) but they are performed in every organisation. The purpose of each task is clear from the definitions (Table 3.2).

The eight constituent component tasks of *EEVi* are discussed below. They are each defined, along with the identification of the analyst who performs the task, the data used to perform the task, and the characteristics of visualisation that would help visualisation designers design a cyber-security visualisation. These are explained with the codes, distance measures between codes and their corresponding excerpts of data to demonstrate the logic that led to the development of the cognitive relationship for each task, and hence the guidelines.

3.3.1 Guidelines for Triage Analysis

Table 3.6 presents the data illustrating which associated codes appeared within 20 words, before or after, the 'Triage Analysis' code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code 'Triage Analysis' and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of the cognitive relationship, is displayed in Figure 3.4.

Table 3.6: Results of Searches in NVivo to find Association between Associated Codes and **'Triage Analysis'** Code.

Code	**Appeared within 20 Words (*n* times)**
Real-Time Analyst	Yes (8)
Raw Data	Yes (2)
Interesting Activities	Yes (4)
Filter	Yes (3)
Speed	Yes (6)
Situational Awareness	Yes (2)

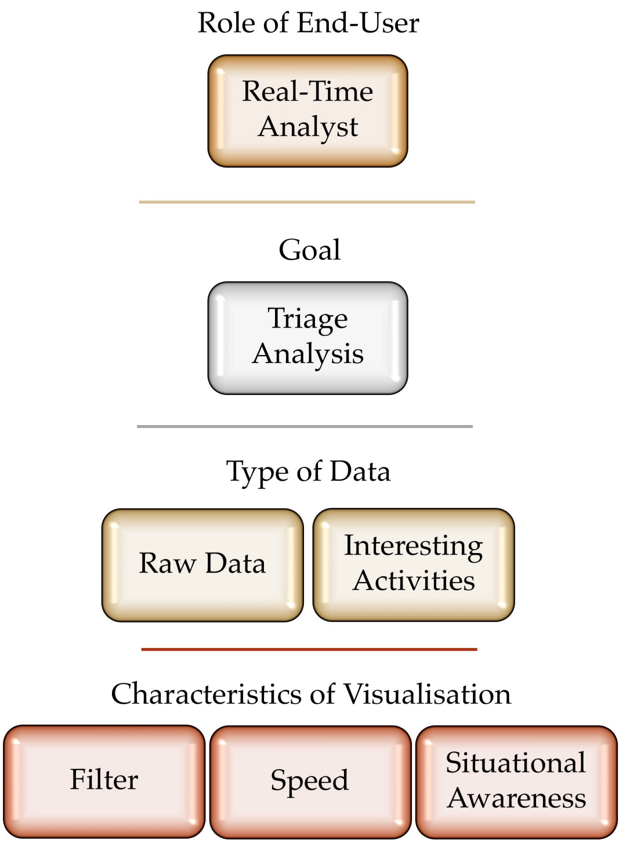


Figure 3.4: Visual representation of cognitive relationship for 'Triage Analysis', with themes and their constituent codes, showing the guidelines for designing the task.

The excerpts and codes that led to this relationship are explained below:

Goal: Triage Analysis is the first look at raw data (D'Amico & Whitley, 2007). At this stage, the analyst weeds out false positives for further analysis (D'Amico et al., 2005), which is performed within an order of a few minutes (Erbacher et al., 2010).

Role of End-User: Triage Analysis is usually performed by a Real-Time Analyst (D'Amico & Whitley, 2007).

Type of Data: It is the "...first look at the raw data and interesting activity" (D'Amico & Whitley, 2007) and hence uses Raw Data and Interesting Activities as types of Data. Raw Data is the most elemental data, usually in very large quantity and is passed through an automated process to filter. Interesting Activity is data that has been flagged by automated processes on raw data and is inspected by an analyst. This usually contains a large number of false positives (D'Amico & Whitley, 2007).

Characteristics of Visualisation: Visualisation for Triage Analysis requires Filter for "...initial filtering" (D'Amico & Whitley, 2007) and for "...weeding out false positives..." (D'Amico et al., 2005). Filter allows the ability to easily filter, join or transform data without changing the original (Fink et al., 2009) and also allows an analyst to filter out noise in order to identify trends (Erbacher et al., 2010). It also requires Speed of data access as the "...triage period should be on the order of minutes" (Erbacher et al., 2010) and a "...relatively fast decision..." (D'Amico & Whitley, 2007) needs to be made. Another important feature for Triage Analysis is having Situational Awareness as triage is performed at "...a highly abstract, situational-awareness level" (Erbacher et al., 2010). Situational Awareness gives an accurate picture of external and internal information in an overview to allow for rapid decision making and to allow for analysts to understand the state of all resources (Erbacher et al., 2010).

This would help to design a visualisation for a Real-Time Analyst performing Triage Analysis.

3.3.2 Guidelines for Escalation Analysis

Table 3.7 presents the illustrating which associated codes appeared within 20 words, before or after, the 'Escalation Analysis' code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code 'Escalation Analysis' and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.5.

Table 3.7: Results of Searches in NVivo to find Association between Associated Codes and **'Escalation Analysis'** Code.

Code	**Appeared within 20 words (n times)**
Lead Analyst	Yes (1)
Tactical Defender	Yes (1)
Suspicious Activities	Yes (5)
Incidents	Yes (2)
Communication	Yes (2)
Interoperation	Yes (5)

The excerpts and codes that led to this relationship are explained:

Goal: Escalation Analysis is an investigation of suspicious activities from the Triage stage and production of reports (D'Amico & Whitley, 2007). It may take from hours to multiple weeks to complete (D'Amico et al., 2005).

Role of End-User: Escalation Analysis is usually performed by Lead Analyst (D'Amico & Whitley, 2007) along with a Tactical Defender (Fink et al., 2009). A Tactical

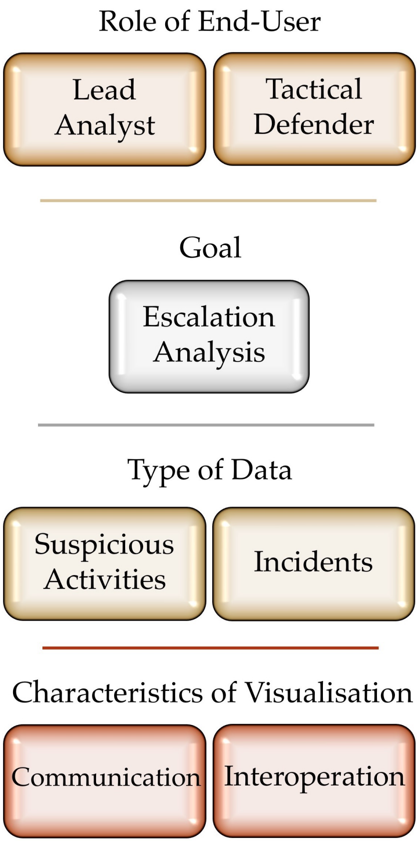


Figure 3.5: Visual representation of cognitive relationship for 'Escalation Analysis', with themes and their constituent codes, showing the guidelines for designing the task.

Defender defends against current and immediate attacks (D'Amico & Whitley, 2007) by maintaining situational awareness of the system and rapid rectification of problems (Fink et al., 2009).

Type of Data: They "...investigate suspicious activity[ies]" (D'Amico & Whitley, 2007) and hence use Suspicious Activity as a type of Data. Suspicious Activities is data that is anomalous after the initial triage analysis and needs to be monitored (D'Amico & Whitley, 2007). It also uses Incidents as a "...goal of escalation analysis is to produce incident reports" (D'Amico & Whitley, 2007) as the type of Data. Incidents are defined at the point when the occurrence and seriousness of an event is confirmed and formally reported (D'Amico & Whitley, 2007).

Characteristics of Visualisation: Visualisation for Escalation Analysis requires Communication as it is based on "...tip-offs from colleagues and cooperating organisations" (D'Amico et al., 2005). Communication enables analysts to communicate and collaborate with other analysts (Erbacher et al., 2010) by sharing findings (Fink et al., 2009; Mckenna et al., 2015) and providing support for report building (D'Amico & Whitley, 2007). It also requires Interoperation of data as "...the analyst marshals more data, usually from multiple data sources..." (Erbacher et al., 2010). Interoperation is the ability of a tool to work efficiently with other tools, applications, utilities or databases (Fink et al., 2009).

This would help to design a visualisation for a Lead Analyst or Tactical Defender performing Escalation Analysis.

3.3.3 Guidelines for Correlation Analysis

Table 3.8 presents the data illustrating which associated codes appeared within 20 words, before or after, the 'Correlation Analysis' code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code 'Correlation Analysis' and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.6.

Table 3.8: Results of Searches in NVivo to find Association between Associated Codes and **'Correlation Analysis'** Code.

Code	**Appeared within 20 words (*n* times)**
Site-Specific Analyst	Yes (1)
Tactical Defender	Yes (1)
Intrusion Sets	Yes (2)
Timeline	Yes (1)
Flexibility	Yes (2)
Investigation	Yes (1)

The excerpts and codes that led to this relationship are explained below:

Goal: Correlation Analysis is the search for patterns and trends in data, which may have been previously unrecognised (D'Amico & Whitley, 2007; D'Amico et al., 2005).

Role of End-User: Correlation Analysis is performed by Site-Specific Analyst (D'Amico & Whitley, 2007) along with a Tactical Defender (Fink et al., 2009).

Type of Data: It "...includes grouping data into intrusion sets" (D'Amico & Whitley, 2007) and hence uses Intrusion Sets as a type of Data. Intrusion Sets are sets of related Incidents that are given an increase in attention and resources to detect, understand, and respond (D'Amico & Whitley, 2007).

Characteristics of Visualisation: Visualisation for Correlation Analysis requires a Timeline view for "...search...in current and historical data..." (D'Amico & Whitley, 2007) and Flexibility for "...searches for patterns and trends..." (D'Amico et al., 2005).

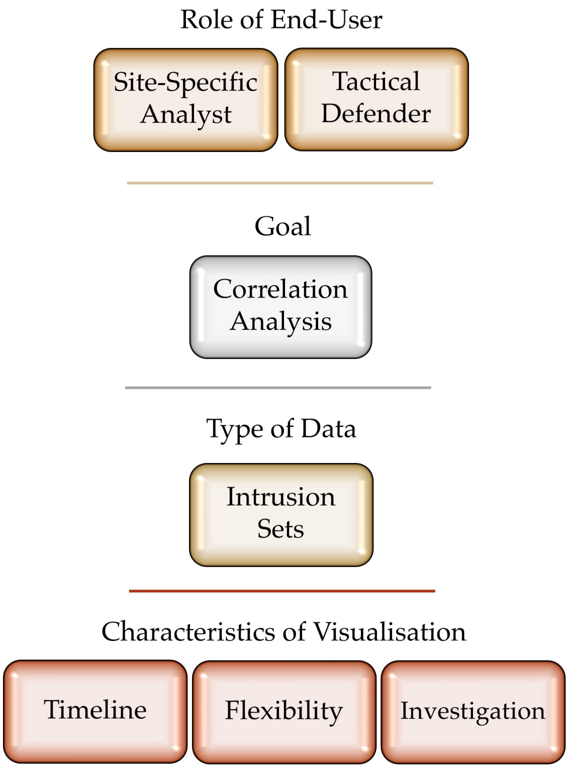


Figure 3.6: Visual representation of cognitive relationship for 'Correlation Analysis', with themes and their constituent codes, showing the guidelines for designing the task.

A timeline displays an order of incidents that have taken place over a period of time (Erbacher et al., 2010), and is used to coordinate all views of information over a period of time (Mckenna et al., 2015). Flexibility of visualisation gives the ability to manipulate the focus point of the visualisation (Erbacher et al., 2010) to support the analytical process (Fink et al., 2009). Another important feature for Correlation Analysis is the capability of Investigation for "...retrospectively reviewing...data...looking for unexplained patterns" (D'Amico & Whitley, 2007). Investigation capabilities would allow users to investigate data by supporting simultaneous investigations (Fink et al., 2009) by providing extensive capabilities for vulnerability assessment (Erbacher et al., 2010) and a platform for visually clarified distinctions between vulnerabilities and alerts (Mckenna et al., 2015).

This would help to design a visualisation for a Site-Specific Analyst or a Tactical Defender performing Correlation Analysis.

3.3.4 Guidelines for Threat Analysis

Table 3.9 presents the data illustrating which associated codes appeared within 20 words, before or after, the 'Threat Analysis' code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code 'Threat Analysis' and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.7.

Table 3.9: Results of Searches in NVivo to find Association between Associated Codes and **'Threat Analysis'** Code.

Code	**Appeared within 20 Words (n times)**
Threat Analyst	Yes (1)
Tactical Defender	Yes(2)
Strategic Analyst	Yes (4)
Intrusion Sets	Yes (2)
Correlation	Yes (3)
Interoperation	Yes (2)

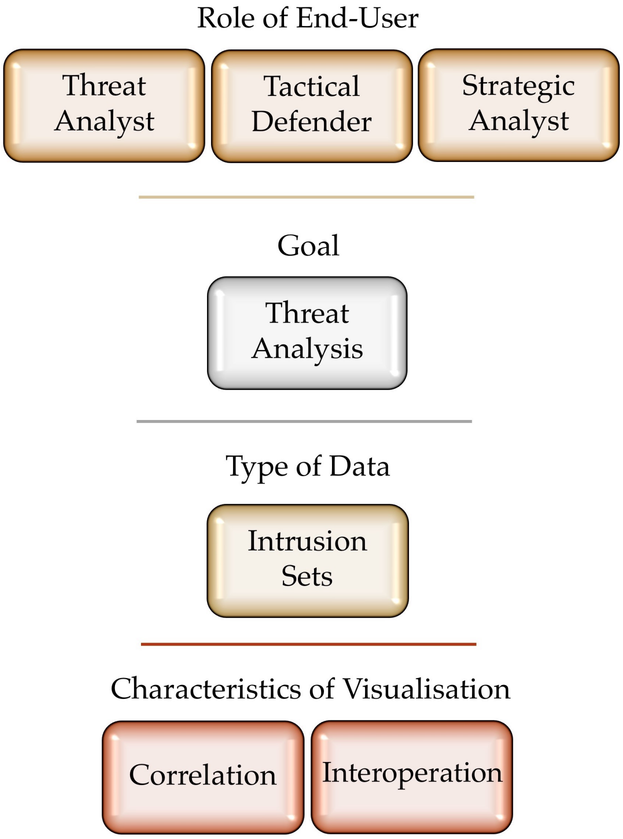


Figure 3.7: Visual representation of cognitive relationship for 'Threat Analysis', with themes and their constituent codes, showing the guidelines for designing the task.

The excerpts and codes that led to this relationship are explained below:

Goal: Threat Analysis is an intelligent analysis (D'Amico & Whitley, 2007) using multiple data sources to profile attackers and their motivations (D'Amico et al., 2005).

Role of End-User: Threat Analysis is performed by a Threat Analyst (D'Amico & Whitley, 2007) along with Tactical Defender and Strategic Analyst (Fink et al., 2009). A Strategic Analyst works at the community level (D'Amico & Whitley, 2007) to understand the implications of an attack and categorise it (Fink et al., 2009).

Type of Data: They also work with Intrusion Sets as a type of Data as "once incidents are confirmed...[the analysis] moves to...threat analysis..." (D'Amico & Whitley, 2007).

Characteristics of Visualisation: Visualisation for Threat Analysis requires Correlation as it uses "...additional data sources..." (D'Amico et al., 2005) and Interoperation as it uses "[additional other tools]...to gain additional insight..." (D'Amico & Whitley, 2007). Correlation visualises relationships between different data dimensions to improve analyst performance (Fink et al., 2009).

This would help to design a visualisation for a Threat Analyst, a Tactical Defender or a Strategic Analyst performing Threat Analysis.

3.3.5 Guidelines for Incident Response Analysis

Table 3.10 presents the data illustrating which associated codes appeared within 20 words, before or after, the 'Incident Response Analysis' code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code 'Incident Response Analysis' and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.8.

Table 3.10: Results of Searches in NVivo to find Association between Associated Codes and **'Incident Response Analysis'** Code.

Code	Appeared within 20 Words (*n* times)
Incident Handler/Responder	Yes (1)
Tactical Defender	Yes (2)]
Strategic Analyst	Yes (2)
Intrusion Sets	Yes (2)
Mitigation	Yes (3)
Situational Awareness	Yes (1)

The excerpts and codes that led to this relationship are explained below:

Goal: Incident Response Analysis requires the analyst to recommend or implement actions against a confirmed incident (D'Amico & Whitley, 2007; D'Amico et al., 2005).

Role of End-User: Incident Response Analysis is usually performed by Incident Handler/Responder (D'Amico & Whitley, 2007) along with Tactical Defender or Strategic Analyst (Fink et al., 2009).

Type of Data: It is a "...reaction to a confirmed incident" (D'Amico et al., 2005) and hence uses Intrusion Sets as a type of Data.

Characteristics of Visualisation: Visualisation for Incident Response Analysis requires Mitigation as it "...recommends and/or implements a course of action..." (D'Amico & Whitley, 2007). Mitigation capabilities would perform clean-up and containment and would also provide mitigation solution and/or activities (Erbacher et al., 2010). Situational Awareness, is another feature of visualisation as it "...involves assessing the tradeoffs of potential responses and how the responses will impact organisational mission" (D'Amico & Whitley, 2007).

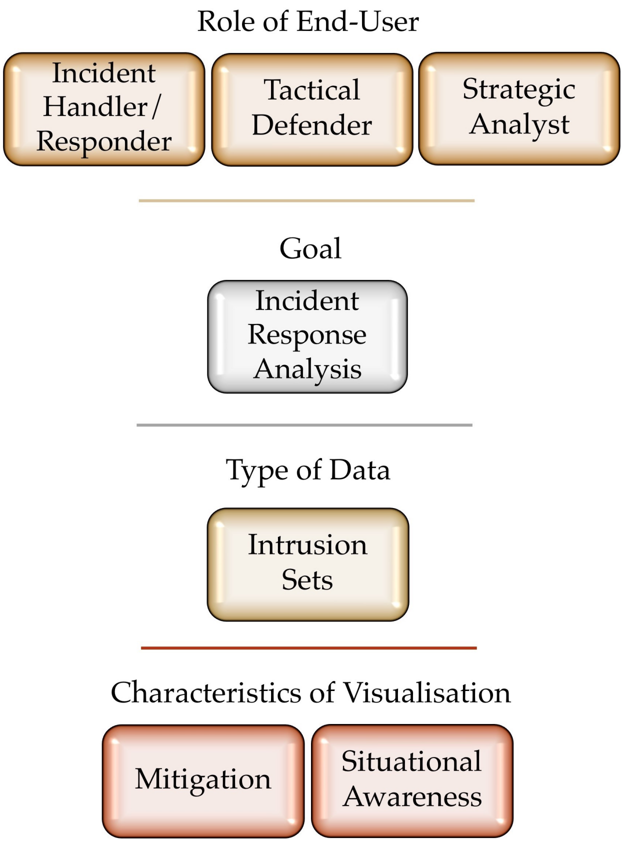


Figure 3.8: Visual representation of cognitive relationship for 'Incident Response Analysis', with themes and their constituent codes, showing the guidelines for designing the task.

This would help to design a visualisation for an Incident Handler/Responder, a Tactical Defender, or a Strategic Analyst performing Incident Response Analysis.

3.3.6 Guidelines for Forensic Analysis

Table 3.11 presents the data illustrating which associated codes appeared within 20 words, before or after, the ‘Forensic Analysis’ code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code ‘Forensic Analysis’ and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.9.

Table 3.11: Results of Searches in NVivo to find Association between Associated Codes and **‘Forensic Analysis’** Code.

Code	Appeared within 20 Words (n times)
Forensic Analyst	Yes (1)
Source Data	Yes (4)
Security Policies	Yes (4)
Reporting	Yes (2)
Investigation	Yes (3)

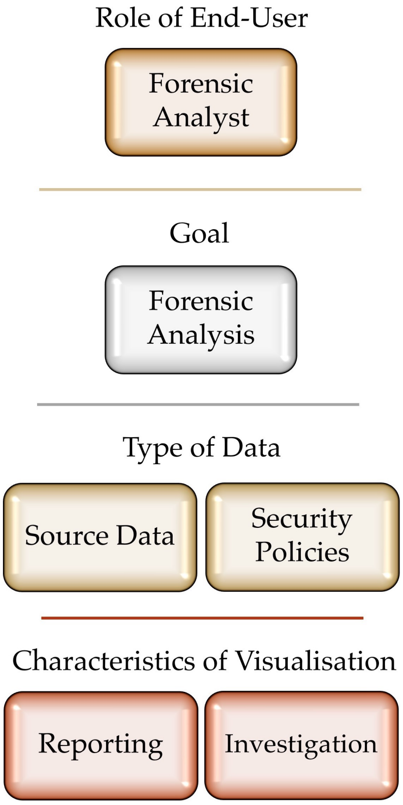


Figure 3.9: Visual representation of cognitive relationship for ‘Forensic Analysis’, with themes and their constituent codes, showing the guidelines for designing the task.

The excerpts and codes that led to this relationship are explained below:

Goal: Forensic Analysis is the gathering and preservation of data to support law enforcement agencies (D'Amico & Whitley, 2007; D'Amico et al., 2005). It may take from hours to a few weeks to perform (Erbacher et al., 2010).

Role of End-User: Forensic Analysis is performed by Forensic Analyst (D'Amico & Whitley, 2007).

Type of Data: It "...preserves evidence in support of a law enforcement investigation" (D'Amico et al., 2005) and hence uses Security Policies as a type of Data. These are policies defined by the government or organisations (Erbacher et al., 2010) relating to cyber-security, including cyber law. It would also require Source Data of the confirmed incident found.

Characteristics of Visualisation: Visualisation for Forensic Analysis requires Investigation for "...gathering evidence..." (D'Amico & Whitley, 2007) and Reporting to create reports for law-enforcement agencies.

This would help to design a visualisation for a Forensic Analyst performing Forensic Analysis.

3.3.7 Guidelines for Impact Assessment

Table 3.12 presents the data illustrating which associated codes appeared within 20 words, before or after, the 'Impact Assessment' code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code 'Impact Assessment' and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.10.

Table 3.12: Results of Searches in NVivo to find Association between Associated Codes and **'Impact Assessment'** Code.

Code	**Appeared within 20 Words (*n* times)**
Network Manager	Yes (2)
Source Data	Yes (2)
Identification	Yes (3)
Situational Awareness	Yes (2)

The excerpts and codes that led to this relationship are explained below:

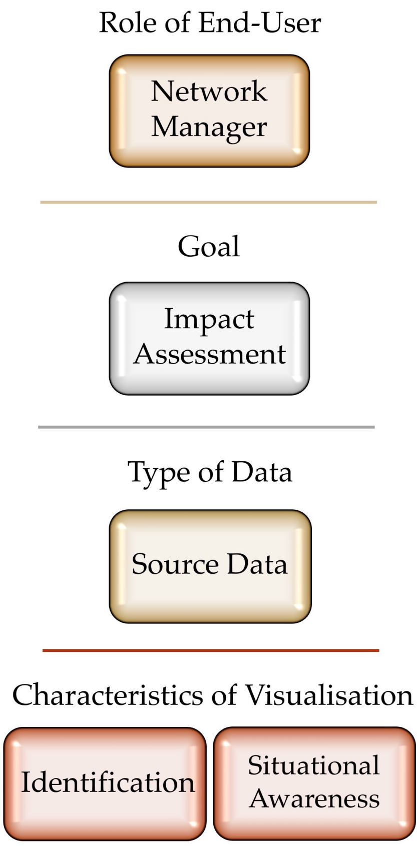


Figure 3.10: Visual representation of cognitive relationship for Impact Assessment, with themes and their constituent codes, showing the guidelines for designing the task.

Goal: Impact Assessment is the task of identification of impact, damage, and potential critical nodes that may be reachable after a breach (Erbacher et al., 2010).

Role of End-User: Impact Assessment is performed by a Network Manager.

Type of Data: An analyst uses Source Data of the confirmed incident as a type of Data to perform Impact Assessment.

Characteristics of Visualisation: Visualising Impact Assessment would require "Impact identification...[for identification of] mission impact and system impact..." (Erbacher et al., 2010). It refers to the capabilities to identify vulnerabilities, malicious users, intended target of attacks, and main resources of the system affected (Erbacher et al., 2010). Situational Awareness is also required, to find which "...domain...[of the system under attack] is not protected enough..." (Erbacher et al., 2010).

This would help to design a visualisation for a Network Manager performing Impact Assessment.

3.3.8 Guidelines for Security Quality Management

Table 3.13 presents the data illustrating which associated codes appeared within 20 words, before or after, the ‘Security Quality Management’ code, and the number of occurrences. Looking at the data, 20 words is within 2 sentences of the code ‘Security Quality Management’ and the data was still referring to the code. Beyond that the data refers to other topics. Appendix A presents the results for all identified codes. A visual representation of this relationship is displayed in Figure 3.11.

Table 3.13: Results of Searches in NVivo to find Association between Associated Codes and **‘Security Quality Management’** Code.

Code	**Appeared within 20 Words (n times)**
Network Manager	Yes (1)
Source Data	Yes (1)
Security Policies	Yes (2)
Communication	Yes (3)

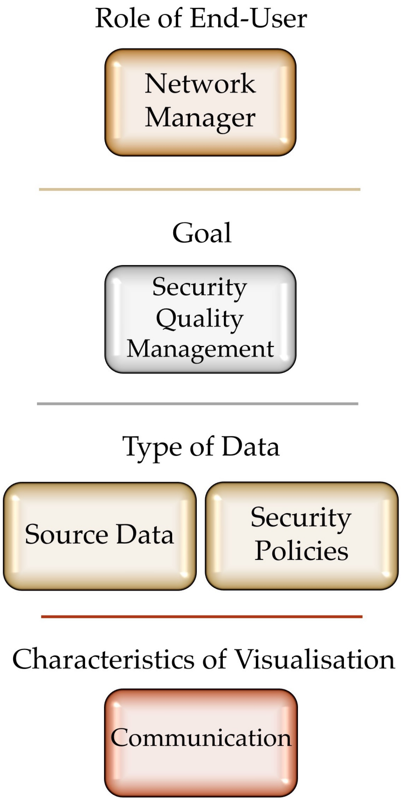


Figure 3.11: Visual representation of cognitive relationship for ‘Security Quality Management’, with themes and their constituent codes, showing the guidelines for designing the task.

The excerpts and codes that led to this relationship are explained below:

Goal: Security Quality Management is a task related to services that support information security (D'Amico et al., 2005) in an organisation like tutorials or training (Erbacher et al., 2010).

Role of End-User: Security Quality Management is performed by a Network Manager

Type of Data: An analyst uses Source Data of the incident and Security Policies of the organisation as types of Data, to perform Security Quality Management activities.

Characteristics of Visualisation: Visualising Security Quality Management would require Communication as it includes "...services that support information security..." (D'Amico & Whitley, 2007) and these [services] need to be communicated back to the Network Manager.

This would help to design a visualisation for a Network Manager performing Security Quality Management.

3.4 Discussion

EEVi was developed to bridge the research gap by standardising design techniques for cyber-security visualisation for the performed task. These guidelines are formed as a result of cognitive relationships associated with the performed task, in the logic sequence derived from *EEVi*'s structure (Figure 3.3). Using 'Thematic Analysis' to develop *EEVi* led to the identification of storylines which represented guidelines for each task that supports cyber-security visualisation solutions. The guidelines for eight component tasks were represented in this section. These tasks were identified during the process of qualitative coding as these were the most common tasks conducted by cyber-security analysts. A good domain model such as *EEVi*, as based on the information in this chapter, must consist of *Goal*, *Type of Data*, *Role of End-User* and *Characteristics of Visualisation*, as outlined for each task.

EEVi addresses SRQ_1 by developing an appropriate model to design and evaluate cyber-security visualisation for the end-user (cyber-security analysts). Additionally, SRQ_2 is addressed by the associated guidelines presented by the component tasks of the model. However, there was a need to incorporate the feedback from cyber-security analysts and visualisation designers to include their perspectives in the model. This was executed by a validation process, as explained in Chapter 4.

Chapter 4

Validation of *EEVi*

An expert-review by seven cyber-security analysts and six visualisation designers was conducted to update and validate the model developed in Chapter 3. This chapter details the techniques used, the arrangements for the expert-review, the demographics of the experts, and the feedback from the review.

4.1 Background of Techniques Used

The purpose of performing validation is to ensure that the product fulfils its intended purpose (ISO/IEC TR 19759:2015, 2015). Validation provides assurance that a product or system meets the needs of end-users and any other identified stakeholders (ANSI/PMI 99-001-2013, 2013). Validation is commonly undertaken by a group of reviewers inspecting the product for mistaken assumptions, lack of clarity, or divergence from standard practice. Validations such as this can illustrate that a novel model like *EEVi* will meet the needs of the cyber-security analysts to help visualisation designers in designing cyber-security visualisations for a specific task.

4.1.1 Expert-Review

Expert-reviews are used to determine the quality of an analysis according to criteria, which increases the credibility of the analysis (Patton, 2014). Laboratory experimental evaluation techniques are not very useful during exploratory phases when ideas are still being defined (Tory & Moller, 2005). Expert-reviews provide quick and valuable insights, along with highlighting important issues at a higher cognitive level.

To ensure equal representation, the experts were selected from the cyber-security and visualisation design fields. The number of experts was determined by Nielsen (1994)'s Discounted Expert Review Theory. According to this theory, 75% of the usability issues can be found between three and five experts, after which the responses reach a point of saturation. Hence, to avoid omitting salient facts, at least five experts from each area are required to evaluate the model.

4.1.2 Integrative Mixed Methods Approach

Integrative Mixed Methods (IMM) is an approach for the concurrent use of qualitative and quantitative methods in a manner that offers the benefits of both analysis types on the same set of data (Castro, Kellison, Boyd, & Kopak, 2010). An analysis using IMM follows this process, defined by (Castro et al., 2010):

Step 1 ***Eliciting Responses:*** Identify the relevant responses that answer a specific focus question;

Step 2 ***Identifying Response Codes:*** Encode the identified relevant responses to the focus question;

Step 3 ***Creating Thematic Categories:*** Create categories that are assigned several response codes with functionally equivalent meanings;

Step 4 ***Scale Coding:*** Add the dimension of a frequency of response, or intensity of response, to the thematic category. At this stage, the qualitative data represents their quantitative measure, Section 4.1.2.1;

Step 5 ***Data Analytic Approaches:*** Conduct statistical analyses on the measured values to examine the associations of the data. The statistical analysis used is explained in Section 4.1.2.2;

Step 6 ***Creating Storylines and Re-contextualisation:*** Re-contextualise the data by returning to the original context in which the observations were made. This is performed by relating the results of the statistical analysis to generate stories relevant to the analysed data. This is explained in Section 4.1.2.3.

4.1.2.1 Scale Coding - Quantification of Qualitative Data

Quantification of this qualitative data was performed by following the first four steps of the IMM approach. The indicator measurements by Purwandari (2013) inspired the use of a Likert scale from very negative (-2) to very positive (+2) for the responses. The results were used to match responses to the scales and quantify the responses. This is detailed in Section 4.4.2.

4.1.2.2 Data Analytic Approaches for Statistical Analysis

The Data Analytical approaches used for this study are defined below:

Test for Differences - *Mixed Design ANOVA:* This tests for differences between data sets. Here, it is used to check whether there are any statistically significant differences between the responses of visualisation designers and cyber-security analysts for each characteristic of visualisation for each component task. ANOVA (ANalysis Of VAriance) is used to detect statistically significant differences between sample means and is used to determine what proportion of variation in the dependent variable can be attributed to independent variable(s) or groups (Rutherford, 2012). Mixed Design ANOVA is used in this research. It combines repeated measures (or repeated results) with the proportion of variation between the independent variable(s) or groups (Field, 2013).

Test for Agreement - *Pearson's r Correlation:* This tests for agreement between different data elements. In this case, *Pearson's r Correlation* is used to check whether there is any statistically significant agreement between the responses of visualisation designers and cyber-security analysts for each of the characteristics of visualisation for each component task.

4.1.2.3 Creating *Storylines* and Re-contextualisation for Modification of Component Tasks

The final step of the IMM approach was to re-contextualise the results in the original context. For this purpose, the quantified responses from the cyber-security analysts were divided by average score into three regions; those with a mean between +1 and +2, those with a mean between 0 and +1, and those with means less than 0. The scatterplot formed as a result of *Pearson's r Correlation* was used to display these results. The regions were divided on the basis of feedback from the cyber-security analysts, because they would be the end-users of the cyber-security visualisations.

4.2 Arrangements for Expert-Review

Seven cyber-security analysts and six visualisation designers were interviewed in a semi-structured format (see Appendix C). The experts were asked some general questions about their work and knowledge of their respective fields. This was followed by a discussion of the model structure in detail. Then, there was a conversation about the structure and definition of each constituent component task. Finally, they were asked about the usefulness of the model and if they had any comments. The interviews were qualitatively analysed using NVivo[1], and quantitatively analysed using IBM SPSS[2], and GraphPad Prism[3].

All participants were interviewed to understand their individual points of view in order to update the model to accommodate both analysts' and designers' perspectives to minimise the disparity between the two groups.

4.2.1 Ethics Approval for Expert-Review

The expert-review was conducted with approval from Ethics and Research Governance (ERGO) committee under reference number $ERGO/FPSE/23974$.

Under the guidelines of the ethical approval, interviews and questionnaire surveys undertaken in the period from 16 November 2016 to 1 November 2019 were approved, conforming to the Data Protection Act (DPA) Plan and Participant Information Sheet, which was approved with the application. Each participant was given a copy of the DPA Plan and Participant Information Sheet before they gave written or verbal consent to take part in the interviews. See Appendix B for a copy of the DPA Plan and Participant Information Sheet.

4.3 Demographic Information concerning the Experts

The experts were identified in three ways: (i) using work connections at the University of Southampton by recognising academics with technical expertise, (ii) through professional connections made at relevant international conferences (ICITST[4] 2016) and summer school (Social Aspects of Cyber Security Risk 2016) targeting industry and academic practitioners, (iii) by contacting practitioners in the author's home country with the relevant expertise in performing tasks related to cyber-security. 25 experts were identified and contacted directly by email. Of these, 13 experts (seven cyber-security analysts and six visualisation designers) were selected to take part in the review, to ensure a heterogeneous mix of geographical location, and expertise. They were interviewed after gathering explicit written or verbal consent, following the ethical approval guidelines (Section 4.2.1). Table 4.1 displays the consolidated information concerning each expert.

[1] https://www.qsrinternational.com/product/nvivo-mac [Accessed: 5 May, 2017]

[2] https://www.ibm.com/analytics/us/en/technology/spss/ [Accessed: 5 May, 2017]

[3] https://www.graphpad.com/scientific-software/prism/ [Accessed: 5 May, 2017]

[4] International Conference for Internet Technology and Secured Transactions - https://icitst.org/ [Accessed: 14th May, 2019]

Table 4.1: Demographic information concerning the experts, interviewed for the expert-review to validate *EEVi*.

Participant ID		Country	Current Job Description	Experience
Cyber-Security Analyst	C1	UK	System Analysis Engineer and PhD student at University of Southampton	7 years
	C2	India	Cyber Crime Investigator (Law Enforcement)	3 years
	C3	India	Network Security Superintendent at Central Bureau of Investigation (Law Enforcement)	10+ years
	C4	India	Cyber Law Enforcement Officer at Indian Police Service (Law Enforcement)	9 years
	C5	Malaysia	Cyber-Security Policy and Strategy Expert at PriceWaterhouseCoopers	29 years
	C6	India	Lead Cyber-Security Consultant	16 years
	C7	USA	Cyber-Security Operations and Project Manager at Hindustan Computers Limited America	18 years
Visualisation Designers	V1	USA	PhD in Data Visualisation Design at University of Utah	4+ years
	V2	UK	PhD in HCI Design at University of Southampton	11 years
	V3	UK	Research Staff at University of Southampton	6 years
	V4	Brazil	Design Researcher	10+ years
	V5	UK	Postdoctoral Researcher at Royal Holloway, University of London	6 years
	V6	UK	Director of a User Experience Design Company	10+ years

4.3.1 Cyber-Security Analysts

This section presents demographic information concerning the cyber-security analysts who participated in the expert-review.

Participant C1 is a systems analysis engineer and a PhD student at the University of Southampton, UK, with 7 years of experience in the field of cyber-security. C1 has experience using some cyber-security visualisation tools and rates their knowledge of the field as 2 on a scale from 1 to 10.

Participant C2 is a cyber crime investigator dealing with network security at a law enforcement agency in India with 3 years of experience in the field of cyber-security. C2 has no experience using cyber-security visualisation tools.

Participant C3 is a network security superintendent dealing with network security and e-governance projects at the Central Bureau of Investigation (law enforcement agency), India, with over 10 years of experience in the field of cyber-security. C3 has no experience using cyber-security visualisation tools.

Participant C4 is a cyber-regulatory and enforcement issues officer with the Indian Police Service, India, with 9 years of experience in the field of cyber-security. C4 has no experience using cyber-security visualisation tools but rates their knowledge of the field as 5.5 on a scale from 1 to 10.

Participant C5 is a cyber-security policy and strategies expert at PricewaterhouseCoopers, Malaysia, with 29 years of experience in the field of cyber-security. C5 has experience using some cyber-security visualisation tools and rates their knowledge of the field as 3 on a scale from 1 to 10.

Participant C6 is the lead cyber-security consultant at Ebusiness Management Consultancy, India, with 16 years of experience in the field of cyber-security. C6 has experience using some cyber-security visualisation tools and rates their knowledge of the field as 6 on a scale from 1 to 10.

Participant C7 is a cyber-security operations and project manager at Hindustan Computers Limited America, USA, with 18 years of experience in the field of cyber-security. C7 has experience using some cyber-security visualisation tools and rates their knowledge of the field as 8 on a scale from 1 to 10.

4.3.2 Visualisation Designers

This section presents demographic information concerning the visualisation designers who participated in the expert-review.

Participant V1 is a PhD student pursuing data visualisation design at the University of Utah, USA, who has also worked in data design at MIT Lincoln Laboratory, USA with over 4 years of experience in the field of visualisation design. V1 has experience using some cyber-security visualisation tools and rates their knowledge of the field as 7 on a scale from 1 to 10.

Participant V2 is a PhD student pursuing design in HCI at the University of Southampton, UK, who has also worked in data design in Brazil with 11 years of experience in the field of visualisation design. V2 has no experience using cyber-security visualisation tools and rates their knowledge of data visualisation as 10 on a scale from 1 to 10.

Participant V3 is a research staff member pursuing qualitative participation design for HCI at the University of Southampton, UK, with 6 years of experience in the field of visualisation design. V3 has no experience using cyber-security visualisation tools and rates their knowledge of data visualisation as 4 on a scale from 1 to 10.

Participant V4 is a design and visual analytics researcher at an IT company in Brazil with over 10 years of experience in the field of visualisation design. V4 has no experience using cyber-security visualisation tools.

Participant V5 is a postdoctoral researcher pursuing mapping social data for cyber-security at Royal Holloway, University of London, UK, with 6 years of experience in the field of visualisation design. V5 has experience using some cyber-security visualisation tools and rates their knowledge of data visualisation as 3 on a scale from 1 to 10.

Participant V6 is the director of a user experience (UX) design company that develops customised design solutions in the UK with over 10 years of experience in the field of visualisation design. V6 has no experience using cyber-security visualisation tools and rates their knowledge of data visualisation as 6.5 on a scale from 1 to 10.

4.4 Findings from Expert-Review

General findings from the expert-review are presented below:

1. All experts unanimously agreed that the model represented good fundamental guidelines for cyber-security visualisation;
2. All experts unanimously agreed that the model is useful to evaluate cyber-security visualisation;
3. The experts observed that some characteristics of visualisation are useful for all component tasks: *Reporting* (*C1, C2, C5, V1, V2 and V6*), *Interoperation* (*C5, C7, V1 and V2*), *Collaboration* (*V1, V2 and V6*), *Flexibility* (*C1, V1 and V3*), *Situational Awareness* (*C3, V2 and V4*) and *Filter* (*C7 and V1*) (Table 3.5 defines these characteristics).

The experts commented about *EEVi* as follows:

- *C3* said that such a model is the *"...need of the hour...[and this] can fill the [knowledge] gap...[and] nobody has thought of this..."*.
- *C1* said that *"...we need this... [and its] going in the right direction..."*.
- *C6* said that the *"...[component tasks are] covered in a good manner and across all controls we know..."*.
- Finally, *C4* and *V2* applauded the research by saying that it is a *"...great effort..."* and *"...it's good [and] specific [to the task at hand]..."*.

It was concluded that the experts believed the model to be useful to help design visualisations for cyber-security. The following sub-sections focus on revising the model based on the feedback received from the experts.

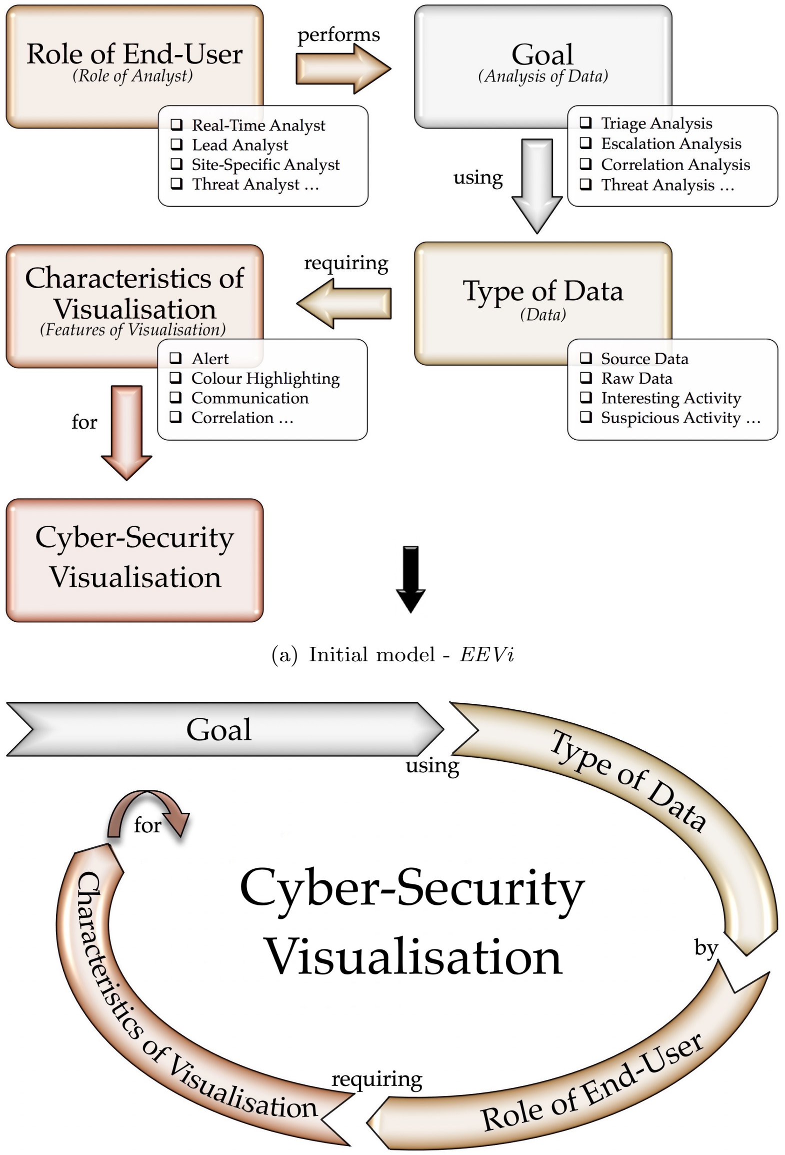
4.4.1 Revisions of *EEVi* on the basis of the Expert-Review

The thirteen experts were presented with the original model (Chapter 3). On the basis of their assessment, some revisions were made to the terminology and structure of *EEVi*. All experts unanimously agreed with the logic of the model, but four experts (*C2, C4, V1 and V4*) did not agree with the model representing their organisations' logic of how tasks are performed. Their feedback can be divided into two main areas: the terminology used, and the structure of *EEVi*. The revised version of *EEVi* is displayed in Figure 4.1(b).

4.4.1.1 Terminology used in *EEVi*

Some experts (*C6, V4 and V6*) believed that the terminology used to define the model could be more distinct. On the basis of their comments, the terminology was modified:

- The term *Analysis of Data* was replaced by *Goal* to make the distinction more apparent about what the goal of each task is, which in turn sets the goal for the visualisation for the task at hand;
- *Data* was updated to *Type of Data* to make the elements of this category more distinct;
- The term *Role of Analyst* was revised to *Role of End-User* to clearly identify the end-user who would be using the resultant visualisations;



(a) Initial model - *EEVi*

(b) Revised and Validated *EEVi*

Figure 4.1: Transformation of *EEVi* from sequential flow to an iterative cyclic flow, with updated terminology.

- *Features of Visualisation* was modified to *Characteristics of Visualisation* to focus on the aspects of visualisation that aid cyber-security analysts with their task rather than the features, which could be interpreted as aesthetics.

The revised *EEVi* is shown in Figure 4.1(b) The *Goal* identifies the goals of each task at hand, which can be performed using the *Type of Data* by the *Role of End-User* requiring the *Characteristics of Visualisation* to make the resultant visualisation for cyber-security analysts. The eight constituent component tasks of *EEVi*, introduced in Section 3.3, are revised in Section 4.4.4.

4.4.1.2 Structure of *EEVi*

Some experts (*C2, C3, C4, C6, C7 and V5*) believed that representation of the model could be enhanced by changing the flow of logic and structure of the model.

They claimed that *Goal* and *Type of Data* should be the first aspects to be considered, followed by the *Role of End-User* and lastly the *Characteristics of Visualisation* which represent the critical resources identified to perform the task. This logic flow more accurately represented the way in which organisations perform these tasks.

The experts also speculated about the structure of the model being sequential and not allowing for an iterative flow, when necessary. As a result, the structure of *EEVi* was revised from a sequential flow (Figure 4.1(a)) to a cyclic flow (Figure 4.1(b)). The initial aspect is clearly defined as the entry point into a cyclic flow, and the final aspect can either iterate back to the initial task and continue the loop or close the loop with *Cyber-Security Visualisation.*

4.4.2 Quantification of Qualitative Data for Statistical Analyses

Following revisions to *EEVi*, the next step was to analyse the data and update the component tasks on basis of the feedback received. Prior to these updates, statistical analysis was conducted assess the differences and agreement between responses of the visualisation designers and the cyber-security analysts on the *Characteristics of Visualisation* for specific tasks. However, to perform these tests, the data for each component task had to be quantified.

The first four steps of the IMM approach (see Section 4.1.2) were implemented to quantify the qualitative feedback from the expert-review on the basis of the indicator measurements defined for each expert. The IMM steps, as defined by Castro et al. (2010), are:

Step 1 **Eliciting Responses:** Identify the relevant responses of *Characteristics of Visualisation* for each component task;

Step 2 **Identifying Response Codes:** Encode the identified relevant responses to each *characteristic of visualisation* defined;

Step 3 **Creating Thematic Categories:** The five thematic categories were created: 'very positive response', 'positive response', 'neutral or no response', 'negative response', and 'very negative response', similar to the indicator measurements defined by Purwandari (2013). Each response code was assigned to one of these categories on the basis of the relevant responses encoded by it;

Step 4 **Scale Coding:** The thematic categories were quantified with values +2, +1, 0, -1 and -2, respectively.

Each *Characteristic of Visualisation* was quantified in this manner. Figure 4.2 shows an example of the process applied to the component task 'Triage Analysis' (TA) for *Participant V6*. As can be seen, the relevant responses for the *Characteristics of Visualisation* were given to response codes[5], which represented the three characteristics of visualisation for TA. The response codes, based on the level of positivity or negativity, are assigned to one thematic category. This category represents a quantifiable number which is identified in the scale coding. For example, 'TA_Speed' is quantified as +2; 'TA_SA' (Situational Awareness) is quantified as 0; and 'TA_Filter' is quantified as +2.

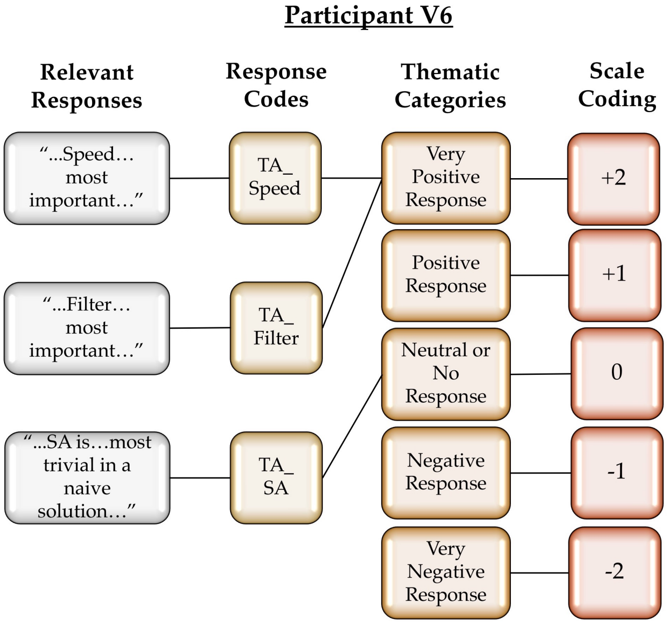


Figure 4.2: IMM process (first four steps) used to quantify qualitative data, as illustrated by the example of participant *V6* for responses regarding *characteristics of visualisation* for 'triage analysis'.

The quantified data for all characteristics of visualisation is given in Table 4.2. +2 represents a *very positive response* down to -2 representing a *very negative response*. The rows are the participant identity, where *C* is for cyber-security analysts and *V* is for visualisation designers, and the first column presents the *characteristics of visualisation* (Refer to Table 3.5 for definitions of these) per task.

[5] In this example, there was one relevant response for each response code. However, it is possible for more than one relevant response to be found for each response code.

Table 4.2: Data quantified from qualitative data in to numeric values -2 to +2, using the IMM process for statistical analysis of expert-review.

Characteristic of Visualisation	C1	C2	C3	C4	C5	C6	C7	V1	V2	V3	V4	V5	V6
Triage Analysis - Filter (TA-F)	0	2	2	2	2	2	2	2	1	1	1	1	2
Triage Analysis - Situational Awareness (TA-SA)	2	1	0	2	1	2	0	-1	2	2	2	2	0
Triage Analysis - Speed (TA-S)	2	2	1	0	0	0	1	2	1	1	1	1	2
Escalation Analysis - Communication (EA-C)	2	2	2	2	1	2	2	2	1	2	2	2	2
Escalation Analysis - Interoperation (EA-I)	2	2	1	1	2	1	0	2	2	1	0	1	0
Correlation Analysis - Timeline (CA-T)	2	2	-2	0	2	1	0	2	1	2	0	-1	2
Correlation Analysis - Flexibility (CA-F)	2	2	2	0	0	1	0	2	1	2	1	2	1
Correlation Analysis - Investigation (CA-I)	0	1	-1	0	2	2	1	1	2	1	1	2	1
Threat Analysis - Correlation (ThA-C)	2	2	2	0	0	2	2	1	2	1	2	2	2
Threat Analysis - Interoperation (ThA-I)	2	2	0	0	0	0	1	1	1	2	2	0	0
Incident Response Analysis - Mitigation (IRA-M)	2	2	0	2	1	2	2	2	1	1	2	1	2
Incident Response Analysis - Situational Awareness (IRA-SA)	2	1	0	0	2	1	0	1	2	2	0	2	1
Forensic Analysis - Investigation (FA-I)	2	1	2	1	2	0	2	2	2	2	2	2	2
Forensic Analysis - Reporting (FA-R)	1	2	0	1	2	2	2	-1	2	-2	2	0	2
Impact Assessment - Identification (IA-I)	1	0	0	2	1	2	2	2	2	2	2	1	2
Impact Assessment - Situational Awareness (IA-SA)	2	0	0	0	0	0	0	1	1	2	0	2	0
Security Quality Management - Communication (SQM-C)	2	0	0	1	2	2	0	1	1	2	0	2	1

4.4.3 Results of Statistical Analyses on the basis of Expert-Review

Tests of statistical significance were conducted to compare the responses for individual component tasks between the two groups of respondents. Two tests were used: a test for differences, and a test for agreement, as explained in Section 4.1.2.2.

4.4.3.1 Test for Differences: Mixed Design *ANOVA*

For this analysis, the dependent variable is a quantitative variable represented by the means of each characteristic of visualisation of each component task. The independent variable is represented by the two response groups: visualisation designers and cyber-security analysts. The data in Table 4.2 was used to perform Mixed Design *ANOVA* and led to the following results.

The null hypothesis (H0) assumption is:

H0: "There is no significant difference between the responses of cyber-security analysts and visualisation designers"

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be applied from Table 4.3. According to Field (2013), the *Greenhouse-Geisser* correction is recommended if the estimated value is less than 0.75, while *Huynh-Feldt* is recommended otherwise.

Table 4.3: Estimates used to determine which corrected values to use for characteristics of visualisation.

Greenhouse-Geisser	**Huynh-Feldt**	**Lower-bound**
0.37	0.91	0.06

Table 4.3 shows that the Greenhouse-Geisser estimate in this case is 0.37, which is less than 0.75. Therefore, the Greenhouse-Geisser corrected significant values were used.

Table 4.4: Results of mixed design *ANOVA* (using Greenhouse-Geisser Correction) showing statistically non-significant differences.

Source	**df**	**Mean Square**	**F-Value**	**Sig (p)**
Type of Expert	1	2.14	1.54	**0.24**
Characteristics of Visualisation * Type of Expert	*5.87*	*1.70*	*0.84*	**0.54**
Error (Characteristics of Visualisation)	*64.57*	*2.03*	-	-

The results of the Mixed Design *ANOVA* are presented in Table 4.4. 'F-Ratio(dfB,dfE)','df' stands for degrees of freedom, where B is for between the groups and E represents error between the groups, and F-ratio is the ratio of the mean squares between groups and the mean squares within groups represented by F-value. This gives a measure of how much the means differ relative to the variability between groups (Field, 2013). ‘Sig (p)’ represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect.

The results in Table 4.4 show that there was a non-significant effect, as the significant values are greater than 0.05. According to the table, Sig. value for Type of Expert = 0.24, which is greater than 0.05. The table also shows the interaction between Characteristics of Visualisation and Type of Expert is *F(5.87,64.57) = 0.84, where 0.54(Sig.) > 0.05.*

These results demonstrate that there is no statistically significant difference between the responses of cyber-security analysts and the visualisation designers. It can be concluded that *H0* cannot be rejected for each characteristic of visualisation.

4.4.3.2 Test for Agreement: *Pearson’s r Correlation*

For this analysis, there are two groups, visualisation designers and cyber-security analysts, and seventeen cases, represented by the characteristics of visualisation. It is performed by calculating (i) correlation of average responses of cyber-security analysts per task, (ii) correlations between each cyber-security analyst with each visualisation designer, (iii) correlations within the group of cyber-security analysts, and (iv) correlations within the group of visualisation designers.

Correlation of Average Responses of Cyber-Security Analysts and Visualisation Designers per Task

Average data used to perform *Pearson’s r Correlation* of averages is displayed in Table 4.5, based on the raw data in Table 4.2. The interpretation of the results of *Pearson’s r correlation* is explained below:

The results of the Pearson’s r correlation analysis were:

r=0.395, n=17 as the Sig. (2-Tailed) value, p=0.12 > 0.05.
This shows that the correlation was not significant. This means that increases or decreases for cyber-security analysts do not significantly relate to increases or decreases for visualisation designers.

Table 4.5: Average responses for a given task by cyber-security analysts and visualisation designers, used for test for agreement: *Pearson's r Correlation*.

Characteristic of Visualisation	Cyber-Security Analysts	Visualisation Designers
TA-Filter	1.71	1.33
TA-SA	1.14	1.17
TA-Speed	0.86	1.33
EA-Communication	1.86	1.83
EA-Interoperation	1.29	1.00
CA - Timeline	0.71	1.00
CA - Flexibility	1.00	1.50
CA - Investigation	0.71	1.33
ThA - Correlation	1.43	1.67
ThA - Interoperation	0.71	1.00
IRA - Mitigation	1.57	1.50
IRA - SA	0.86	1.33
FA - Investigation	1.43	2.00
FA - Reporting	1.43	0.50
IA - Identification	1.14	1.83
IA - SA	0.29	1.00
SQM - Communication	1.00	1.17

Correlations Between Each Cyber-Security Analyst Against Each Visualisation Designer

Pearson's r Correlation is calculated for each cyber-security analysts against each visualisation designer, using the data in Table 4.2. Results of *Pearson's r Correlation* Coefficient (r) with the Significant (2-Tailed) Value (Sig.) for each combination is presented in Table 4.6.

The average of Pearson's r correlation analysis were:

r=0.075, n=17 as the Sig. (2-Tailed) value, p=0.44 > 0.05.
This shows that the correlation was not statistically significant.

Table 4.6: Summary of results of *Pearson's r Correlation* between each cyber-security analyst (C) against each visualisation designer (V), where r is the correlation coefficient and *Sig.* is the significant value.

		C1	C2	C3	C4	C5	C6	C7
V1	r	0.069	0.155	0.288	-0.008	-0.063	-0.259	0.136
	Sig.	0.792	0.553	0.262	0.974	0.809	0.315	0.604
V2	r	-0.204	-0.198	-0.024	0.057	0.356	0.236	0.130
	Sig.	0.433	0.447	0.926	0.829	0.161	0.362	0.619
V3	r	0.397	-0.382	0.016	-0.054	-0.228	-0.298	-0.399
	Sig.	0.115	0.13	0.953	0.837	0.378	0.246	0.112
V4	r	-0.095	0.246	0.325	0.443	-0.283	0.260	0.757
	Sig.	0.717	0.341	0.203	0.075	0.271	0.314	0
V5	r	0.074	-0.432	0.482	0.068	-0.145	0.122	-0.073
	Sig.	0.778	0.083	0.050	0.796	0.579	0.64	0.782
V6	r	-0.234	0.272	0.209	0.240	0.177	0.306	0.708
	Sig.	0.365	0.290	0.420	0.353	0.498	0.232	0.001

Correlations Within the Group of Cyber-Security Analysts

Pearson's r Correlation is calculated for within the group of cyber-security analysts, using the data in Table 4.2. Results of *Pearson's r Correlation* Coefficient (r) with the Significant (2-Tailed) Value (Sig.) for each combination is presented in Table 4.7.

Table 4.7: Summary of results of *Pearson's r Correlation* within the group of cyber-security analysts (C), where r is the correlation coefficient and *Sig.* is the significant value.

		C1	C2	C3	C4	C5	C6
C2	r	-0.053					
	Sig.	0.841					
C3	r	0.089	0.286				
	Sig.	0.734	0.265				
C4	r	-0.208	-0.068	0.215			
	Sig.	0.424	0.795	0.406			
C5	r	-0.398	-0.110	-0.276	0.283		
	Sig.	0.114	0.674	0.284	0.271		
C6	r	-0.444	-0.005	-0.040	0.574	0.343	
	Sig.	0.074	0.983	0.878	0.016	0.177	
C7	r	-0.381	0.252	0.397	0.454	0	0.315
	Sig.	0.132	0.329	0.115	0.067	1.000	0.218

The average of Pearson's r correlation analysis were:

r=0.063, n=17 as the Sig. (2-Tailed) value, p=0.42 > 0.05.
This shows that the correlation was not statistically significant. This shows that there was no significant agreement between cyber-security analysts themselves.

Correlations Within the Group of Visualisation Designers

textitPearson's r Correlation is calculated for within the group of visualisation designers, using the data in Table 4.2. Results of *Pearson's r Correlation* Coefficient (r) with the Significant (2-Tailed) Value (Sig.) for each combination is presented in Table 4.8.

Table 4.8: Summary of results of *Pearson's r Correlation* within the group of visualisation designers (V), where *r* is the correlation coefficient and *Sig.* is the significant value.

		V1	V2	V3	V4	V5
V2	*r*	-0.413				
	Sig.	0.099				
V3	*r*	0.439	-0.278			
	Sig.	0.078	0.281			
V4	*r*	-0.207	0.219	-0.228		
	Sig.	0.425	0.399	0.378		
V5	*r*	-0.032	0.218	0.335	0.009	
	Sig.	0.902	0.402	0.189	0.972	
V6	*r*	0.339	-0.051	-0.298	0.343	-0.198
	Sig.	0.184	0.847	0.246	0.177	0.447

The average of Pearson's r correlation analysis were:

r=0.013, n=17 as the Sig. (2-Tailed) value, p=0.40 > 0.05.
This shows that the correlation was not statistically significant. This shows that there was no significant agreement amongst the visualisation designers.

Discussion

Correlation of Average Responses of Cyber-Security Analysts and Visualisation Designers per Task and Correlations Between Each Cyber-Security Analyst Against Each Visualisation Designer gave a non-significant effect, which illustrates that there is no statistically significant agreement between the average responses of both groups. Additionally, Correlations Within the Group of Cyber-Security Analysts and Correlations Within the Group of Visualisation Designers showed that there was no significant agreement amongst the analysts and designers within their own groups.

The cases and upper right quartile of the scatterplot illustrate the results of the correlation, as shown in Figure 4.3. The scatterplot presents the correlation between the averages of each characteristic of visualisation for each component task and the two groups. Although there is no statistically significant correlation between the two groups, the scatterplot shows the clustering of data-points in the upper right quartile. On the basis of the quantisation performed in Section 4.4.2, it can be concluded that the *characteristics of visualisations* generally received positive responses, as the means were all between 0.3 and 2. The regions represented in Figure 4.3 are described in the next section, as these are used to modify and update the components tasks of *EEVi*.

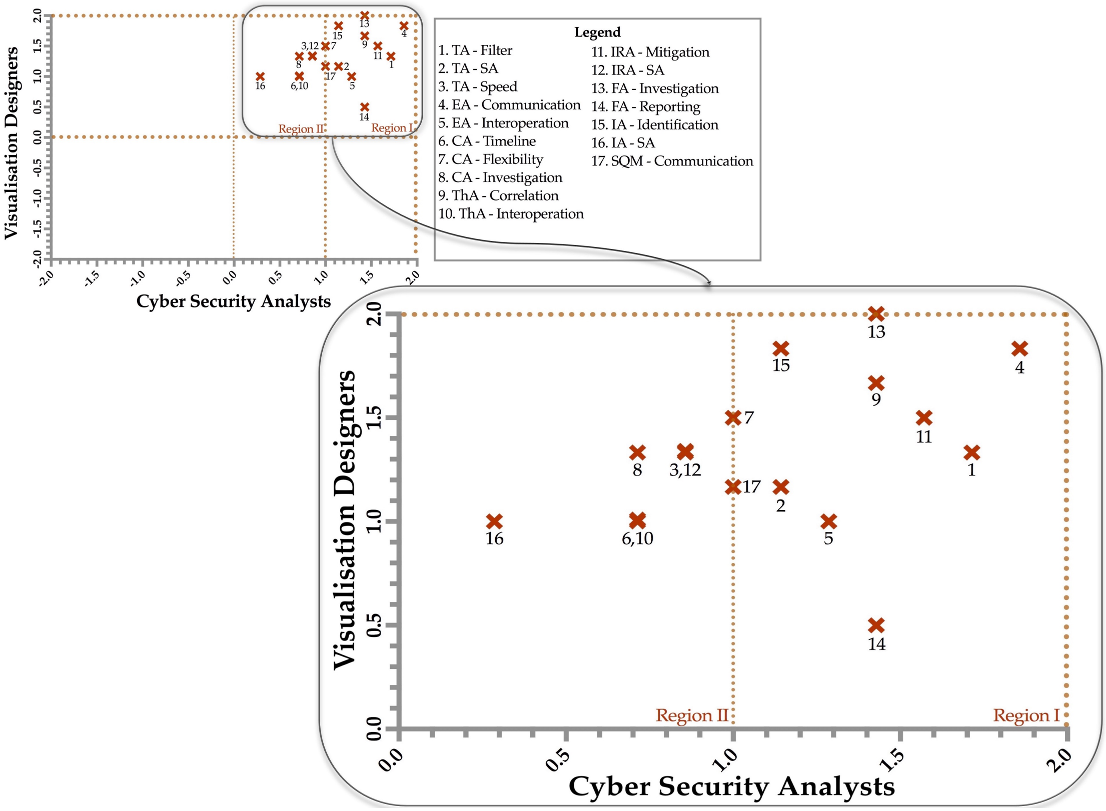


Figure 4.3: Scatterplot between cyber-security analysts (x axis) and visualisation designers (y axis), zoomed in on the upper right quartile.

4.4.4 Modifications of Component Tasks of *EEVi* on the basis of the Expert-Review

Analysis of the interviews from the expert-review led to the modification of the component tasks, which were initially defined in Chapter 3. The steps undertaken to update each component task were:

Step 1 Data relating to the component tasks was transposed into a quantified tabular format to compare the feedback from all experts.

Step 2 This feedback led to two major changes: the structure of representation of the guidelines from a hierarchical structure to a simple cyclic list (*C1, C2 and C4*), and the change in the terminology.

Step 3 Applying the results from the regions described in Figure 4.3, the characteristics of visualisation were divided into two categories: *confirmed* and *unresolved*.

The characteristics in *Region I*, on the right of the figure, received a $mean >= 1$ from the cyber-security analysts and a $mean > 0$ from visualisation designers. These *characteristics of visualisation* were assigned to the *confirmed* category, as they received positive to very positive responses from analysts and neutral to very positive responses from the designers.

The characteristics in *Region II*, on the left of the figure, received a $0 < mean < 1$ from the cyber-security analysts and a $mean > 0$ from visualisation designers. These *characteristics of visualisation* were assigned to the *unresolved* category, as these characteristics received neutral to positive responses from the analysts and neutral to very positive responses from the designers.

Initially, there was a third category, *discard*, for characteristics that had a $mean < 0$ from the cyber-security analysts and a $mean < 0$ from the visualisation designers. However, none of the characteristics fell into this category and the category was removed altogether.

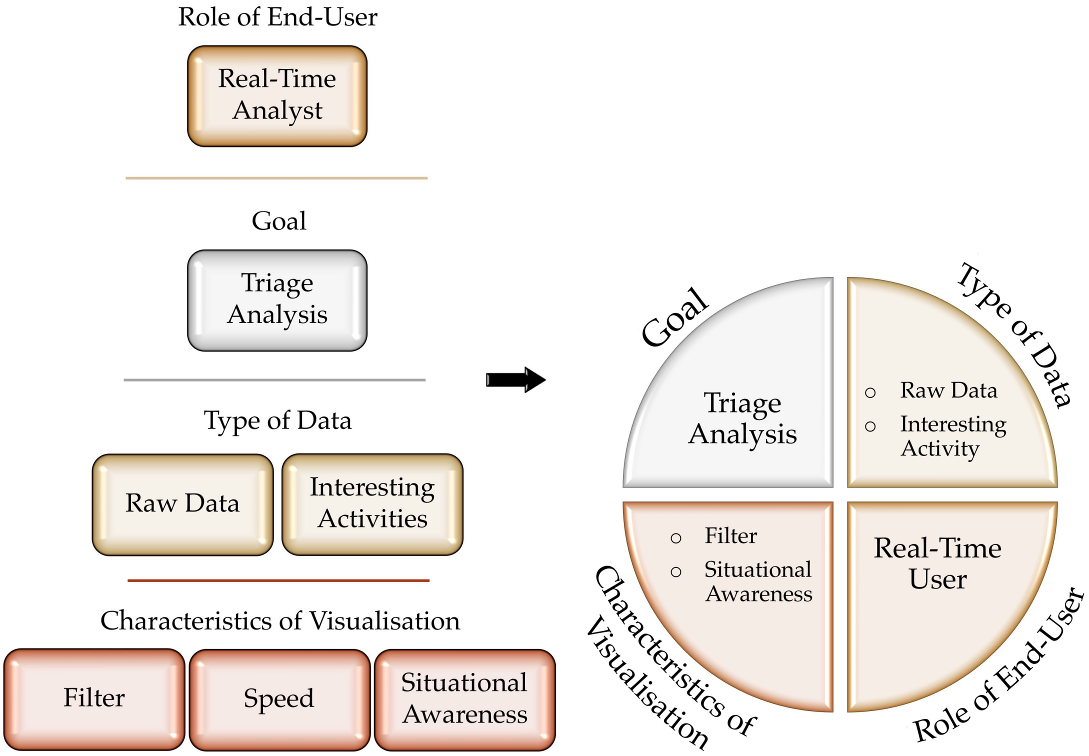
Step 4 The feedback also included responses which highlighted possible missing characteristics from each component task. These characteristics were added to the *unresolved* category when mentioned by more than one expert.

Step 5 The updated component task representations were re-drawn with the modification from the expert-review. The *confirmed* characteristics were displayed in the component task diagrams, whereas the *unresolved* characteristics were only mentioned in the text. These would subject to questionnaire analysis, as explained in Chapter 5, where they will either be *discarded*, *recommended* or *confirmed*, and the component task representations will be updated again.

To enhance understanding of the component tasks, Tables 3.2, 3.3, 3.4 and 3.5 present definitions of codes for all identified themes that are used in the component task representations.

4.4.4.1 Modification of Guidelines for Visualisation for Triage Analysis (TA)

The thirteen experts reviewed 'Triage Analysis' and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. (*V1, V3 and V4*) believed *Situational Awareness* to be the most difficult to implement, while (*V5 and V6*) said *Real-Time Access* was most difficult to implement. (*V2*) assumed *Filter* to be the most difficult to implement.



(a) Initial Triage Analysis (b) Modified and Validated Triage Analysis

Figure 4.4: Transformation of the visual representation of 'Triage Analysis' from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.4(a)) which identified *Real-Time Analyst* performing 'Triage Analysis' using *Raw Data* and *Interesting Activity* and requiring *Situational Awareness*, *Filter*, and *Speed* for visualisation. Table 4.9 shows the quantified responses for each of these characteristics for each expert.

Once the structure was modified to a circular list, the terminology was altered from the feedback received from *C1, C2 C4, C5, C6 and V1*: *Speed* was too ambiguous and was replaced by *Real-Time Access.*

Table 4.9: Quantified Results of *Characteristics of Visualisation* for 'Triage Analysis' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participant	TA-Filter	TA-SA	TA-Speed
C1	0	2	2
C2	2	1	2
C3	2	0	1
C4	2	2	0
C5	2	1	0
C6	2	2	0
C7	2	0	1
V1	2	-1	2
V2	1	2	1
V3	1	2	1
V4	1	2	1
V5	1	2	1
V6	2	0	2

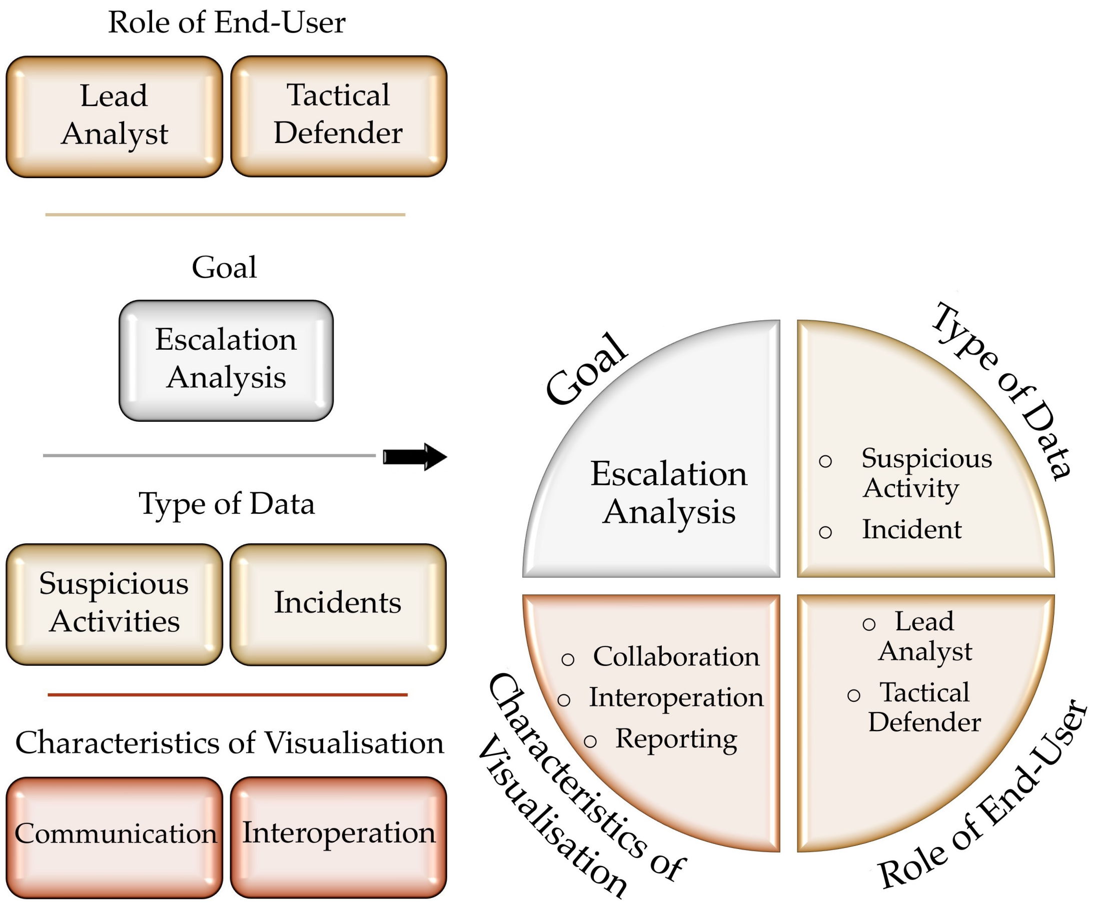
The next step was to apply the results from Figure 4.3. As can be seen, 'TA-Filter' and 'TA-SA' fall within *Region I* and were moved into the *confirmed* category. However, 'TA-Speed' falls within *Region II* and was moved into the *unresolved* category.

Three experts (*C1, C4 and C5*) requested an *Alerts* characteristic while two experts (*C1 and C5*) requested a *Colour Highlighting* characteristic. These were added to the *unresolved* category.

Figure 4.4(b) now shows the component task representation for 'Triage Analysis'. Furthermore, *Real-Time Access*, *Alerts* and *Colour Highlighting* were in the *unresolved* category.

4.4.4.2 Modification of Guidelines for Visualisation for Escalation Analysis (EA)

The thirteen experts reviewed ‘Escalation Analysis’ and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. *V1, V3 and V5* believed *Collaboration* to be the most difficult to implement,while the rest of the visualisation designers (*V2, V4 and V6*) assumed *Interoperation* to be the most difficult to implement.



(a) Initial Escalation Analysis (b) Modified and Validated Escalation Analysis

Figure 4.5: Transformation of the visual representation of ‘Escalation Analysis’ from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.5(a)) which identified *Lead Analyst* and *Tactical Defender* performing ‘Escalation Analysis’ using *Suspicious Activity* and *Incident* and requiring *Communication* and *Interoperation* for visualisation. Table 4.10 shows the quantified responses for each of these characteristics for each expert.

Table 4.10: Quantified Results of *Characteristics of Visualisation* for 'Escalation Analysis' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participant	EA-Communication	EA-Interoperation
C1	2	2
C2	2	2
C3	2	1
C4	2	1
C5	1	2
C6	2	1
C7	2	0
V1	2	2
V2	1	2
V3	2	1
V4	2	0
V5	2	1
V6	2	0

Once the structure was modified to a circular list, the terminology was altered from the feedback received from *C4, C7 and V1*: *Communication* was too ambiguous and was broken down into *Collaboration* and *Reporting*.

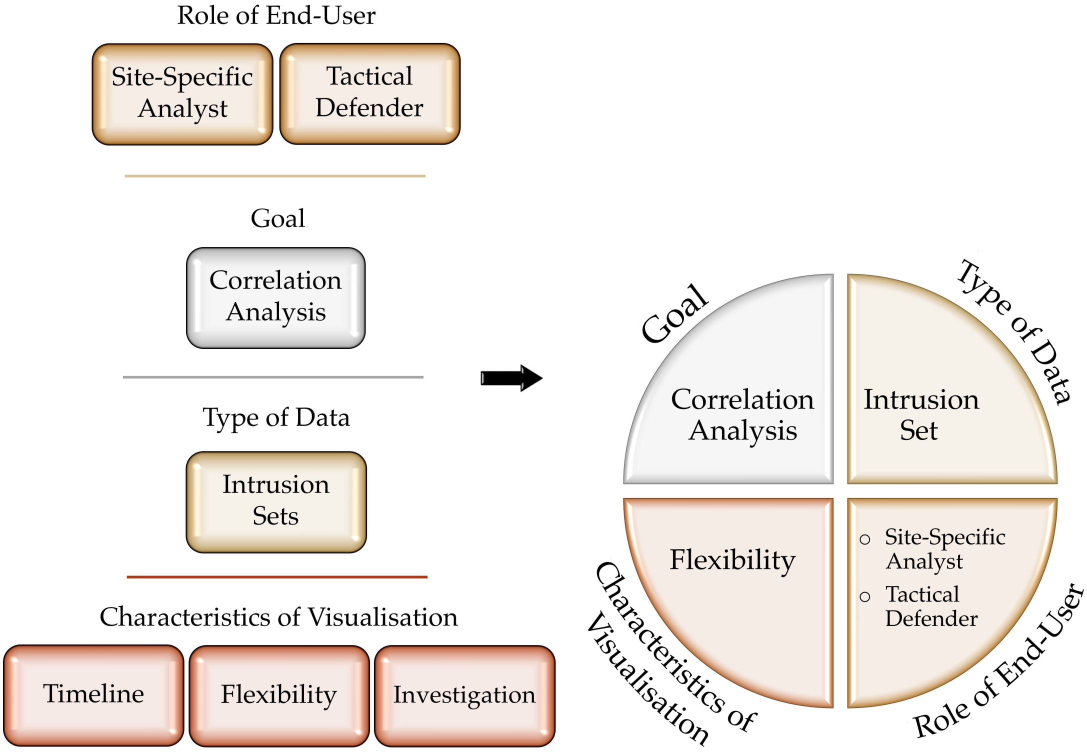
The next step was to apply the results from Figure 4.3. As can be seen, 'EA-Communication' and 'EA-Interoperation' fall within *Region I* and were moved into the *confirmed* category.

V3 and V4 requested a *Priorities* characteristic on the basis of risk level, which was added to the *unresolved* category.

Figure 4.5(b) now shows the component task representation for 'Escalation Analysis'. Furthermore, *Priorities* was in the *unresolved* category.

4.4.4.3 Modification of Guidelines for Visualisation for Correlation Analysis (CA)

The thirteen experts reviewed 'Correlation Analysis' and their feedback directed the modification of this component task. All experts but *C3* agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. *V1, V2, V3, V4 and V5* believed *Investigation* to be the most difficult to implement.



(a) Initial Correlation Analysis (b) Modified and Validated Correlation Analysis

Figure 4.6: Transformation of the visual representation of 'Correlation Analysis' from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.6(a)) which identified *Site-Specific Analyst* and *Tactical Defender* performing 'Correlation Analysis' using *Intrusion Set* and requiring *Timeline*, *Flexibility* and *Investigation* for visualisation. Table 4.11 shows the quantified responses for each of these characteristics for each expert.

Once the structure was modified to a circular list, the terminology was altered from the feedback received from *C1 and C5*; *Investigation* was too ambiguous and was replaced by *Investigatory Capabilities.*

Table 4.11: Quantified Results of *Characteristics of Visualisation* for 'Correlation Analysis' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

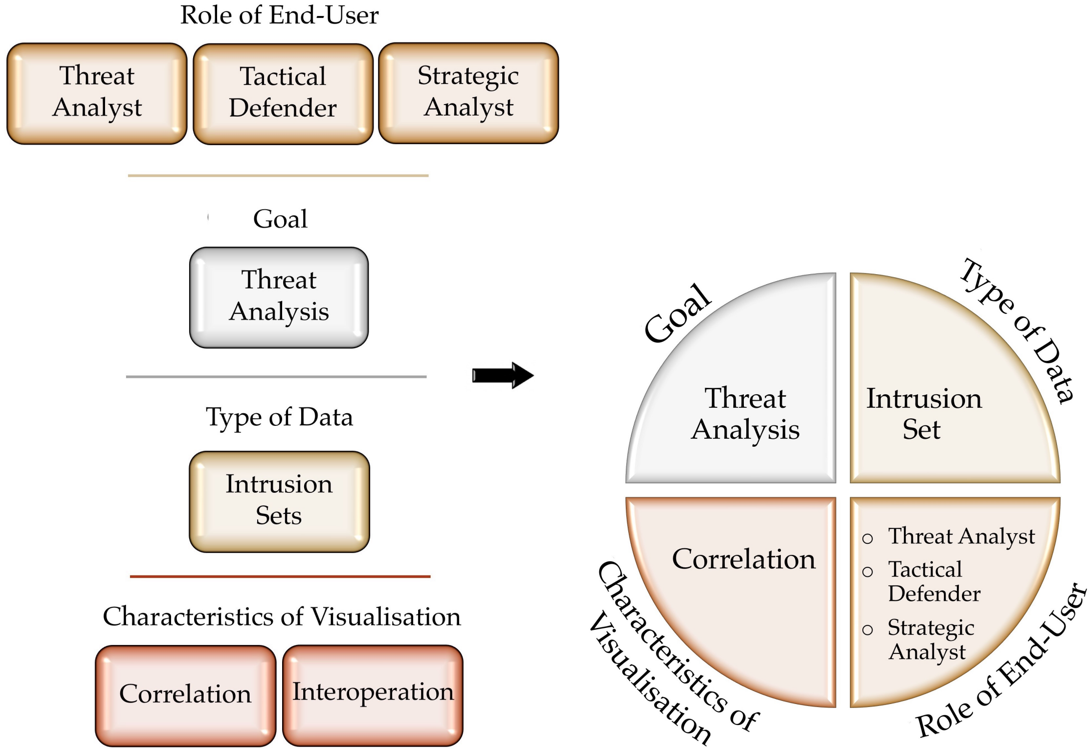
Participant	CA-Timeline	CA-Flexibility	CA-Investigation
C1	2	2	0
C2	2	2	1
C3	-2	2	-1
C4	0	0	0
C5	2	0	2
C6	1	1	2
C7	0	0	1
V1	2	2	1
V2	1	1	2
V3	2	2	1
V4	0	1	1
V5	-1	2	2
V6	2	1	1

The next step was to apply the results from Figure 4.3. As can be seen, 'CA-Flexibility' falls within *Region I* and was moved into the *confirmed* category. However, 'CA-Timeline' and 'CA-Investigation' fall within *Region II* and were moved into the *unresolved* category.

Figure 4.6(b) now shows the component task representation for 'Correlation Analysis'. Furthermore, *Timeline* and *Investigatory Capabilities* were in the *unresolved* category.

4.4.4.4 Modification of Guidelines for Visualisation for Threat Analysis (ThA)

The thirteen experts reviewed 'Threat Analysis' and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. *V2, V4, V5 and V6* believed *Correlation* to be the most difficult to implement, while *V1 and V3* assumed *Interoperation* to be most difficult to implement.



(a) Initial Threat Analysis

(b) Modified and Validated Threat Analysis

Figure 4.7: Transformation of the visual representation of 'Threat Analysis' from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.7(a)) which identified *Threat Analyst*, *Tactical Defender* and *Strategic Analyst* performing 'Threat Analysis' using *Intrusion Set* and requiring *Correlation* and *Interoperation* for visualisation. Table 4.12 shows the quantified responses for each of these characteristics for each expert.

Table 4.12: Quantified Results of *Characteristics of Visualisation* for 'Threat Analysis' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participant	ThA-Correlation	ThA-Interoperation
C1	2	2
C2	2	2
C3	2	0
C4	0	0
C5	0	0
C6	2	0
C7	2	1
V1	1	1
V2	2	1
V3	1	2
V4	2	2
V5	2	0
V6	2	0

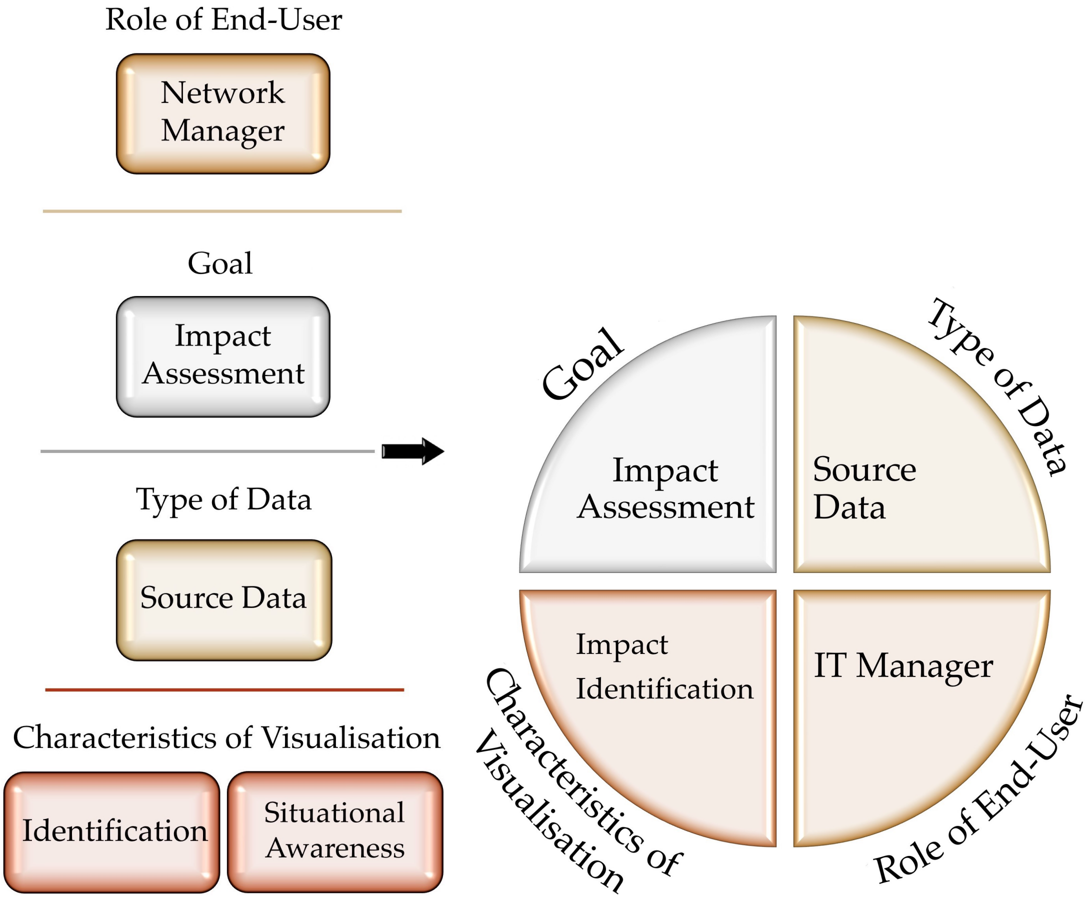
The next step was to apply the results from Figure 4.3. As can be seen, 'ThA-Correlation' falls within *Region I* and was moved into the *confirmed* category. However, 'ThA-Interoperation' falls within *Region II* and was moved into the *unresolved* category.

C4, V1 and V6 requested a *Collaboration* characteristic, while *C7 and V3* requested for a *Priorities* characteristic on the basis of risk level. These were added to the *unresolved* category.

Figure 4.7(b) now shows the component task representation for 'Threat Analysis'. Furthermore, *Interoperation*, *Priorities* and *Collaboration* were in the *unresolved* category.

4.4.4.5 Modification of Guidelines for Visualisation for Impact Assessment (IA)

The thirteen experts reviewed 'Impact Assessment' and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. *V2, V4 and V5*) believed *Identification* to be the most difficult to implement, while *V1, V3 and V6* assumed *Situational Awareness* to be most difficult to implement. Additionally, according to *C5, C6 and V3* 'Impact Assessment' is a subset of 'Threat Analysis' and these are usually performed in collaboration.



(a) Initial Impact Assessment (b) Modified and Validated Impact Assessment

Figure 4.8: Transformation of the visual representation of 'Impact Assessment' from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.8(a)) which identified *Network Manager* performing 'Impact Assessment' using *Source Data* and requiring *Identification* and *Situational Awareness* for visualisation. Table 4.13 shows the quantified responses for each of these characteristics for each expert.

Table 4.13: Quantified Results of *Characteristics of Visualisation* for 'Impact Assessment' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participant	IA-Identification	IA-SA
C1	1	2
C2	0	0
C3	0	0
C4	2	0
C5	1	0
C6	2	0
C7	2	0
V1	2	1
V2	2	1
V3	2	2
V4	2	0
V5	1	2
V6	2	0

Once the structure was modified to a circular list, the terminology was altered from the feedback received from *C1 and C3)*; *Identification* was too ambiguous and was replaced by *Impact Identification*. Also, *C7 and V5* believed that this task was performed by an *IT Manager* and not a *Network Manager* as it is performed on the system as a whole, not just the network layer.

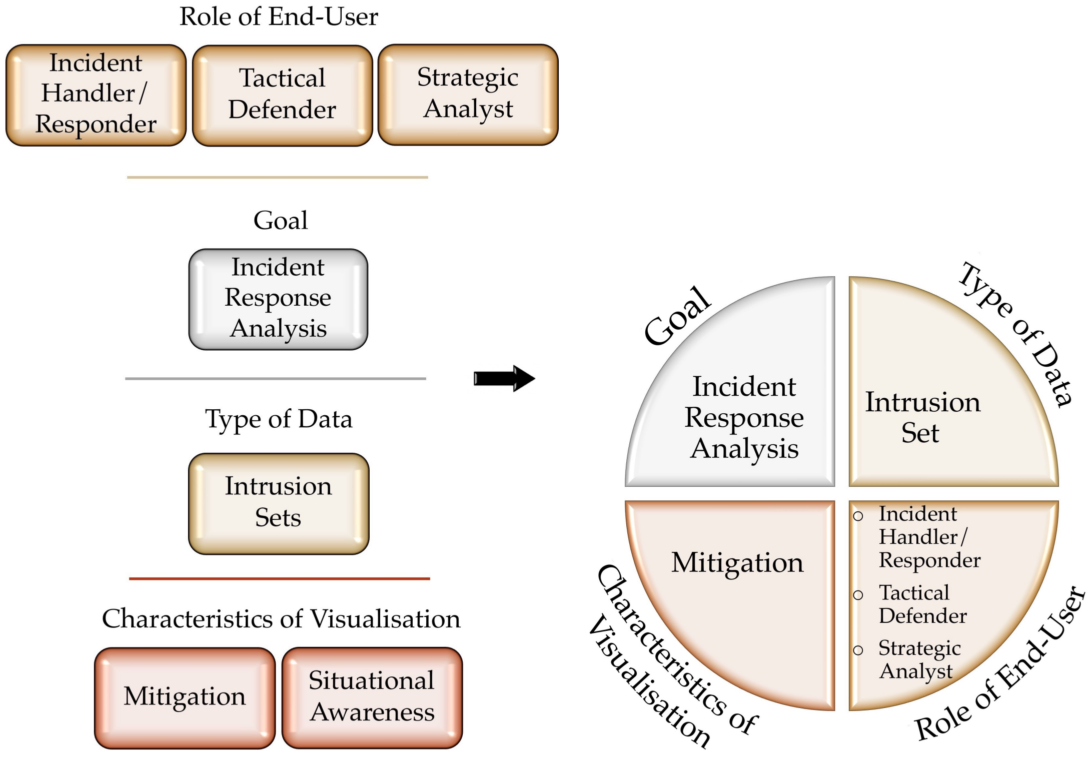
The next step was to apply the results from Figure 4.3. As can be seen, 'IA-Identification' falls within *Region I* and was moved into the *confirmed* category. However, 'IA-SA' falls within *Region II* and was moved into the *unresolved* category.

Three experts (*C2, C5 and V2*) requested a *Reporting* characteristic. This was added to the *unresolved* category.

Figure 4.8(b) now shows the component task representation for 'Impact Assessment'. Furthermore, *Situational Awareness* and *Reporting* were in the *unresolved* category.

4.4.4.6 Modification of Guidelines for Visualisation for Incident Response Analysis (IRA)

The thirteen experts reviewed ‘Incident Response Analysis’ and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. *V2, V4 and V5* believed *Mitigation* to be the most difficult to implement, while *V3 and V6* assumed *Situational Awareness* to be most difficult to implement, and *V1* believed *Mitigation* and *Situational Awareness* to be equally difficult to implement.



(a) Initial Incident Response Analysis

(b) Modified and Validated Incident Response Analysis

Figure 4.9: Transformation of the visual representation of ‘Incident Response Analysis’ from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.9(a)) which identified *Incident Responder/Handler*, *Tactical Defender* and *Strategic Analyst* performing ‘Incident Response Analysis’ using *Intrusion Set* and requiring *Mitigation* and *Situational Awareness* for visualisation. Table 4.14 shiows the quantified responses for each of these characteristics for each expert.

Table 4.14: Quantified Results of *Characteristics of Visualisation* for 'Incident Response Analysis' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participant	IRA-Mitigation	IRA-SA
C1	2	2
C2	2	1
C3	0	0
C4	2	0
C5	1	2
C6	2	1
C7	2	0
V1	2	1
V2	1	2
V3	1	2
V4	2	0
V5	1	2
V6	2	1

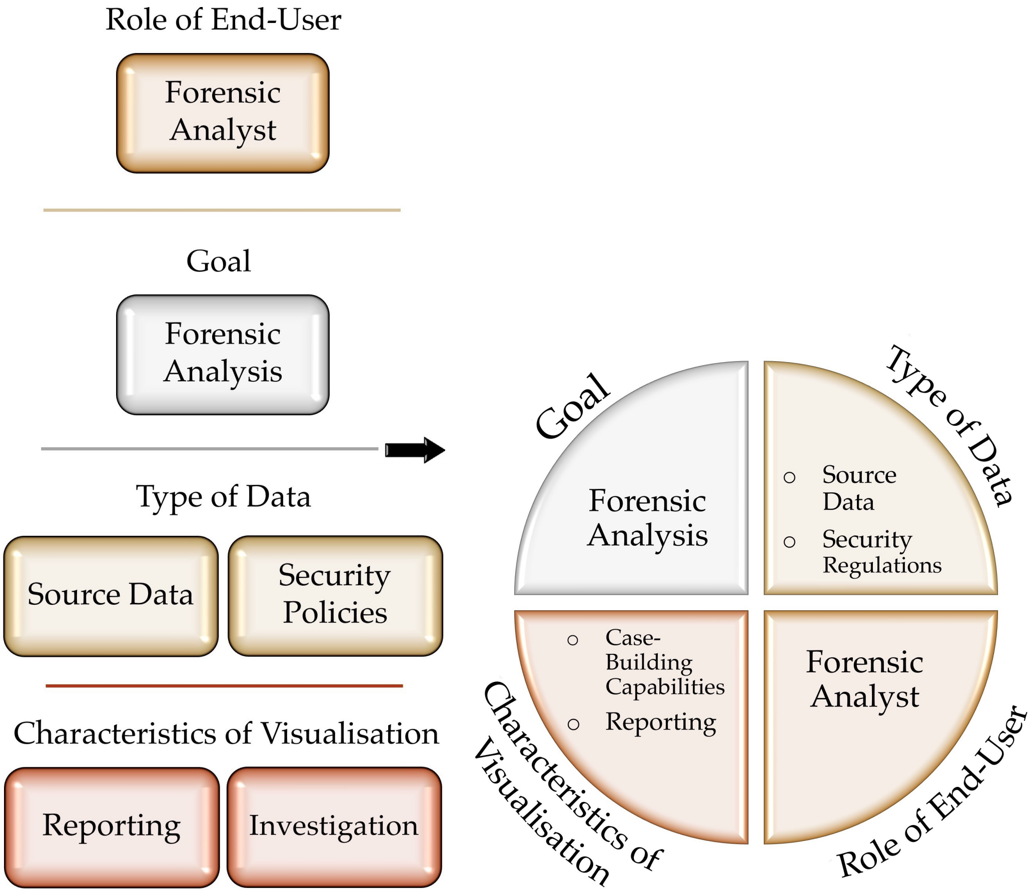
The next step was to apply the results from Figure 4.3. As can be seen, 'IRA-Mitigation' falls within *Region I* and was moved into the *confirmed* category. However, 'IRA-SA' falls within *Region II* and was moved into the *unresolved* category.

Two experts (*C1 and V1*) requested an *Interoperation* characteristic, while *C7 and V1* requested a *Collaboration* characteristic, and *C2 and C5*) requested a *Reporting* characteristic. These were added to the *unresolved* category.

Figure 4.9(b) now shows the component task representation for 'Incident Response Analysis'. Furthermore, *Situational Awareness*, *Interoperation*, *Collaboration* and *Reporting* were in the *unresolved* category.

4.4.4.7 Modification of Guidelines for Visualisation for Forensic Analysis (FA)

The thirteen experts reviewed ‘Forensic Analysis’ and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable. *V2, V3, V4, V5 and V6* believed *Investigation* to be the most difficult to implement.



(a) Initial Forensic Analysis

(b) Modified and Validated Forensic Analysis

Figure 4.10: Transformation of the visual representation of ‘Forensic Analysis’ from a hierarchical structure to a cyclic list with updated terminology and *confirmed Characteristics of Visualisation.*

The original component task was a hierarchical structure (Figure 4.10(a)) which identified *Forensic Analyst* performing F̀orensic Analysis’ using *Source Data* and *Security Policies* and requiring *Investigation* and *Reporting* for visualisation. Table 4.15 shows the quantified responses for each of these characteristics for each expert.

Once the structure was modified to a circular list, the terminology was altered from the feedback received from *C1 and C5*: *Investigation* was too ambiguous and was replaced by

Table 4.15: Quantified Results of *Characteristics of Visualisation* for 'Forensic Analysis' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participant	FA-Reporting	FA-Investigation
C1	2	1
C2	1	2
C3	2	0
C4	1	1
C5	2	2
C6	0	2
C7	2	2
V1	2	-1
V2	2	2
V3	2	-2
V4	2	2
V5	2	0
V6	2	2

Case-Building Capabilities; and *Security Policies* was replaced with *Security Regulations* as it is the more appropriate term.

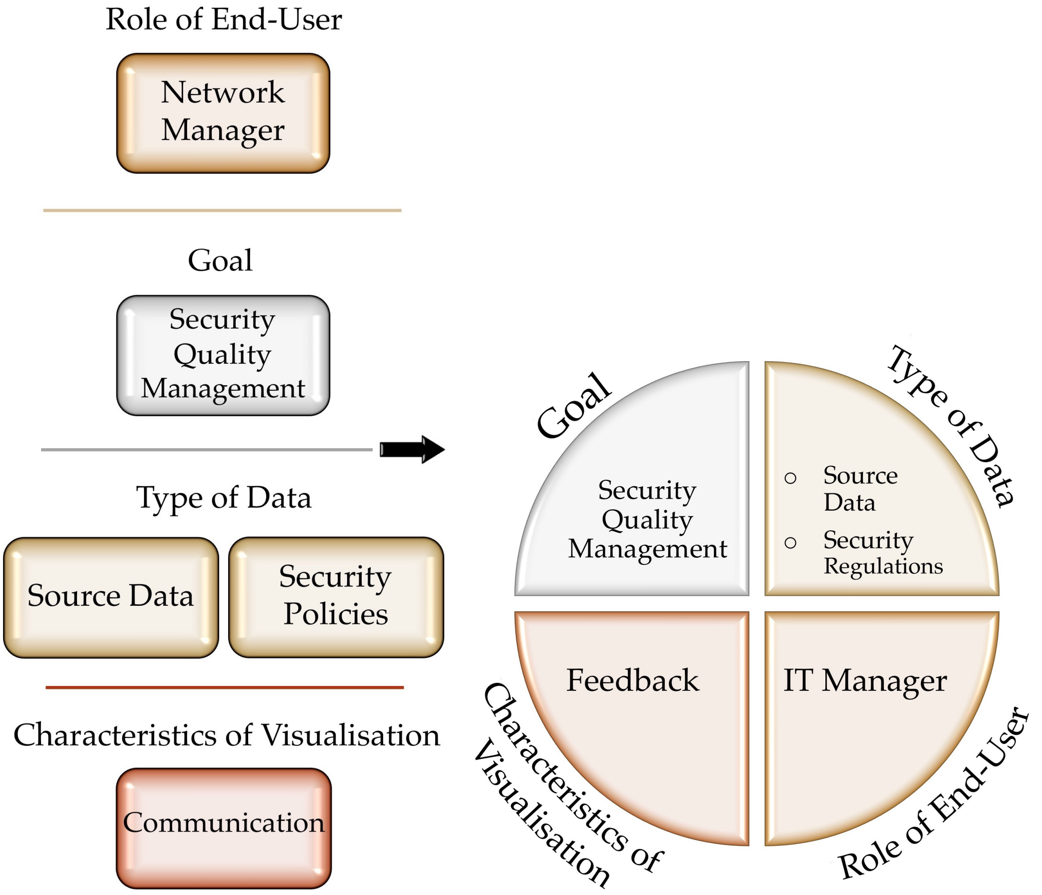
The next step was to apply the results from Figure 4.3. As can be seen, 'FA-Investigation' and 'FA-Reporting' fall within *Region I* and were moved into the *confirmed* category.

Four experts (*C1, C2, C5 and C7*) requested a *Chain of Custody* characteristic, while *C1 and V1* requested an *Interoperation* characteristic. These were added to the *unresolved* category.

Figure 4.10(b) now shows the component task representation for 'Forensic Analysis'. Furthermore, *Chain of Custody* and *Interoperation* were in the *unresolved* category.

4.4.4.8 Modification of Guidelines for Visualisation for Security Quality Management (SQM)

The thirteen experts reviewed 'Security Quality Management' and their feedback directed the modification of this component task. All experts unanimously agreed with the task and the various aspects that represent it, along with the importance of this task. The six visualisation designers unanimously agreed that the characteristics of visualisation were implementable.



(a) Initial Security Quality Management (b) Modified and Validated Security Quality Management

Figure 4.11: Transformation of the visual representation of Security Quality Management from a hierarchical structure to a cyclic list with updated terminology and *confirmed* Characteristics of Visualisation.

The original component task was a hierarchical structure (Figure 4.11(a)) which identified *Network Manager* performing 'Security Quality Management' using *Source Data* and *Security Policies* and requiring *Communication* for visualisation. Table 4.16 shows the quantified responses for each of these characteristics for each expert.

Table 4.16: Quantified Results of *Characteristics of Visualisation* for 'Security Quality Management' for each expert on a scale of -2 (very negative response) to +2 (very positive response).

Participants	SQM-Communication
C1	2
C2	0
C3	0
C4	1
C5	2
C6	2
C7	0
V1	1
V2	1
V3	2
V4	0
V5	2
V6	1

Once the structure was modified to a circular list, terminology was altered from the feedback received from *V3, V5 and V6*; *Communication* was too ambiguous and was replaced by *Feedback*. Additionally, *C5 and C7* believed that this task was performed by an *IT Manager* and not *Network Manager*.

The next step was to apply the results from Figure 4.3. As can be seen, 'SQM-Communication' falls within *Region I* and was moved into the *confirmed* category.

Two experts (*C4 and V2*) requested a *Reporting* characteristic. This was added to the *unresolved* category.

Figure 4.11(b) now shows the component task representation for 'Security Quality Management'. Furthermore, *Reporting* was in the *unresolved* category.

4.5 Discussion

EEVi was validated and revised on the basis of a review of thirteen experts (seven cyber-security analysts and six visualisation designers) from academia and industry. On the basis of their assessment, the component tasks of the model were modified and updated. This minimised the disparity of domain-knowledge between the two groups by accommodating both their perspectives in the revised version.

Statistical analyses were performed on the responses; qualitative responses were quantified for this purpose. The statistical analyses showed that there were no statistically significant differences between responses for the two groups, neither was there statistically significant correlation between the two groups. It can be concluded that *EEVi* represents a useful model to help design cyber-security visualisations for cyber-security analysts through the characteristics of visualisation.

At this stage, SRQ_1 was being been addressed by *EEVi*, and SRQ_2 was being addressed as the characteristics of visualisation that support cyber-security analyst to perform a task have been identified and validated. Chapter 5 talks about the confirmation of validated and updated *EEVi*.

Chapter 5

Confirmation of *EEVi*

Thirty respondents completed an online questionnaire designed to confirm *EEVi*, which was validated and modified in the previous chapter. Confirmation is used to strengthen the results from validation, by ensuring the rationale of *EEVi* by taking it through another evaluation process. This chapter presents the results and findings from the questionnaire, and subsequent revisions to *EEVi*'s component tasks based on respondent feedback.

5.1 Background of Technique Used

Questionnaires are the most popular method for data collection using a standardised set of questions (Bhattacherjee, 2012; Bourque & Fielder, 2003). According to Bourque and Fielder (2003), the main advantage of using a self-administered questionnaire is the ability to reach a large sample of potential participants covering a wide geographic area, quite easily and at low cost. An online-based self-administered questionnaire was used as part of this research, because complete anonymity and convenience would allow respondents to be more candid and truthful in their responses.

5.2 Arrangements for Questionnaire

Cyber-security analysts were asked to complete a questionnaire on iSurvey[1] (see Appendix D) to confirm the updated model *EEVi*.

In the questionnaire, participants were asked general questions about knowledge of their fields to confirm their technical expertise. This was followed by questions on the updated

[1] iSurvey is a survey generation and research tool for distributing online questionnaires, free to use for University of Southampton students - https://www.isurvey.soton.ac.uk/ [Accessed: 24 October, 2018]

model structure. Then, they were asked about the structure and definitions of each validated and updated component task. Finally, they were asked about the usefulness of the model and whether they had additional comments.

The characteristics of visualisation for the component tasks were rated on a 5-point Likert scale from 'Strongly Disagree' to 'Strongly Agree'. According to Revilla, Saris, and Krosnick (2014), the 5-point scale is the optimal choice as the quality of results decreases with higher point scales. As a result, the 5-point 'Strongly Disagree' to 'Strongly Agree' scale yields better data and higher quality of responses.

Power analysis was first used to determine the number of respondents required for the questionnaire. G* Power Calculation was used to implement a two-tailed t-test. A large effect size of 0.8, as described by J. Cohen (1992), was taken. The type I error probability was 0.05 and the type II error probability was 0.2, which gave a power value of 0.8. A sample size of 15 respondents was found to be an appropriate sample size. However, the central limit theorem shows that the sample size should be at least 30 (Christou, 2017). As a result, there was a requirement of at least 30 participants.

The respondents were recruited by distributing the questionnaire to (i) cyber-security researchers within the University of Southampton through mailing-lists, and (ii) contacting professional contacts made at relevant international conferences (ICITST[2] 2016, VizSec[3] 2017 and VIS[4] 2017) and summer school (Social Aspects of Cyber Security Risk 2016) via email and LinkedIn[5]. The respondents gave explicit consent by checking the relevant box, following the guidelines for ethical approval (Section 5.2.1).

5.2.1 Ethics Approval for Questionnaire

The questionnaire was sent out with approval from Ethics and Research Governance (ERGO) under reference number $ERGO/FPSE/23974$.

Under the guidelines for ethical approval, interviews and questionnaire surveys undertaken in the period from 16 November 2016 to 1 November 2019 are approved, conforming to the DPA Plan and Participant Information Sheet approved with the application.

Each participant provided informed consent to the Participant Information Sheet and DPA Plan by accepting the following statement "I have read and understood the Participant Information Sheet (version 1, dated 2016-11-07) and have had the

[2] International Conference for Internet Technology and Secured Transactions - https://icitst.org/ [Accessed: 14th May, 2019]

[3] IEEE Symposium on Visualization for Cyber Security - https://vizsec.org [Accessed: 14th May, 2019]

[4] IEEE VIS - http://ieeevis.org/year/2017/welcome [Accessed: 14th May, 2019]

[5] A social network to build and engage with professional networks - https://www.linkedin.com/ [Accessed: 14th May, 2019].

opportunity to ask questions about the study and agree to take part in this study. I understand my participation is voluntary and I may withdraw at any time". They gave their consent by selecting the box, before moving on to the page with the questionnaire. No personal or sensitive information was collected about the participants. A copy of the DPA Plan and Participant Information Sheet are detailed in Appendix B.

5.3 Findings from the Questionnaire

Table 5.1: Demographic information concerning questionnaire respondents

Age Group	7 (23.3%) were in the age range 18 - 25 years 17 (56.7%) were in the age range 26 - 40 years 6 (20%) were in the age range 41 - 60 years
Industry or Academia	16 (53.3%) were from Higher Education Institutes (HEI) 13 (43.3%) were from industry
Area of Expertise	24 (80%) had expertise in cyber-security 4 (13.3%) had experience in both cyber-security and visualisation design 2 (6.7%) had a technical background but expertise in neither The areas covered by the respondents were: Information Security (4), Penetration Testing (3), Network Security (3), Information Assurance (2), Security Information and Event Management (SIEM, 2), Cyber Forensics (2), Design (1), Threat Analysis (1), IOT Security (1), Formal Modelling and Verification (1), Cyber Defence (1), Blockchain Security (1), Information System Audits for Cyber-Security (1), Security Management (1), Application Security (1), Security Risk and Strategy (1), Financial Security (1), Phishing (1), Human-Computer Interaction (1), and SIEM Visualisations (1).
Average Expertise Rating	They rated their expertise on an average of **3.33** out of 5 with a mode and median of 3.
Average Years of Experience	They had an average of **6.67 years** of experience ranging from 1 year to 25 years with a mode and median of 5 years.
Cyber-Security Visualisation Solutions	22 (73.3%) had never used a cyber-security visualisation solution 8 (26.7%) had some experience using them

Thirty respondents from different age-groups, organisations and areas of expertise in their respective fields, completed the questionnaire for the confirmation of *EEVi*. The demographics of the respondents are shown in Table 5.1. The respondents were also asked to confirm some general questions about *EEVi*:

1. Of the questionnaire's 30 respondents, 19 (63.3%) confirmed that *EEVi* represents good fundamental guidelines for cyber-security visualisation, whereas 7 (23.3%) respondents were not sure and commented that it would depend on usage and would differ from task to task. Only 1 (3.3%) respondent answered that this would not be possible.

2. 20 (66.7%) respondents confirmed that *EEVi* represents a useful model to evaluate cyber-security visualisation solutions, whereas 7 (23.3%) respondents were not sure and commented that it would depend on usage and how solutions would be evaluated. No respondent answered that this would not be possible.

3. Most respondents did not have additional comments. However, there were a few suggestions. One respondent thought the addition of use-cases would add more strength to the model. Another believed that *EEVi* is a good place to start but adding the process of how it was built would give more confidence.

4. The respondents confirmed that some of the characteristics of visualisation, found in Section 4.4, should be present in all cyber-security visualisation solutions. This is shown in Figure 5.1, with the number of respondents that selected the characteristic.

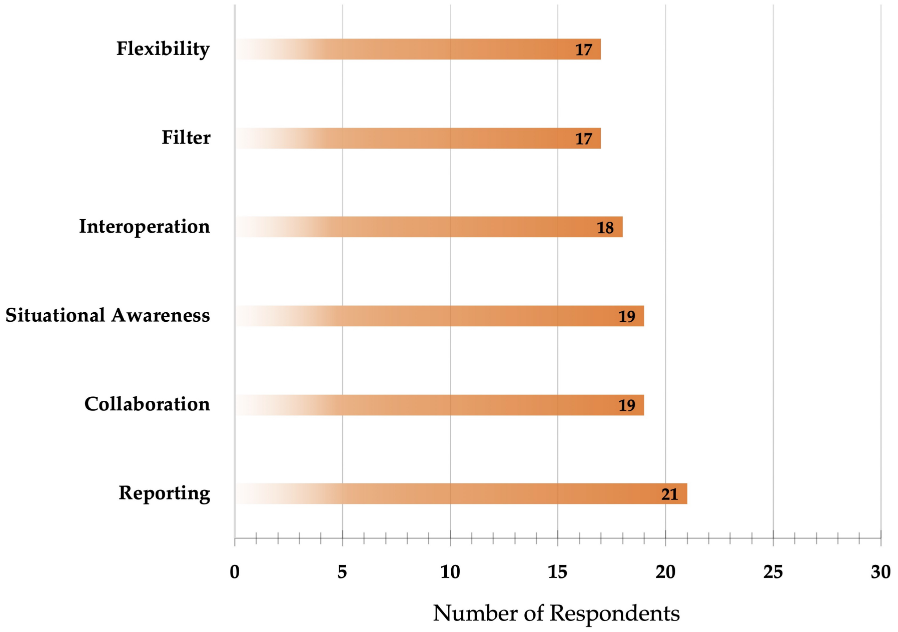


Figure 5.1: A bar graph representing the number of respondents answering 'Yes' on a dichotomous scale of Yes/No for each characteristic of visualisation to be represented in all cyber-security visualisation solutions.

5.3.1 Confirmation of *EEVi* on the basis of the Questionnaire

The structure and terminology of the validated *EEVi* (Figure 4.1(b)) was confirmed by the respondents:

1. 27 (90%) respondents agreed that the structure of *EEVi* made sense logically;
2. 21 (70%) respondents agreed that the logical flow of *EEVi* was followed by their organisation. However, one commented that every project was different and required a different logical flow, based on information available, which another respondent believed was a "good way to think about key decision-makers in strategic, tactical and operational [sectors]".

The high positive responses ratifies, that the structure and terminology of *EEVi* were confirmed after the validation stage, and do not require another iteration of updates.

5.3.2 Revision of Component Tasks of *EEVi* on the basis of the Questionnaire

Analysis of the questionnaire led to modification of the component tasks, which were initially defined in Chapter 3. The steps undertaken to update each component task were:

Step 1 The ratings for the characteristics of visualisations of the component tasks were transformed into a tabular format so that it could be compared with the feedback from the experts. The scale of the ratings ranged from -2 (Strongly Disagree) to 2 (Strongly Agree).

Step 2 The characteristics of visualisation were divided into three categories: *confirmed*, *recommended* and *discarded* based on their means, as in *Step 5*in Section 4.4.4.

The characteristics of visualisation with a *mean* >= 1 were assigned to the *confirmed* category, as illustrated by the confidence intervals. These characteristics received positive to very positive responses.

The characteristics of visualisation with a $0 < mean < 1$ were to be to assigned to the *recommended* category. Those characteristics of visualisation with a $mean < 0$ were to be assigned to the *discarded* category. However, none of the characteristics received a $mean < 1$, as illustrated by the confidence intervals. Thus, the *recommended* and *discarded* categories were omitted.

Step 3 The component task diagrams were updated with the *confirmed* characteristics.

5.3.2.1 Revision of Guidelines for Visualisation for Triage Analysis (TA)

The results of the 30 respondents of the updated 'Triage Analysis' showed:

1. 28 (93.3%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Triage Analysis';
2. 26 (86.7%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Triage Analysis'.

Table E.1 in Appendix E shows the ratings given by each respondent to the overall task and characteristics of visualisation for 'Triage Analysis'. To revise the component task, the ratings from Table E.1 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), shown in Table E.2, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.2 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed to determine if there exist of any significant differences between the means of the characteristics of visualisation. This is followed by calculating confidence interval boundaries. Typically, 95% confidence intervals are calculated, which means that 95% of the samples will have the true mean falling between the intervals.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.2 for the results of Mauchly's Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.2: Results of Mauchly's Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of 'Triage Analysis'.

Mauchly's W	**Sig (p)**	**Greenhouse-Geisser**	**Huynh-Feldt**	**Lower-bound**
0.70	**0.36**	0.89	1.0	0.25

As shown in Table 5.2 the significant value (Sig) for Mauchly's W is 0.36
=> *0.36 > 0.05*
Therefore, sphericity is not violated and the results of *ANOVA* do not require any adjustment. The results of *ANOVA* are presented in Table 5.3.

Table 5.3: Results of *ANOVA* for Characteristics of Visualisation of 'Triage Analysis'

Source	df	Mean Square	F-Value	Sig (p)
Characteristics of Visualisation	*4*	*0.81*	*1.81*	**0.13**
Error (Characteristics of Visualisation)	*116*	*0.45*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.3, the differences between the characteristics is

=> *F(4,116) = 1.81 where 0.13(Sig.) > 0.05*
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Triage Analysis'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.2 and numerically in Table 5.4.

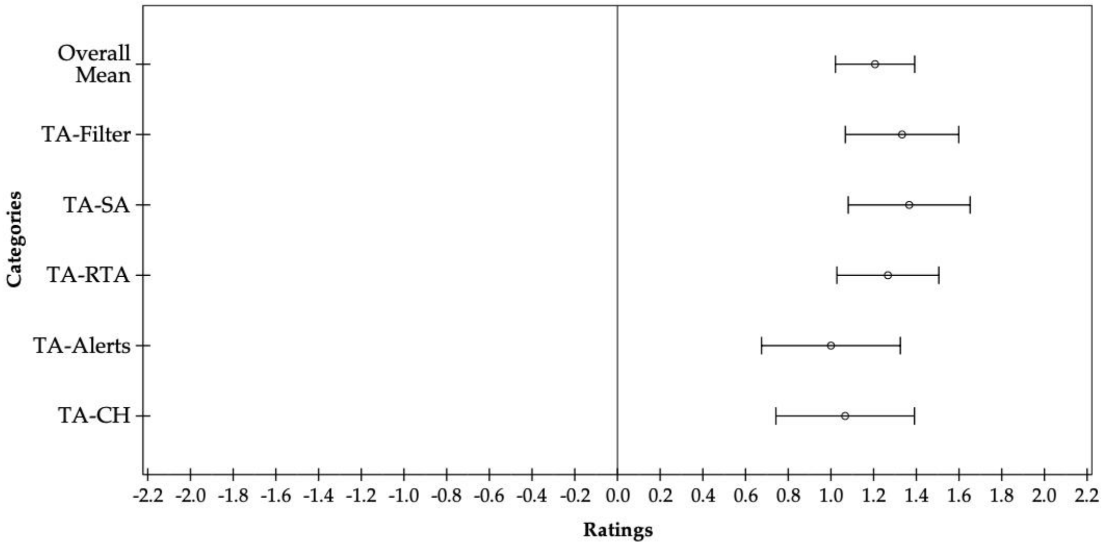


Figure 5.2: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Triage Analysis'.

Figure 5.2 shows that the overall task has Mean = 1.21, 95% CI [1.02,1.40] (Table 5.4), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.2 and Table 5.4:

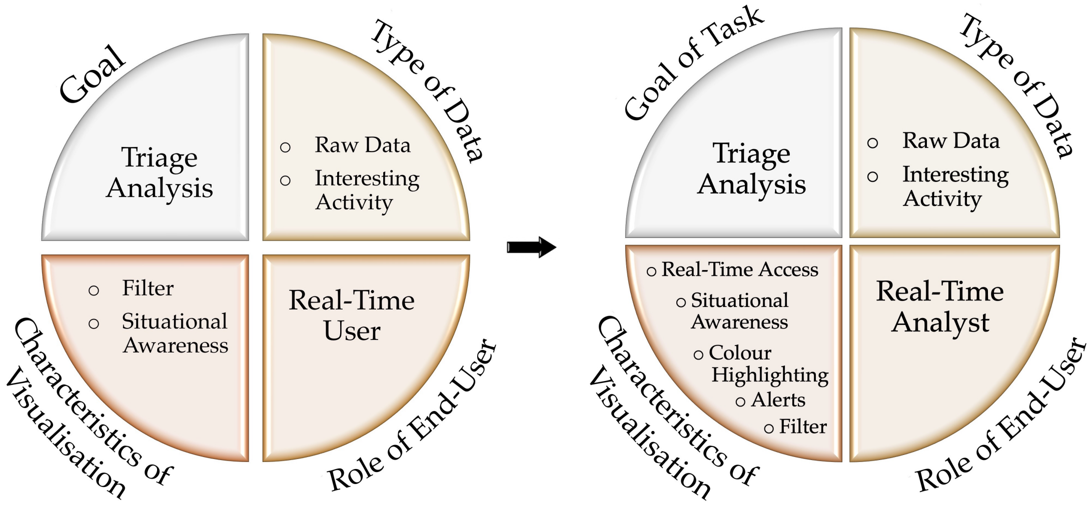
- 'TA-Filter' has Mean = 1.33, 95% CI [1.07,1.60], which is greater than zero. It is moved into the *confirmed* category.

Table 5.4: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Triage Analysis'.

Category	Lower Bound	Upper Bound
Overall	1.02	1.40
TA-Filter	1.07	1.60
TA-SA	1.08	1.65
TA-RTA	1.03	1.51
TA-Alerts	0.68	1.33
TA-CH	0.74	1.39

- 'TA-SA' (Situational Awareness) has Mean = 1.37, 95% CI [1.08,1.65], which is greater than zero. It is moved into the *confirmed* category.
- 'TA-RTA' (Real-Time Access) has Mean = 1.27, 95% CI [1.03,1.51], which is greater than zero. It is moved into the *confirmed* category.
- 'TA-Alerts' has Mean = 1.00, 95% CI [0.68,1.33], which is greater than zero. It is moved into the *confirmed* category.
- 'TA-CH' (Colour Highlighting) has Mean = 1.07, 95% CI [0.74,1.39], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Triage Analysis' is shown in Figure 5.3.



(a) Validated Triage Analysis (b) Revised and Confirmed Triage Analysis

Figure 5.3: Transformation of the visual representation of 'Triage Analysis' from the validated representation to *confirmed Characteristics of Visualisation.*

5.3.2.2 Revision of Guidelines for Visualisation for Escalation Analysis (EA)

The results of the 30 respondents of the updated 'Escalation Analysis' showed:

1. 29 (96.7%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Escalation Analysis';
2. 26 (86.7%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Escalation Analysis'.

Table E.3 in Appendix E shows the ratings given by each respondent to the overall task and characteristics of visualisation for 'Escalation Analysis'. To revise the component task, the ratings from Table E.3 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.4, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.4 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.5 for the results of Mauchly's Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.5: Results of Mauchly's Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of 'Escalation Analysis'.

Mauchly's W	**Sig (p)**	**Greenhouse-Geisser**	**Huynh-Feldt**	**Lower-bound**
0.61	**0.18**	0.79	0.86	0.33

As shown in Table 5.5 the significant value (Sig) for Mauchly's W is 0.18
=> *0.18 > 0.05*
Therefore, sphericity is not violated and the results of *ANOVA* do not require any adjustment. The results of *ANOVA* are presented in Table 5.6.

Table 5.6: Results of *ANOVA* for Characteristics of Visualisation of 'Escalation Analysis'

Source	**df**	**Mean Square**	**F-Value**	**Sig (p)**
Characteristics of Visualisation	*3*	*0.50*	*1.86*	**0.14**
Error (Characteristics of Visualisation)	*87*	*0.27*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.6, the differences between the characteristics is

=> F(3,87) = 1.86 where 0.14(Sig.) > 0.05
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Escalation Analysis'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.4 and numerically in Table 5.7.

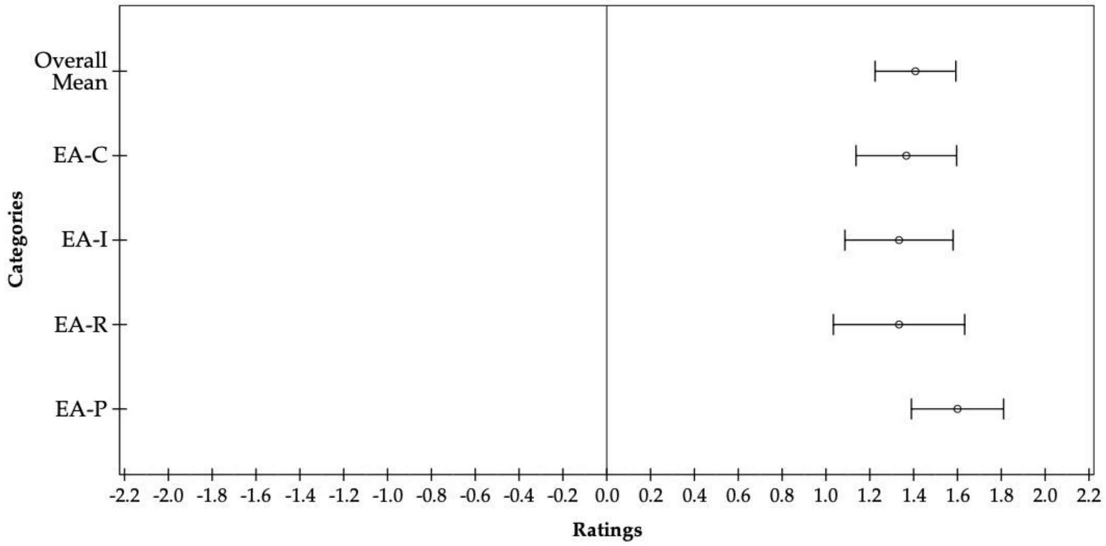


Figure 5.4: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Escalation Analysis'.

Figure 5.4 shows that the overall task has Mean = 1.41, 95% CI [1.22,1.59] (Table 5.7), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.4 and Table 5.7:

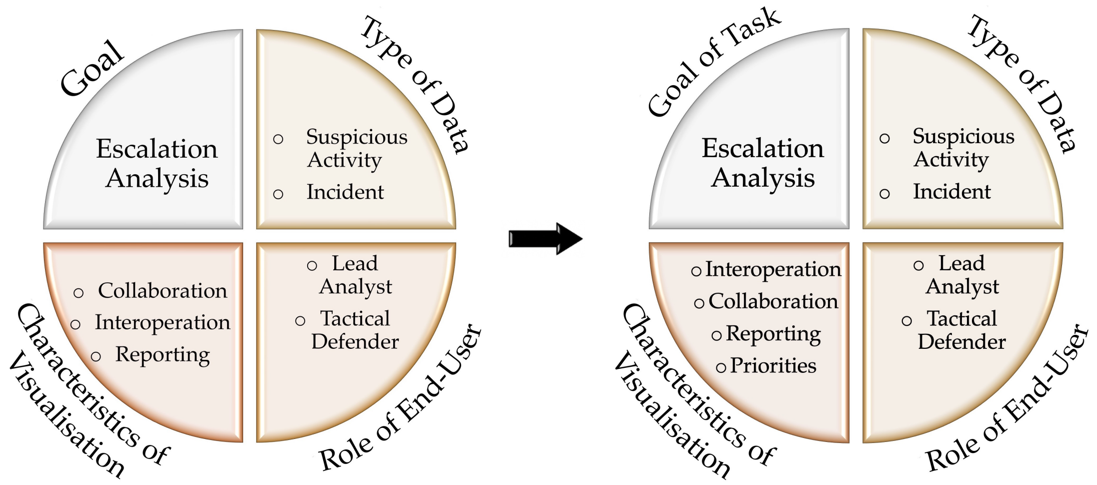
- 'EA-C' (Collaboration) has Mean = 1.37, 95% CI [1.14,1.60], which is greater than zero. It is moved into the *confirmed* category.

Table 5.7: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Escalation Analysis'.

Category	Lower Bound	Upper Bound
Overall	1.22	1.59
EA-C	1.14	1.60
EA-I	1.09	1.58
EA-R	1.03	1.63
EA-P	1.39	1.81

- 'EA-I' (Interoperation) has Mean = 1.33, 95% CI [1.09,1.58], which is greater than zero. It is moved into the *confirmed* category.
- 'EA-R' (Reporting) has Mean = 1.33, 95% CI [1.03,1.63], which is greater than zero. It is moved into the *confirmed* category.
- 'EA-P' (Priorities) has Mean = 1.60, 95% CI [1.39,1.81], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Escalation Analysis' is shown in Figure 5.5.



(a) Validated Escalation Analysis

(b) Revised and Confirmed Escalation Analysis

Figure 5.5: Transformation of the visual representation of 'Escalation Analysis' from the validated representation to *confirmed Characteristics of Visualisation*.

5.3.2.3 Revision of Guidelines for Visualisation for Correlation Analysis (CA)

The results of the 30 respondents of the updated 'Correlation Analysis' showed:

1. 25 (83.3%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Correlation Analysis';
2. 29 (96.7%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Correlation Analysis'.

Table E.5 in Appendix E represents the ratings given by each respondent to the overall task and characteristics of visualisation for 'Correlation Analysis'. To revise the component task, the ratings from Table E.5 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.6, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.6 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.8 for the results of Mauchly's Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.8: Results of Mauchly's Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of 'Correlation Analysis'.

Mauchly's W	**Sig (p)**	**Greenhouse-Geisser**	**Huynh-Feldt**	**Lower-bound**
0.92	**0.32**	0.93	0.99	0.50

As shown in Table 5.8 the significant value (Sig) for Mauchly's W is 0.32
=> *0.32 > 0.05*
Therefore, sphericity is not violated and the results of *ANOVA* do not require any adjustment. The results of *ANOVA* are presented in Table 5.9.

Table 5.9: Results of *ANOVA* for Characteristics of Visualisation of 'Correlation Analysis'

Source	**df**	**Mean Square**	**F-Value**	**Sig (p)**
Characteristics of Visualisation	*2*	*0.41*	*1.00*	**0.37**
Error (Characteristics of Visualisation)	*58*	*0.41*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.9, the differences between the characteristics is

=> F(2,58) = 1.0 where 0.37(Sig.) > 0.05
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Correlation Analysis'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.6 and numerically in Table 5.10.

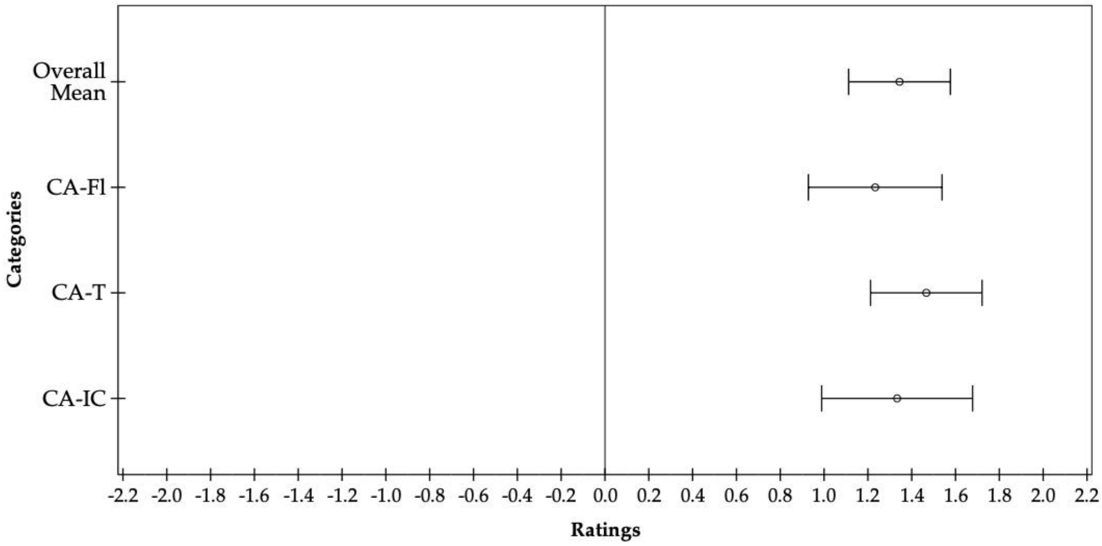


Figure 5.6: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Correlation Analysis'.

Figure 5.6 shows that the overall task has Mean = 1.34, 95% CI [1.11,1.58] (Table 5.10), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.6 and Table 5.10:

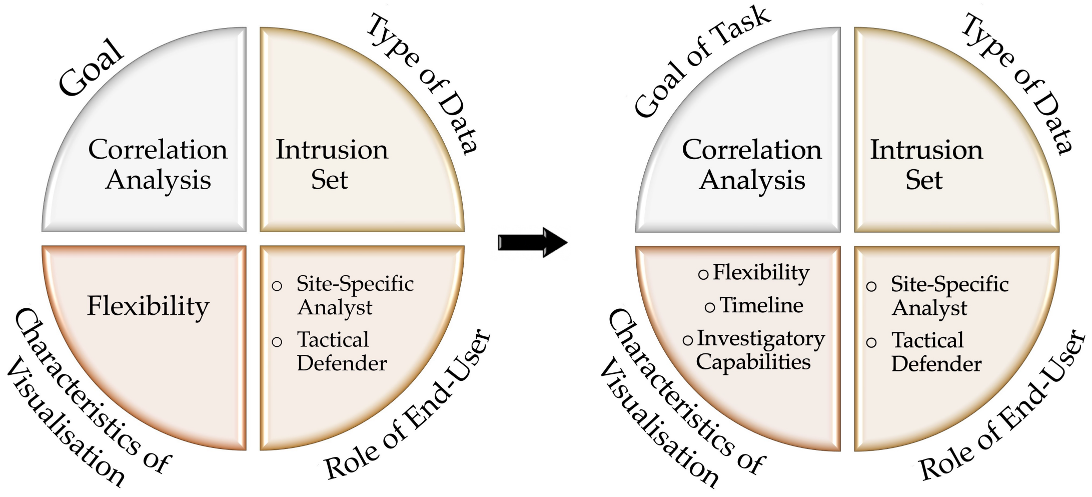
- 'CA-Fl' (Flexibility) has Mean = 1.23, 95% CI [0.93,1.54], which is greater than zero. It is moved into the *confirmed* category.

Table 5.10: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for ‘Correlation Analysis’.

Category	Lower Bound	Upper Bound
Overall	1.11	1.58
CA-Fl	0.93	1.54
CA-T	1.21	1.72
CA-IC	0.99	1.68

- ‘CA-T’ (Timeline) has Mean = 1.47, 95% CI [1.21,1.72], which is greater than zero. It is moved into the *confirmed* category.
- ‘CA-IC’ (Investigatory Capabilities) has Mean = 1.33, 95% CI [0.99,1.68], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed ‘Correlation Analysis’ is shown in Figure 5.7.



(a) Validated Correlation Analysis (b) Revised and Confirmed Correlation Analysis

Figure 5.7: Transformation of the visual representation of ‘Correlation Analysis’ from the validated representation to *confirmed Characteristics of Visualisation.*

5.3.2.4 Revision of Guidelines for Visualisation for Threat Analysis (ThA)

The results of the 30 respondents of the updated 'Threat Analysis' showed:

1. 28 (93.3%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Threat Analysis';
2. 26 (86.7%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Threat Analysis'.

Table E.7 in Appendix E represents the ratings given by each respondent to the overall task and characteristics of visualisation for 'Threat Analysis'. To revise the component task, the ratings from Table E.7 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.8, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.8 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.11 for the results of Mauchly's Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.11: Results of Mauchly's Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of 'Threat Analysis'.

Mauchly's W	**Sig (p)**	**Greenhouse-Geisser**	**Huynh-Feldt**	**Lower-bound**
0.72	**0.11**	0.83	0.91	0.33

As shown in Table 5.11 the significant value (Sig) for Mauchly's W is 0.11
=> *0.11 > 0.05*
Therefore, sphericity is not violated and the results of *ANOVA* do not require any adjustment. The results of *ANOVA* are presented in Table 5.12.

Table 5.12: Results of *ANOVA* for Characteristics of Visualisation of 'Threat Analysis'

Source	df	Mean Square	F-Value	Sig (p)
Characteristics of Visualisation	*3*	*0.20*	*0.47*	**0.70**
Error (Characteristics of Visualisation)	*87*	*0.42*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.12, the differences between the characteristics is

=> *F(3,87) = 0.47 where 0.70(Sig.) > 0.05*
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Threat Analysis'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.8 and numerically in Table 5.13.

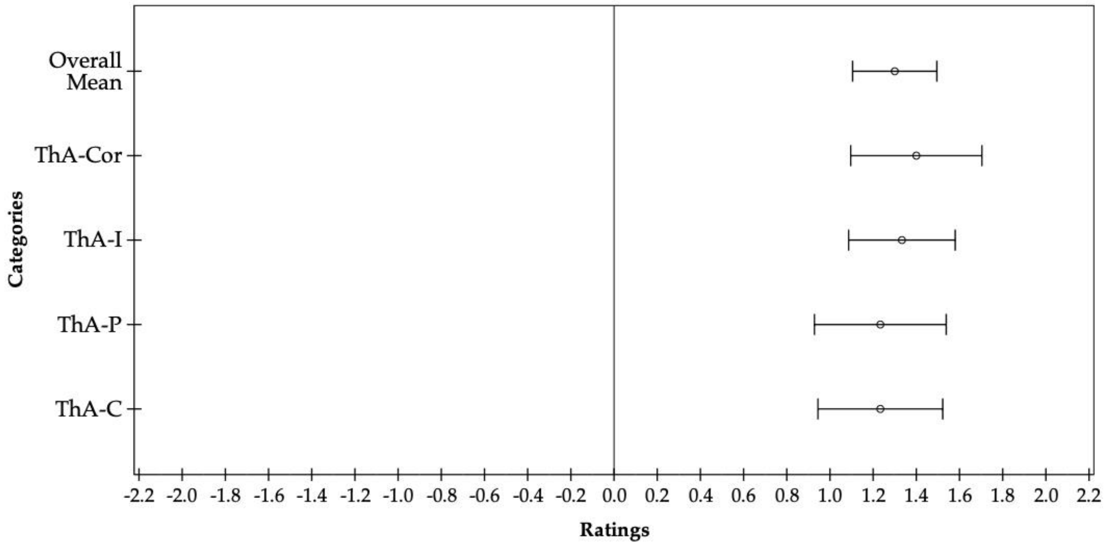


Figure 5.8: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Threat Analysis'.

Figure 5.8 shows that the overall task has Mean = 1.30, 95% CI [1.11,1.50] (Table 5.13), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.8 and Table 5.13:

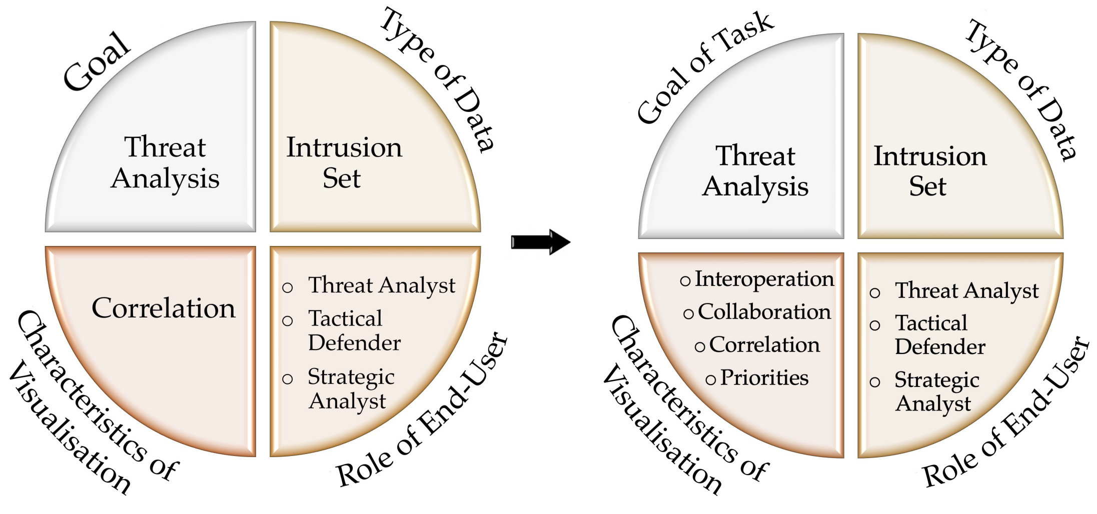
- 'ThA-Cor' (Correlation) has Mean = 1.40, 95% CI [1.10,1.70], which is greater than zero. It is moved into the *confirmed* category.

Table 5.13: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Threat Analysis'.

Category	Lower Bound	Upper Bound
Overall	1.11	1.50
ThA-Cor	1.10	1.70
ThA-I	1.09	1.58
ThA-P	0.93	1.54
ThA-C	0.94	1.52

- 'ThA-I' (Interoperation) has Mean = 1.33, 95% CI [1.09,1.58], which is greater than zero. It is moved into the *confirmed* category.
- 'ThA-P' (Priorities) has Mean = 1.23, 95% CI [0.93,1.54], which is greater than zero. It is moved into the *confirmed* category.
- 'ThA-C' (Collaboration) has Mean = 1.23, 95% CI [0.94,1.52], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Threat Analysis' is shown in Figure 5.9.



(a) Validated Threat Analysis

(b) Revised and Confirmed Threat Analysis

Figure 5.9: Transformation of the visual representation of 'Threat Analysis' from the validated representation to *confirmed Characteristics of Visualisation.*

5.3.2.5 Revision of Guidelines for Visualisation for Impact Assessment (IA)

The results of the 30 respondents of the updated 'Impact Assessment' showed:

1. 26 (86.7%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Impact Assessment';
2. 23 (76.7%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Impact Assessment'.

Table E.9 in Appendix E represents the ratings given by each respondent to the overall task and characteristics of visualisation for 'Impact Assessment'. To revise the component task, the ratings from Table E.9 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.10, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.10 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.14 for the results of Mauchly's Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.14: Results of Mauchly's Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of 'Impact Assessment'.

Mauchly's W	Sig (p)	Greenhouse-Geisser	Huynh-Feldt	Lower-bound
0.98	**0.75**	0.98	1.00	0.50

As shown in Table 5.14 the significant value (Sig) for Mauchly's W is 0.75
=> *0.75 > 0.05*
Therefore, sphericity is not violated and the results of *ANOVA* do not require any adjustment. The results of *ANOVA* are presented in Table 5.15.

Table 5.15: Results of *ANOVA* for Characteristics of Visualisation of 'Impact Assessment'

Source	**df**	**Mean Square**	**F-Value**	**Sig (p)**
Characteristics of Visualisation	*2*	*0.13*	*0.74*	**0.48**
Error (Characteristics of Visualisation)	*58*	*0.18*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.15, the differences between the characteristics is

=> F(2,58) = 0.74 where 0.48(Sig.) > 0.05
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Impact Assessment'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.10 and numerically in Table 5.16.

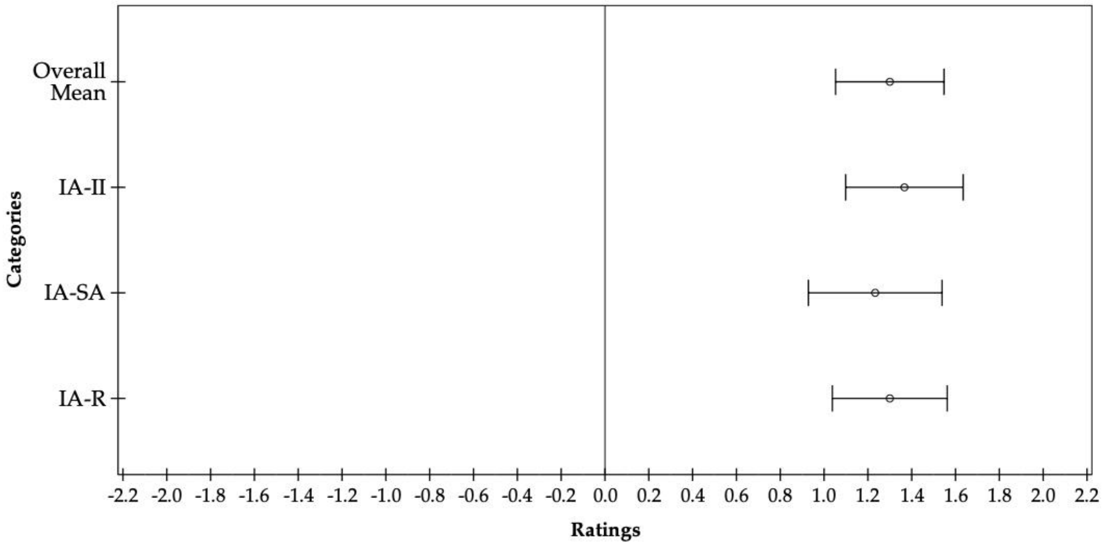


Figure 5.10: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Impact Assessment'.

Figure 5.10 shows that the overall task has Mean = 1.30, 95% CI [1.05,1.55] (Table 5.16), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.10 and Table 5.16:

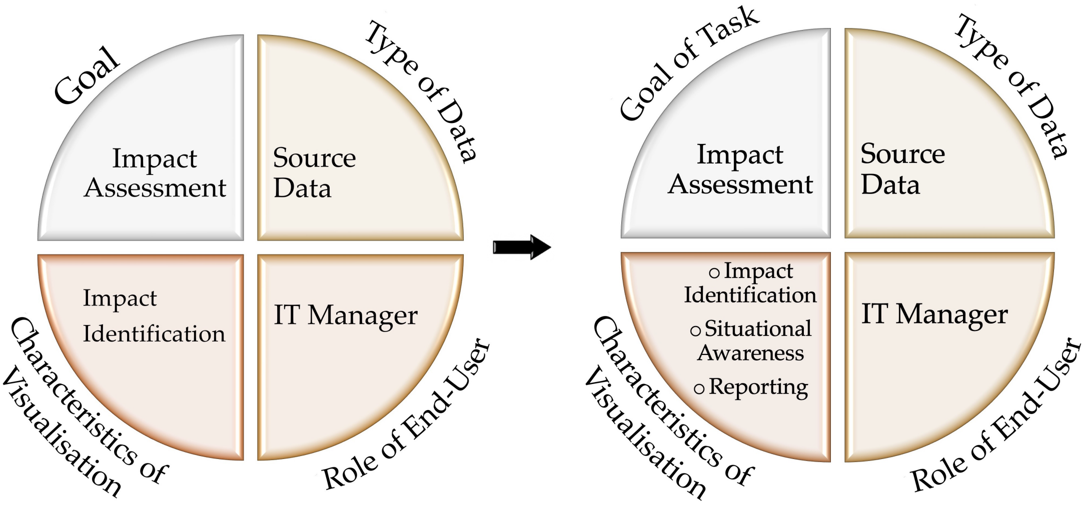
- 'IA-II' (Impact Identification) has Mean = 1.37, 95% CI [1.10,1.64], which is greater than zero. It is moved into the *confirmed* category.

Table 5.16: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Impact Assessment'.

Category	**Lower Bound**	**Upper Bound**
Overall	1.05	1.55
IA-II	1.10	1.64
IA-SA	0.93	1.54
IA-R	1.04	1.56

- 'IA-SA' (Situational Awareness) has Mean = 1.23, 95% CI [0.93,1.54], which is greater than zero. It is moved into the *confirmed* category.
- 'IA-R' (Reporting) has Mean = 1.30, 95% CI [1.04,1.56], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Impact Assessment' is shown in Figure 5.11.



(a) Validated Impact Assessment

(b) Revised and Confirmed Impact Assessment

Figure 5.11: Transformation of the visual representation of 'Impact Assessment' from the validated representation to *confirmed Characteristics of Visualisation.*

5.3.2.6 Revision of Guidelines for Visualisation for Incident Response Analysis (IRA)

The results of the 30 respondents of the updated ‘Incident Response Analysis’ showed:

1. 27 (90%) respondents agreed that the validated characteristics of visualisation made sense for performing ‘Incident Response Analysis’;
2. 24 (80%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of ‘Incident Response Analysis’.

Table E.11 in Appendix E represents the ratings given by each respondent to the overall task and characteristics of visualisation for ‘Incident Response Analysis’. To revise the component task, the ratings from Table E.11 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.12, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.12 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.17 for the results of Mauchly’s Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.17: Results of Mauchly’s Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of ‘Incident Response Analysis’.

Mauchly’s W	**Sig (p)**	**Greenhouse-Geisser**	**Huynh-Feldt**	**Lower-bound**
0.317	**0**	0.60	0.66	0.25

As shown in Table 5.17 the significant value (Sig) for Mauchly’s W is 0
=> *0 < 0.05*
Therefore, sphericity is violated and the results of *ANOVA* require adjustment. As explained in Section 4.4.3.1, in such a case, *Greenhouse-Geisser* adjustment is recommended if the estimate is below 0.75. Table 5.17 shows,
=> *0.60 < 0.75*
Consequently, results of *ANOVA* with the *Greenhouse-Geisser* adjustment are presented in Table 5.18.

Table 5.18: Results of *ANOVA* (using *Greenhouse-Geisser* Correction) for Characteristics of Visualisation of 'Incident Response Analysis'

Source	df	Mean Square	F-Value	Sig (p)
Characteristics of Visualisation	*2.42*	*0.20*	*0.28*	**0.80**
Error (Characteristics of Visualisation)	*70.29*	*0.72*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.18, the differences between the characteristics is

=> *F(2.42,70.29) = 0.28 where 0.80(Sig.) > 0.05*
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Incident Response Analysis'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.12 and numerically in Table 5.19.

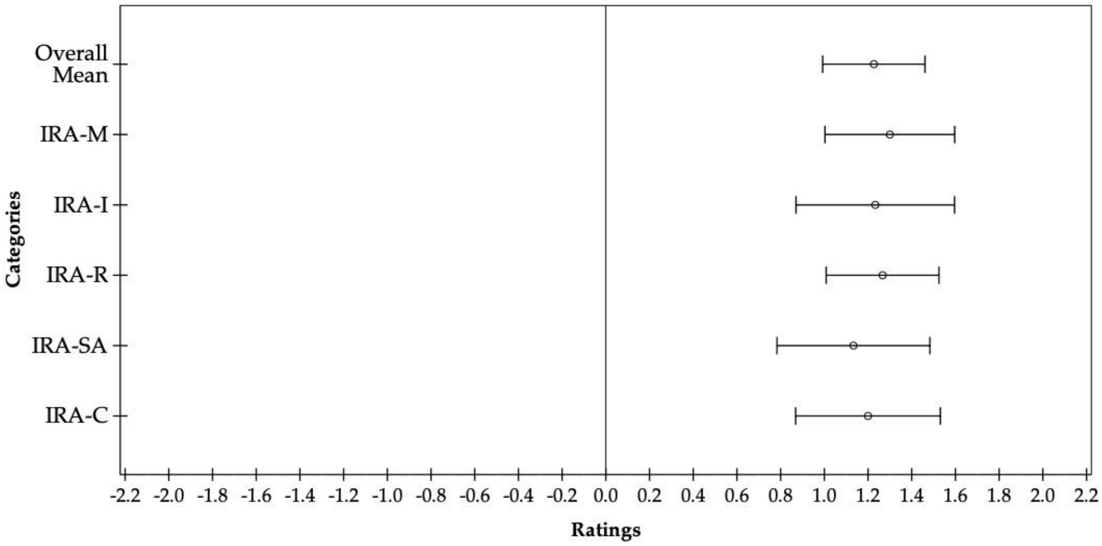


Figure 5.12: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Incident Response Analysis'.

Figure 5.12 shows that the overall task has Mean = 1.23, 95% CI [0.99,1.46] (Table 5.19), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.12 and Table 5.19:

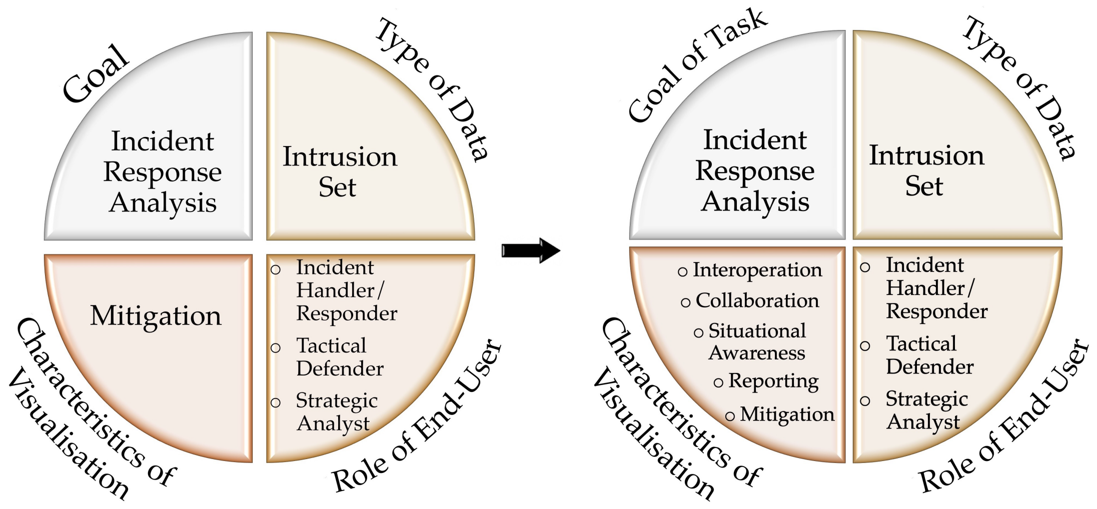
- 'IRA-M' (Mitigation) has Mean = 1.30, 95% CI [1.00,1.60], which is greater than zero. It is moved into the *confirmed* category.

Table 5.19: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Incident Response Analysis'.

Category	**Lower Bound**	**Upper Bound**
Overall	0.99	1.46
IRA-M	1.00	1.60
IRA-I	0.87	1.60
IRA-R	1.01	1.53
IRA-SA	0.79	1.48
IRA-C	0.87	1.53

- 'IRA-I' (Interoperation) has Mean = 1.23, 95% CI [0.87,1.60], which is greater than zero. It is moved into the *confirmed* category.
- 'IRA-R' (Reporting) has Mean = 1.27, 95% CI [1.01,1.53], which is greater than zero. It is moved into the *confirmed* category.
- 'IRA-SA' (Situational Awareness) has Mean = 1.13, 95% CI [0.79,1.48], which is greater than zero. It is moved into the *confirmed* category.
- 'IRA-C' (Collaboration) has Mean = 1.20, 95% CI [0.87,1.53], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Incident Response Analysis' is shown in Figure 5.13.



(a) Validated Incident Response Analysis

(b) Revised and Confirmed Incident Response Analysis

Figure 5.13: Transformation of the visual representation of 'Incident Response Analysis' from the validated representation to *confirmed Characteristics of Visualisation.*

5.3.2.7 Revision of Guidelines for Visualisation for Forensic Analysis (FA)

The results of the 30 respondents of the updated 'Forensic Analysis' showed:

1. 26 (86.7%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Forensic Analysis';
2. 26 (86.7%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Forensic Analysis'.

Table E.13 in Appendix E represents the ratings given by each respondent to the overall task and characteristics of visualisation for 'Forensic Analysis'. To revise the component task, the ratings from Table E.13 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.14, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.14 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. Refer to Table 5.20 for the results of Mauchly's Test of Sphericity to determine if sphericity is met, and if not then which adjustments are to be used.

Table 5.20: Results of Mauchly's Test of Sphericity and Adjustments for Violation of Sphericity for Characteristics of Visualisation of 'Forensic Analysis'.

Mauchly's W	**Sig (p)**	**Greenhouse-Geisser**	**Huynh-Feldt**	**Lower-bound**
0.78	**0.28**	0.85	0.94	0.33

As shown in Table 5.20 the significant value (Sig) for Mauchly's W is 0.28
=> *0.28 > 0.05*
Therefore, sphericity is not violated and the results of *ANOVA* do not require adjustment. The results of *ANOVA* are presented in Table 5.21.

Table 5.21: Results of *ANOVA* for Characteristics of Visualisation of 'Forensic Analysis'

Source	df	Mean Square	F-Value	Sig (p)
Characteristics of Visualisation	*3*	*0.22*	*1.03*	**0.39**
Error (Characteristics of Visualisation)	*87*	*0.22*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.21, the differences between the characteristics is

=> F(3,87) = 1.03 where 0.39(Sig.) > 0.05
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Forensic Analysis'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.14 and numerically in Table 5.22.

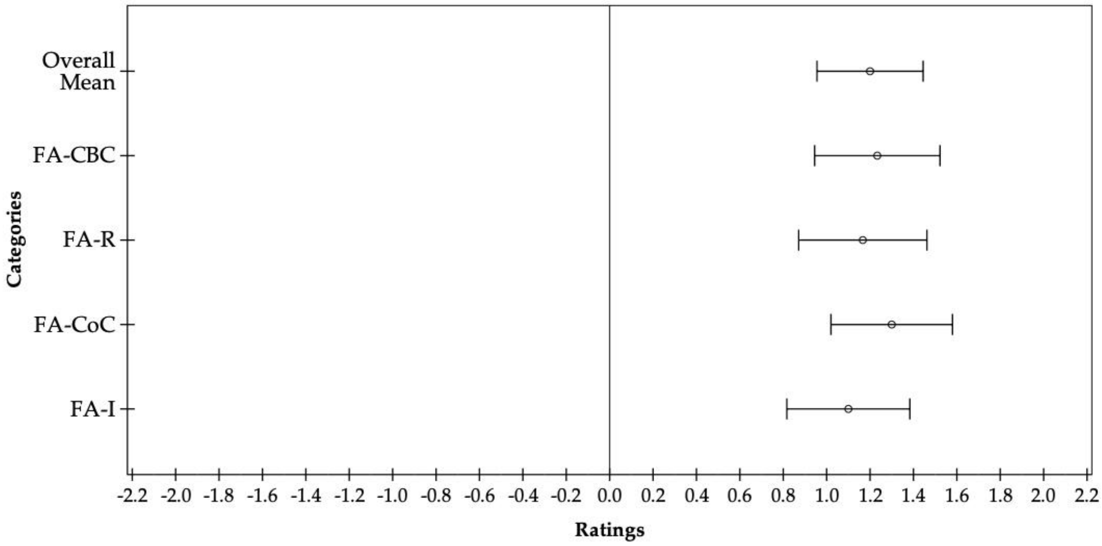


Figure 5.14: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Forensic Analysis'.

Figure 5.14 shows that the overall task has Mean = 1.20, 95% CI [0.96,1.44] (Table 5.22), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.14 and Table 5.22:

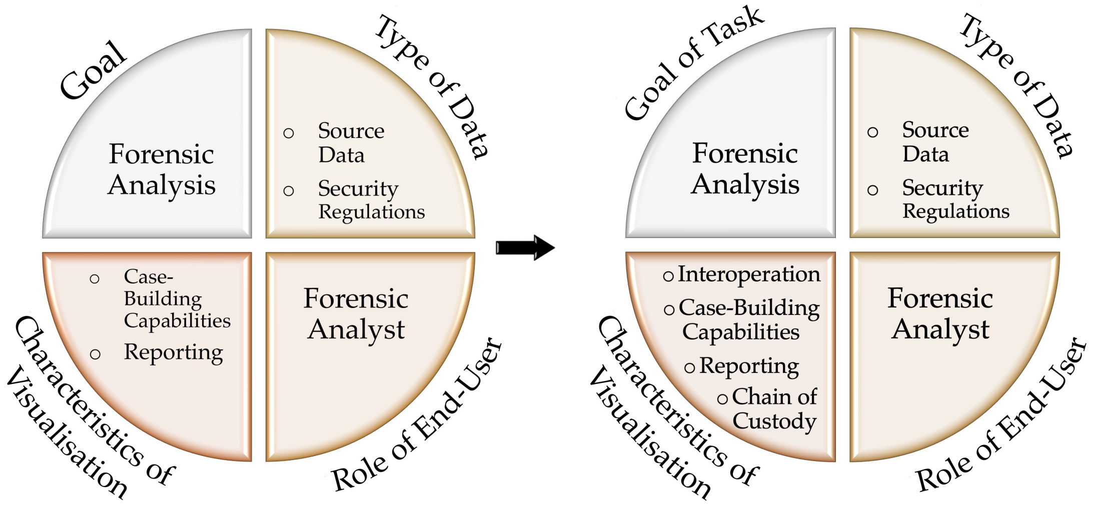
- 'FA-CBC' (Case-Building Capabilities) has Mean = 1.23, 95% CI [0.94,1.52], which is greater than zero. It is moved into the *confirmed* category.

Table 5.22: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Forensic Analysis'.

Category	Lower Bound	Upper Bound
Overall	0.96	1.44
FA-CBC	0.94	1.52
FA-R	0.87	1.46
FA-CoC	1.02	1.58
FA-I	0.82	1.38

- 'FA-R' (Reporting) has Mean = 1.17, 95% CI [0.87,1.46], which is greater than zero. It is moved into the *confirmed* category.
- 'FA-CoC' (Chain of Custody) has Mean = 1.30, 95% CI [1.02,1.58], which is greater than zero. It is moved into the *confirmed* category.
- 'FA-I' (Interoperation) has Mean = 1.10, 95% CI [0.82,1.38], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Forensic Analysis' is shown in Figure 5.15.



(a) Validated Forensic Analysis (b) Revised and Confirmed Forensic Analysis

Figure 5.15: Transformation of the visual representation of 'Forensic Analysis' from the validated representation to *confirmed Characteristics of Visualisation.*

5.3.2.8 Revision of Guidelines for Visualisation for Security Quality Management (SQM)

The results of the 30 respondents of the updated 'Security Quality Management' showed:

1. 25 (83.3%) respondents agreed that the validated characteristics of visualisation made sense for performing 'Security Quality Management';
2. 25 (83.3%) respondents agreed that the validated characteristics of visualisation cover all important characteristics to enable competent performance of 'Security Quality Management'.

Table E.15 in Appendix E represents the ratings given by each respondent to the overall task and characteristics of visualisation for 'Security Quality Management'. To revise the component task, the ratings from Table E.15 were quantified on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree) shown in Table E.16, along with the means of each characteristic of visualisation.

To demonstrate that all values in Table E.16 represent means greater than 0, statistical tests were performed. An *ANOVA* is performed, followed by calculating confidence interval boundaries.

To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be used, as explained in Section 4.4.3.1. To estimate the correct results from the results of *ANOVA*, the first task is to recognise which corrected values are to be applied from Table 5.23.

Table 5.23: Adjustments for results of *ANOVA* for Characteristics of Visualisation of 'Security Quality Management'.

Greenhouse-Geisser	Huynh-Feldt	Lower-bound
1.00	**1.00**	1.00

As explained in Section 4.4.3.1, *Greenhouse-Geisser* adjustment is recommended if the estimate is below 0.75, while *Huynh-Feldt* is recommended otherwise. Table 5.23 shows,
=> *1.00 > 0.75*
Consequently, results of *ANOVA* with the *Huynh-Feldt* adjustment are presented in Table 5.24.

Table 5.24: Results of *ANOVA* (using *Huynh-Feldt* Correction) for Characteristics of Visualisation of 'Security Quality Management'

Source	**df**	**Mean Square**	**F-Value**	**Sig (p)**
Characteristics of Visualisation	*1*	*0*	*0*	**1.00**
Error (Characteristics of Visualisation)	*29*	*0.24*	-	-

Following from Section 4.4.3.1, 'Sig (p)' represents the significant value or p-value, if this value is less than 0.05 then there is a significant effect. According to Table 5.24, the differences between the characteristics is

=> *F(1,29) = 0 where 1.00(Sig.) > 0.05*
which shows a non-significant effect. Thus, there are no significant differences between the means of the characteristics of visualisation for 'Security Quality Management'.

Following the results of the *ANOVA*, 95% confidence intervals for the overall mean and means of individual characteristics of visualisation are calculated, and presented graphically in Figure 5.16 and numerically in Table 5.25.

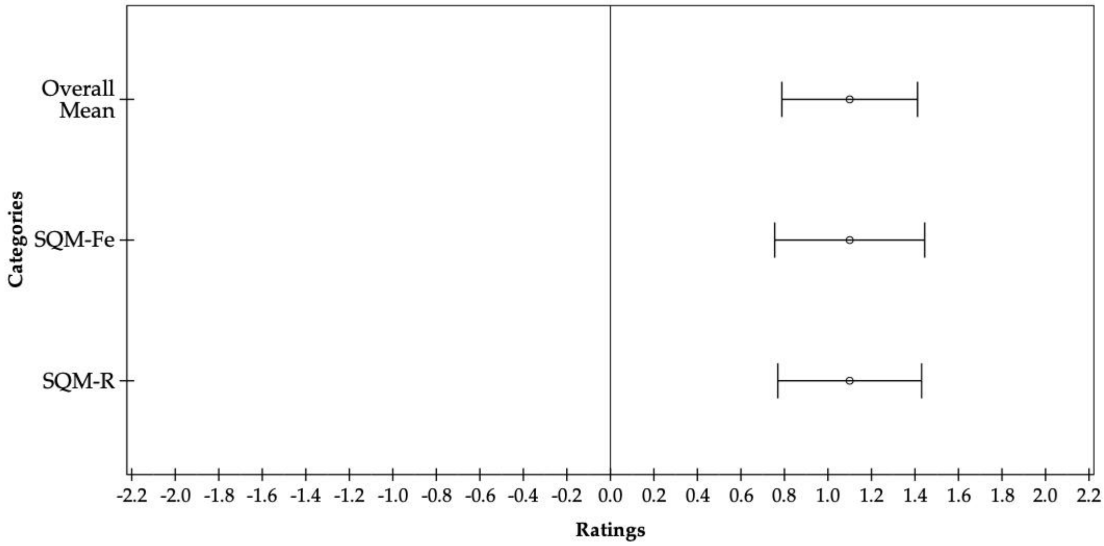


Figure 5.16: Illustration of the confidence Intervals (95%) of ratings (x axis) for all categories (y axis) of 'Security Quality Management'.

Figure 5.16 shows that the overall task has Mean = 1.10, 95% CI [0.79,1.41] (Table 5.25), which is greater than zero and the overall task is of a high standard. For the characteristics of visualisation, as per Figure 5.16 and Table 5.25:

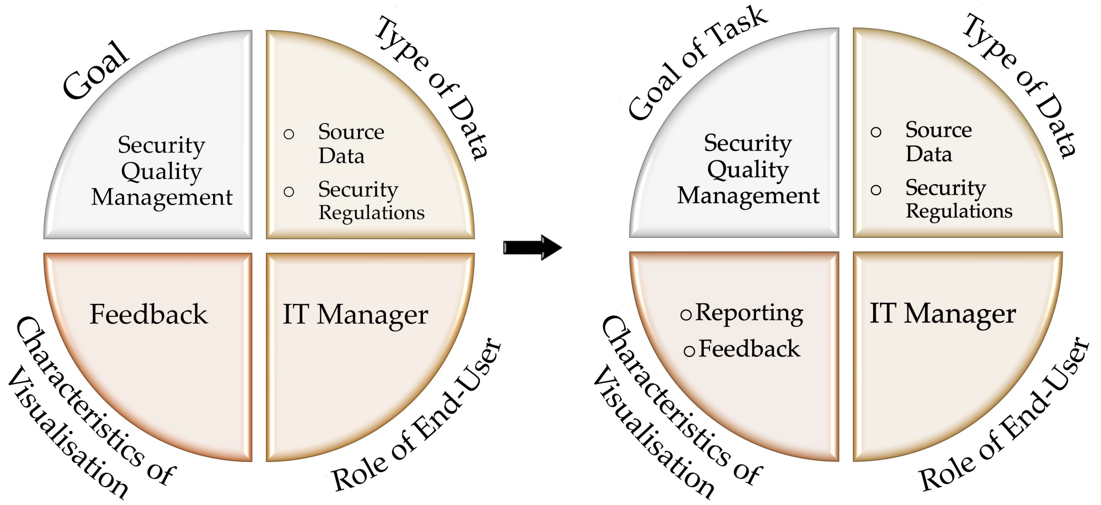
- 'SQM-Fe' (Feedback) has Mean = 1.10, 95% CI [0.76,1.45], which is greater than zero. It is moved into the *confirmed* category.

Table 5.25: Tabulation of lower and upper bounds of the confidence Intervals (95%) of ratings for all categories for 'Security Quality Management'.

Category	Lower Bound	Upper Bound
Overall	0.79	1.41
SQM-Fe	0.76	1.45
SQM-R	0.77	1.43

- 'SQM-R' (Reporting) has Mean = 1.10, 95% CI [0.77,1.43], which is greater than zero. It is moved into the *confirmed* category.

Based on the above results, all characteristics of visualisation have been moved into the *confirmed* category. The revised and confirmed 'Security Quality Management' is shown in Figure 5.17.



(a) Validated Security Quality Management

(b) Revised and Confirmed Security Quality Management

Figure 5.17: Transformation of the visual representation of 'Security Quality Management' from the validated representation to *confirmed Characteristics of Visualisation.*

5.4 Discussion

This chapter presented the results of feedback by 30 respondents to an online-based self-administered questionnaire, confirming *EEVi*. The feedback was used to confirm the model and revise the component tasks, which are shown in Figure 5.18 and Figure 5.19.

Respondents mostly had expertise in cyber-security (80%), or in both cyber-security and visualisation design (13.3%). On average, the respondents rated their expertise as 3.33

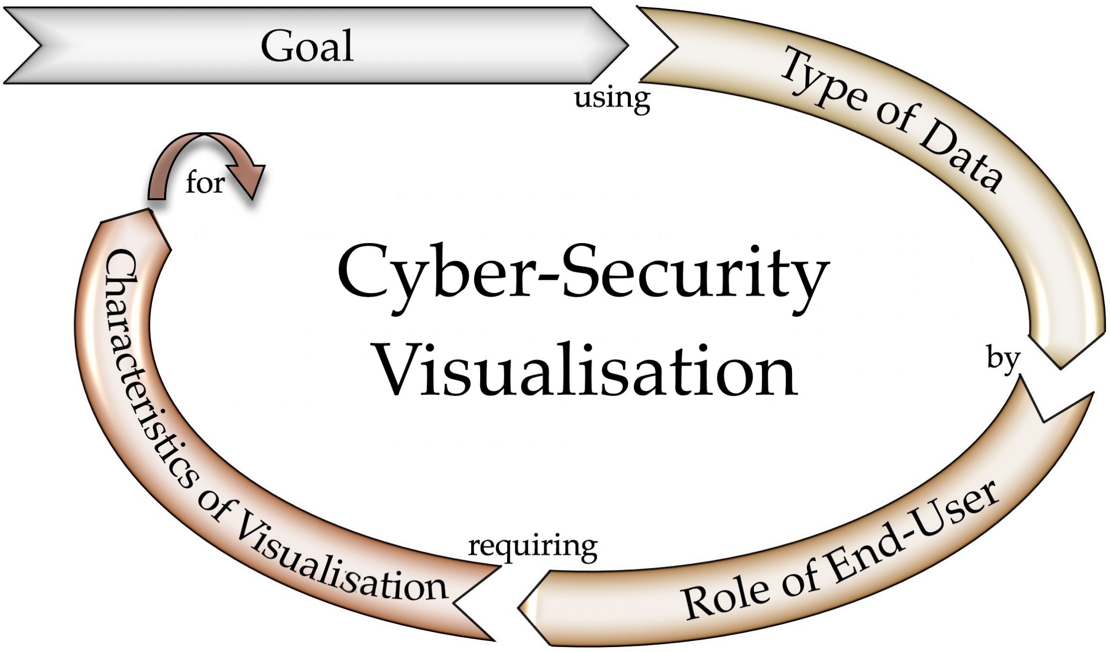

Goal
using
Type of Data
by
Role of End-User
requiring
Characteristics of Visualisation
for
Cyber-Security Visualisation

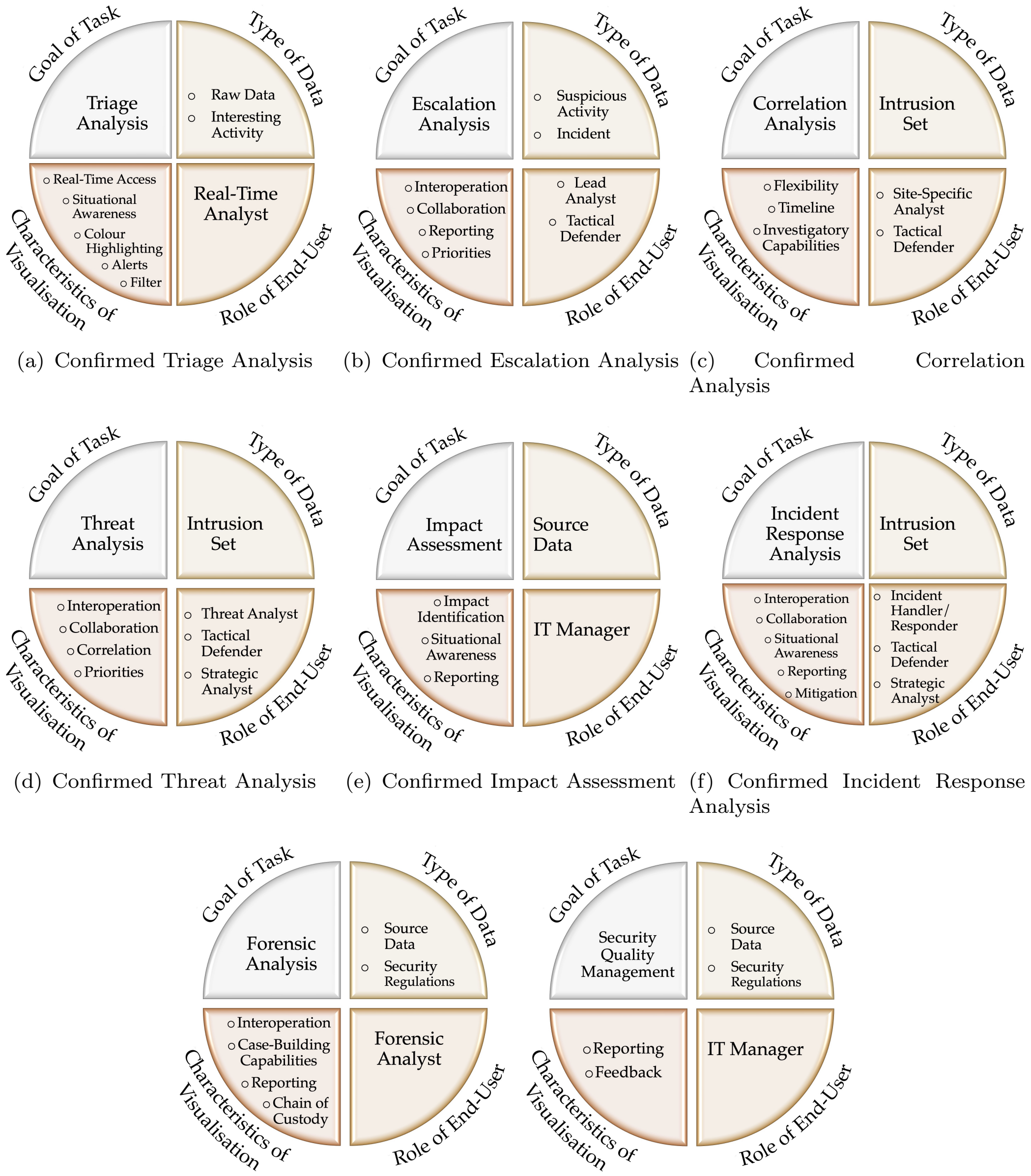
Figure 5.18: *EEVi*, a model that represents the *confirmed* guidelines for making visualisations for cyber-security analysts

on a scale of 1 (lowest) to 5 (highest), and had an average of 6.67 years of experience in their respective fields.

The respondents confirmed *EEVi* by concurring with its structure and logic (90%), and agreeing that the logic flow matches the one followed by their organisation (70%). They also confirmed that *EEVi* represents good fundamental guidelines for cyber-security visualisation (63.3%), and that it can be used to evaluate cyber-security visualisation solutions (66.7%).

Their feedback also aided in revision of the component tasks to confirm characteristics of visualisation for designing cyber-security visualisation solutions for each task. All the *unresolved* characteristics of visualisation from Chapter 4 were added to the component task guideline diagrams when they received a mean score of 1 or greater, on a scale from -2 to +2.

Figure 5.18 shows the confirmed *EEVi* model, addressing SRQ_1 and Figure 5.19 shows the confirmed component tasks of *EEVi*, addressing SRQ_2. Together, they represent guidelines for the design of cyber-security visualisation solutions for cyber-security analysts performing a specific task, addressing RQ_1. Chapter 6 illustrates *EEVi*'s utilisation in the real world, in order to determine its applicability.



(a) Confirmed Triage Analysis (b) Confirmed Escalation Analysis (c) Confirmed Correlation Analysis

(d) Confirmed Threat Analysis (e) Confirmed Impact Assessment (f) Confirmed Incident Response Analysis

(g) Confirmed Forensic Analysis (h) Confirmed Security Quality Management

Figure 5.19: The component tasks of *EEVi* that represent the *confirmed* guidelines to make visualisations for cyber-security analysts

Chapter 6

Real World Utilisation

The previous chapters (Chapters 3, 4 and 5) illustrated the development, validation and confirmation of *EEVi*. Interviews with experts were conducted to understand the usage of *EEVi* in the real world. *EEVi*, the model, was used to create sample user interface mockups, and an abstraction hierarchy diagram, for presentation to the experts. The rationale behind the user interface mockups and the work domain analysis is explained in this chapter, followed by the setup of the interviews, the demographics of the experts and the results from the interviews. The goal of the interviews was to validate the hypothesis that the user interface mockups and work domain analysis diagrams promote communication between cyber-security analysts and visualisation designers.

6.1 Background of Techniques Used

The following section elaborates on the background of user interface mockups and work domain analysis (abstraction hierarchy) techniques used.

6.1.1 User Interface Mockups

User Interface Mockups are early design prototypes, made of low-fidelity materials, to obtain valuable feedback from the end-users concerning functionality, usability or understanding of the basic design (The Interaction Design Foundation, 2019). Mockups bridge the gap between the end-user and the developer (Mukasa & Kaindl, 2008) as mockups are fully comprehensible by end-users and technologically valuable for the developer (Rivero et al., 2014).

Mockups also help discover functional requirements in a format more familiar to end-users (Rivero et al., 2014). Studies by Ricca, Scanniello, Torchiano, Reggio, and Astesiano (2014) showed the significance of using mockups to facilitate the understanding of the functional requirements in the early stages of the development process, 69% improvement on average. They also showed that using mockups can promote communication among stakeholders. Mockups also enable the developers to understand the users' requirements that are expressed informally and are often ignored (Rivero et al., 2014).

6.1.2 Work Domain Analysis (Abstraction Hierarchy)

Work Domain Analysis (WDA) is the first and most commonly used phase of Cognitive Work Analysis (CWA), a technique developed by Jens Rasmussen, that aims to model a formative approach of how a system *could* work by focusing on the functions and constraints (Jenkins, Stanton, Salmon, & Walker, 2009; McIlroy & Stanton, 2015).

WDA is used to identify a functional set of constraints in a number of abstraction levels, so as to demonstrate means-ends relationships between system functions and components (Jenkins et al., 2009; McIlroy & Stanton, 2015). WDA also organises information in a systematic manner to support user-interface design (Fay, Stanton, & Roberts, 2018; Lintern, 2016).

WDA also notes the affordances and purposes of the objects of a system, represented by the Abstraction Hierarchy (Fay et al., 2018). The abstraction hierarchy is a diagram that models the work domain with five levels of abstraction, which range from the system's functional purpose to the component physical objects (Fay et al., 2018; McIlroy & Stanton, 2015). In the abstraction hierarchy, the relationships between the different abstraction levels form the basis of decision-making as they represent the affordances of the system, and helps the means available to develop the system to be understood (Jenkins et al., 2009). The means-ends relationships address the questions: 'what is performed', 'how it can be implemented' and 'why it exists'? (Fay et al., 2018). Often there are many-to-many relationships which require the user to decide between different arrangements to satisfy a certain purpose. These represent the resources at one level that must be used to satisfy the resources one level up, which helps describe the resources required to achieve a specific function (Lintern, 2016).

The five levels of the abstraction hierarchy, as summarised by Jenkins et al. (2009) are:

1. **Functional Purpose:** The overall purpose or goal of the system and external constraints on operation, if any;
2. **Values and Priority Measures:** The criteria that can be used to measure whether the system is achieving its functional purposes and/or satisfying external constraints;
3. **Purpose-Related Functions:** The general functions required in the system that are required to achieve value and priority measures and/or satisfy external constraints;

4. **Object-Related Processes:** The functionality required in the system that enables purpose-related functions using the physical objects;
5. **Physical Objects:** The physical objects in the system that are necessary to enable the processes and functions.

The abstraction hierarchy allows the application of the system at different levels. A bottom-up approach can model existing systems (Jenkins et al., 2009),but new systems can use a top-down approach in a technologically agnostic way, providing analysts with the an understanding of what goal a system is trying to achieve or why different aspects exist, rather than what it actually does (Fay et al., 2018; Jenkins et al., 2009). In other words,, the abstraction hierarchy supports the development of new systems without any prior understanding of the system.

6.2 Arrangements for Interviews

Five cyber-security analysts and five visualisation designers were interviewed in a semi-structured format (see Appendix F). The interviewees were presented with the guidelines for only one of *EEVi*'s component tasks, namely, 'Escalation Analysis'.

Cyber-Security Analysts: The experts were asked some general questions about their work and knowledge of cyber-security. This was followed by discussion in detail of the mockups for 'Escalation Analysis'. Subsequently, the WDA diagrams were examined.

Visualisation Designers: Visualisation Designers: The experts were asked some general questions about their work and knowledge of Human Factors, Visualisation Design and Human-Computer Interaction. This was followed by discussion of the WDA diagrams for 'Escalation Analysis'. Subsequently, the mockups were examined.

The two sets of experts were interviewed to understand their unique points of view, so that the disparity of domain-knowledge between the two disciplines could be minimised and a basis of communication could be formed.

To determine the number of experts required for the interviews, as discussed in Section 4.1.1, Discounted Expert Review Theory (Nielsen, 1994) was used. According to this theory, 75% of all usability issues can be found by between three and five experts, after which the responses reach a point of saturation. Hence, to avoid omitting salient facts, at least five experts from each area were required.

6.2.1 Ethics Approval for Interviews

The interviews were conducted with approval from the Ethics and Research Governance (ERGO) committee, reference number $ERGO/FPSE/23974$.

Following the guidelines for ethical approval, interviews and questionnaire surveys conformed to the DPA Plan and Participant Information Sheet approved with the application. Each respondent was given a copy of the DPA Plan and Participant Information Sheet before they gave written or verbal consent to be interviewed. The DPA Plan and the Participant Information Sheet are shown in Appendix B.

6.3 Demographic concerning the Interviewees

The researcher identified experts in three ways: (i) using work connections at the University of Southampton to recognise academics practitioners with technical expertise, (ii) through professional connections made at relevant international conferences (ICITST[1] 2016, VizSec[2] 2017 and VIS[3] 2017) targeting industry and academic practitioners, (iii) by contacting practitioners in the author's home country with relevant expertise in performing tasks related to cyber-security. 18 experts were identified and all were contacted directly by email. The result was that 10 experts (five cyber-security analysts and five visualisation designers) were selected, with a mix of geographical locations and expertise, to take part in the review. They were interviewed after submitting explicit written or verbal consent, as required by the ethics approval (Section 6.2.1). Table 6.1 shows a consolidated summary of the data.

6.3.1 Cyber-Security Analysts

This section presents demographic information concerning the cyber-security analysts who participated in the interviews.

Participant CS1 is an information systems auditor at Trusted Infosystems Pvt. Ltd., India, with over 16 years' experience in the field of cyber-security. CS1 rates their own experience of performing 'Escalation Analysis' as 5, on a scale of 1 to 5. They have no experience using cyber-security visualisation solutions.

Participant CS2 is a cyber-security analyst for Trusted Infosystems Pvt. Ltd., India, with over 20 years of experience in the field of cyber-security. CS2 rates their own experience of performing 'Escalation Analysis' as 4.5 on a scale of 1 to 5. They also have experience using cyber-security visualisation solutions, but not to perform 'Escalation Analysis' specifically.

[1] International Conference for Internet Technology and Secured Transactions - https://icitst.org/ [Accessed: 14th May, 2019]

[2] IEEE Symposium on Visualization for Cyber Security - https://vizsec.org [Accessed: 14th May, 2019]

[3] IEEE VIS - http://ieeevis.org/year/2017/welcome [Accessed: 14th May, 2019]

Table 6.1: Demographic Information of the Experts interviewed for Real World Utilisation of *EEVi*.

Participant	ID	Country	Current Job Description	Experience
Cyber-Security Analysts	CS1	India	Information Systems Auditor at Trusted Infosystems	16 years
	CS2	India	Cyber-Security Analyst at Trusted Infosystems	20+ years
	CS3	Italy	Post-doctoral Cyber-Security and Visual Analytics Expert at Sapienza University of Rome	6 years
	CS4	India	Security Consultant for Government Risk Management Projects	18+ years
	CS5	UK	Post-doctoral Information Security Specialist at University of Southampton	11 years
Visualisation Designers	VD1	UK	Post-doctoral Interaction, Games and UX Designer at Winchester School of Art	8 years
	VD2	USA	HCI and UX Designer at Pacific Northwest National Laboratory	8 years
	VD3	UK	Post-doctoral Human Factors Designer at University of Southampton	10 years
	VD4	USA	UX Designer at Pacific Northwest National Laboratory	5 years
	VD5	UK	Lecturer in HCI at University of Southampton	8 years

Participant CS3 is a post-doctoral cyber-security and visual analytics expert and academic practitioner at the Sapienza University of Rome, Italy, with 6 years' experience in the field of cyber-security. CS3 rates their own experience of performing 'Escalation Analysis' as 2.5 on a scale of 1 to 5. They also have experience using and designing cyber-security visualisation solutions, but not to perform 'Escalation Analysis' specifically.

Participant CS4 is a security consultant for government risk management projects in India, with over 18 years' experience in the field of cyber-security and over 36 years in the field of information technology. CS4 rates their own experience of performing 'Escalation Analysis' as 1.5 on a scale of 1 to 5. They also have experience using cyber-security visualisation solutions, but not to perform 'Escalation Analysis' specifically.

Participant CS5 is a post-doctoral information security specialist and academic practitioner at the University of Southampton, with 11 years' experience in the field of cyber-security. CS5 rates their own experience of performing 'Escalation Analysis' as 5 on a scale of 1 to 5. They have no experience using cyber-security visualisation solutions.

6.3.2 Visualisation Designers

This section presents demographic information concerning the visualisation designers who participated in the interviews.

Participant VD1 is a post-doctoral interaction, games and UX designer at the Winchester School of Art, with 8 years' experience in the field of visualisation design. VD1 has no experience using or designing cyber-security visualisation solutions.

Participant VD2 is a post-doctoral HCI and UX designer at Pacific Northwest National Laboratory, USA, with 8 years' experience in the field of visualisation design. VD2 has some experience designing cyber-security visualisation solutions.

Participant VD3 is a post-doctoral human factors designer and academic practitioner at the University of Southampton, with 10 years experience in the field of visualisation design. VD3 has no experience using or designing cyber-security visualisation solutions.

Participant VD4 is a UX designer at the Pacific Northwest National Laboratory, USA, with 5 years' experience in the field of visualisation design. VD4 has substantial experience designing cyber-security visualisation solutions.

Participant VD5 is a lecturer and academic practitioner in HCI at the University of Southampton, with 8 years' experience in the field of visualisation design. VD5 has no experience designing cyber-security visualisation solutions.

6.4 Findings from the Interviews

The interviews were qualitatively analysed using NVivo[4]. General findings from the interviews are presented below:

1. All the cyber-security analysts agreed that they would use the visualisation solution to perform 'Escalation Analysis' (when not considering costs for the solution).

    - *CS1* said *"...[this would be useful] in terms of helping me or enabling me to complete my job..."*.
    - *CS2* said *"...any organisation using cyber-security would love to have such a visualisation tool..."*.
    - *CS4* simply said *"Of course, Yes. Definitely"*.
    - *CS3* and *CS5* said that they would use it but would *"...explore it [first]..."* and check *"...[if it is the] most efficient way to display data..."* before using it.

2. Some cyber-security experts observed that certain characteristics would be useful for cyber-security visualisation solutions for all component tasks:

    - *CS1* noticed that there is no placeholder text at the top of the mockup to indicate the name and other details of the business. These details can include information about tasks that hold a higher priority for the business goals.
    - *CS3* believed that many solutions would require support for report building as one of the core characteristics.
    - *CS4* would prefer a graphical dashboard to make the final product more attractive.
    - *CS5* would prefer a search feature added to the core characteristics.

3. Subsequently, the experts made some final statements about *EEVi*, the mockups and work-domain analysis (abstraction hierarchy) diagrams:

    - *CS1* said *"...the functional purpose is captured [and you can] get the business flavour of the analysis which is sufficient..."*.
    - *CS2* said *"...this is very good, there is nothing like this available in the market for [the] cyber-security domain, especially taking management's perspective [into consideration]..."*. They also said *"...[there is] a lack of [such] visualisation tools in [the] market...[and] it is [a] good place to start..."*.
    - *VD3* said *"...[this] is a very interesting application of work-domain analysis..."*.
    - *VD1* and *VD2* applauded the research saying *"...[it all] looks good...[and] it all makes sense..."* and *"...cyber-security [analysts] really want this...[and they will] love this..."*.

[4] https://www.qsrinternational.com/product/nvivo-mac [Accessed: 5 May, 2017]

- *VD4* commended the research saying they *"...really like the work-domain analysis... [and asked when would] this be published so I can use and reference it"*. They also added *"...people will be really excited about this...[and] it is brilliant..."*.

It is clear that the experts' critique was very positive. The following paragraphs delve deeper into the feedback received from the experts.

6.4.1 Work-Domain Analysis (Abstraction Hierarchy)

An abstraction hierarchy of *EEVi* was developed to demonstrate the means-ends relationships for the abstraction levels and to support the development of a new system for cyber-security visualisation.

The abstraction hierarchy levels of *EEVi* (Figure 6.1), are defined as:

1. **Functional Purpose:** The functional purpose was to develop systems that can lead to effective visualisations for cyber-security analysis;
2. **Values and Priority Measures:** The criteria were to minimise or maximise measures that can lead to effective cyber-security analysis, depending on the task;
3. **Purpose-Related Functions:** The component tasks of *EEVi* make up the general functions of the system;
4. **Object-Related Processes:** The characteristics of visualisation provide the functionality to perform the purpose-related functions;
5. **Physical Objects:** The type of data that will enable certain processes and functions to be performed.

Figure 6.1 shows there are lots of relationships between the constituents of different levels, while Figure 6.2 represents the subset of the means-ends relationships of the abstraction hierarchy for 'Escalation Analysis'. The experts were presented with both these figures. The following sub-sections present the findings from the interviews concerning the abstraction hierarchy.

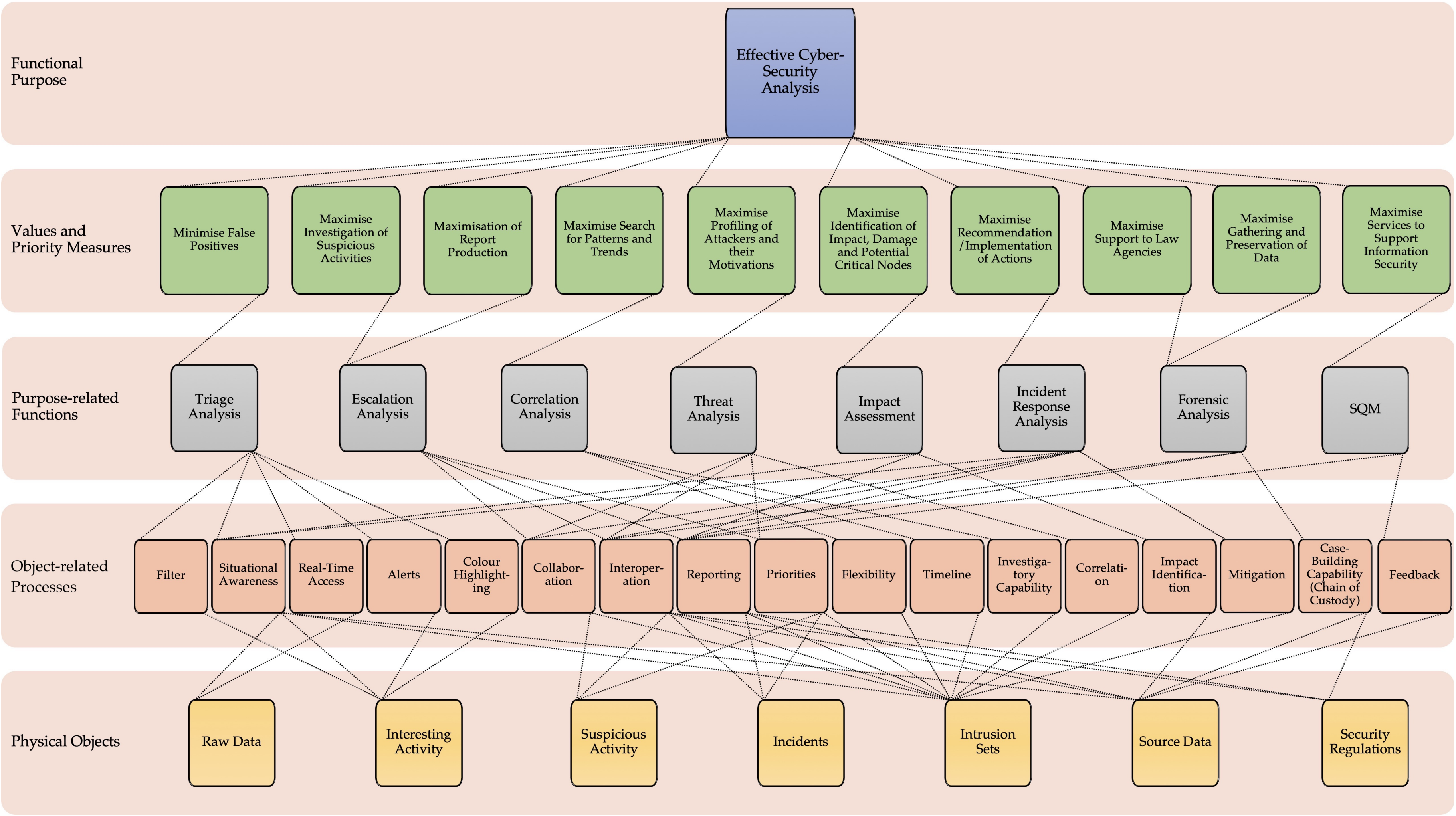

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.1: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for all component tasks (purpose-related functions) to reach their goal (functional purpose) following their respective criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain their goal.

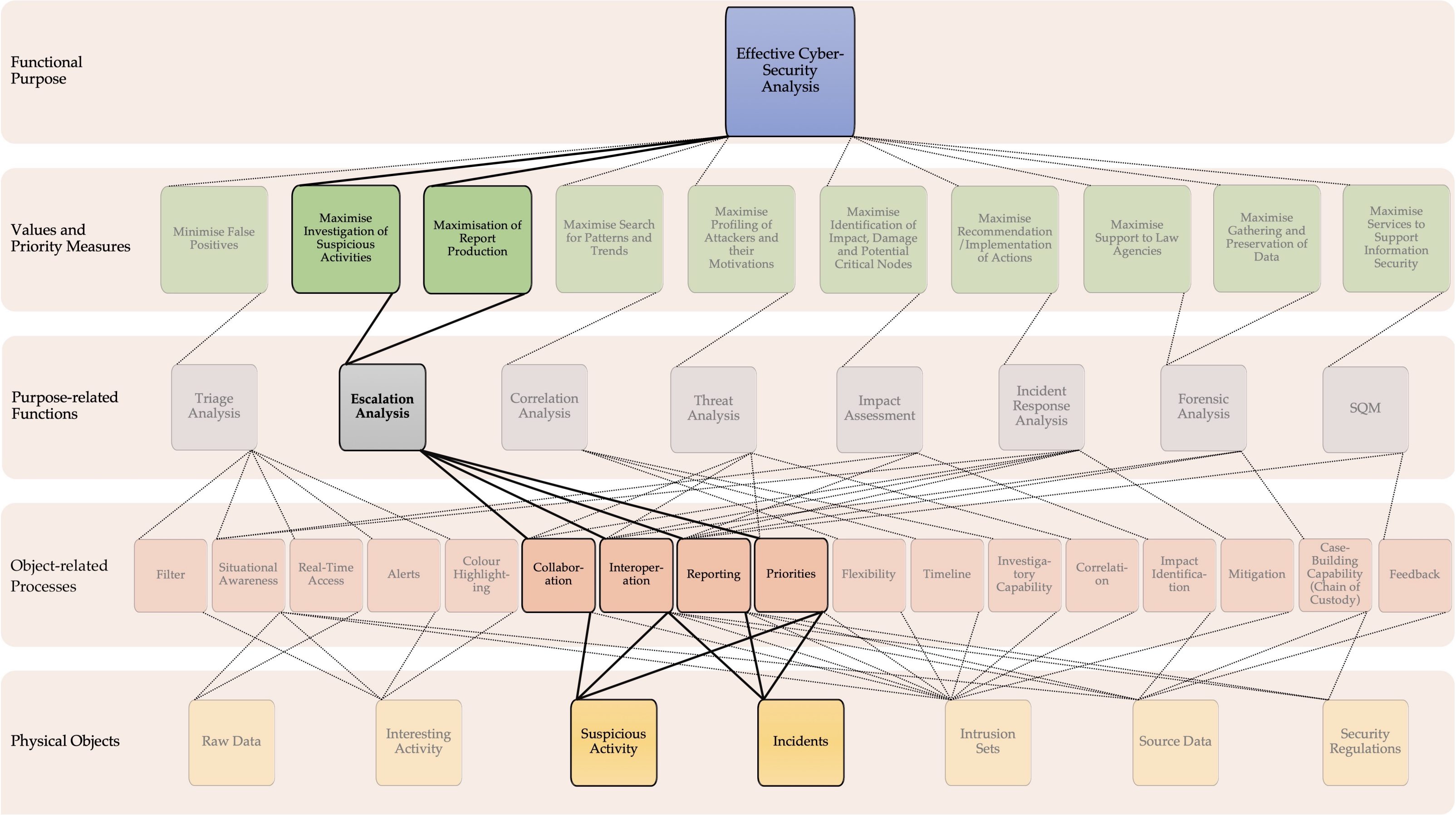

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.2: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for ‘Escalation Analysis’ (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

6.4.1.1 Visualisation Designers

The findings for the abstraction hierarchy from the visualisation designers are presented below:

1. All visualisation designers agreed that the abstraction hierarchy looks like it is derived from the *EEVi*.

   They saw that there seemed to be a clear relationship between *EEVi* and the abstraction hierarchy for each of its levels. *VD3* commented that the abstraction hierarchy was presented in a different and interesting way, as it was usually used in designing physical objects and not software systems However, it did make sense.

2. All visualisation designers agreed that the abstraction hierarchy could be used to have an inform a conversation with cyber-security analysts on their needs.

   VD1 commented on the intuitive nature of the abstraction hierarchy, making it a good basis for conversation. *VD3* enthusiastically agreed that the abstraction hierarchy was a valuable tool for conversation as it informed the needs of the design, while *VD5* added that it was a good place to start as the mapping forms a relevant base for discussion. *VD4* said that the abstraction hierarchy used a language that both cyber-security analysts and visualisation designers could understand, which made it easy to discuss. They also appreciated the different roles defined for cyber-security analysts, as it was not a “one-size-fits-all” situation.

3. All visualisation designers agreed that the abstraction hierarchy could potentially be used to design a visualisation solution for cyber-security.

   VD2 clarified that it was not the only tool available for use in designing a solution, but it was a good place to start, especially when designing technologically agnostic solutions. *VD3* added that there were many steps between the abstraction hierarchy and the design. However, using *EEVi*, the system, in its entirety could be appreciated and it could help test designs once ready, to make sure they followed the means-ends relationships with the functionality they support. *VD5* similarly felt that the abstraction hierarchy was a very useful starting point for context, but not a standalone technique for designing cyber-security visualisation solutions.

6.4.1.2 Cyber-Security Analysts

The findings for the abstraction hierarchy from the cyber-security analysts are presented below:

1. All cyber-security analysts agreed that the abstraction hierarchy represented *EEVi*. They believed that it represented the requirements quite well and the correlation between the two is apparent.
2. All cyber-security analysts agreed that the abstraction hierarchy could be used to explain the analysts' needs and requirements to the visualisation designers. *CS1* felt that the abstraction hierarchy was complete in all respects so that a conversation could reach a solution. *CS3* also believed it would be a good basis for a conversation, with visualisation designers, enabling discussion of the different levels and how they could be properly implemented in a solution.

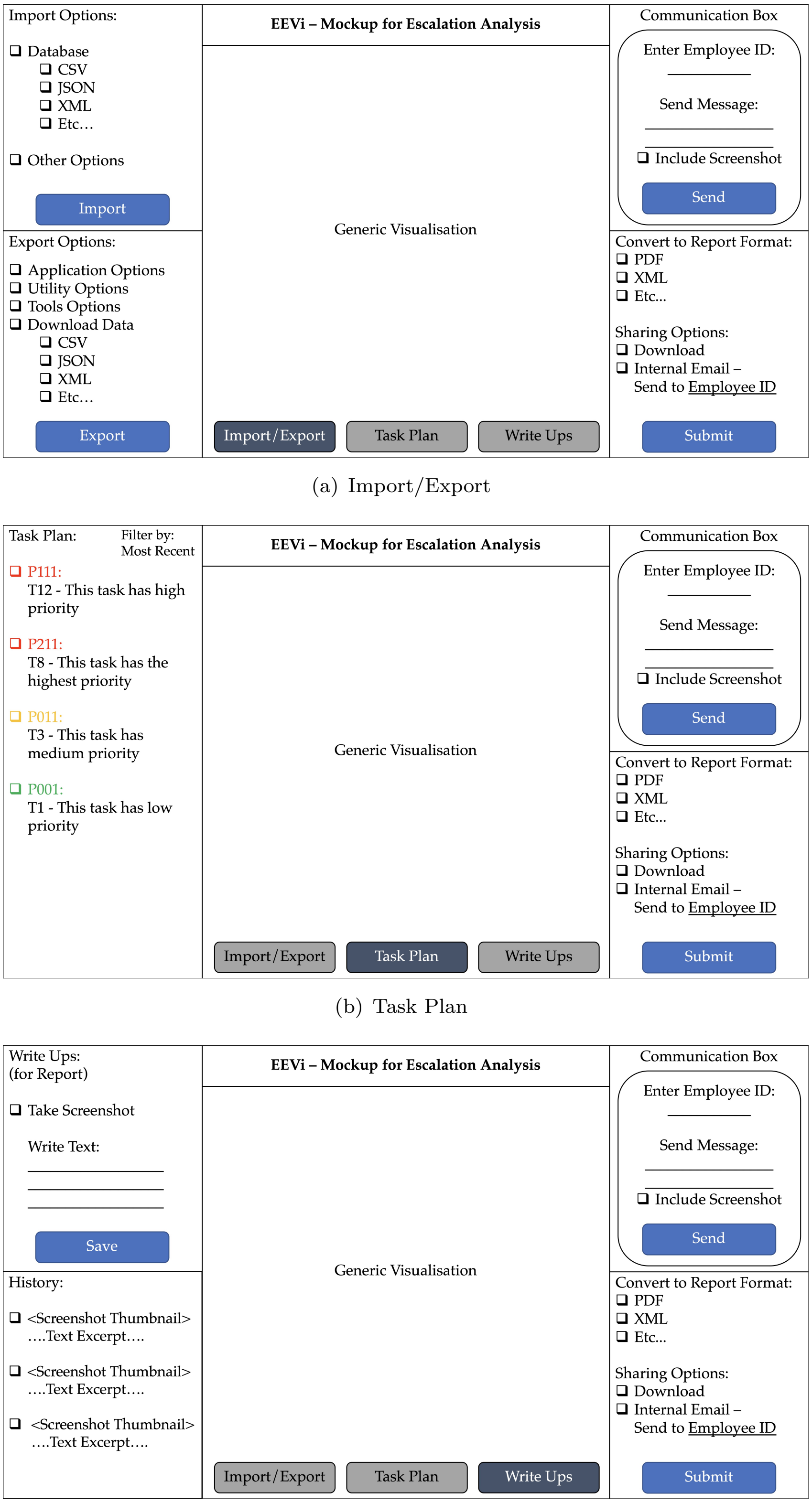
6.4.2 User Interface Mockups

The experts were presented with mockups of the user interface 'Escalation Analysis' one of *EEVi*'s component tasks (Figure 6.3). These mockups were designed using the guidelines for 'Escalation Analysis' for *EEVi* (Figure 5.5(b)) and interpreting the *Characteristics of Visualisation* as explained below. The *Goal* is to perform 'Escalation Analysis', *Type of Data* is underlying data not represented in the mockups and *Role of End-User* would be the users who are represented by the experts examining the mockups.

Figure 6.3 shows that, 'generic visualisation' is written in the centre of each screen instead of a sample visualisation, to draw attention to the characteristics offered by the visualisation solution rather than focusing on the discussion of colour, type or aesthetics of the visualisation. The three screens correspond to the user interface mockups, each one corresponding to the button selected from the options at the bottom.

The left side of the screen changes according to the option selected. The right side remains unaltered, and has two characteristics:

- *Communication Box*: is used to communicate messages and/or screenshots to employees within the organisation;
- *Convert to Report Format*: is used to convert information into a report, which can have different formats, and can either be downloaded or emailed directly to an employee within the organisation.



(a) Import/Export

(b) Task Plan

(c) Write Ups

Figure 6.3: User Interface Mockups of *EEVi*'s constituent component task, 'Escalation Analysis', created by the researcher. Each figure displays the screen corresponding to the button selected from the three options at the bottom.

Figure 6.3(a) is the screen corresponding to the *Import/Export* button. This screen allows the user to perform two main operations:

- *Import Options*: Can be used to import data from other tools or databases, and allows the user to choose which format for data to use for fast and intelligent importing;
- *Export Options*: Can be used to export data to different applications, tools, utilities or to download the data in different formats.

Figure 6.3(b) is the screen corresponding to the *Task Plan* button. This screen presents information on the priority of each incoming task. The *Filter By* option allows the user to filter the tasks by importance. Tasks listed in the task plan are sorted by colour and codes. The colours represent the importance of a task (red for high, yellow for medium, and green for low), while the codes represent the highest priorities within each colour to signify importance.

Figure 6.3(c) is the screen corresponding to the *Write Ups* button. This screen would allow the user to perform two main operations:

- *Write Ups (for Reports)*: Can be used to take screenshots of the corresponding visualisation and attach text pertaining to the captured visualisation;
- *History*: Can be used to view the record of write ups, along with a thumbnail of screenshots, so that all the information is organised in one place.

Following from above, the following characteristics of visualisation are represented in the mockups (Figure 6.3):

- *Interoperation* is represented by the *Import Options* and *Export Options* operations on *Import/Export* screen.
- *Collaboration* is represented by the *Communication Box* on the right side of all screens.
- *Reporting* is represented by the *Convert to Report Format* on the right side of all screens and is aided by the *Write Ups (for Reports)* operation on the *Write Ups* screen.
- *Priorities* is represented by the list on the left side of the *Task Plan* screen.

The following sub-sections present the findings from the interviews concerning the user-design mockups displayed in Figure 6.3.

6.4.2.1 Cyber-Security Analysts

The findings from the interviews with the cyber-security analysts for the user interface mockups are presented below:

1. All cyber-security analysts agreed that the user interface mockups made sense and would enable them to perform 'Escalation Analysis'. They believed it put in place something formal and relevant for sufficiently performing the task at hand.

2. All cyber-security analysts agreed that the data is sufficient to perform 'Escalation Analysis'. However, said that the data may not be rich enough to conduct the analyses (*CS3*) and that there needs to be a defined guideline on when an attack is formally confirmed (*CS4*).

3. All cyber-security analysts agreed that the visualisation characteristics were sufficient to enable them to perform 'Escalation Analysis'. They believed it was a good starting point, but might require more refinement after user experience with the solution (*CS2*) or functional requirements (*CS3*).

4. All cyber-security analysts suggested improvements to the implementation of the characteristics of visualisation presented in the mockups (Figure 6.3). These are explained below:

   4.1 *Collaboration:* On average, the cyber-security analysts thought the implementation was on the higher side between 'well implemented' and 'very well implemented'. *CS3* believed that the implementation was good for asynchronous collaboration rather than real-time collaboration, which could be implemented as a chat box rather than single message sharing (like e-mails).

   4.2 *Priority:* On average, the cyber-security analysts thought the implementation was on the lower side between 'well implemented' and 'very well implemented'. The analysts were especially pleased with the colour-coded aspect of the visualisation. However, *CS3* felt that a timeline for the tasks and their level of completion would enhance the visualisation.

   4.3 *Interoperation:* On average, the cyber-security analysts thought the implementation was on the higher side between 'well implemented' and 'very well implemented'. The analysts were pleased with this functionality and *CS4* believed this ability was required to be able to perform the task.

   4.4 *Reporting:* On average, the cyber-security analysts thought the implementation was on the higher side between 'well implemented' and 'very well implemented'. The analysts were satisfied with the ability to convert to report format and different sharing options which could include screenshots (*CS1, CS2 and CS4*).

However, *CS3* conjectured that the ability to preview a report before downloading or transmitting it would be more useful to the end-user and benefit the visualisation solution as a whole.

5. Most of the cyber-security analysts agreed that the visualisation solution did not require anything else to be able to perform 'Escalation Analysis'. They believed the mockups capture the problem correctly (*CS1*) and that there was a lack of such visualisation solutions in the market (*CS2*). However, some analysts thought that the analyses and monitoring of tasks could be separated, even though they could be interleaved (*CS3*) and that a search option in the solution would amplify the effectiveness of the visualisation solution.

6.4.2.2 Visualisation Designers

The findings for the interviews with the visualisation designers for the user interface mockups are presented below:

1. All visualisation designers agreed that the user-interface mockups were clearly derived and follow from the work domain analysis (abstraction hierarchy) and included all the requirements for 'Escalation Analysis'. They believed that the mockups represented the elements of the abstraction hierarchy and the interplay of elements was visible. They could easily find the object-related processes trying to achieve functionality for the purpose-related function.

2. All visualisation designers suggested improvements to the implementation of the characteristics of visualisation as presented in the mockups (Figure 6.3). These are explained below:

   2.1 *Collaboration:* On average, the visualisation designers thought the implementation was on the lower side between 'neutral' and 'well implemented'. They had many comments on the implementation. *VD1* was happy with the communication box and the ability to share visualisations, while *VD2* was neutral as they were not sure how such functionality would work, including decisions about what could and could not be shared. *VD3* would have preferred a messenger style chat box, while *VD4* thought that the solution lacked the ability to hand-off tasks and communicate with multiple people simultaneously. *VD5* believed that each organisation had a different way of communicating whose existing communication channels could make such a characteristic obsolete. They thought the functionality could be increased by linking the send button to another screen or a set of options which could be used to add more information, such as the corresponding data.

2.2 *Priority:* On average, the visualisation designers thought the implementation was on the higher side between 'well implemented' and 'very well implemented'. The designers generally liked this characteristic and believed it was the most logical way to implement it. However, *VD5* felt that the implementation could be improved by allowing an option to click on the task which could lead to a further set of options.

2.3 *Interoperation:* On average the visualisation designers thought the implementation was on the higher side between 'neutral' and 'well implemented'. They had many comments on the implementation. *VD3* was concerned how the import and export features would work together and with other utilities or tools. From an HCI perspective, *VD5* thought that the input box was well placed at the top-left side of the screen, but that the implementation could be cleaned by allowing an import or export button which would pop up another box, or produce a drop-down list of options, rather than have them visible all the time.

2.4 *Reporting:* On average, the visualisation designers thought the implementation was on the lower side between 'neutral' and 'well implemented'. They had many comments on the implementation. *VD2* thought there should be a lot more background work trying to understand the elements to be added to the report and to combine it all into a report format. From a HCI perspective, *VD3 and VD5* believed that the box could be cleaner, which would lead to fewer clicks than currently designed. They also said there could be an export to report button providing that functionality and clean the GUI for the end-user. *VD4* was concerned about how the solution would follow standard reporting templates that were organisation specific.

6.4.3 Work-Domain Analysis (Abstraction Hierarchy) or User Interface Mockups

Most of the visualisation designers (*VD1, VD2 and VD4*) believed the abstraction hierarchy to be a better technique that currently used as a basis for designing and for having a conversation, with cyber-security analysts. *VD3 and VD5* argued that the abstraction hierarchy along with the user interface mockups would provide a good, but added that they would rely more heavily on the abstraction hierarchy.

The visualisation designers believed that the abstraction hierarchy diagram gave them a good overview of the relationships in the model. The diagram also presented the information in a hierarchy with the different levels and categories which made everything, including the relationships between the levels, easier to see in one view. This also made it easier to discuss their requirements with end-user and with stakeholders (if any).

Conversely, the user interface mockups required more context but were easier to communicate as a concept. They also felt that the end-users or stakeholders might focus more on the usability aspects of the mockups rather than the functionality behind each aspect.

The visualisation designers had a clear preference for work domain analysis (abstraction hierarchy) diagrams. (Figure 6.4 to Figure 6.10) represent the subset of the means-ends relationships of the abstraction hierarchy for each purpose-related function (or component tasks of *EEVi*), apart from 'Escalation Analysis' (Figure 6.2).

6.5 Discussion

Work domain analysis (abstraction hierarchy) diagrams and user interface mockups were created from *EEVi* to understand the model's use in the real world. Mockups were used to present user interface ideas as well as gather functional requirements at early stages of development. Abstraction hierarchy diagrams represented the means-ends relationships between abstraction levels to show how each element related to the elements in the other levels. These levels displayed the relationships in *EEVi* as a whole (Figure 6.1), as well as that of each constituent component task (Figure 6.2, Figure 6.4 to Figure 6.10) with the conditions to be fulfilled to achieve the final goal for each task.

The value of mockups and abstraction hierarchy diagrams were evaluated by ten experts (five cyber-security analysts and five visualisation designers) who were industry or academic practitioners. The interviews were positive, with some useful suggestions to further improve the mockups and abstraction hierarchy diagrams. The feedback confirmed that the abstraction hierarchies represented the interplay of all relationships that enabled understanding of the system as a whole, and the mockups were concrete pieces of information that could show the workings of a solution using *EEVi* guidelines. The visualisation designers all declared that the abstraction hierarchy diagrams would be their starting point in designing cyber-security visualisation solutions for a task. They appreciated the mockups as well, but did feel that they would work better in the later stages of the design process.

The interviews validated the hypothesis that *EEVi* can be used in the real world in the design process for cyber-security visualisation, by using the abstraction hierarchy diagrams and the user interface mockups. The results also indicate that the abstraction hierarchy diagrams can enable better informed conversation between cyber-security analysts and visualisation designers. This would alleviate the disparity of domain-knowledge between the two groups by using a common medium. *EEVi* was also used to develop a quantitative value calculator to score cyber-security visualisation solutions, this is detailed in Chapter 7.

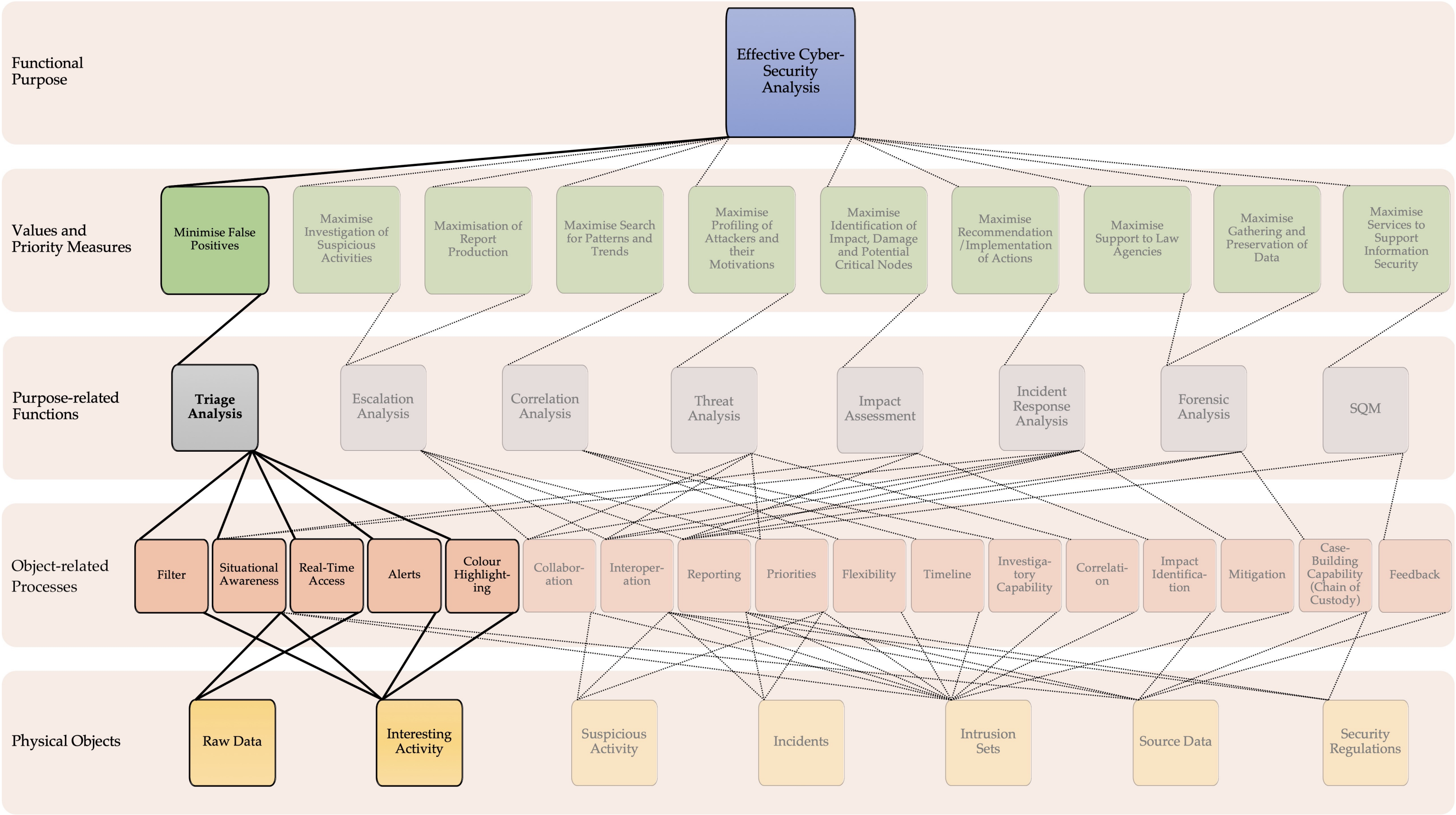

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.4: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for 'Triage Analysis' (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

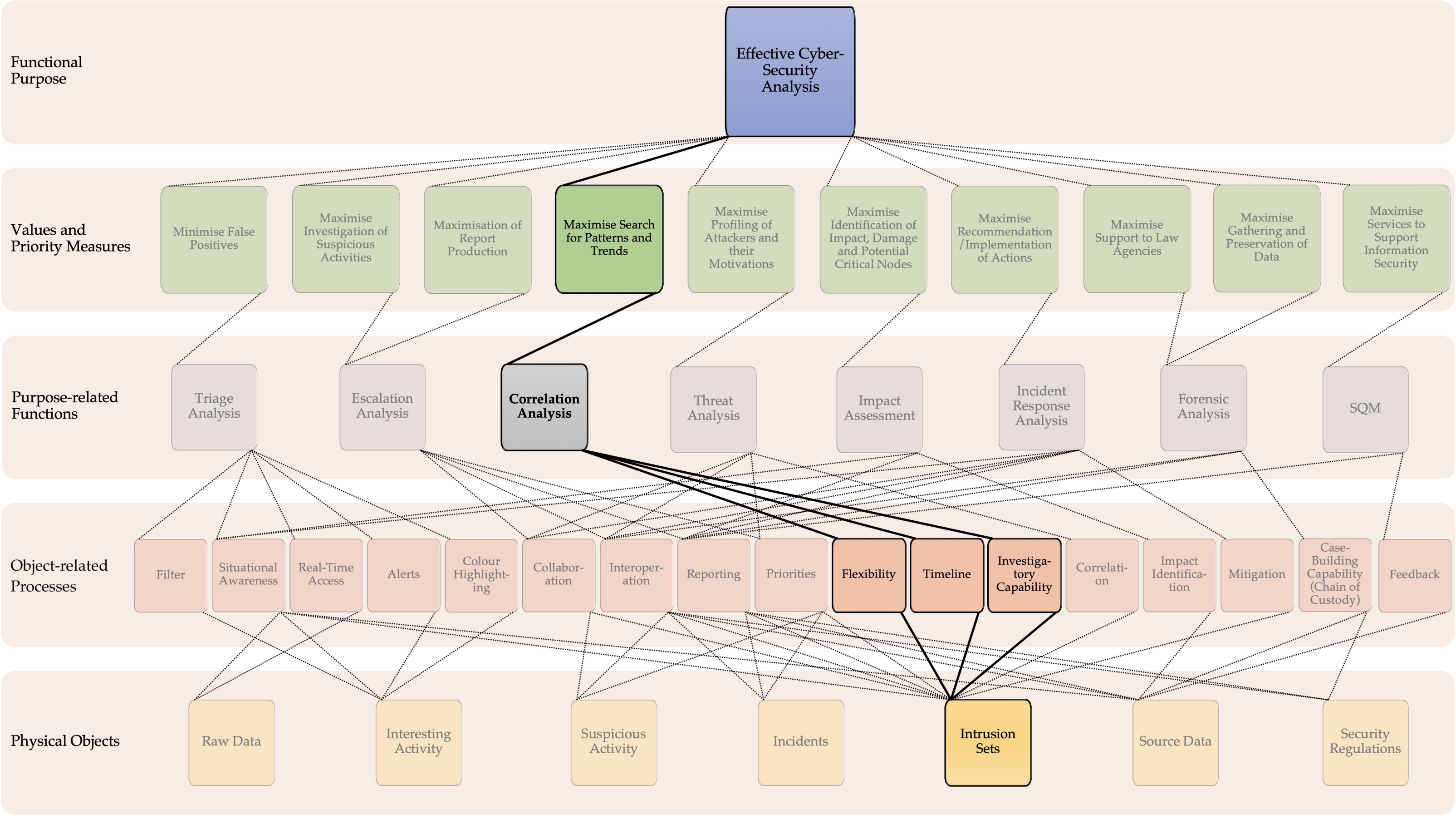

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.5: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for ‘Correlation Analysis’ (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

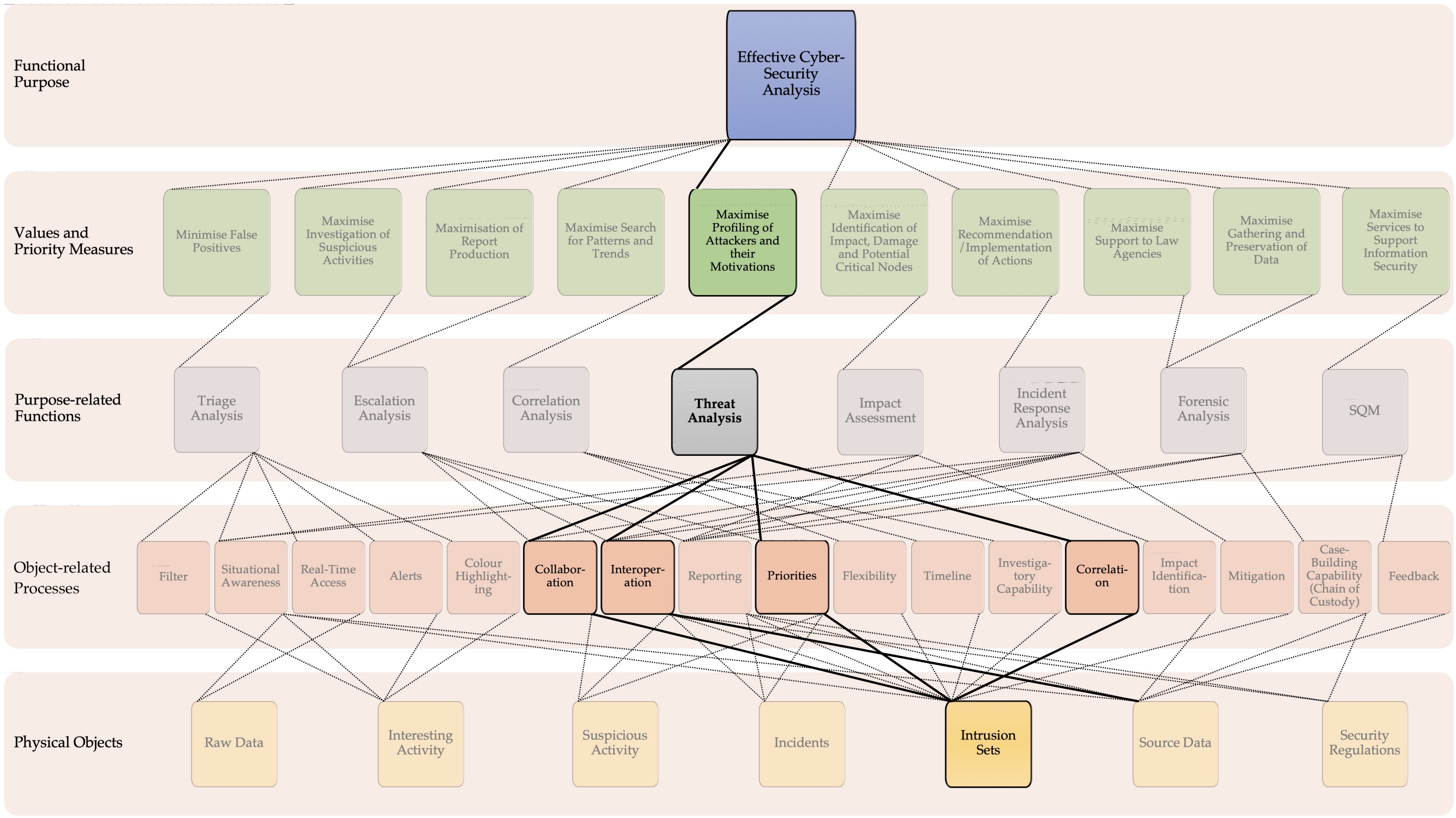

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.6: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for ‘Threat Analysis’ (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

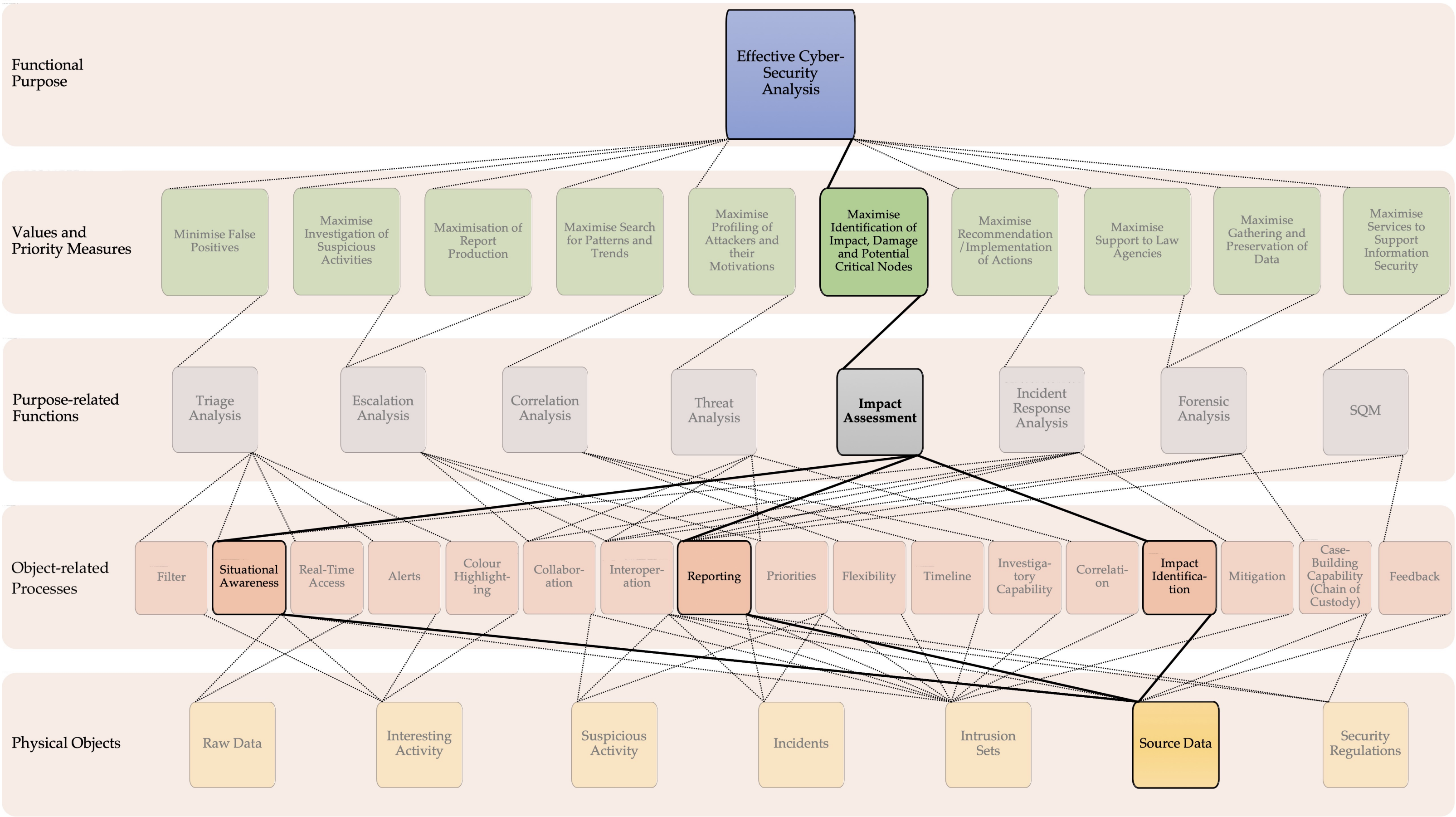

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.7: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for 'Impact Assessment' (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

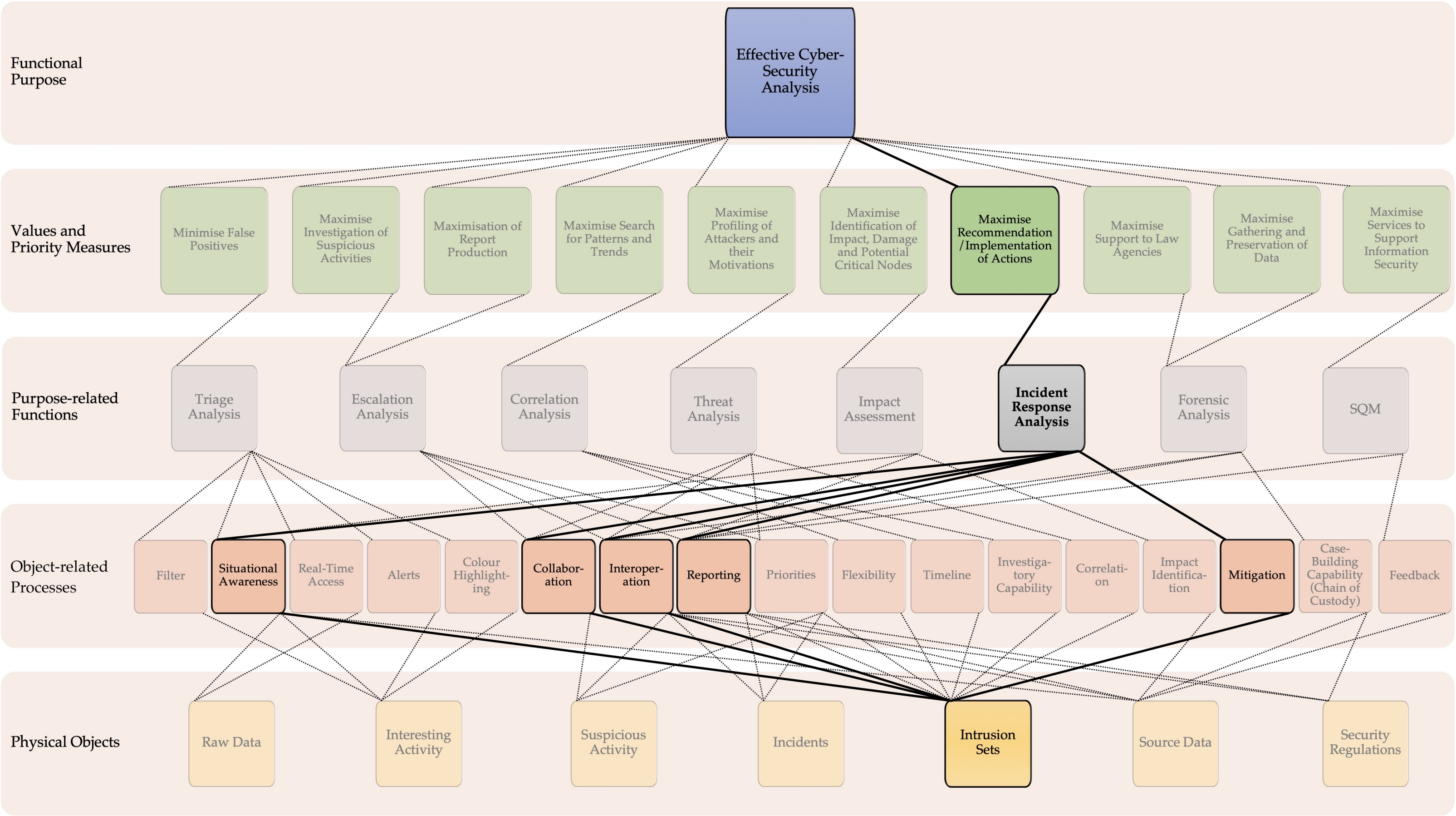

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlight-ing
Collabor-ation
Interoper-ation
Reporting
Priorities
Flexibility
Timeline
Investiga-tory Capability
Correlati-on
Impact Identifica-tion
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.8: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for 'Incident Response Analysis' (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

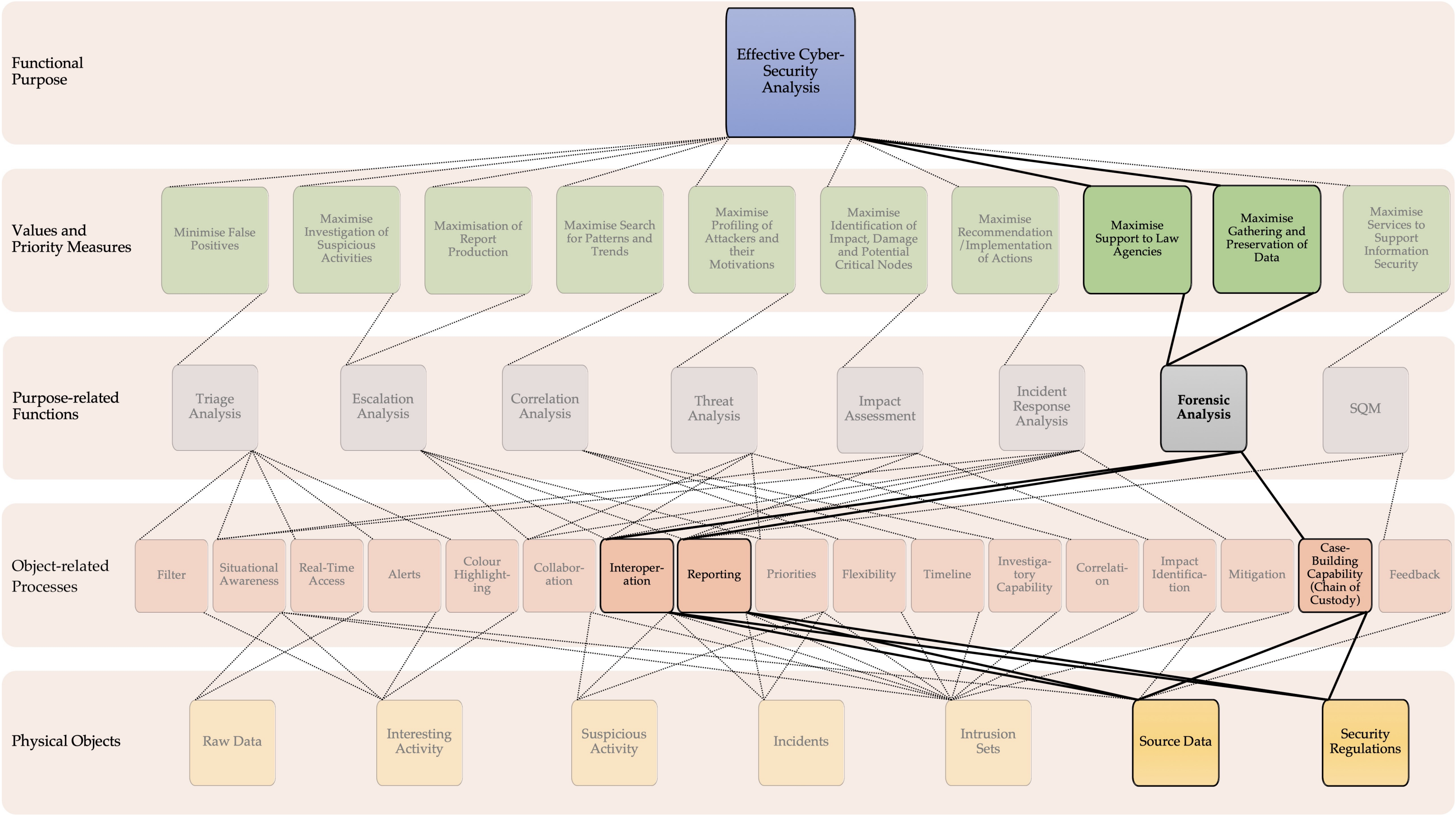

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlighting
Collaboration
Interoperation
Reporting
Priorities
Flexibility
Timeline
Investigatory Capability
Correlation
Impact Identification
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.9: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for ‘Forensic Analysis’ (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

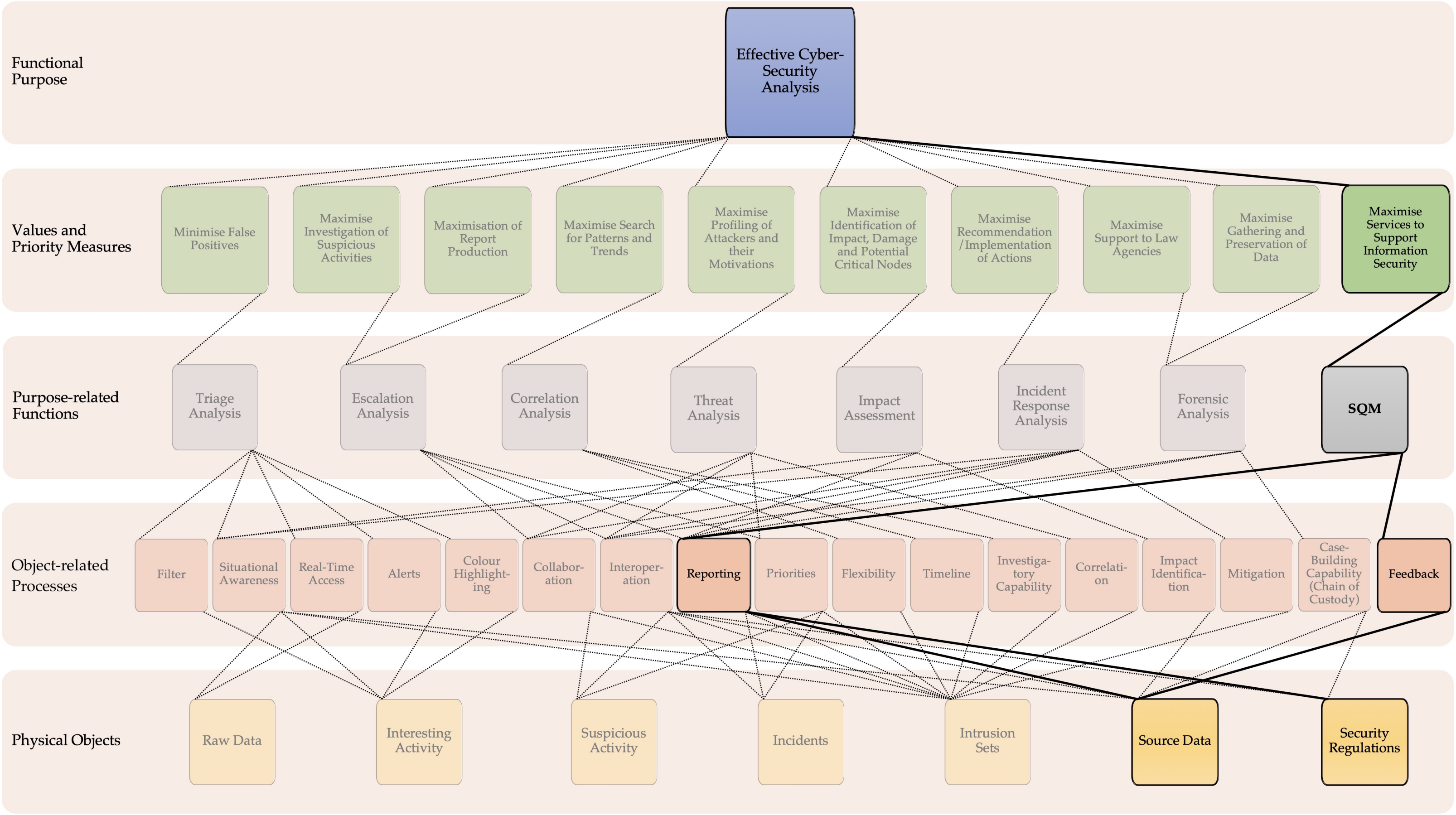

Functional Purpose
Effective Cyber-Security Analysis
Values and Priority Measures
Minimise False Positives
Maximise Investigation of Suspicious Activities
Maximisation of Report Production
Maximise Search for Patterns and Trends
Maximise Profiling of Attackers and their Motivations
Maximise Identification of Impact, Damage and Potential Critical Nodes
Maximise Recommendation /Implementation of Actions
Maximise Support to Law Agencies
Maximise Gathering and Preservation of Data
Maximise Services to Support Information Security
Purpose-related Functions
Triage Analysis
Escalation Analysis
Correlation Analysis
Threat Analysis
Impact Assessment
Incident Response Analysis
Forensic Analysis
SQM
Object-related Processes
Filter
Situational Awareness
Real-Time Access
Alerts
Colour Highlight-ing
Collabor-ation
Interoper-ation
Reporting
Priorities
Flexibility
Timeline
Investiga-tory Capability
Correlati-on
Impact Identifica-tion
Mitigation
Case-Building Capability (Chain of Custody)
Feedback
Physical Objects
Raw Data
Interesting Activity
Suspicious Activity
Incidents
Intrusion Sets
Source Data
Security Regulations

Figure 6.10: Abstraction Hierarchy of *EEVi* representing the means-ends relationships for 'Security Quality Management' (purpose-related functions) to reach its goal (functional purpose) following the criteria (value and priority measures). It also shows the characteristics of visualisation (object-related functions) and type of data required (physical objects) to attain the goal.

Chapter 7

Development of *C-EEVi*

C-EEVi (Calculator for *EEVi*) can be used to calculate scores for different cyber-security visualisation solutions, based on how their functionality satisfies a specific task. It follows the *EEVi* model (developed, validated and confirmed in Chapters 3, 4 and 5, respectively) and uses the questionnaire results from Chapter 5 to form the backend of the calculator. This chapter introduces the technique used to develop the backend of *C-EEVi* from the questionnaire results, followed by the development process.

7.1 Background of Techniques Used

This section elaborates on the background of the technique used to develop *C-EEVi*, the quantitative value calculator, followed by the mathematical process used to calculate values that form the backend of the calculator.

7.1.1 Multi-Criteria Decision-Making (MCDM)

MCDM methods are mathematical models that help decision-making in scenarios where a number of criteria exist (Ceballos, Lamata, & Pelta, 2016; Triantaphyllou, Shu, Sanchez, & Ray, 1998). They use numerical techniques to identify the best alternative, based on values of preferences given by the decision makers (Samant et al., 2015). To select the most appropriate MCDM method for this research, some of the most common methods are listed:

- Analytic Hierarchy Process (AHP): Developed by Thomas Saaty (1980), AHP involves structuring criteria into a hierarchy, evaluating the importance of these criteria, and finding the best alternative based on the criteria.

Table 7.1: Comparative Analysis of MCDM methods (Hodgett, 2016; Linkov et al., 2006; Velasquez & Hester, 2013; Samant et al., 2015).

Method	Advantages	Disadvantages
AHP	Easy to use; scalable; can adjust to fit any size of problem; assists group decision-making; can check for inconsistencies; alternatives evaluated at end; pairwise comparisons provide an uncomplicated way to enter qualitative preferences.	Large number of comparisons can lead to inconsistencies; problems with interdependence between criteria and alternatives.
TOPSIS	Easy to implement; number of steps remains the same regardless of number of criteria.	Unreliable results; difficult to weight and keep consistency of judgment; Euclidean Distance is used; correlation is not considered.
MAUT	Takes uncertainty into account; easier to compare alternatives with single number scores.	Very data intensive as it needs a lot of input; preferences need to be precise, requiring rigorous preference elicitation which is expensive.
ELECTRE	Takes qualitative and quantitative criteria; takes uncertainty into consideration; Extremely poor preference value on any one criteria can take an alternative out of consideration.	Very complex process which is not easy to understand; outcomes are hard to explain in layman's terms; complete ranking of alternatives is not always achieved.
PROMETHEE	Very easy to use; requires fewer inputs; does not require assumption that criteria are proportionate.	Does not provide a clear method to assign criteria weights; alternatives are required from the start; suffers when a new alternative is introduced later; does not provide opportunity to structure decision problem.

- Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS): Developed by Hwang and Yoon (1981), TOPSIS identifies the alternative with the shortest distance from the ideal solution in a multi-dimension computing space (Qin, Huang, Chakma, Nie, & Lin, 2008).

- Multi-Attribute Utility Theory (MAUT): This utility theory helps choose the best decision by assigning utility to every possible decision, and calculating the decision with the best possible utility (Konidari & Mavrakis, 2007).

- ELimination and Choice Translating REality (ELECTRE): Developed by Bernard Roy (1968), ELECTRE selects the best alternative by building several outranking connections to compare each pair of alternative, which is used to further elaborate the recommendations (Samant et al., 2015).
- Preference Ranking Organization METHod for Enrichment of Evaluations (PROMETHEE): Developed by Jean-Pierre Brans (1982), PROMETHEE ranks comparisons of different pairs of alternatives to find the best possible alternative (Samant et al., 2015).

Table 7.1 summarises the MCDM methods discussed above. The key criteria for selecting an MCDM method are:

- the ability to score alternatives at the end of the process, after the backend has been built,
- the ability to check for inconsistencies in the data, which can arise from using the results from the questionnaire in Chapter 5,
- support for group decision-making (from the results of 30 participants).

Table 7.1 shows that AHP is the only method that allows all of these criteria in the decision-making process. Therefore, AHP was used to calculate the backend of *C-EEVi*, as explained in the following sections.

7.1.2 Analytical Hierarchy Process

AHP is a flexible model that allows decision-making by logically combining judgemental and personal values (Saaty, 2012). AHP reflects the way in which people naturally think and act, but it aims to broaden and accelerate their thought processes by including more factors than they would consider ordinarily (Saaty, 2012). Additionally, AHP helps multi-criteria decision-making with its intuitive nature (Mu & Pereyra-Rojas, 2018) and its ability to deal with intangible criteria (Brunelli, 2015). Saaty (2012) outlines three major principles of logical analysis that underlie AHP:

1. **Constructing Hierarchies**: The human mind structures detailed knowledge hierarchically in constituent parts in order to be able to perceive, identify, and communicate what it perceives. Integrating large amounts of information into homogeneous clusters as part of a problem allows a complete picture to be

formed. The problem is structured into a hierarchy which depicts the interdependence of constituent elements of the problem.

2. **Establishing Priorities**: The human mind has the ability to observe, compare, and discriminate between relationships based on certain criteria. This allows people to judge the relative importance of elements by the intensity of their preference for each, through a sequential process. These judgements are synthesised and quantified mathematically using the established desirability of each criterion.

3. **Logical Consistency**: The human mind can also establish coherent relationships among objects or ideas so that they present consistency. There should exist some form of homogeneity and relevance for grouped ideas, and the intensities (judgements) of relationships on particular criteria should be justified in a logical manner to achieve consistency. Even judgements made by experts could be erroneous at times due to mistakes in setting up the hierarchy or judging the priorities; the consistency of judgements is also tested which leads to recalculation in case of inconsistencies.

Use of these principles leads to the incorporation of qualitative and quantitative aspects of human analytical thought processes into the Analytical Hierarchy Process (Saaty, 2012). The theory and methodology of AHP use *relative measurement*[1] to compare elements and assign them priorities, which are then used for decision-making (Brunelli, 2015).

AHP can be performed in different ways, depending on the scenarios and the decisions required. Here, the 'Ratings Model' in AHP will be employed. Mu and Pereyra-Rojas (2018) introduced the 'Ratings Model' which allows the calculation of a rating scale for each criterion, from the most important to the least important. These ratings form the backend of *C-EEVi*, enabling it to quantitatively score cyber-security visualisation solutions.

7.1.3 Development Process for Ratings Model in AHP

This section presents the use of AHP in decision-making and in developing the quantitative value calculator. The process of developing the ratings model is divided into four steps, also shown in Figure 7.1:

1. **Developing the Decision Hierarchy Model**: Follows the first principle of AHP (Constructing Hierarchies) and presents the breakdown of a complex problem into constituent parts that display essential relationships.

[1] Relative Measurement means that the methodology uses proportions between elements rather than exact values

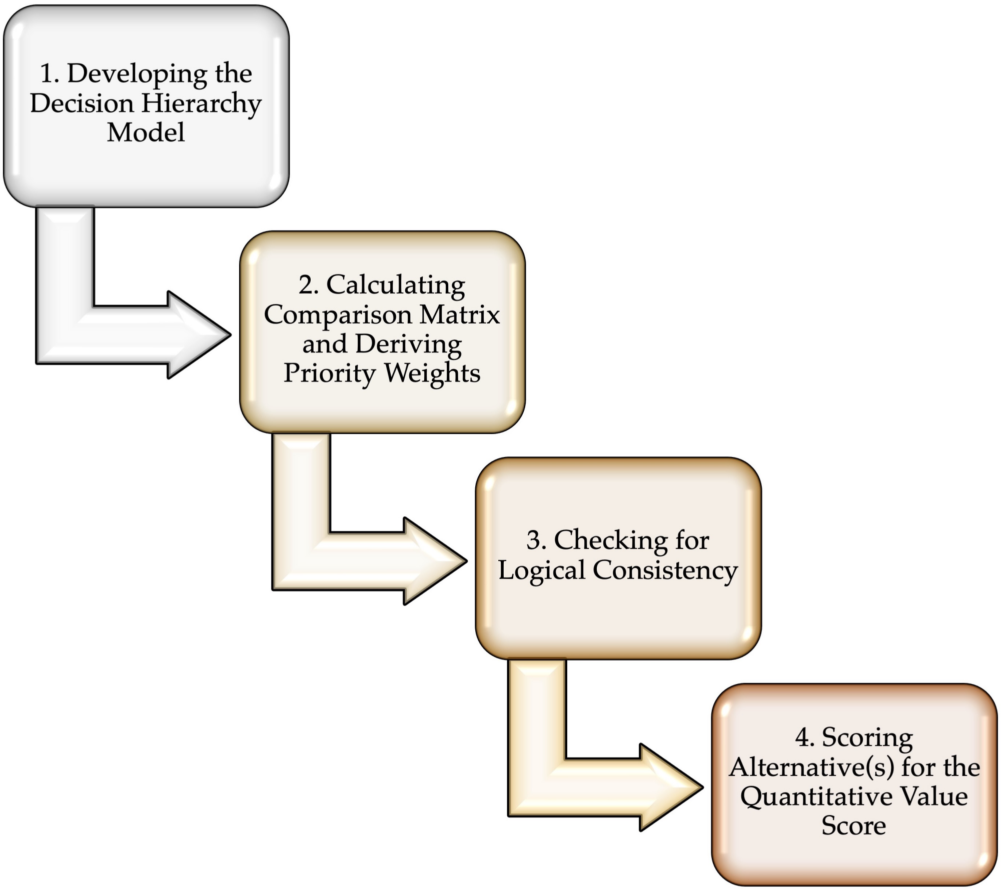

1. Developing the Decision Hierarchy Model
2. Calculating Comparison Matrix and Deriving Priority Weights
3. Checking for Logical Consistency
4. Scoring Alternative(s) for the Quantitative Value Score

Figure 7.1: Overview of Ratings Model in the Analytical Hierarchy Process, the methodology followed for the development of *C-EEVi*.

2. **Calculating the Comparison Matrix and Deriving Priority Weights**: Follows the second principle of AHP (Establishing Priorities) and presents the comparison matrix (Equation 7.2) for a set of criteria compared with each other. The comparison matrix then leads to the calculation of priority weights required for *C-EEVi*.

3. **Checking for Logical Consistency**: Follows the third principle of AHP (Logical Consistency) and presents the judgement of coherence in the calculated comparison matrix. Inconsistencies are representative of a lack of information or understanding of the problem and criteria, and require recalculation.

4. **Scoring Alternative(s) for the Quantitative Value Score**: Once proven consistent, the priority weights are further calculated to give a quantitative score for the alternative(s) (Mu & Pereyra-Rojas, 2018; Saaty, 2012).

The equations in the following sections, explaining the development process of AHP, have been adapted from the material by Mu and Pereyra-Rojas (2018), and by following a YouTube tutorial by Gloria Starns (M E Capstone Design (415/466), 2014).

7.1.3.1 Development Process of *C-EEVi* for Triage Analysis

For ease of understanding, the development process will be illustrated with an example that calculates the priority weights for 'Triage Analysis'. In the example, priority weights will be calculated for the *characteristics of visualisation* (criterion), which will then be used to quantitatively score cyber-security visualisation solutions using *C-EEVi*. The ratings from Chapter 5 are used to calculate the comparison matrix and priority weights. The priority weights for all the component tasks are calculated and listed in Appendix H.

7.1.3.2 Developing the Decision Hierarchy Model

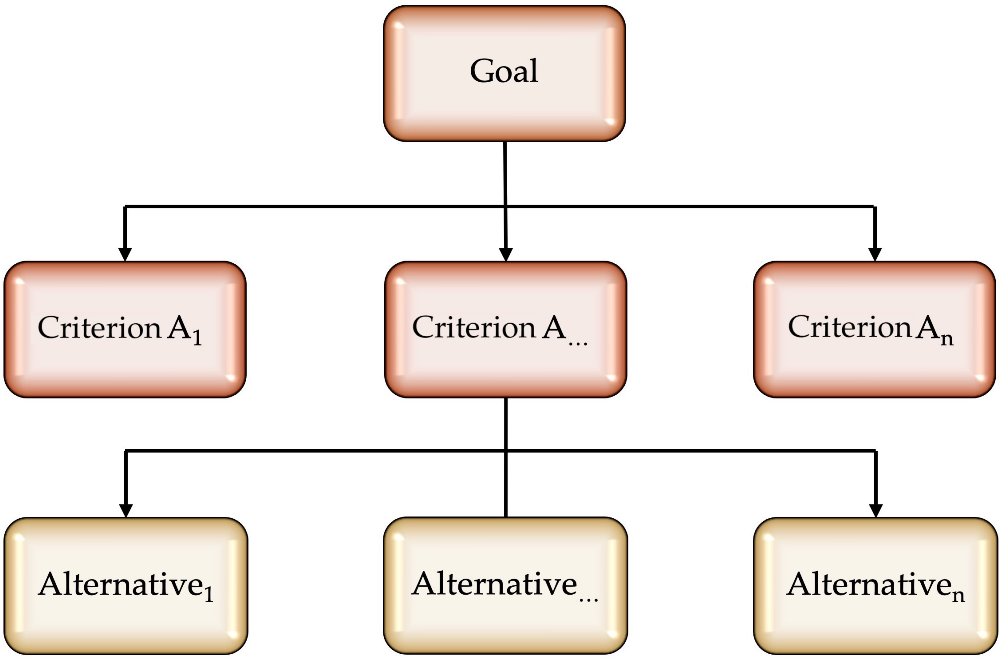


Figure 7.2: Decision Hierarchy when using AHP

The first step of AHP is structuring the problem into a hierarchy of goal, criteria, and alternatives (Mu & Pereyra-Rojas, 2018), which fulfils the first principle above. Figure 7.2 represents a general Decision Hierarchy Model that is constructed. The advantage of developing such a decision hierarchy model is that it helps to clearly understand the decision to be made and what criteria the decision should be based on.

Figure 7.2 shows the top-most level represents the goal or overall objective, the second-level deals with the criteria that help with the decision-making, while the third-level gives alternatives upon which decision needs to be made, based on criteria from the level above.

The proposed Decision Hierarchy Model for 'Triage Analysis' is presented in Figure 7.3. The overall goal of the model is '*Effective Visualisation for Triage Analysis*' and the

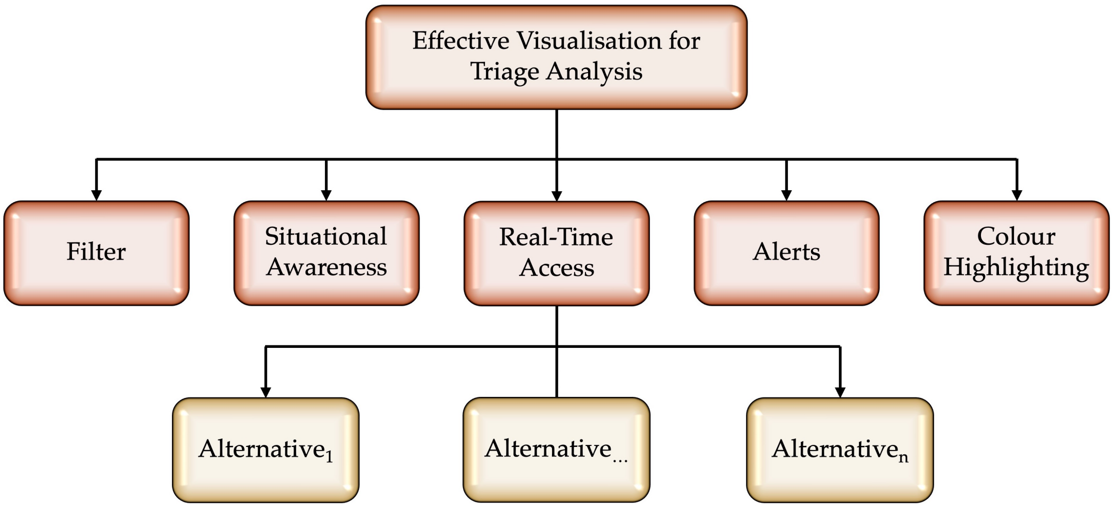


Figure 7.3: Decision Hierarchy for 'Triage Analysis' using AHP

characteristics of visualisation represent the criteria upon which the priority weights would be assigned. Once the priority weights for each characteristic of visualisation for 'Triage Analysis' have been generated, they can be used to score any alternative (cyber-security solutions) for cyber-security analysis.

7.1.3.3 Calculating The Comparison Matrix and Deriving Priority Weights

Once the decision hierarchy model had been constructed, the next step derives the priority weights for the different criteria, fulfilling the second principle above. To determine these, a pairwise comparison of the criteria is made, whereby each criterion is judged against all the others to yield preference intensity scores for the criteria (Saaty, 2012). To perform pairwise comparison (PC), the scale in Table 7.2 is used to compare each criterion in the decision hierarchy model (Mu & Pereyra-Rojas, 2018).

Table 7.2: Saaty (2012)'s Pairwise Comparison Scale

Intensity	Definition
9	Extreme Importance
7	Very Strong Importance
5	Strong Importance
3	Moderate Importance
1	Equal Importance

Equation 7.2 shows the original matrix which displays the PC for each criterion (A_n). For 'n' *number of criteria*, an n x n comparison matrix is constructed called [W]. Cells in [W] have values from the scale in Table 7.2.

As shown in Equation 7.1: $[W_{11}]$ shows the pairwise comparison between criteria A_1 and A_1 which will be 1. $[W_{1n}]$ shows the PC between criteria A_1 and A_n which will show a value from the table depending on the intensity of importance between criteria A_1 and A_n. $[W_{n1}]$ shows the PC between criteria A_n and A_1 which can be represented as the reciprocal of value in $[W_{1n}]$. Each cell of the comparison matrix is similarly filled.

$$W = \begin{array}{c} \begin{array}{ccc} A_1 & \dots & A_n \end{array} \\ \left[\begin{array}{ccc} \text{PC between } A_1 \text{ and } A_1 & \dots & \text{PC between } A_1 \text{ and } A_n \\ \vdots & \ddots & \vdots \\ \text{PC between } A_n \text{ and } A_1 & \dots & \text{PC between } A_n \text{ and } A_n \end{array}\right] \end{array} \begin{array}{c} \\ A_1 \\ \vdots \\ A_n \end{array} \tag{7.1}$$

The following steps present the calculations for deriving priority weights:

Step 1 Calculate the Original Comparison Matrix showing pairwise comparisons of all criteria. Calculate the sums of each column (A_{CSum}) after the matrix is complete.

$$W = \begin{array}{cccc} A_1 & \dots & A_n & \\ \left[\begin{array}{c} w_1/w_1 \\ \vdots \\ w_n/w_1 \end{array}\right. & \begin{array}{c} \dots \\ \ddots \\ \dots \end{array} & \left.\begin{array}{c} w_1/w_n \\ \vdots \\ w_n/w_n \end{array}\right] & \begin{array}{c} A_1 \\ \vdots \\ A_n \end{array} \\ \text{A}_{CSum_1} & \dots & \text{A}_{CSum_n} & \text{A}_{CSum} \end{array} \tag{7.2}$$

Note: For the example, the source values from Chapter 5, are given in Table E.1. These values were converted to a PC and formulated in a comparison matrix. The calculations to convert the values from Likert Scale to PC (Kallas, 2011) are shown in Appendix G.

The Comparison Matrix for 'Triage Analysis' is calculated as:

$$W_{TA} = \begin{array}{c} \begin{array}{ccccc} \text{TA\_Filter} & \text{TA\_SA} & \text{TA\_RTA} & \text{TA\_Alerts} & \text{TA\_CH} \end{array} \\ \left[\begin{array}{ccccc} 1.00 & 0.96 & 1.10 & 1.28 & 1.29 \\ 1.04 & 1.00 & 1.09 & 1.35 & 1.37 \\ 0.91 & 0.91 & 1.00 & 1.29 & 1.28 \\ 0.78 & 0.74 & 0.78 & 1.00 & 0.99 \\ 0.77 & 0.73 & 0.78 & 1.01 & 1.00 \end{array}\right] \end{array} \begin{array}{l} \\ \text{TA\_Filter} \\ \text{TA\_SA} \\ \text{TA\_RTA} \\ \text{TA\_Alerts} \\ \text{TA\_CH} \end{array} \tag{7.3}$$

The sums of each column in the matrix $[W_{TA}]$ are given below:

$$W_{TA} = \begin{array}{cccccc} \text{TA\_Filter} & \text{TA\_SA} & \text{TA\_RTA} & \text{TA\_Alerts} & \text{TA\_CH} & \\ \left[\begin{array}{c} 1.00 \\ 1.04 \\ 0.91 \\ 0.78 \\ 0.77 \end{array}\right. & \begin{array}{c} 0.96 \\ 1.00 \\ 0.91 \\ 0.74 \\ 0.73 \end{array} & \begin{array}{c} 1.08 \\ 1.094 \\ 1.00 \\ 0.78 \\ 0.78 \end{array} & \begin{array}{c} 1.28 \\ 1.35 \\ 1.29 \\ 1.00 \\ 1.01 \end{array} & \left.\begin{array}{c} 1.30 \\ 1.37 \\ 1.28 \\ 0.99 \\ 1.00 \end{array}\right] & \begin{array}{l} \text{TA\_Filter} \\ \text{TA\_SA} \\ \text{TA\_RTA} \\ \text{TA\_Alerts} \\ \text{TA\_CH} \end{array} \\ 4.50 & 4.35 & 4.75 & 5.92 & 5.94 & A_{CSum} \end{array} \tag{7.4}$$

Step 2 Calculate the Normalised Matrix by dividing each cell by the respective column sum, as shown in Equation 7.5. Calculate the average of each row (A_{RAv}) once the Normalised Matrix has been calculated.

$$\begin{array}{cccc} A_1 & \dots & A_n & A_{RAv} \\ \left[\begin{array}{c} (w_1/w_1)/A_{CSum_1} \\ \vdots \\ (w_n/w_1)/A_{CSum_1} \end{array}\right. & \begin{array}{c} \dots \\ \ddots \\ \dots \end{array} & \left.\begin{array}{c} (w_1/w_n)/A_{CSum_n} \\ \vdots \\ (w_n/w_n)/A_{CSum_n} \end{array}\right] & \begin{array}{c} A_{RAv_1} \\ \vdots \\ A_{RAv_n} \end{array} \end{array} \tag{7.5}$$

The Normalised Matrix for 'Triage Analysis' is:

$$\begin{array}{cccccc} \text{TA\_Filter} & \text{TA\_SA} & \text{TA\_RTA} & \text{TA\_Alerts} & \text{TA\_CH} & \\ \left[\begin{array}{c} 0.22 \\ 0.23 \\ 0.20 \\ 0.17 \\ 0.17 \end{array}\right. & \begin{array}{c} 0.22 \\ 0.23 \\ 0.21 \\ 0.17 \\ 0.17 \end{array} & \begin{array}{c} 0.23 \\ 0.23 \\ 0.21 \\ 0.16 \\ 0.17 \end{array} & \begin{array}{c} 0.22 \\ 0.29 \\ 0.29 \\ 0.17 \\ 0.17 \end{array} & \left.\begin{array}{c} 0.22 \\ 0.23 \\ 0.22 \\ 0.17 \\ 0.17 \end{array}\right] & \begin{array}{l} \text{TA\_Filter} \\ \text{TA\_SA} \\ \text{TA\_RTA} \\ \text{TA\_Alerts} \\ \text{TA\_CH} \end{array} \end{array} \tag{7.6}$$

Average of each row of the normalised matrix are given below:

$$\begin{array}{cccccc} \text{TA\_Filter} & \text{TA\_SA} & \text{TA\_RTA} & \text{TA\_Alerts} & \text{TA\_CH} & A_{RAv} \\ \left[\begin{array}{c} 0.22 \\ 0.23 \\ 0.20 \\ 0.17 \\ 0.17 \end{array}\right. & \begin{array}{c} 0.22 \\ 0.23 \\ 0.21 \\ 0.17 \\ 0.17 \end{array} & \begin{array}{c} 0.23 \\ 0.23 \\ 0.21 \\ 0.16 \\ 0.17 \end{array} & \begin{array}{c} 0.22 \\ 0.29 \\ 0.29 \\ 0.17 \\ 0.17 \end{array} & \left.\begin{array}{c} 0.22 \\ 0.23 \\ 0.22 \\ 0.17 \\ 0.17 \end{array}\right] & \begin{array}{l} 0.222 \\ 0.230 \\ 0.211 \\ 0.169 \\ 0.169 \end{array} \end{array} \tag{7.7}$$

Step 3 Priority Weights for each of the criterion (A) are calculated from the corresponding normalised matrix row averages (A_{RAv}), as shown in Equation

7.8.

$$Priority\ Weights\ for \begin{bmatrix} \mathrm{A}_1 \\ \vdots \\ \mathrm{A}_n \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathrm{A}_{RAv_1} \\ \vdots \\ \mathrm{A}_{RAv_n} \end{bmatrix} \tag{7.8}$$

For 'Triage Analysis', the priority weights for characteristics of visualisation are:

$$\therefore Priority\ Weights\ for \begin{bmatrix} \text{TA\_Filter} \\ \text{TA\_SA} \\ \text{TA\_RTA} \\ \text{TA\_Alerts} \\ \text{TA\_CH} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.222} \\ \mathbf{0.230} \\ \mathbf{0.211} \\ \mathbf{0.169} \\ \mathbf{0.169} \end{bmatrix} \tag{7.9}$$

Therefore, the priority weights for each criterion have been determined. Equation 7.9 shows the priority weights for the characteristics of visualisation for 'Triage Analysis'. This result shows that, *Situational Awareness* has the highest priority closely followed by *Filter, Real-Time Access, Alerts* and finally *Colour Highlighting.*

7.1.3.4 Checking for Logical Consistency

Once the priority weights have been determined, their consistency is checked to ensure the results are accurate and the pairwise comparisons were justified. This fulfils the third principle of AHP.

It is important to check the consistency of the judgements so they appear coherent and not random. Decisions are not made on judgements that have low consistency, which can lead to poor decision-making (Saaty, 2012). The overall consistency of judgements is measured by the Consistency Ratio (CR), which should be less than 0.1, otherwise, the judgements may be random and the pairwise comparisons would have to be revised to locate the cause of inconsistency (Mu & Pereyra-Rojas, 2018).

The procedure for checking logical consistency of the priority weights determined in the previous section follows this process:

Step 1 Determine the Weight Sum Vector $[W_s]$

$$[W_s] = [A_{RAv}][W] \tag{7.10}$$

The Weight Sum Vector $[W_s]$ in case of 'Triage Analysis' is

$$[W_s] = \begin{bmatrix}0.222\\0.230\\0.211\\0.169\\0.169\end{bmatrix}\begin{bmatrix}1.00 & 0.96 & 1.10 & 1.28 & 1.29\\1.04 & 1.00 & 1.09 & 1.35 & 1.37\\0.91 & 0.91 & 1.00 & 1.29 & 1.28\\0.78 & 0.74 & 0.78 & 1.00 & 0.99\\0.77 & 0.73 & 0.78 & 1.01 & 1.00\end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix}1.11\\1.15\\1.06\\0.84\\0.84\end{bmatrix} \tag{7.11}$$

Step 2 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}] \tag{7.12}$$

The Consistency Vector [CV] for 'Triage Analysis' is

$$[CV] = \begin{bmatrix}1.11\\1.15\\1.06\\0.84\\0.84\end{bmatrix} \cdot \begin{bmatrix}1/0.222\\1/0.230\\1/0.211\\1/0.169\\1/0.169\end{bmatrix} = \begin{bmatrix}1.11\\1.15\\1.06\\0.84\\0.84\end{bmatrix} \cdot \begin{bmatrix}4.51\\4.35\\4.74\\5.93\\5.93\end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix}5.00105\\5.00093\\5.00095\\5.00076\\5.00082\end{bmatrix} \tag{7.13}$$

Step 3 Determine the average of all elements of [CV], which is represented by λ_{max}. λ_{max} for 'Triage Analysis' is

$$\lambda_{max} = (5.00105 + 5.00093 + 5.00095 + 5.00076 + 5.00082)/5 = 5.0009 \tag{7.14}$$

Step 4 Determine the Consistency Index (CI), where n is the number of criteria

$$CI = (\lambda_{max} - n)/(n - 1) \tag{7.15}$$

The Consistency Index (CI) for 'Triage Analysis', where n=5, is

$$CI = (5.0009 - 5)/(5 - 1) = 0.0009/4$$

$$\therefore CI = 0.00023 \tag{7.16}$$

Step 5 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = CI/RI \tag{7.17}$$

Table 7.3: Consistency Indices for a Randomly Generated Matrix (RI) (Mu & Pereyra-Rojas, 2018), where n is the number of criteria.

n	3	4	5	6
RI	0.58	0.90	1.12	1.24

The Consistency Ratio (CR) for 'Triage Analysis' is

$$CR = 0.00023/1.12$$

$$\therefore CR = 0.0002 \tag{7.18}$$

Step 6 Consistency is achieved if the value of CR < 0.1, which means the rankings in the pairwise comparison are consistent. However, if CR ≥ 0.1 then it does not achieve consistency and the pairwise comparisons in the original matrix [W] need to be recalculated, as the matrices are non-transitive.

In the case of 'Triage Analysis', CR $= 0.0002$ (Equation 7.18) < 0.1. Therefore, consistency has been achieved and the priority weights in the pairwise comparison (Equation 7.9) do not need to be recalculated.

Once the consistency of the priority weights has been achieved, the priority weights can be used to rank the characteristics from most important to least important. The priority weights for all the component tasks are calculated, checked for consistency and listed in Appendix H.

7.1.3.5 Scoring Alternative(s) for the Quantitative Value Score

The priority weights can also be used to score the alternative(s). The following steps demonstrate how a quantitative value score can be calculated for alternatives:

For One Alternative: If there is a single alternative then the process to give its quantitative value score is (Mu & Pereyra-Rojas, 2018):

Step 1 Count the Presence of each Criterion (PoC) in the alternative. If the criterion is present, PoC = 1, and if the criterion is not present, PoC = 0.

Step 2 Calculate the Final Score (FS) by following Equation 7.19, where the score is the presence of each criterion (PoC) multiplied by the priority weight assigned to the criterion in Equation 7.8.

$$\begin{aligned} FS = PoC(AlternativeCritera_1) * A_{RAv_1} + \cdots + \\ PoC(AlternativeCriteria_n) * A_{RAv_n} \end{aligned} \tag{7.19}$$

Step 3 FS represents the Quantitative Value Score for the alternative.

For More than One Alternative (with an example for 'Escalation Analysis'): If there are more than one alternative then the process to give them their quantitative value scores is (Mu & Pereyra-Rojas, 2018) given below. As an example, the mockups from Figure 6.3 will be used. However, the mockups were built for 'Escalation Analysis', so the priority weights for 'Escalation Analysis' from Equation H.3 in Appendix H will be used.

Step 1 Count the presence of each criterion (PoC) in the alternatives. If the criterion is present, PoC = 1, and if the criterion is not present, PoC = 0.

The mockups from Figure 6.3 being used as a sample cyber-security visualisation solution, Figure 6.3a, Figure 6.3b and Figure 6.3c will be treated as three different alternatives. For a cyber-security visualisation solution performing 'Escalation Analysis', the presence of *Interoperation, Collaboration, Reporting* and *Priorities* would be required for the visualisation solution to be used by cyber-security analysts. The presence of these characteristics of visualisation in the three criteria is given below:

For Criterion A: In Figure 6.3a, *Interoperation, Reporting* and *Collaboration* are present.

For Criterion B: In Figure 6.3b, *Priorities, Reporting* and *Collaboration* are present.

For Criterion C: In Figure 6.3c, *Reporting* and *Collaboration* are present.

Step 2 Calculate FS for each alternative by following Equation 7.20, where the score is the PoC multiplied by the priority weight assigned to the criterion in Equation 7.8.

$$\begin{aligned} FS_1 = PoC(Alternative_1Critera_1) * A_{RAv_1} + \cdots + \\ PoC(Alternative_1Criteria_n) * A_{RAv_n} \\ \vdots \\ FS_n = PoC(Alternative_nCritera_1) * A_{RAv_1} + \cdots + \\ PoC(Alternative_nCriteria_n) * A_{RAv_n} \end{aligned} \tag{7.20}$$

FS for ‘Escalation Analysis’, where the score is Presence of each Criterion (PoC) multiplied with priority weight assigned to the criteria in Equation H.3:

$$\begin{aligned}FS_1 &= PoC(Alternative_1 Critera_1) * A_{RAv_1} + \cdots + \\ &\quad PoC(Alternative_1 Criteria_n) * A_{RAv_n} \\ &\vdots \\ FS_n &= PoC(Alternative_n Critera_1) * A_{RAv_1} + \cdots + \\ &\quad PoC(Alternative_n Criteria_n) * A_{RAv_n}\end{aligned}$$

$$\begin{aligned}FS_n = {} & PoC(EA\_Collaboration) * 0.236 + \\ & PoC(EA\_Priority) * 0.307 + \\ & PoC(EA\_Interoperation) * 0.217 + \\ & PoC(EA\_Reporting) * 0.240\end{aligned}$$

The quantitative value score for Criterion A is

$$\begin{aligned}FS_A &= 1 * 0.236 + 0 * 0.307 + 1 * 0.217 + 1 * 0.240 \\ \therefore FS_A &= 0.693\end{aligned} \tag{7.21}$$

Similarly, the quantitative value score for Criterion B is

$$\begin{aligned}FS_B &= 1 * 0.236 + 1 * 0.307 + 0 * 0.217 + 1 * 0.240 \\ \therefore FS_B &= 0.783\end{aligned} \tag{7.22}$$

and for Criterion C is

$$\begin{aligned}FS_C &= 1 * 0.236 + 0 * 0.307 + 0 * 0.217 + 1 * 0.240 \\ \therefore FS_C &= 0.476\end{aligned} \tag{7.23}$$

Step 3 The Final Scores (FS_1 to FS_n) represent the Quantitative Value Score for their respective Alternative.

The Final Scores, for ‘Escalation Analysis’, (FS_A, FS_B and FS_C) represent the Quantitative Value Score for their respective alternatives.

Step 4 Normalise the columns to calculate Overall Prioritisation List:

$$FS_{Sum} = FS_1 + \cdots + FS_n \tag{7.24}$$

The normalised List for ‘Escalation Analysis’ is:

$$\begin{aligned}FS_{Sum} &= FS_1 + \cdots + FS_n \\ FS_{Sum} &= FS_A + FS_B + FS_C\end{aligned}$$

$$\begin{aligned} FS_{Sum} &= 0.693 + 0.783 + 0.476 \\ \therefore FS_{Sum} &= 1.952 \end{aligned} \tag{7.25}$$

Step 5 Calculate Overall Prioritisation (OP) List

$$\begin{aligned} OP_1 &= FS_1/FS_{Sum)} \\ &\vdots \\ OP_n &= FS_n/FS_{Sum)} \end{aligned} \tag{7.26}$$

The Overall Prioritisation (OP) List for 'Escalation Analysis' is

$$\begin{aligned} OP_1 &= FS_1/FS_{Sum)} \\ &\vdots \\ OP_n &= FS_n/FS_{Sum)} \end{aligned}$$

$$\begin{aligned} OP_A &= FS_A/FS_{Sum)} \\ OP_B &= FS_B/FS_{Sum)} \\ OP_C &= FS_C/FS_{Sum)} \end{aligned}$$

$$\begin{aligned} OP_A &= 0.693/1.952 \\ OP_B &= 0.783/1.952 \\ OP_C &= 0.476/1.952 \end{aligned}$$

$$\begin{aligned} \therefore OP_A &= 0.355 \\ \therefore OP_B &= 0.401 \\ \therefore OP_C &= 0.244 \end{aligned} \tag{7.27}$$

Step 6 The values in the Overall Prioritisation List (OP_1 to OP_n) rank the alternatives from highest score to lowest score. The criteria in Equation 7.27, can be rated (most preferred to least preferred): Criterion B; followed by Criterion A; and finally, Criterion C.

The Final Scores (Equations 7.21, 7.22 and 7.23) represent the Quantitative Value Scores for the three mockups for 'Escalation Analysis' in Figure 6.3. Figure 6.3b was rated highest with a score of 0.783, followed by Figure 6.3a with a score of 0.693, and lastly, Figure 6.3c with a score of 0.476.

7.2 Final Look of *C-EEVi*

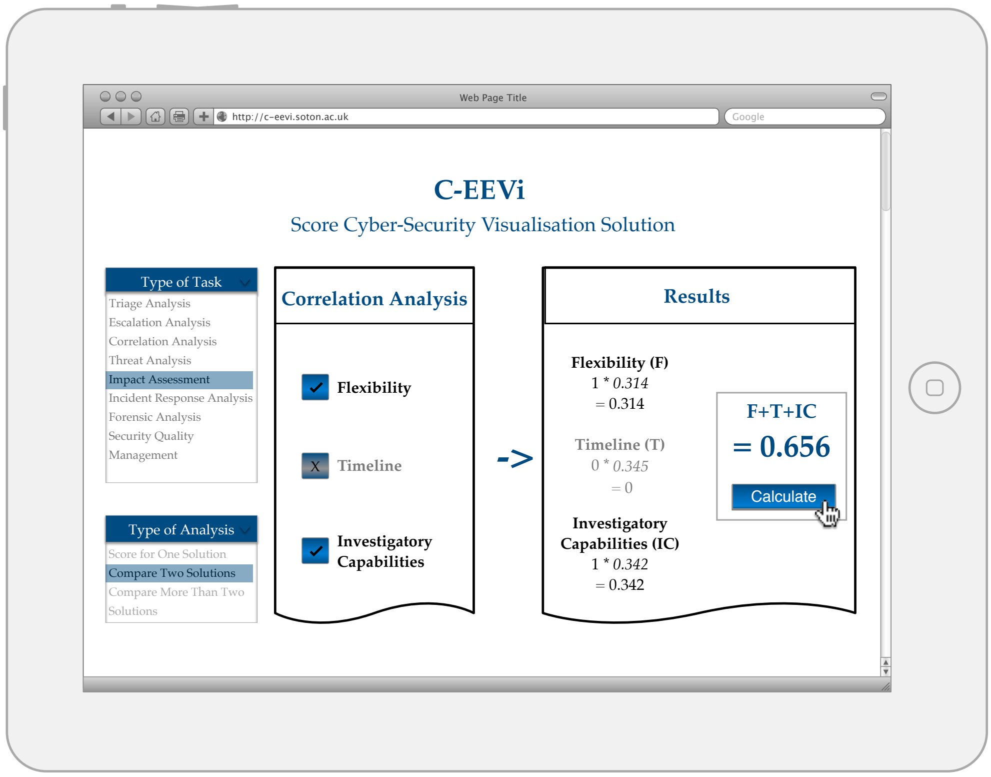
Priority weights for all component tasks of *EEVi* were calculated using the previous sections and these values are collated in Table 7.4.

Table 7.4: Priority weights calculated for each component task of *EEVi*

Component Task	**Characteristic of Visualisation**	**Priority Weight**
Triage Analysis (Equation 7.9)	Situational Awareness	0.230
	Filter	0.222
	Real-Time Access	0.211
	Alerts	0.169
	Colour Highlighting	0.169
Escalation Analysis (Equation H.3)	Priorities	0.307
	Reporting	0.240
	Collaboration	0.236
	Interoperation	0.217
Correlation Analysis (Equation H.11)	Timeline	0.345
	Investigatory Capabilities	0.342
	Flexibility	0.314
Threat Analysis (Equation H.19)	Correlation	0.273
	Interoperation	0.260
	Priorities	0.237
	Collaboration	0.229
Impact Assessment (Equation H.27)	Impact Identification	0.362
	Reporting	0.332
	Situational Awareness	0.306
Incident Response Analysis (Equation H.35)	Mitigation	0.211
	Reporting	0.205
	Collaboration	0.201
	Situational Awareness	0.192
	Interoperation	0.191
Forensic Analysis (Equation H.43)	Chain of Custody	0.272
	Case-Building Capabilities	0.254
	Reporting	0.246
	Interoperation	0.228
Security Quality Management (Equation H.51)	Reporting	0.515
	Feedback	0.485

These priority weights are represented in order from highest to lowest priority within each task. The priority weights in Table 7.4 were used to create *C-EEVi*, the quantitative value calculator, which scores cyber-security solutions for each performed task. The backend of *C-EEVi* requires a priority-based weighted sum to score the solutions because the implemented task may have different needs. The weighted sum gives preference to one characteristic over another, within each task. For example, there may be two different cyber-security visualisation solutions for ‘Triage Analysis’: A and B. A may have the ability to Filter (0.222) and Situational Awareness (0.230), which sums up to a score of 0.452. B may have the ability to present Alerts (0.169) and Colour Highlighting (0.169), which sums up to a score of 0.338. A and B both have two characteristics of visualisation for ‘Triage Analysis’, but A (0.452) is better than B (0.338) because the characteristics it has have a higher priority for performing ‘Triage Analysis’.

An example wireframe interface of *C-EEVi* showing the calculation of score for one solution performing ‘Correlation Analysis’, is presented in Figure 7.4.As shown in the figure, the user selects the task and what kind of analysis they would perform, then enters the presence of each *characteristic of visualisation*. These are used to calculate the Final Score for the solution by following Equation 7.19 and using the derived priority weights.



C-EEVi

Score Cyber-Security Visualisation Solution

Correlation Analysis

☑ Flexibility

☒ Timeline

☑ Investigatory Capabilities

Results

Flexibility (F)
1 * *0.314*
= 0.314

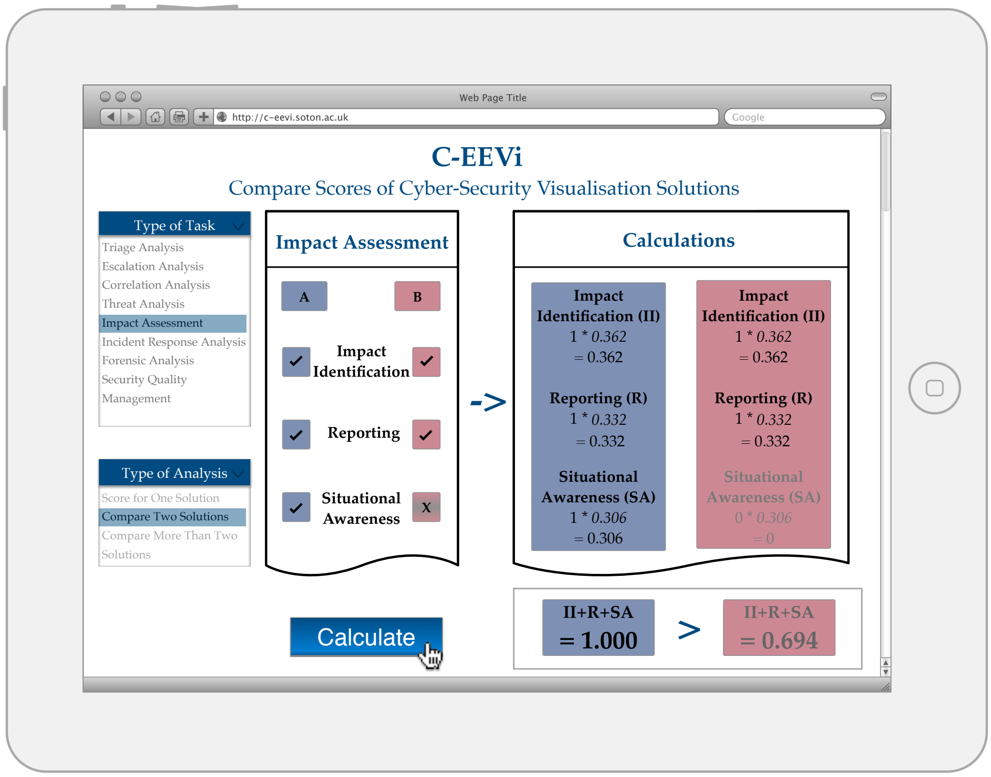
Timeline (T)
0 * *0.345*
= 0

Investigatory Capabilities (IC)
1 * *0.342*
= 0.342

F+T+IC
= 0.656

Figure 7.4: Wireframe for *C-EEVi* scoring one cyber-security solution performing ‘Correlation Analysis’, following the steps demonstrated in Section 7.1.3.5.

Figure 7.5 shows another instance of *C-EEVi* where it is used to compare the scores of two solutions performing 'Impact Assessment'. As shown in the figure, the user selects the task and what kind of analysis they would like performed, then enters the presence for each characteristic of visualisation for each solution. These are used to calculate the Final Score for both the solutions by following Equation 7.20 and using the derived priority weights. Finally, *C-EEVi* displays the scores of both solutions, along with a comparison of which solution would be better for performing 'Impact Assessment'.



C-EEVi

Compare Scores of Cyber-Security Visualisation Solutions

Type of Task: Triage Analysis; Escalation Analysis; Correlation Analysis; Threat Analysis; **Impact Assessment** (selected); Incident Response Analysis; Forensic Analysis; Security Quality Management

Type of Analysis: Score for One Solution; **Compare Two Solutions** (selected); Compare More Than Two Solutions

Impact Assessment

A		B
✓	Impact Identification	✓
✓	Reporting	✓
✓	Situational Awareness	X

->

Calculations

A	B
Impact Identification (II) 1 * *0.362* = 0.362	Impact Identification (II) 1 * *0.362* = 0.362
Reporting (R) 1 * *0.332* = 0.332	Reporting (R) 1 * *0.332* = 0.332
Situational Awareness (SA) 1 * *0.306* = 0.306	Situational Awareness (SA) 0 * *0.306* = 0

Calculate

II+R+SA = 1.000 > II+R+SA = 0.694

Figure 7.5: Wireframe for *C-EEVi* comparing two cyber-security solutions performing 'Impact Assessment', following the steps demonstrated in Section 7.1.3.5.

7.3 Discussion

This chapter introduced the Analytical Hierarchy Process (AHP), which was performed on the results from the questionnaire used in Chapter 5. The responses collected were converted into comparison matrices, in Appendix G, that were used to calculate the priority weights for each *characteristic of visualisation* for each component task of EEVi, in this chapter and Appendix H. To ensure reliability of the responses, priority weights were also checked for logical consistency. The priority weights gave each *characteristic of visualisation* a rating based on how critical they are for the respective task.

The priority weights were used to develop *C-EEVi*, a quantitative value calculator, to score cyber-security visualisation solutions for a specific task, based on the presence of *characteristics of visualisation*. *C-EEVi* provides the ability to check any cyber-security visualisation solution for a specific task. Each solution was given a score which could be used to determine the usefulness of the solution to perform a specific task and to compare its efficacy with other solutions.

This chapter presented *C-EEVi*, which was based on *EEVi*, a theoretically underpinned, validated and confirmed model, based on gaps found in the literature. The implications of this are fully discussed in the next chapter.

Chapter 8

Conclusions and Future Recommendations

Aristotle's observation is a fitting reminder of the rewards of the hard work: "The roots of education are bitter, but the fruit is sweet".

8.1 Conclusion

Cyber-security visualisation aims to provide cyber-security analysts with proficient and competent solutions to easily see patterns, trends, and anomalies in data, so that potential cyber attacks may be protected against.

The literature review in Chapter 2 drew attention to major issues in the field of cyber-security visualisation. A number of cyber-security visualisation solutions exist (Section 2.3), but they lack the ability to directly support tasks performed by cyber-security analysts, as depicted in Figure 2.2. The biggest drawback of these solutions was the lack of involvement by cyber-security analysts (end-users) in the development process, both during the design phase (Section 2.4.1) and in the evaluation phase. Further, evaluation techniques rarely assessed the effectiveness of solutions and lacked any form of standardisation (Section 2.4.2). Another issue was the disparity of domain-knowledge between cyber-security analysts and visualisation designers, resulting from their expertise in different domains (Section 2.4.3). These shortcomings led to ineffective cyber-security visualisation solutions, which subsequently resulted in low adoption rates.

There is a need for a common standardised model with guidelines, to design and evaluate cyber-security visualisation solutions for specific tasks. The model should appreciate the requirements of cyber-security analysts and focus on helping to create cyber-security visualisation solutions based on the tasks performed by them, which would lead to the solutions being more effective. The model will also be used to develop better communication between cyber-security analysts, visualisation designers, and other stakeholders (if any).

8.1.1 Recalling the Research Questions

The research questions listed in Chapter 1 were devised to overcome these shortcomings. They are recalled here to discuss the research that went into developing useful answers to each question. The research questions that show the relevance of the research study, are:

RQ_1 *What suitable method would help design cyber-security visualisation solutions for cyber-security analysts for a given task?*

- SRQ_1 *What is an appropriate model to help visualisation designers design cyber-security visualisation solutions for cyber-security analysts?*
- SRQ_2 *What are the characteristic(s) that enable a visualisation to support a cyber-security analyst in performing a given task?*

RQ_2 *What instrument can be used to promote communication between cyber-security analysts and visualisation designers who build cyber-security visualisations?*

RQ_3 *What quantitative metric can be proposed that will score cyber-security visualisation solutions?*

The ensuing sections summarise the development process and the outputs for each research question. Figure 1.1 shows the methodology followed.

8.1.2 What suitable method would help design cyber-security visualisation solutions for cyber-security analysts for a given task?

To address RQ_1, *EEVi* was developed consisting of eight component tasks. *EEVi* is a cognitive model that can help design cyber-security visualisation solutions for the performed task (SRQ_1). The eight component tasks represent the most common tasks performed by cyber-security analysts, each with written guidelines for the *characteristics of visualisation* for each task (SRQ_2).

Because of limited access to cyber-security analysts who could provide the knowledge required to conduct the thematic analysis, existing Cognitive Task Analysis (CTA) papers were used (Chapter 3). These papers were based on interviews and observations of cyber-security analysts and cyber-security visualisation solutions.

Undertaking Thematic Analysis on five of these CTA papers (D'Amico & Whitley, 2007; D'Amico et al., 2005; Erbacher et al., 2010; Fink et al., 2009) and (Mckenna et al., 2015), provided the foundation for developing *EEVi*, as discussed in Section 3.2.1. The Thematic Analysis followed the steps outlined in Figure 3.1. This process led to the identification of four themes. The terminology of these themes was modified during validation of *EEVi*, as presented below:

1. ***Goal:*** Task performed by cyber-security analysts;

2. ***Type of Data:*** Type of data used to perform the tasks;

3. ***Characteristics of Visualisation:*** Characteristics required to perform tasks;

4. ***Role of End-User:*** Role of the cyber-security analyst who performs the tasks.

Each of these themes encompassed a set of codes within it. The lists and descriptions of identified codes and themes were shown in Tables 3.2 to Table 3.5. These themes (and the codes within) formed cognitive relationships with each other were linked together to form *EEVi* (Figure 3.3).

The descriptions of the theme codes are purposely ambiguous to ensure that visualisation designers or end-users are not led in a pre-defined direction. Visualisation designers can converse with stakeholders and end-users (cyber-security analysts), and ask for their interpretation of how a characteristic of visualisation can be implemented, so that their perspectives can be included in the resulting solutions. The characteristics of visualisation are not a one-size-fits-all situation and require careful consideration in the design process in accordance with the custom requirements of cyber-security analysts. For example, the characteristic 'Alert' in Table 3.5, can be defined as *"a system to alert the user of the status of activity being investigated."* In different implementations it can have different interpretations; it could be an alert for a suspicious activity, an alert for new data relating to an activity, or an alert that an issue has been resolved. Consequently, every characteristic of visualisation can have various interpretations depending on the requirements of the tasks and stakeholders.

The thematic analysis also led to the identification of eight tasks commonly performed by cyber-security analysts: 'Triage Analysis'; 'Escalation Analysis'; 'Correlation Analysis'; 'Threat Analysis'; 'Impact Assessment'; 'Incident Response Analysis'; 'Forensic Analysis'; and 'Security Quality Management' (Table 3.2 has the definitions). The codes and themes were used to formulate guidelines to design visualisation solutions for each of these tasks, as shown in Figure 3.4 to Figure 3.11. The figures represent the codes corresponding to each theme, which can be substituted in *EEVi* to represent guidelines for design.

EEVi was reviewed by thirteen experts (seven cyber-security analysts and six visualisation designers) (Chapter 4). Feedback from the review led to a revision of *EEVi* on the basis of end-user requirements. These revisions ensured that the terminology and structure of the model clearly conveyed the requirements of cyber-security analysts to the visualisation designers, minimising the disparity between the groups. *EEVi*'s structure and terminology was revised, as shown in Figure 4.1. The component tasks underwent more substantial revisions, along with their structure and some terminology; the characteristics of visualisation were also updated (Figure 4.4 to Figure 4.11). Some characteristics of visualisation for each task were added to an *unresolved* category; these characteristics required confirmation before they were added to the component task diagrams (Section 4.4.4).

Statistical analysis of the experts' responses was also undertaken. The qualitative responses were quantified, using the integrative mixed methods approach, to a five-point Likert scale ranging from very positive response (+2) to very negative response (-2), as shown in Section 4.4.2, Test for Differences and Test for Agreement were subsequently carried out on the quantified responses.

Test for Differences: A mixed design ANOVA was conducted in Section 4.4.3.1. The results demonstrated that there was no statistically significant difference between the cyber-security analysts and visualisation designers to the characteristics of visualisation.

Test for Agreement: *Pearson's r Correlation* was conducted in Section 4.4.3.2. The results demonstrated that there was no statistically significant agreement between the responses of the two groups or amongst themselves.

The inclusion of visualisation designers in the review led to their perspective guiding modifications made to the terminology and to the structure of *EEVi* as much as the views of the cyber-security analysts, thereby minimising the disparity between the two groups.

EEVi was subsequently confirmed by 30 participants in an online self-administered questionnaire (Chapter 5). 80% of the participants had expertise in cyber-security while 13% had expertise in both cyber-security and visualisation design, with an average experience of 6.7 years in their respective fields. Results from the questionnaire enabled confirmation of *EEVi* and further revisions of the component tasks. 90% of the participants agreed with the logical flow and structure of *EEVi*, and hence no further revisions were made (Section 5.3.1). Component tasks were also confirmed by the participants, along with modifications to be added to the *characteristics of visualisation* previously assigned to the *unresolved* category (Section 5.3.2). The modified component tasks are shown in Figure 5.3 to Figure 5.17.

From the expert review and questionnaire it can be concluded that *EEVi* represents a model to help design cyber-security visualisation solutions. The validated and confirmed model fulfils SRQ_1. The validation and confirmation of the component tasks led to identification of the *characteristics of visualisation* fulfilling SRQ_2.

Incorporating information from the component tasks with *EEVi* led to the preparation of guidelines for designing cyber-security visualisation solutions for cyber-security analysts, fulfilling RQ_1. These are presented in Figure 5.18 and Figure 5.19.

8.1.2.1 Research Methodology for Development of *EEVi*

Triangulation is a research methodology that confirms the reliability and validity of findings from a study by using two or more methods of data collection (L. Cohen, Manion, & Morrison, 2013; Recker, 2013; Mathison, 2005). These methods vary for each study according to their respective criteria (Golafshani, 2003). Triangulation arises from the idea that "...to establish a fact you need more than one source of information" (Bogdan & Biklen, 2007). In other words, triangulation is used to verify facts by corroborating the results from more than one source of information to fully understand and gain a more nuanced picture (Bogdan & Biklen, 2007; Recker, 2013).

Methodological Triangulation was used for the development of *EEVi* (Mathison, 2005). It uses different methods to study (in this case evaluate) and bring together multiple forms of analyses to get closer to the truth (Denzin & Lincoln, 2012).

Development of *EEVi*, based on Thematic Analysis of the CTA papers, was validated by an expert-review and confirmed with an online-based self-administered questionnaire, to gain a comprehensive view, incorporating the different views of the stakeholders, as shown in Figure 8.1.

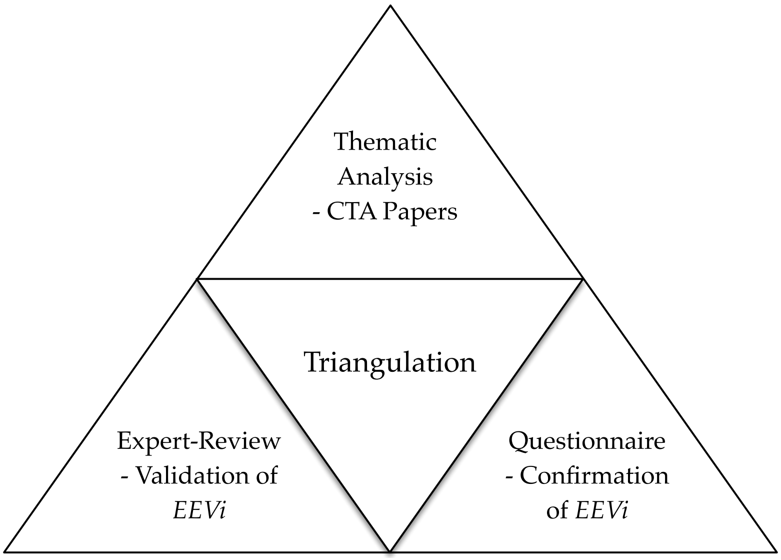


Figure 8.1: Triangulation, research methodology used for development of *EEVi*.

8.1.3 What instrument can be used to promote communication between cyber-security analysts and visualisation designers who build cyber-security visualisations?

To address RQ_2, a work domain analysis (abstraction hierarchy) diagram of *EEVi* was constructed, along with subsets for the component tasks (Chapter 6). The resulting diagrams can be a useful instrument to promote communication by presenting information from the cyber-security domain in a format that is familiar to visualisation designers. Figure 6.1 shows the work domain analysis diagram for *EEVi*.

Work domain analysis (abstraction hierarchy) diagrams (Section 6.4.1) and sample user interface mockups (Section 6.4.2) were produced to investigate the real world use of *EEVi* as a basis of communication between cyber-security analysts and visualisation designers. Interviews with 10 experts (five cyber-security analysts and five visualisation designers) were conducted to find the most useful instrument in the real world, using as an example the component task, 'Escalation Analysis'.

The experts presented good arguments for employing both user interface mockups and work domain analysis diagram. However, the participants favoured work domain analysis (abstraction hierarchy) diagram as the most useful instrument (Section 6.4.3). The cyber-security analysts believed that they could use these diagrams to convey their requirements. Likewise, the visualisation designers felt that they could use these diagrams as a basis of communication to ask questions about the requirements of cyber-security analysts. All the experts agreed that the abstraction hierarchy was developed from the guidelines of *EEVi*. Figure 6.2, Figure 6.4 to Figure 6.10 were created as a result, to highlight each task clearly as a subset from Figure 6.1.

The participants were positive and provided a useful critique of the abstraction hierarchy diagram and mockups. According to them, the diagrams represented the interplay of all relationships that would be useful in understanding the whole system, whereas the mockups were concrete pieces of information that could show the workings of a solution developed by following *EEVi*. All the cyber-security analysts agreed that they would use the developed mockups for illustrating a cyber-security visualisation solution to perform 'Escalation Analysis' (ignoring costs).

8.1.4 What quantitative metric can be proposed that will score cyber-security visualisation solutions?

To address RQ_3, *C-EEVi* was developed (Chapter 7 and Appendix H). *C-EEVi* is a quantitative value calculator used to score a cyber-security visualisation solution and to compare them. *C-EEVi* was developed using the Analytical Hierarchy Process (AHP), following the process outline in Figure 7.1.

Results from the confirmation of *EEVi* (Appendix E) were used to develop the calculator's backend. The respondents, listed in Chapter 5, were asked to rate the importance of each *characteristic of visualisation* for each task on a five-point Likert scale, from 'Strongly Agree' to 'Strongly Disagree'. These ratings were quantified in accordance with Saaty (2012)'s pairwise comparison scale (Table 7.2) and then converted into a comparison matrix to perform AHP, detailed in Appendix G.

Following the AHP, the priority weights of each characteristic of visualisation for each component task were calculated (Table 7.4). These formed the backend of *C-EEVi* by producing a quantified value of importance for each characteristic for each task.

These values could then be used to calculate the score for any cyber-security visualisation solution for a certain task. Figure 7.4 shows a wireframe of *C-EEVi* used to calculate the score for one solution. Another example presented in Figure 7.5, illustrates the working of *C-EEVi* to compare two solutions.

8.2 Research Contributions

The aim of this research was to address the gaps that show that many visualisations for cyber-security analysts often impedes understanding since the visualisation designers often focus on HCI rather than the complexities of performing a certain task, which affects what the analyst is trying to do. The contributions of this research are:

Contribution 1: *EEVi* (Figure 5.18 and 5.19) is a model, along with constituent guidelines that describe the underpinning characteristics of visualisation. These guidelines are used by visualisation designers to produce a visualisation solution for analysts undertaking cyber-security tasks. Visualisation designers can directly use the model as the basis for developing a new solution and build on that. *EEVi* was developed by using Thematic Analysis, as demonstrated in Chapter 3, updated and validated by an expert-review, as shown in Chapter 4, and finally revised and confirmed by a questionnaire, as shown in Chapter 5.

Contribution 2: Work Domain Analysis (Abstraction Hierarchy) Diagram of *EEVi* (Figure 6.1) is an instrument that can promote communication between cyber-security analysts and visualisation designers (and any other stakeholders), in order to promote communication between them. Chapter 6 discussed the expert interviews, confirming that the diagrams would help improve communication and could be used as a basis for developing cyber-security visualisation solutions.

Visualisation designers can use the work domain analysis (abstraction hierarchy) diagram, which represents the guidelines for *EEVi*'s constituent component tasks and the interplay of their relationships in one view. Figure 6.1, can be used in early-design phases as a common medium of communication between visualisation designers and cyber-security analysts to discuss the requirements and plan the design of a solution. The interplay of relationships visible in a single view can also help cyber-security analysts understand which task the solution can be used to perform and how it would be employed in their organisations. Additionally, visualisation designers can use the work domain analysis diagram to design a cyber-security visualisation solution using cognitive work analysis, as explained in Section 8.4.1.

Contribution 3: *C-EEVi* is a tool to evaluate cyber-security visualisation solutions by scoring them on the basis of how effective they can be in performing a certain task. Chapter 7 and Appendix H demonstrate the calculations of the priority weights that would form the back-end of the calculator and can be used to score or compare any cyber-security visualisation solutions. *C-EEVi* can be used by visualisation designers, cyber-security analysts, and any other stakeholders to score or compare solutions. *C-EEVi* has developed a priority rating for each characteristic of visualisation of each task in *EEVi*. The final score(s) provided by *C-EEVi* provides a quantitative measure for rating cyber-security visualisation solutions, which currently does not exist.

8.3 Research Limitations

The limitations of this research are described below:

Limitation 1: The constituent component tasks of *EEVi* provide validated and confirmed guidelines for visualisation solely for the field of cyber-security. It could be applied to other fields; however, this has not been addressed in this research.

Limitation 2: The initial research involved two cross-disciplinary literature research tools and reviewing papers up to 2015. Of that review only five relevant CTA research papers were found out of the total of 312 that matched the keywords, as described in Section 3.2.1. Future research may want to look for any new developments.

Limitation 3: While this research has identified the underpinning components required for effectiveness, it has not evaluated effectiveness of a given implementation or solution.

Limitation 4: Implementation of the visualisation components is not part of this research. Effectiveness and usefulness of cyber-security visualisation solutions would depend on how well the visualisation designers implement each characteristic of visualisation.

Limitation 5: While the guidelines have been validated and confirmed with experts, best practice to implement the characteristics of visualisation is currently not defined and can be undertaken during future research (Section 8.4.2).

8.4 Recommendations for Future Research

This section recommends the direction of future research that can be undertaken on the basis of the research conducted in this thesis. It also attempts to overcome some of the research limitations outlined above.

8.4.1 Using Ecological Interface Design to Develop a Cyber-Security Visualisation Solution Following *EEVi*

Combined with other phases of cognitive work analysis, work domain analysis (defined in Section 6.1.2) can be used to design novel user interfaces (Fay, Stanton, & Roberts, 2019). Ecological Interface Design (EID) is a theoretical framework that has been used for the design of human-computer interaction machines for complex sociotechnical systems (Vicente, 2002). According to Vicente (2002), work domain analysis provides a robust basis for supporting the design of novel user interfaces as it has the flexibility required to cope with change. EID incorporates work domain analysis. It capitalises on end-users' pattern recognition skills and other innate abilities to understand the system. EID has been shown to improve performance by allowing end-users flexibility in the problem-solving of unknown and unencountered situations, which is very useful in the cyber-security domain. The work domain analysis (abstraction hierarchy) diagram developed for *EEVi* could be used to develop a cyber-security visualisation solution, following the EID framework.

As an example, Burns, Kuo, and Ng (2003) developed a visualisation solution for network management using the EID framework. However, *EEVi* can add more efficacy to the resultant cyber-security visualisation solution because of its development process. It would also decrease the development time for the design, as the work domain analysis (abstraction hierarchy) diagram is already available and approved by experts.

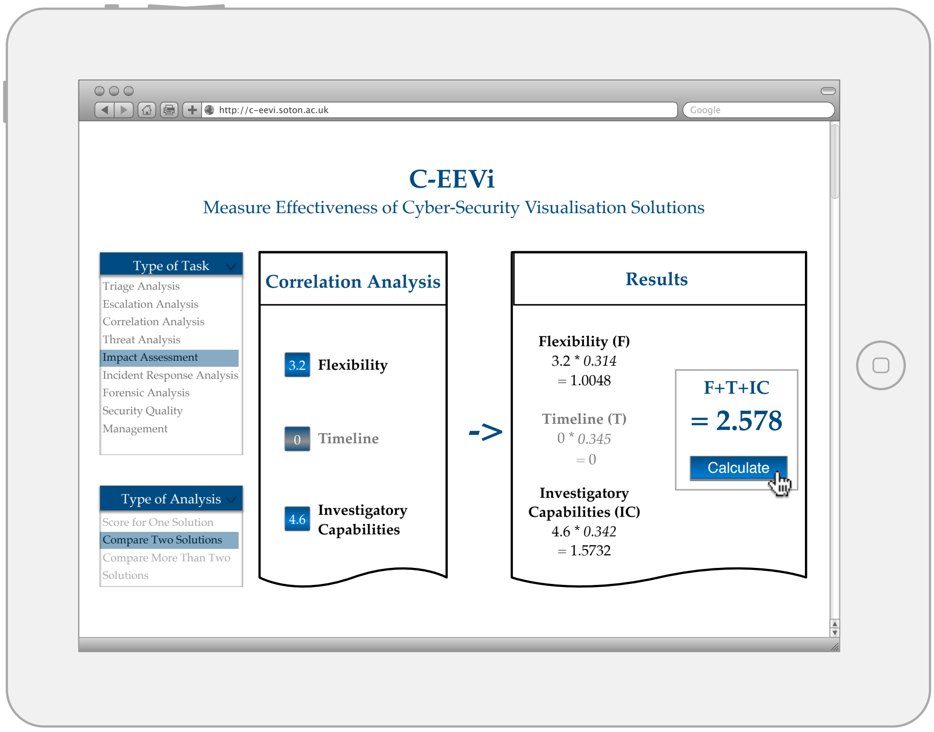


Figure 8.2: Post Future Work Wireframe for *C-EEVi* scoring one cyber-security visualisation solution performing 'Correlation Analysis'.

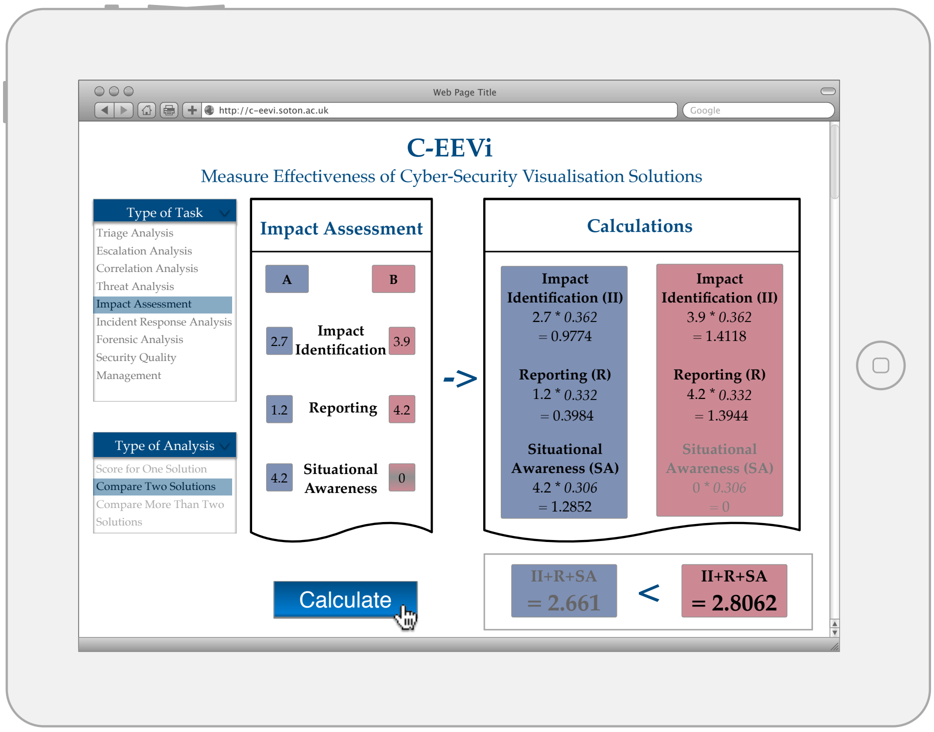


Figure 8.3: Post future work wireframe for *C-EEVi* comparing two cyber-security visualisation solutions performing 'Impact Assessment', using ratings for each characteristic of visualisation.

8.4.2 Further Research on *Characteristics of Visualisation*

A future study could clarify how *characteristics of visualisation* should be implemented, for maximum effectiveness and ease of use by cyber-security analysts. It could include aspects such as culture or technical ability of end-users. The study could also include best practice, details on the representation of visualisation, aesthetic, choice of colours, etc. *Characteristics of visualisation* for each task can be represented in multiple ways, ranging from the type of graphic to the level of interaction ability.

There is also a need to fully understand and improve the ontological structure of the classification of characteristics of visualisation. The study could include further development and discrimination of the characteristics of visualisation in *EEVi*, to better understand the nature of each characteristic.

8.4.3 Further Development of *C-EEVi*

C-EEVi could be further developed to include ratings of how well each *characteristic of visualisation* is implemented, based on the results of the study in Section 8.4.2. This could provide a scale of how to rate each *characteristic of visualisation.* An example of the working of *C-EEVI* after the application of this proposed work is shown in Figure 8.2 and Figure 8.3.

Appendix A

Associations Matrix of Identified Codes

Table A.1 presents the association between codes, which appeared within 20 words, before or after, the task.

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	Searched With	Appeared within 20 Words	Notes
Triage Analysis (TA)	Lead Analyst	No	-
	Tactical Defender	No	-
	Suspicious Activities	Yes (3)	Appears for EA, but close to TA code.
	Incidents	No	-
	Communication	Yes (1)	Appears for feedback loops.
	Interoperation	No	-
	Site-Specific Analyst	No	-
	Timeline	No	-
	Flexibility	No	-
	Investigation	No	-
	Threat Analyst	No	-
	Strategic Analyst	No	-
	Intrusion Sets	No	-
	Correlation	Yes (1)	Negative result for TA.

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	Searched With	Appeared within 20 Words	Notes
	Incident Handler/Responder	No	-
	Mitigation	No	-
	Forensic Analyst	No	-
	Source Data	No	-
	Security Policies	No	-
	Reporting	No	-
	Network Manager	Yes(1)	If an organisation does not have a Real-Time Analysts, then a Network Manager can perform the task.
	Identification	No	-
Escalation Analysis (EA)	Real-Time Analyst	No	-
	Raw Data	Yes (1)	Appears for TA, but close to EA code.
	Interesting Activities	Yes (1)	Appears for TA, but close to EA code.
	Filter	No	-
	Speed	Yes (1)	Appears for CA, but close to EA code.
	Situational Awareness	No	-
	Site-Specific Analyst	No	-
	Timeline	Yes (1)	Appears for TA, but close to EA code.
	Flexibility	No	-
	Investigation	No	-
	Threat Analyst	No	-
	Strategic Analyst	No	-
	Intrusion Sets	No	-
	Correlation	No	-
	Incident Handler/Responder	No	-
	Mitigation	No	-
	Forensic Analyst	No	-
	Source Data	No	-

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	**Searched With**	**Appeared within 20 Words**	**Notes**
	Security Policies	No	-
	Reporting	No	-
	Network Manager	Yes (1)	Appears for TA, but close to EA code.
	Identification	No	-
Correlation Analysis (CA)	Real-Time Analyst	No	-
	Raw Data	Yes (1)	Appears for TA, but close to CA code.
	Interesting Activities	Yes (1)	Appears for TA, but close to CA code.
	Filter	No	-
	Speed	No	-
	Situational Awareness	No	-
	Lead Analyst	Yes (1)	Appears for EA, but close to CA code.
	Suspicious Activities	Yes (3)	Appears for EA, but close to CA code.
	Incidents	Yes (2)	Appears for EA, but close to CA code. Also appears for Intrusion Set.
	Communication	Yes (1)	Appears for feedback loops.
	Interoperation	No	-
	Threat Analyst	No	-
	Strategic Analyst	No	-
	Correlation	No	-
	Incident Handler/Responder	No	-
	Mitigation	No	-
	Forensic Analyst	No	-
	Source Data	No	-
	Security Policies	No	-
	Reporting	No	-
	Network Manager	No	-
	Identification	No	-

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	**Searched With**	**Appeared within 20 Words**	**Notes**
Threat Analysis (ThA)	Real-Time Analyst	No	-
	Raw Data	No	-
	Interesting Activities	No	-
	Filter	No	-
	Speed	Yes (1)	Appears for TA, but close to ThA code.
	Situational Awareness	No	-
	Lead Analyst	No	-
	Suspicious Activities	No	-
	Incidents	Yes(3)	Appears for EA, but close to ThA code.
	Communication	Yes (1)	Appears for feedback loops.
	Site-Specific Analyst	No	-
	Timeline	No	-
	Flexibility	No	-
	Investigation	No	-
	Incident Handler/Responder	No	-
	Mitigation	No	-
	Forensic Analyst	No	-
	Source Data	No	-
	Security Policies	No	-
	Reporting	No	-
	Network Manager	No	-
	Identification	No	-
Incident Response Analysis (IRA)	Real-Time Analyst	No	-
	Raw Data	No	-
	Interesting Activities	No	-
	Filter	No	-
	Speed	No	-
	Lead Analyst	No	-
	Suspicious Activities	No	-

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	**Searched With**	**Appeared within 20 Words**	**Notes**
	Incidents	Yes (1)	Appears for Intrusion Sets, but close to IRA code.
	Communication	No	-
	Interoperation	No	-
	Site-Specific Analyst	No	-
	Timeline	No	-
	Flexibility	No	-
	Investigation	No	-
	Threat Analyst	No	-
	Correlation	No	-
	Forensic Analyst	No	-
	Source Data	No	-
	Security Policies	No	-
	Reporting	Yes (1)	Appears for FA, but close to IRA code.
	Network Manager	No	-
	Identification	No	-
Forensic Analysis (FA)	Real-Time Analyst	No	-
	Raw Data	No	-
	Interesting Activities	No	-
	Filter	No	-
	Speed	No	-
	Situational Awareness	No	-
	Lead Analyst	No	-
	Tactical Defender	No	-
	Suspicious Activities	No	-
	Incidents	No	-
	Communication	No	-
	Interoperation	No	-
	Site-Specific Analyst	No	-
	Timeline	No	-
	Flexibility	No	-
	Threat Analyst	No	-

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	Searched With	Appeared within 20 Words	Notes
	Strategic Analyst	No	-
	Correlation	No	-
	Incident Handler/Responder	Yes (1)	Appears for IRA, but close to FA code.
	Intrusion Sets	No	-
	Mitigation	No	-
	Network Manager	No	-
	Identification	No	-
Impact Assessment (IA)	Real-Time Analyst	No	-
	Raw Data	No	-
	Interesting Activities	No	-
	Filter	No	-
	Speed	No	-
	Lead Analyst	No	-
	Tactical Defender	No	-
	Suspicious Activities	No	-
	Incidents	Yes(1)	Appears for EA, but close to IA code.
	Communication	No	-
	Interoperation	No	-
	Site-Specific Analyst	No	-
	Timeline	No	-
	Flexibility	No	-
	Investigation	No	-
	Threat Analyst	No	-
	Strategic Analyst	No	-
	Correlation	No	-
	Incident Handler/Responder	No	-
	Intrusion Sets	No	-
	Mitigation	No	-
	Forensic Analyst	No	-
	Security Policies	No	-
	Reporting	No	-

Table A.1: Results of searches in NVivo to find Association between Codes.

Task Code	**Searched With**	**Appeared within 20 Words**	**Notes**
Security Quality Management (SQM)	Real-Time Analyst	No	-
	Raw Data	No	-
	Interesting Activities	No	-
	Filter	No	-
	Speed	No	-
	Situational Awareness	No	-
	Lead Analyst	No	-
	Tactical Defender	No	-
	Suspicious Activities	No	-
	Incidents	No	-
	Interoperation	No	-
	Site-Specific Analyst	No	-
	Timeline	No	-
	Flexibility	No	-
	Investigation	No	-
	Threat Analyst	No	-
	Strategic Analyst	No	-
	Correlation	No	-
	Incident Handler/Responder	No	-
	Intrusion Sets	No	-
	Mitigation	No	-
	Forensic Analyst	No	-
	Identification	No	-
	Reporting	No	-

Appendix B

Ethics Approval for Expert-Review, Questionnaire and Interviews

B.1 Approved DPA Plan

Ethics reference number: $ERGO/FPSE/23974$
Version: 1
Dated: 2016-11-07
Period Covered: 16th November 2016 to 1st November 2019
Study Title: EEVi-Effective Visualisation for Visualisation in Cyber-Security
Investigator: Aneesha Sethi

The following is an exhaustive and complete list of all the data that will be collected (through questionnaires, interviews, extraction from records, etc): Contact Details (Email Addresses), Consent Forms, Names of Participants and Voice recording from the interview. Notes from Interviews would be anonymised by participant numbers.

The data is not excessive because it contains contact details used to contact the experts and their consent to take part in the study. Notes from interviews would be anonymous and the voice recordings would be destroyed after the interview has been transcribed.

The data will be processed fairly because the participants will have given explicit consent through a consent sheet.

Data will be stored on the Investigator's desktop in a secure lab on a password-protected computer. The data will be held in accordance with the University policy on data retention.

Data files will be protected by desktop which will be protected by a secure lab with card access only to researchers and academics. Physical data will be kept in a locked desk belonging to the investigator and only the investigator will have access to it. This desk would also be in a secure lab with card access to researchers and academics.

The data will be destroyed by the investigator after completion of PhD. The voice recordings will be destroyed after the notes have been transcribed by the investigator.

The data will be processed in accordance with the rights of the participants because they will have the right to withdraw their data at any time and for any reason. Participants will be able to exercise their rights by contacting the investigator (Aneesha.Sethi@soton.ac.uk) or the project supervisor (gbw@ecs.soton.ac.uk).

The data will be anonymised by participant numbers. Consent forms will be linked to the data by these participant numbers.

B.2 Approved Participation Information Sheet

Ethics reference number: $ERGO/FPSE/$23974
Version: 1
Dated: 2016-11-07
Period Covered: 16th November 2016 to 1st November 2019
Study Title: EEVi-Effective Visualisation for Visualisation in Cyber-Security
Investigator: Aneesha Sethi

Please read this information carefully before deciding to take part in this research. If you are happy to participate you will be asked to sign a consent form.

Your participation is completely voluntary.

What is the research about? This research is for my PhD Project. I have created a model to determine and create effective visualisations in Cyber-Security. By the means of this survey, I wish to see what your opinions are about the model and resultant analysis.

Why have I been chosen? You have been approached because of your experience in cyber-security.

What will happen to me if I take part? If you decide to take part in this research you will spend about 30 minutes completing the questionnaire or answering the questions in an interview format.

Are there any benefits in my taking part? Participants will not directly benefit by taking part in this research project.

Are there any risks involved? No risks are involved in this research.

Will my data be confidential?
For Expert-Review/Interview: The signed consent sheets and email addresses would be kept separately and safely, at a different location from the questionnaire results. The investigator would record the interview and make notes, afterwards the interview would be transcribed and the recording would be destroyed. Each participant would be given a participant number. Throughout the recording the participant would be referred by his participant number, to avoid recording sensitive information. Data will be held on a password protected computer so nobody except the researcher has access to it. The collection of data complies with the University of Southampton policy under the Data Protection Act.
For Questionnaire: All data collected are anonymous if the participant wants and used only for the purposes of this study. It will be held on password-protected computer so nobody except the researcher has access to it. The collection of data complies with the University of Southampton policy under the Data Protection Act.

What happens if I change my mind? You have the right to withdraw at any time and for any reason without your legal rights being affected.

What happens if something goes wrong? Should you have any concern or complaint, contact me if possible (Aneesha Sethi, Aneesha.Sethi@soton.ac.uk), otherwise please contact my supervisor Dr Gary Wills (gbw@ecs.soton.ac.uk). Otherwise please contact the FPSE Office (ergopse@soton.ac.uk) or any other authoritative body such as the Research Integrity & Governance Team (rgoinfo@soton.ac.uk).

Appendix C

Expert-Review Interview Format

The expert-review was conducted with approval from Ethics and Research Governance (ERGO) under reference number $ERGO/FPSE/23974$.

The semi-structured interview was divided into four sections:

C.1 General Information and Technical Background

QC.1.1 What is your age-group?

QC.1.2 Which company or organisation do you for work for? (If you are studying, please mention the name of the university.)

QC.1.3 Please briefly mention your area of expertise?

QC.1.4 How many years of experience do you have in the field you mentioned above?

QC.1.5 Do you have any experience or knowledge of visualisation in cyber-security? If yes, on a scale of 1-10, can you rate your knowledge/experience of cyber-security visualisation? (1 - low; 10 - high)

QC.1.6 Have you ever used any cyber-security visualisation tool or software?

C.2 Structure of Model

In this section, *EEVi* needs to be validated.

EEVi (Figure 3.3) displays a logical flow of who performs a task, what task do they perform, what data is needed for the task to be performed and what features of visualisation are required to perform the task. Once we are aware of all of these, the visualisation produced will be effective. *Effective* can be defined as the features of visualisation that are crucial to perform a certain task competently.

QC.2.1 Does this structure make sense logically?

QC.2.2 Does the structure match a logical flow of how tasks are formed at your organisation?

C.3 Analysis of Model

The next section is about the analysis derived from the framework.

Triage Analysis

Please look at the following analysis (Figure 3.4) and answer the questions below based on this.

The first task identified is Triage Analysis - It is the first look at data. At this stage, the analyst weeds out false positives for further analysis. It is performed within an order of a few minutes. It is performed by a Real-Time Analyst.

- Raw Data - The most elemental data, usually in very large quantity and is passed through an automated process to filter.
- Interesting Activity - Data that has been flagged by automated processes on Raw Data and is inspected by an analyst, usually consists of a large number of false positives.
- Filter - Allows the ability to easily filter, join or transform data without changing the original; Also allows the ability to filter noise to allow an analyst to see trends.
- Speed - Viewing real-time data within seconds to minutes of an event.
- Situational Awareness - An accurate picture of external and internal information in an overview to allow rapid decision making and to allow for analysts to understand the state of all resources.

QC.3.1.1 Do the features of visualisation make sense for the task?

QC.3.1.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.1.3 Have all important features for the task at hand been covered?

QC.3.1.4 For Visualisation Designers only: Are these features implementable?

QC.3.1.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Escalation Analysis

Please look at the following analysis (Figure 3.5) and answer the questions below based on this.

The second task identified is Escalation Analysis - It is the investigation of suspicious activities from the previous stage and production of reports. It may take from hours to a few weeks to complete. It is performed by a Lead Analyst or Tactical Defender.

- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems.
- Suspicious Activities - Data that is anomalous after the initial Triage Analysis and needs to be monitored.
- Incidents - The point when the occurrence and seriousness of an event is confirmed and formally reported.
- Communication - Enable users to communicate and collaborate with other analysts by sharing findings and providing support for report building.
- Interoperation - Ability of tool to work efficiently with other tools, applications or utilities.

QC.3.2.1 Do the features of visualisation make sense for the task?

QC.3.2.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.2.3 Have all important features for the task at hand been covered?

QC.3.2.4 For Visualisation Designers only: Are these features implementable?

QC.3.2.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Correlation Analysis

Please look at the following analysis (Figure 3.6) and answer the questions below based on this.

The third task identified is Correlation Analysis - It is the search for patterns and trends in data, which may be previously unrecognised. It may take from weeks to a few months to complete. It is performed by a Site-Specific Analyst or Tactical Defender.

- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems.

- Intrusion Sets - Sets of related Incidents that are given an increase in attention and resources to detect, understand and respond.
- Timeline - A order of events and activities that have taken place over a period of time, used to coordinate all views.
- Flexibility - Flexibility of visualisation gives the ability to manipulate the focus point and support the analytical process.
- Investigation - Allow users to investigate data by supporting simultaneous investigations or providing extensive capabilities for vulnerability assessment or providing a platform for rapid, open-ended foraging activities.

QC.3.3.1 Do the features of visualisation make sense for the task?

QC.3.3.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.3.3 Have all important features for the task at hand been covered?

QC.3.3.4 For Visualisation Designers only: Are these features implementable?

QC.3.3.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Threat Analysis

Please look at the following analysis (Figure 3.7) and answer the questions below based on this.

The fourth task identified is Threat Analysis - It is an intelligent analysis using additional data sources to profile attackers and their motivations. It is performed by a Threat Analyst or Tactical Defender or Strategic Analyst.

- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems.
- Strategic Analyst - Works at the community level to understand the implications of attack and categorise it.
- Intrusion Sets - Sets of related Incidents that are given an increase in attention and resources to detect, understand and respond.
- Correlation - Displays relationships between different data dimensions.
- Interoperation -Ability of tool to work efficiently with other tools, applications or utilities.

QC.3.4.1 Do the features of visualisation make sense for the task?

QC.3.4.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.4.3 Have all important features for the task at hand been covered?

QC.3.4.4 For Visualisation Designers only: Are these features implementable?

QC.3.4.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Incident Response Analysis

Please look at the following analysis (Figure 3.8) and answer the questions below based on this.

The fifth task identified is Incident Response Analysis - It is when the analyst recommends or implements actions against a confirmed incident. It is performed by an Incident Handler/Responder or Tactical Defender or Strategic Analyst.

- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems.
- Strategic Analyst - Works at the community level to understand the implications of attack and categorise it.
- Intrusion Sets - Sets of related Incidents that are given an increase in attention and resources to detect, understand and respond.
- Mitigation - Performing clean-up and containment; and providing mitigation solution and/or activities.
- Situational Awareness - An accurate picture of external and internal information in an overview to allow rapid decision making and to allow for analysts to understand the state of all resources.

QC.3.5.1 Do the features of visualisation make sense for the task?

QC.3.5.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.5.3 Have all important features for the task at hand been covered?

QC.3.5.4 For Visualisation Designers only: Are these features implementable?

QC.3.5.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Forensic Analysis

Please look at the following analysis (Figure 3.9) and answer the questions below based on this.

The sixth task identified is Forensic Analysis - It is gathering and preservation of data to support law enforcement agencies. It may take from hours to a few weeks to complete. It is performed by a Forensic Analyst.

- Security Policies - Policies defined by the government or organisations relating to cyber-security; also includes cyber law.
- Investigation - Allow users to investigate data by supporting simultaneous investigations or providing extensive capabilities for vulnerability assessment or providing a platform for rapid, open-ended foraging activities.
- Reporting - Provide support for report building.

QC.3.6.1 Do the features of visualisation make sense for the task?

QC.3.6.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.6.3 Have all important features for the task at hand been covered?

QC.3.6.4 For Visualisation Designers only: Are these features implementable?

QC.3.6.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Impact Assessment

Please look at the following analysis (Figure 3.10) and answer the questions below based on this.

The seventh task identified is Impact Assessment - It is the task of identification of impact, damage and potential critical nodes that may be reachable after a breach. It is performed by a Network Manager.

- Network Manager - Identify and eliminate malicious activity, usually within the domain of network attacks and prioritise events based on the likelihood of maliciousness.
- Source Data - Data gathered from an intrusion used for further analysis or reporting.

- Identification - The identification of vulnerabilities; malicious users; intended target of attacks; main resources of the system.
- Situational Awareness - An accurate picture of external and internal information in an overview to allow rapid decision making and to allow for analysts to understand the state of all resources.

QC.3.7.1 Do the features of visualisation make sense for the task?

QC.3.7.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.7.3 Have all important features for the task at hand been covered?

QC.3.7.4 For Visualisation Designers only: Are these features implementable?

QC.3.7.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

Security Quality Management

Please look at the following analysis (Figure 3.11) and answer the questions below based on this.

The eighth task identified is Security Quality Management - It is the task related to services that support information security in an organisation like tutorials or training. It is performed by a Network Manager.

- Network Manager - Identify and eliminate malicious activity, usually within the domain of network attacks and prioritise events based on the likelihood of maliciousness.
- Source Data - Data gathered from an intrusion used for further analysis or reporting.
- Security Policies - Policies defined by the government or organisations relating to cyber-security; also includes cyber law.
- Communication - Enable users to communicate and collaborate with other analysts by sharing findings and providing support for report building.

QC.3.8.1 Do the features of visualisation make sense for the task?

QC.3.8.2 According to you, are the features of visualisation appropriate for the task at hand? Please rank them in order of importance.

QC.3.8.3 Have all important features for the task at hand been covered?

QC.3.8.4 For Visualisation Designers only: Are these features implementable?

QC.3.8.5 For Visualisation Designers only: Can you please rank the features of visualisation in order of how difficult it is to implement these features?

C.4 After Thoughts

QC.4.1 What general features do you think that every cyber-security visualisation tool should have for any/all tasks? (Eg: Communication)

QC.4.2 Do you think this model represents good fundamental guidelines for cyber-security visualisation?

QC.4.3 Do you think the model is useful to evaluate the effectiveness of cyber-security visualisation for performed tasks?

QC.4.4 Is there anything else you would like to add?

Appendix D

Questionnaire for Confirmation of *EEVi* & Development of *C-EEVi*

The questionnaire will be conducted with approval from Ethics and Research Governance (ERGO) under reference number $ERGO/FPSE/23974$.

D.1 General Information and Technical Background

QD.1.1 What is your age-group?

QD.1.2 Which company or organisation do you for work for? (If you are studying, please mention the name of the university.)

QD.1.3 Do you have any experience in the fields of Cyber-Security or Visualisation Design (HCI)? Please rate the scale of your knowledge or experience on a scale of 1-5? (1-low and 5-high).

QD.1.4 Please briefly mention your area of expertise in the field selected in the previous question.

QD.1.5 How many years of experience do you have in the field you mentioned above?

QD.1.6 Have you ever used any cyber-security visualisation tool or software? If yes, Please specify.

D.2 Structure of Model

This section represents *EEVi* - a model developed to aid in the design and evaluation process of cyber-security visualisations, with a view to make them more effective for cyber-security analysts. A visualisation is considered *effective* if the characteristics of the visualisation are essential for an analyst to competently perform a certain task.

Please look at the structure of the model (Figure 4.1(b)) and answer the following questions:

QD.2.1 Does this structure make sense logically?

QD.2.2 Does the structure match a logical flow of how tasks are formed at your organisation?

D.3 Component Tasks of ***EEVi***

This section represents component tasks of the model, *EEVi*. Please look at the component tasks in terms of the model and answer the questions.

This section has 8 component tasks which represent the task and the aspects that would make the task *effective*.

Triage Analysis

Please look at the following analysis (Figure 4.4(b)) and answer the questions below based on this.

Definitions

- Triage Analysis - It is the first look at data, false positives are weeded out for further analysis, within an order of a few minutes;
- Raw Data - The most elemental data, usually in very large quantity and is passed through automated process to filter;
- Interesting Activity - Data that has been flagged by an automated processes on Raw Data and is inspected by an analyst, usually consists of a large number of false positives;
- Real-Time Analyst - Performs Triage Analysis;
- Filter - Allows the ability to easily filter, join or transform data without changing the original. Also allows the ability to filter noise to allow an analyst to see trends;
- Situational Awareness - An accurate picture of external and internal information in an overview to understand the state of all resources;
- Real-Time Access - Viewing real-time data within seconds to minutes of an event;
- Alerts - A system to alert the user of the status of an activity being investigated;

- Colour Highlighting - Using colour to highlight the risk level of activity to bring it to the attention of a user.

QD.3.1.1 Do the features of visualisation make sense for the task?

QD.3.1.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA
Filter	○	○	○	○	○	○
Situational Awareness	○	○	○	○	○	○
Real-Time Access	○	○	○	○	○	○
Alerts	○	○	○	○	○	○
Colour Highlighting	○	○	○	○	○	○

QD.3.1.3 Have all important features for the task at hand been covered?

Escalation Analysis

Please look at the following analysis (Figure 4.5(b)) and answer the questions below based on this.

Definitions

- Escalation Analysis - It is the investigation of suspicious activities and production of reports;
- Suspicious Activity - Data that is anomalous after the initial TA and needs to be monitored;
- Incident - The point when the occurrence and seriousness of an activity is confirmed and formally reported;
- Lead Analyst - Performs Escalation Analysis;
- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems;
- Collaboration - Enable users to communicate and collaborate with other analysts by sharing findings and other information;

- Interoperation - Ability to work efficiently with other tools, applications, utilities or data-sets;
- Reporting - Provide support for report building;
- Priorities - Using a priority system to inform the user of the severity of an attack.

QD.3.2.1 Do the features of visualisation make sense for the task?

QD.3.2.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA
Collaboration	○	○	○	○	○	○
Interoperation	○	○	○	○	○	○
Reporting	○	○	○	○	○	○
Priorities	○	○	○	○	○	○

QD.3.2.3 Have all important features for the task at hand been covered?

Correlation Analysis

Please look at the following analysis (Figure 4.6(b)) and answer the questions below based on this.

Definitions

- Correlation Analysis - It is the search for previously unrecognised patterns and trends in data;
- Intrusion Set - Sets of related Incidents that are given an increase in attention and resources to detect, understand and respond;
- Site-Specific Analyst - Performs Correlation Analysis;
- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems;
- Flexibility - Gives the ability to manipulate the focal point and support the analytical process;
- Timeline - Order of events and activities that have taken place over a period of time, used to coordinate all views;

- Investigatory Capabilities - Allow users to investigate data by supporting providing platform for rapid, open-ended foraging activities.

QD.3.3.1 Do the features of visualisation make sense for the task?

QD.3.3.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA
Flexibility	○	○	○	○	○	○
Timeline	○	○	○	○	○	○
Investigatory Capabilities	○	○	○	○	○	○

QD.3.3.3 Have all important features for the task at hand been covered?

Threat Analysis

Please look at the following analysis (Figure 4.7(b)) and answer the questions below based on this.

Definitions

- Threat Analysis - It is an intelligent analysis to profile attackers and their motivations using additional sources;
- Intrusion Set - Sets of related Incidents that are given an increase in attention and resources to detect, understand and respond;
- Threat Analyst - Performs Threat Analysis;
- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems;
- Strategic Analyst - Works at the community level to understand the implications of an attack and categorise it;
- Correlation - Displays relationships between different data dimensions;
- Interoperation - Ability to work efficiently with other tools, applications, utilities or data-sets;
- Priorities - Using a priority system to inform a user of the severity of an attack;
- Collaboration - Enable users to communicate and collaborate with other analysts by sharing findings and other information.

QD.3.4.1 Do the features of visualisation make sense for the task?

QD.3.4.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA
Correlation	○	○	○	○	○	○
Interoperation	○	○	○	○	○	○
Priorities	○	○	○	○	○	○
Collaboration	○	○	○	○	○	○

QD.3.4.3 Have all important features for the task at hand been covered?

Impact Assessment

Please look at the following analysis (Figure 4.8(b)) and answer the questions below based on this.

Definitions

- Impact Assessment - It is the task to identify impact, damage and critical nodes that may be compromised or potentially reachable after a breach;
- Source Data - Data gathered from an intrusion used for further analysis or reporting;
- IT Manager - Identifies impact damage after an intrusion and executes training and development;
- Impact Identification - The identification of vulnerabilities, malicious users or external source of attacks, the intended target of attacks and/or main resources of the system affected;
- Situational Awareness - An accurate picture of external and internal information in an overview to understand the state of all resources;
- Reporting - Provide support for report building.

QD.3.5.1 Do the features of visualisation make sense for the task?

QD.3.5.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA

Impact Identification	○	○	○	○	○	○
Situational Awareness	○	○	○	○	○	○
Reporting	○	○	○	○	○	○

QD.3.5.3 Have all important features for the task at hand been covered?

Incident Response Analysis

Please look at the following analysis (Figure 4.9(b)) and answer the questions below based on this.

Definitions

- Incident Response Analysis - It is a recommendation or implementation of action against a confirmed incident;
- Intrusion Set - Sets of related Incidents that are given an increase in attention and resources to detect, understand and respond;
- Incident Handler/Responder - Performs Incident Response Analysis;
- Tactical Defender - Defends against current and immediate attacks by maintaining situational awareness and rapid remediation of problems;
- Strategic Analyst - Works at the community level to understand the implications of an attack and categorise it;
- Mitigation - Performs clean-up and containment and provides support for mitigation activities;
- Interoperation - Ability to work efficiently with other tools, applications, utilities or data-sets;
- Reporting - Provide support for report building;
- Situational Awareness - An accurate picture of external and internal information in an overview to understand the state of all resources;
- Collaboration - Enable users to communicate and collaborate with other analysts by sharing findings and other information.

QD.3.6.1 Do the features of visualisation make sense for the task?

QD.3.6.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA
Mitigation	○	○	○	○	○	○
Interoperation	○	○	○	○	○	○
Reporting	○	○	○	○	○	○
Situational Awareness	○	○	○	○	○	○
Collaboration	○	○	○	○	○	○

QD.3.6.3 Have all important features for the task at hand been covered?

Forensic Analysis

Please look at the following analysis (Figure 4.10(b)) and answer the questions below based on this.

Definitions

- Forensic Analysis - It is when an analyst gathers and preserves data to inform and support law enforcement agencies;
- Source Data - Data gathered from an intrusion used for further analysis or reporting;
- Security Regulations - Regulations defined by the government or organisations relating to cyber-security, also includes cyber law;
- Forensic Analyst - Performs Forensic Analysis;
- Case-Building Capabilities - Provides support to a user for the purpose of building a case.
- Reporting - Provide support for report building;
- Chain of Custody - Maintains a log of users who have analysed data or had access to data from an incident.
- Interoperation - Ability to work efficiently with other tools, applications, utilities or data-sets;

QD.3.7.1 Do the features of visualisation make sense for the task?

QD.3.7.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA
Case-Building Capabilities	○	○	○	○	○	○
Reporting	○	○	○	○	○	○
Chain of Custody	○	○	○	○	○	○
Interoperation	○	○	○	○	○	○

QD.3.7.3 Have all important features for the task at hand been covered?

Security Quality Management

Please look at the following analysis (Figure 4.11(b)) and answer the questions below based on this.

Definitions

- Security Quality Management - It is the task related to services, like tutorials or training, that maintain the quality of information security in an organisation;
- Source Data - Data gathered from an intrusion used for further analysis or reporting;
- Security Regulations - Regulations defined by the government or organisations relating to cyber-security, also includes cyber law;
- IT Manager - Identifies impact damage after an intrusion and executes training and development;
- Feedback - Provides feedback (to a manager) for tasks performed, could be quantitive or qualitative.
- Reporting - Provide support for report building;

QD.3.8.1 Do the features of visualisation make sense for the task?

QD.3.8.2 According to you, are the characteristics of visualisation appropriate for the task at hand? (If a characteristic is not critical for a task to be effective, please select NA)

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA

Feedback Capabilities	○	○	○	○	○	○
Reporting	○	○	○	○	○	○

QD.3.8.3 Have all important features for the task at hand been covered?

D.4 After Thoughts

QD.4.1 Do you think that visualisations should have any of these general characteristics of visualisation in cyber-security for all tasks? Please select all the characteristics that would be useful.

□ Reporting - Provide support for report building;

□ Interoperation - Ability to work efficiently with other tools, applications, utilities or data-sets;

□ Collaboration - Enable users to communicate and collaborate with other analysts by sharing findings and other information;

□ Flexibility - Gives the ability to manipulate the focal point and support the analytical process;

□ Situational Awareness - An accurate picture of external and internal information in an overview to understand the state of all resources;

□ Filter - Allows the ability to easily filter, join or transform data without changing the original. Also allows the ability to filter noise to allow an analyst to see trends.

□ Other

QD.4.2 Do you think this model represents good fundamental guidelines for cyber-security visualisation?

QD.4.3 Do you think the model is useful to evaluate the effectiveness of cyber-security visualisation for the component tasks?

QD.4.4 Do you have any further comments?

Appendix E

Ratings for Characteristics of Visualisation for Each Component Task by Questionnaire Respondents

The following tables (Table E.1 to Table E.15) present the ratings given to characteristics of visualisation of all component tasks, by participants of the questionnaire in Chapter 5.

These quantification of these ratings are used in Section 5.3.2 to revise the component tasks of *EEVi*. Additionally, they are also used in Appendix G to calculate the comparison matrices to be able to perform AHP, for the development of *C-EEVi*.

In Table E.1, the ratings for 'Triage Analysis' (TA) are presented for characteristics of visualisation: Filter (TA-Filter), Situational Awareness (TA-SA), Real-Time Access (TA-RTA), Alerts (TA-Alerts) and Colour Highlighting (TA-CH). Table E.2 represents the quantified ratings from Table E.1 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.1 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.3, the ratings for 'Escalation Analysis' (EA) are presented for characteristics of visualisation: Collaboration (EA-C), Interoperation (EA-I), Reporting (EA-R) and Priorities (EA-P). Table E.4 represents the quantified ratings from Table E.3 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.2 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.5, the ratings for 'Correlation Analysis' (CA) are presented for characteristics of visualisation: Flexibility (CA-Fl), Timeline (CA-T) and Investigatory Capabilities (CA-IC). Table E.6 represents the quantified ratings from Table E.5 on a scale of -2

(Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.3 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.7, the ratings for 'Threat Analysis' (ThA) are presented for characteristics of visualisation: Correlation (ThA-Cor), Interoperation (ThA-I), Priorities (ThA-P) and Collaboration (ThA-C). Table E.8 represents the quantified ratings from Table E.7 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.4 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.9, the ratings for 'Impact Assessment' (IA) are presented for characteristics of visualisation: Impact Identification (IA-II), Situational Awareness (IA-SA) and Reporting (IA-R). Table E.10 represents the quantified ratings from Table E.9 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.5 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.11, the ratings for 'Incident Response Analysis' (IRA) are presented for characteristics of visualisation: Mitigation (IRA-M), Interoperation (IRA-I), Reporting (IRA-R), Situational Awareness (IRA-SA) and Collaboration (IRA-C). Table E.12 represents the quantified ratings from Table E.11 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.6 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.13, the ratings for 'Forensic Analysis' (FA) are presented for characteristics of visualisation: Case Building Capabilities (FA-CBC), Reporting (FA-R), Chain of Custody (FA-CoC) and Interoperation (FA-I). Table E.14 represents the quantified ratings from Table E.13 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.7 to perform statistical analysis to demonstrate that the ratings were overall positive.

In Table E.15, the ratings for 'Security Quality Management' (SQM) are presented for characteristics of visualisation: Feedback (SQM-Fe) and Reporting (SQM-R). Table E.16 represents the quantified ratings from Table E.15 on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree), used in Section 5.3.2.8 to perform statistical analysis to demonstrate that the ratings were overall positive.

Table E.1: Ratings for the overall task and *Characteristics of Visualisation* for 'Triage Analysis' from each respondent from Strongly Disagree to Strongly Agree

Respondent	TA-Filter	TA-SA	TA-RTA	TA-Alerts	TA-CH
(1)	Agree	Agree	Agree	Agree	Agree
(2)	Agree	Agree	Agree	Agree	Agree
(3)	Neutral	Agree	Agree	Neutral	Agree
(4)	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Agree
(5)	Agree	Strongly Agree	Agree	Agree	Agree
(6)	Neutral	Agree	Neutral	Agree	Strongly Agree
(7)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Agree	Strongly Agree	Agree	Agree	Neutral
(9)	Strongly Agree	Strongly Agree	Agree	Neutral	Strongly Agree
(10)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(11)	Agree	Disagree	Neutral	Neutral	Disagree
(12)	Agree	Strongly Agree	Agree	Agree	Agree
(13)	Strongly Agree	Strongly Agree	Agree	Agree	Agree
(14)	Strongly Agree	Strongly Agree	Neutral	Neutral	Strongly Agree
(15)	Agree	Agree	Strongly Agree	Strongly Agree	NA
(16)	Agree	Agree	Agree	Agree	Agree
(17)	Neutral	Strongly Agree	Strongly Agree	Agree	Agree
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(19)	Strongly Agree	Strongly Agree	Agree	Disagree	Disagree
(20)	Strongly Agree	Agree	Agree	Strongly Agree	Neutral
(21)	Agree	Agree	Agree	Strongly Agree	Strongly Agree
(22)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Strongly Agree
(24)	Agree	Neutral	Agree	Neutral	Strongly Agree
(25)	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Agree	Agree	Neutral	Neutral
(27)	Agree	Agree	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Neutral	Strongly Agree	Strongly Agree	Agree	Agree
(30)	Strongly Agree	Neutral	Agree	Neutral	Agree

Table E.2: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Triage Analysis' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	TA-Filter	TA-SA	TA-RTA	TA-Alerts	TA-CH	Overall Mean
(1)	1	1	1	1	1	1
(2)	1	1	1	1	1	1
(3)	0	1	1	0	1	0.6
(4)	2	1	2	2	1	1.6
(5)	1	2	1	1	1	1.2
(6)	0	1	0	1	2	0.8
(7)	2	2	2	2	2	2
(8)	1	2	1	1	0	1
(9)	2	2	1	0	2	1.4
(10)	2	2	2	2	1	1.8
(11)	1	-1	0	0	-1	-0.2
(12)	1	2	1	1	1	1.2
(13)	2	2	1	1	1	1.4
(14)	2	2	0	0	2	1.2
(15)	1	1	2	2	0	1.2
(16)	1	1	1	1	1	1
(17)	0	2	2	1	1	1.2
(18)	2	2	2	2	1	1.8
(19)	2	2	1	-1	-1	0.6
(20)	2	1	1	2	0	1.2
(21)	1	1	1	2	2	1.4
(22)	2	2	2	2	2	2
(23)	2	2	2	0	2	1.6
(24)	1	0	1	0	2	0.8
(25)	2	1	2	2	2	1.8
(26)	1	1	1	0	0	0.6
(27)	1	1	1	1	1	1
(28)	2	2	2	2	2	2
(29)	0	2	2	1	1	1.2
(30)	2	0	1	0	1	0.8
Mean	1.33	1.37	1.27	1.00	1.07	1.21

Table E.3: Ratings for the overall task and *Characteristics of Visualisation* for 'Escalation Analysis' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	EA-C	EA-I	EA-R	EA-P
(1)	Agree	Agree	Agree	Agree	Agree
(2)	Agree	Agree	Agree	Agree	Agree
(3)	Agree	Agree	NA	Disagree	Agree
(4)	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree
(5)	Strongly Agree	Agree	Agree	Strongly Agree	Agree
(6)	Agree	Agree	Agree	Strongly Agree	Strongly Agree
(7)	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Agree	Agree	Strongly Agree	Agree	Strongly Agree
(9)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(10)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(11)	Neutral	Agree	Strongly Agree	Disagree	Neutral
(12)	Agree	Strongly Agree	Agree	Agree	Agree
(13)	Agree	Strongly Agree	Agree	Agree	Strongly Agree
(14)	Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
(15)	Agree	Agree	Agree	Agree	Agree
(16)	Agree	Agree	Agree	Agree	Agree
(17)	Neutral	Agree	Neutral	Agree	Strongly Agree
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Agree	Neutral	Agree	Agree	Agree
(20)	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(21)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(22)	Strongly Agree	NA	NA	Strongly Agree	Strongly Agree
(23)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(24)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(25)	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Strongly Agree	Agree	Agree	Strongly Agree
(27)	Agree	Agree	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Agree	Agree	Agree	Agree	Agree
(30)	Agree	Strongly Agree	Agree	Agree	Strongly Agree

Table E.4: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Escalation Analysis' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	EA-C	EA-I	EA-R	EA-P	Overall Mean
(1)	1	1	1	1	1
(2)	1	1	1	1	1
(3)	1	0	-1	1	0.25
(4)	2	2	1	2	1.75
(5)	1	1	2	1	1.25
(6)	1	1	2	2	1.5
(7)	1	2	2	2	1.75
(8)	1	2	1	2	1.5
(9)	2	2	2	2	2
(10)	2	2	2	2	2
(11)	1	2	-1	0	0.5
(12)	2	1	1	1	1.25
(13)	2	1	1	2	1.5
(14)	2	1	2	2	1.75
(15)	1	1	1	1	1
(16)	1	1	1	1	1
(17)	1	0	1	2	1
(18)	2	2	2	2	2
(19)	0	1	1	1	0.75
(20)	1	2	2	2	1.75
(21)	2	2	2	2	2
(22)	0	0	2	2	1
(23)	2	2	2	2	2
(24)	2	2	2	2	2
(25)	1	2	2	2	1.75
(26)	2	1	1	2	1.5
(27)	1	1	1	1	1
(28)	2	2	2	2	2
(29)	1	1	1	1	1
(30)	2	1	1	2	1.5
Mean	1.37	1.33	1.33	1.60	1.41

Table E.5: Ratings for the overall task and *Characteristics of Visualisation* for 'Correlation Analysis' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	CA-Fl	CA-T	CA-IC
(1)	Agree	Strongly Agree	Agree	Strongly Agree
(2)	Agree	Agree	Agree	Agree
(3)	Agree	Neutral	Disagree	Disagree
(4)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(5)	Strongly Agree	Agree	Strongly Agree	Agree
(6)	Agree	Agree	Strongly Agree	Agree
(7)	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Strongly Agree	Strongly Agree	Agree	Strongly Agree
(9)	Strongly Agree	Agree	Strongly Agree	Strongly Agree
(10)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(11)	Agree	Neutral	NA	Disagree
(12)	Strongly Agree	Strongly Agree	Agree	Agree
(13)	Agree	Agree	Agree	Strongly Agree
(14)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(15)	Agree	Agree	Strongly Agree	Strongly Agree
(16)	Agree	Agree	Agree	Agree
(17)	Strongly Agree	Agree	Agree	Strongly Agree
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Agree	Disagree	Strongly Agree	Strongly Agree
(20)	Agree	Agree	Strongly Agree	Strongly Agree
(21)	Agree	Neutral	Strongly Agree	Strongly Agree
(22)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Neutral	Strongly Agree	Strongly Agree	Neutral
(24)	Agree	Agree	Agree	Neutral
(25)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Neutral	Agree	Agree
(27)	Agree	Agree	Agree	Agree
(28)	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Agree	Strongly Agree	Neutral	Agree
(30)	Agree	Agree	Strongly Agree	Neutral

Table E.6: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Correlation Analysis' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	CA-Fl	CA-T	CA-IC	Overall Mean
(1)	2	1	2	1.67
(2)	1	1	1	1
(3)	0	0	-1	-0.33
(4)	2	2	2	2
(5)	1	2	1	1.33
(6)	1	2	1	1.33
(7)	2	2	2	2
(8)	2	1	2	1.67
(9)	1	2	2	1.67
(10)	2	2	2	2
(11)	0	0	-1	-0.33
(12)	2	1	1	1.33
(13)	1	1	2	1.33
(14)	2	2	2	2
(15)	1	2	2	1.67
(16)	1	1	1	1
(17)	1	1	2	1.33
(18)	2	2	2	2
(19)	-1	2	2	1
(20)	1	2	2	1.67
(21)	0	2	2	1.33
(22)	2	2	2	2
(23)	2	2	0	1.33
(24)	1	1	0	0.67
(25)	2	2	2	2
(26)	0	1	1	0.67
(27)	1	1	1	1
(28)	2	2	2	2
(29)	2	0	1	1
(30)	1	2	0	1
Mean	1.23	1.47	1.33	1.34

Table E.7: Ratings for the overall task and *Characteristics of Visualisation* for 'Threat Analysis' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	ThA-Cor	ThA-I	ThA-P	ThA-C
(1)	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(2)	Agree	Agree	Agree	Agree	Agree
(3)	Agree	Strongly Agree	Strongly Agree	Neutral	Agree
(4)	Agree	Agree	Neutral	Agree	Agree
(5)	Strongly Agree	Strongly Agree	Agree	Agree	Agree
(6)	Agree	Agree	Agree	Agree	Strongly Agree
(7)	Agree	Neutral	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Agree	Strongly Agree	Strongly Agree	Agree	Agree
(9)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(10)	Neutral	Neutral	Neutral	Neutral	Neutral
(11)	Disagree	Neutral	Agree	Agree	Neutral
(12)	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
(13)	Agree	Agree	Agree	Strongly Agree	Strongly Agree
(14)	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(15)	Agree	Agree	Agree	Strongly Agree	Strongly Agree
(16)	Agree	Agree	Agree	Agree	Agree
(17)	Agree	Strongly Agree	Strongly Agree	Agree	Agree
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Strongly Agree	Disagree	Strongly Agree	Agree	Agree
(20)	Agree	Strongly Agree	Agree	Agree	Strongly Agree
(21)	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Agree
(22)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Agree	Strongly Agree	Strongly Agree	Disagree	Disagree
(24)	Agree	Strongly Agree	Agree	Neutral	Agree
(25)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Agree	Agree	Agree	Neutral
(27)	Agree	Agree	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Strongly Agree
(30)	Agree	Agree	Agree	Strongly Agree	Agree

Table E.8: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Threat Analysis' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	ThA-Cor	ThA-I	ThA-P	ThA-C	Overall Mean
(1)	2	2	2	1	1.75
(2)	1	1	1	1	1
(3)	2	0	0	1	0.75
(4)	1	0	1	1	0.75
(5)	2	1	1	1	1.25
(6)	1	1	1	2	1.25
(7)	0	2	2	2	1.5
(8)	2	2	1	1	1.5
(9)	2	2	2	2	2
(10)	0	0	0	0	0
(11)	0	1	1	0	0.5
(12)	2	1	2	2	1.75
(13)	1	1	2	2	1.5
(14)	2	2	2	1	1.75
(15)	1	1	2	2	1.5
(16)	1	1	1	1	1
(17)	2	2	1	1	1.5
(18)	2	2	2	2	2
(19)	-1	2	1	1	0.75
(20)	2	1	1	2	1.5
(21)	2	1	2	1	1.5
(22)	2	2	2	2	2
(23)	2	2	-1	-1	0.5
(24)	2	1	0	1	1
(25)	2	2	2	2	2
(26)	1	1	1	0	0.75
(27)	1	1	1	1	1
(28)	2	2	2	2	2
(29)	2	2	0	2	1.5
(30)	1	1	2	1	1.25
Mean	1.40	1.33	1.23	1.23	1.30

Table E.9: Ratings for the overall task and *Characteristics of Visualisation* for 'Impact Assessment' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	IA-II	IA-SA	IA-R
(1)	Agree	Agree	Strongly Agree	Agree
(2)	Agree	Agree	Agree	Agree
(3)	Agree	Neutral	Disagree	Agree
(4)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(5)	Strongly Agree	Agree	Strongly Agree	Strongly Agree
(6)	Agree	Strongly Agree	Agree	Agree
(7)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(9)	NA	NA	NA	NA
(10)	Agree	Agree	Agree	Agree
(11)	Disagree	Agree	Neutral	Strongly Agree
(12)	Agree	Agree	Agree	Strongly Agree
(13)	Agree	Agree	Strongly Agree	Agree
(14)	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(15)	Agree	Strongly Agree	Strongly Agree	Agree
(16)	Agree	Agree	Agree	Agree
(17)	NA	NA	NA	NA
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(20)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(21)	Agree	Strongly Agree	Agree	Strongly Agree
(22)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Agree	Strongly Agree	Agree	Agree
(24)	Agree	Agree	Neutral	Neutral
(25)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Agree	Neutral	Agree
(27)	Agree	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Neutral	Neutral	Neutral	Neutral
(30)	Strongly Agree	Strongly Agree	Agree	Agree

Table E.10: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Impact Assessment' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	IA-II	IA-SA	IA-R	Overall Mean
(1)	1	2	1	1.33
(2)	1	1	1	1
(3)	0	0	1	0.33
(4)	2	2	2	2
(5)	1	2	2	1.67
(6)	2	1	1	1.33
(7)	2	2	2	2
(8)	2	2	1	1.67
(9)	0	0	0	0
(10)	1	1	1	1
(11)	1	0	2	1
(12)	1	1	2	1.33
(13)	1	2	1	1.33
(14)	2	2	2	2
(15)	2	2	1	1.67
(16)	1	1	1	1
(17)	0	0	0	0
(18)	2	2	2	2
(19)	2	2	2	2
(20)	2	2	2	2
(21)	2	1	2	1.67
(22)	2	2	2	2
(23)	2	1	1	1.33
(24)	1	0	0	0.33
(25)	2	2	2	2
(26)	1	0	1	0.67
(27)	1	1	1	1
(28)	2	2	2	2
(29)	0	0	0	0
(30)	2	1	1	1.33
Mean	1.37	1.23	1.30	1.30

Table E.11: Ratings for the overall task and *Characteristics of Visualisation* for 'Incident Response Analysis' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	IRA-M	IRA-I	IRA-R	IRA-SA	IRA-C
(1)	Agree	Agree	Strongly Agree	Agree	Agree	Agree
(2)	Agree	Agree	Agree	Agree	Agree	Agree
(3)	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(4)	NA	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
(5)	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Agree
(6)	Agree	Agree	Agree	Agree	Strongly Agree	Strongly Agree
(7)	Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Strongly Agree	Strongly Agree	Strongly Agree	Agree	Agree	Strongly Agree
(9)	NA	NA	NA	NA	NA	NA
(10)	NA	NA	NA	NA	NA	NA
(11)	Disagree	Neutral	Strongly Disagree	Agree	Disagree	Strongly Agree
(12)	Agree	Agree	Strongly Agree	Agree	Agree	Agree
(13)	Agree	Neutral	Agree	Agree	Strongly Agree	Strongly Agree
(14)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(15)	Agree	Strongly Agree	Agree	Agree	Strongly Agree	Strongly Agree
(16)	Agree	Agree	Agree	Agree	Agree	Agree
(17)	NA	NA	NA	NA	NA	NA
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree	Strongly Agree
(20)	Neutral	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Neutral
(21)	Neutral	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Neutral
(22)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Neutral	Disagree
(24)	Agree	Strongly Agree	Strongly Agree	Agree	Neutral	Neutral
(25)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Neutral	Agree	Agree	Neutral	Agree
(27)	Agree	Agree	Agree	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Agree	Agree	NA	Agree	Strongly Agree	Strongly Agree
(30)	Agree	Strongly Agree	NA	Neutral	Agree	Agree

Table E.12: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Incident Response Analysis' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	Overall	IRA-M	IRA-I	IRA-R	IRA-SA	IRA-C
(1)	1	2	1	1	1	1.2
(2)	1	1	1	1	1	1
(3)	1	2	2	2	1	1.6
(4)	2	2	1	2	2	1.8
(5)	2	1	2	2	1	1.6
(6)	1	1	1	2	2	1.4
(7)	1	2	2	2	2	1.8
(8)	2	2	1	1	2	1.6
(9)	0	0	0	0	0	0
(10)	0	0	0	0	0	0
(11)	0	-2	1	-1	2	0
(12)	1	2	1	1	1	1.2
(13)	0	1	1	2	2	1.2
(14)	2	2	2	2	2	2
(15)	2	1	1	2	2	1.6
(16)	1	1	1	1	1	1
(17)	0	0	0	0	0	0
(18)	2	2	2	2	2	2
(19)	2	1	2	2	2	1.8
(20)	2	2	2	0	0	1.2
(21)	2	2	2	0	0	1.2
(22)	2	2	2	2	2	2
(23)	2	2	2	0	-1	1
(24)	2	2	1	0	0	1
(25)	2	2	2	2	2	2
(26)	0	1	1	0	1	0.6
(27)	1	1	1	1	1	1
(28)	2	2	2	2	2	2
(29)	1	0	1	2	2	1.2
(30)	2	0	0	1	1	0.8
Mean	1.30	1.23	1.27	1.13	1.20	1.23

Table E.13: Ratings for the overall task and *Characteristics of Visualisation* for 'Forensic Analysis' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	FA-CBC	FA-R	FA-CoC	FA-I
(1)	Agree	Agree	Agree	Agree	Strongly Agree
(2)	Agree	Agree	Agree	Agree	Agree
(3)	Disagree	Neutral	Agree	Neutral	Agree
(4)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(5)	NA	NA	NA	NA	NA
(6)	Neutral	Agree	Agree	Agree	Agree
(7)	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(8)	Agree	Strongly Agree	Agree	Agree	Strongly Agree
(9)	NA	NA	NA	NA	NA
(10)	Agree	Agree	Agree	Agree	Agree
(11)	Neutral	Agree	Disagree	Neutral	Neutral
(12)	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Agree
(13)	Agree	Agree	Agree	Strongly Agree	Agree
(14)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(15)	Agree	Agree	Agree	Strongly Agree	Agree
(16)	Agree	Agree	Agree	Agree	Agree
(17)	NA	NA	NA	NA	NA
(18)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Agree	Agree	Strongly Agree	Agree	Agree
(20)	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Neutral
(21)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Agree
(22)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Agree	Strongly Agree	Strongly Agree	Strongly Agree	Neutral
(24)	Agree	Agree	Agree	Agree	Neutral
(25)	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Neutral	Agree	Agree	Agree
(27)	Agree	Agree	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
(29)	Strongly Agree	Neutral	Agree	Strongly Agree	Agree
(30)	Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree

Table E.14: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Forensic Analysis' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	FA-CBC	FA-R	FA-CoC	FA-I	Overall Mean
(1)	1	1	1	2	1.25
(2)	1	1	1	1	1
(3)	0	0	0	1	0.25
(4)	2	2	2	2	2
(5)	0	0	0	0	0
(6)	1	1	1	1	1
(7)	2	2	2	2	2
(8)	2	1	1	2	1.5
(9)	0	0	0	0	0
(10)	1	1	1	1	1
(11)	1	-1	0	0	0
(12)	2	1	2	1	1.5
(13)	1	1	2	1	1.25
(14)	2	2	2	2	2
(15)	1	1	2	1	1.25
(16)	1	1	1	1	1
(17)	0	0	0	0	0
(18)	2	2	2	2	2
(19)	1	2	1	1	1.25
(20)	2	2	2	0	1.5
(21)	2	2	2	1	1.75
(22)	2	2	2	2	2
(23)	2	2	2	0	1.5
(24)	1	1	1	0	0.75
(25)	2	2	2	2	2
(26)	0	1	1	1	0.75
(27)	1	1	1	1	1
(28)	2	1	2	2	1.75
(29)	0	1	2	1	1
(30)	2	2	1	2	1.75
Mean	1.23	1.17	1.30	1.10	1.20

Table E.15: Ratings for the overall task and *Characteristics of Visualisation* for 'Security Quality Management' from each respondent from Strongly Disagree to Strongly Agree

Respondent	Overall	SQM-Fe	SQM-R
(1)	Agree	Agree	Agree
(2)	Agree	Agree	Agree
(3)	NA	Agree	Agree
(4)	Agree	Strongly Agree	Agree
(5)	NA	NA	NA
(6)	Neutral	Neutral	Neutral
(7)	Agree	NA	Strongly Agree
(8)	Agree	Strongly Agree	Neutral
(9)	NA	NA	NA
(10)	Neutral	Neutral	Neutral
(11)	Disagree	Agree	Neutral
(12)	Agree	Strongly Agree	Strongly Agree
(13)	Agree	Neutral	Agree
(14)	Strongly Agree	Strongly Agree	Strongly Agree
(15)	Agree	Agree	Strongly Agree
(16)	Agree	Agree	Agree
(17)	NA	NA	NA
(18)	Strongly Agree	Strongly Agree	Strongly Agree
(19)	Neutral	Disagree	Neutral
(20)	Strongly Agree	Strongly Agree	Strongly Agree
(21)	Strongly Agree	Strongly Agree	Strongly Agree
(22)	Strongly Agree	Strongly Agree	Strongly Agree
(23)	Strongly Agree	Strongly Agree	Strongly Agree
(24)	Strongly Agree	Strongly Agree	Strongly Agree
(25)	Strongly Agree	Strongly Agree	Strongly Agree
(26)	Agree	Agree	Agree
(27)	Agree	Agree	Agree
(28)	Strongly Agree	Strongly Agree	Strongly Agree
(29)	Strongly Agree	Strongly Agree	Strongly Agree
(30)	Agree	NA	NA

Table E.16: Quantified ratings and averages for the overall task and *Characteristics of Visualisation* for 'Security Quality Management' from each respondent on a scale of -2 (Strongly Disagree) to 2 (Strongly Agree)

Respondent	SQM-Fe	SQM-R	Overall Mean
(1)	1	1	1
(2)	1	1	1
(3)	1	0	0.5
(4)	2	1	1.5
(5)	0	0	0
(6)	0	0	0
(7)	0	2	1
(8)	2	0	1
(9)	0	0	0
(10)	0	0	0
(11)	1	0	0.5
(12)	2	2	2
(13)	0	1	0.5
(14)	2	2	2
(15)	1	2	1.5
(16)	1	1	1
(17)	0	0	0
(18)	2	2	2
(19)	-1	0	-0.5
(20)	2	2	2
(21)	2	2	2
(22)	2	2	2
(23)	2	2	2
(24)	2	2	2
(25)	2	2	2
(26)	1	1	1
(27)	1	1	1
(28)	2	2	2
(29)	2	2	2
(30)	0	0	0
Mean	1.10	1.10	1.10

Appendix F

Real World Utilisation Interview Format

The interviews were conducted with approval from Ethics and Research Governance (ERGO) under reference number $ERGO/FPSE/23974$.

F.1 Cyber-Security Analysts

The semi-structured interview was divided into four sections:

F.1.1 General Information and Technical Background

QF.1.1.1 Which company or organisation do you for work for? (If you are studying, please mention the name of the university.)

QF.1.1.2 What is your area of expertise?

QF.1.1.3 How many years of experience do you have in your area?

QF.1.1.4 Do you have any experience of performing Escalation Analysis (is the investigation of suspicious activities and production of reports)? If yes, how would you rate your expertise from 1 to 5?

QF.1.1.5 Have you ever used any cyber-security visualisation tool or solution in the past?

If yes, Have you used it for Escalation Analysis? Please name the solution. What did you think about the solution? In what way could it have been better? Did it provide the right functionality to be able to perform the task effectively?

F.1.2 Escalation Analysis Mockup

Discuss the following questions on the basis of the user interface mockups presented in Figure 6.3.

QF.1.2.1 Does this visualisation solution mockup make sense for Escalation Analysis? Explain.

QF.1.2.2 Is the data sufficient to perform the Escalation Analysis? Explain.

QF.1.2.3 Do you require any more visualisation characteristics or interaction techniques for this visualisation to be effective for performing Escalation Analysis? Explain.

QF.1.2.4 Did you notice these characteristics or interaction techniques? Would you be able to use each for EA? (Rate from Very well implemented, well implemented, neutral, not well implemented, not at all implemented)

○ Collaboration

○ Interoperation

○ Reporting

○ Priorities

QF.1.2.5 Would you like to add anything else for Escalation Analysis?

QF.1.2.6 If this was available as a visualisation solution to perform Escalation Analysis, would you or your organisation use it? (not considering costs/fees/etc)

F.1.3 Work Domain Analysis (WDA) for Escalation Analysis

Discuss the following questions on the basis of the work domain analysis diagram for *EEVI* presented in Figure 6.1 and work domain analysis diagram for 'Escalation Analysis' presented in Figure 6.2.

QF.1.3.1 Do you think this WDA diagram represents EEVi and the mock-up derived from it? Explain.

QF.1.3.2 Do you think you can use this WDA diagram to explain to visualisation designers what your needs are? Explain.

F.1.4 After Thoughts

QF.1.4.1 What general features do you think that every solution should have for any task, like collaboration or reporting?

QF.1.4.2 Is there anything else you would like to add in the end?

F.2 Visualisation Designers

The semi-structured interview was divided into four sections:

F.2.1 General Information and Technical Background

QF.2.1.1 Which company or organisation do you for work for? (If you are studying, please mention the name of the university.)

QF.2.1.2 What is your area of expertise?

QF.2.1.3 How many years of experience do you have in your area?

QF.2.1.4 Have you ever used or designed any cyber-security visualisation tool or solution in the past?

F.2.2 Work Domain Analysis (WDA) for Escalation Analysis

Discuss the following questions on the basis of the work domain analysis diagram for *EEVI* presented in Figure 6.1 and work domain analysis diagram for 'Escalation Analysis' presented in Figure 6.2.

QF.2.2.1 Does the WDA diagram look like it is derived from EEVi? Explain.

QF.2.2.2 Given this WDA diagram, can you use it to design a tool or solution? Explain.

QF.2.2.3 Given this WDA diagram, can you use it to have an informative conversation regarding cyber-security analysts needs? Explain.

F.2.3 Escalation Analysis Mockup

Discuss the following questions on the basis of the user interface mockups presented in Figure 6.3.

QF.2.3.1 Does the Mock-up follow from the WDA diagram and include all the requirements for EA?

QF.2.3.2 Did you notice these characteristics or interaction techniques? Would you be able to implement each for EA? (Rate from Very well implemented, well implemented, neutral, not well implemented, not at all implemented)

○ Collaboration

○ Interoperation

○ Reporting

○ Priorities

F.2.4 After Thoughts

QF.2.4.1 Which techniques between the mockups and WDA diagrams provides you with the best basis of designing and having a conversation about a cyber-security visualisation solution?

QF.2.4.2 Is there anything else you would like to add in the end?

Appendix G

C-EEVi - Calculation of Comparison Matrix to perform Analytical Hierarchy Process

The values in Chapter 5 were collected on a Likert Scale from Strongly Agree to Strongly Disagree (represented in Appendix E). However, to perform AHP, a comparison matrix with pairwise comparisons are required. The following steps were followed to convert the Likert Scale Values from 30 participants to a single Comparison Matrix:

Step 1 The values from the Likert Scale are converted into numerical values, for consistency with (Saaty, 2012)'s pairwise scale shown in Table 7.2, and collated into a tabular format where,

Strongly Agree = 9,

Agree = 7,

Neutral = 5,

Disagree = 3,

Strongly Disagree = 1 and

NA or missing value = 0.

Step 2 For each participant, where n is the total number of participants: The value of each criterion is compared to the value of the all corresponding criteria to create $n(n-1)/2$ list of pairwise compared values (PCV). The compared values are calculated on the formula adapted from (Kallas, 2011), where C_1 represents the comparison values of criteria A_1 and so on and n is the number of criteria

$$\begin{gathered} If\ (C_1 - C_n)\ is\ positive \\ PCV = (C_1 - C_n) + 1 \end{gathered} \tag{G.1}$$

If the value of $C_1 > C_n$, then C_1 is rated more important than C_n and represents that with the PCV. However, if the value of $C_1 < C_n$, then C_n is rated more important than C_1 and PCV is calculated as follows,

$$\begin{gathered} If\ (C_1 - C_n)\ is\ negative \\ PCV = 1/(|C_1 - C_n| + 1) \end{gathered} \tag{G.2}$$

PCV shows the reciprocal of the value, making it clear that C_n is more important than C_1. After the list for each participant is calculated for each criterion with the other criteria, the lists of PCV are calculated. The numerical values in the list follow from (Saaty, 2012)'s pairwise comparison scale presented in Table 7.2.

Step 3 Geometric mean of each list of PCV (PCV_{GM}) is calculated following the formula and process by (Mu & Pereyra-Rojas, 2018) for group decision making in AHP,

$$PCV_{GM} = \sqrt[n]{(Product\ of\ each\ PCV\ in\ list)} \tag{G.3}$$

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix in the following manner,

$$W = \begin{array}{cc}
\begin{array}{ccc} A_1 & \dots & A_n \end{array} & \\
\left[\begin{array}{ccc} PCV_{GM}(1,1) & \dots & PCV_{GM}(1,n) \\ \vdots & \ddots & \vdots \\ 1/PCV_{GM}(1,n) & \dots & PCV_{GM}(n,n) \end{array}\right] & \begin{array}{c} A_1 \\ \vdots \\ A_n \end{array} \\
\begin{array}{ccc} \mathrm{A}_{CSum_1} & \dots & \mathrm{A}_{CSum_n} \end{array} & \mathrm{A}_{CSum}
\end{array} \tag{G.4}$$

The following sections follow the steps to calculate the comparison matrix for each component task of *EEVi*

G.1 Conversion of Likert Scale to Comparison Matrix for Triage Analysis

Step 1 The values from the Likert Scale in Table E.1 are converted into numerical values and collated into a tabular format represented in Table G.1.

Step 2 For each participant: The value of each criterion is compared to the value of the all corresponding criteria to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Triage Analysis is shown in Table G.2.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.3.

Table G.3: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Triage Analysis'

F, SA	F, R	F, A	F, C	SA, R	SA, A	SA, C	R, A	R, C	A, C
0.96	1.10	1.28	1.30	1.09	1.35	1.37	1.29	1.28	0.99

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Triage Analysis' is,

$$W_{TA} = \begin{array}{c} \begin{array}{ccccc} \text{TA\_Filter} & \text{TA\_SA} & \text{TA\_RTA} & \text{TA\_Alerts} & \text{TA\_CH} \end{array} \\ \begin{bmatrix} 1.00 & 0.96 & 1.10 & 1.28 & 1.29 \\ 1.04 & 1.00 & 1.09 & 1.35 & 1.37 \\ 0.91 & 0.91 & 1.00 & 1.29 & 1.28 \\ 0.78 & 0.74 & 0.78 & 1.00 & 0.99 \\ 0.77 & 0.73 & 0.78 & 1.01 & 1.00 \end{bmatrix} \end{array} \begin{array}{l} \\ \text{TA\_Filter} \\ \text{TA\_SA} \\ \text{TA\_RTA} \\ \text{TA\_Alerts} \\ \text{TA\_CH} \end{array} \tag{G.5}$$

Table G.1: Results of Appropriateness of *Characteristics of Visualisation* for 'Triage Analysis' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	TA_Filter	TA_SA	TA_RTA	TA_Alerts	TA_CH
(1)	7	7	7	7	7
(2)	7	7	7	7	7
(3)	5	7	7	5	7
(4)	9	7	9	9	7
(5)	7	9	7	7	7
(6)	5	7	5	7	9
(7)	9	9	9	9	9
(8)	7	9	7	7	5
(9)	9	9	7	5	9
(10)	9	9	9	9	7
(11)	7	3	5	5	3
(12)	7	9	7	7	7
(13)	9	9	7	7	7
(14)	9	9	5	5	9
(15)	7	7	9	9	0
(16)	7	7	7	7	7
(17)	5	9	9	7	7
(18)	9	9	9	9	7
(19)	9	9	7	3	3
(20)	9	7	7	9	5
(21)	7	7	7	9	9
(22)	9	9	9	9	9
(23)	9	9	9	5	9
(24)	7	5	7	5	9
(25)	9	7	9	9	9
(26)	7	7	7	5	5
(27)	7	7	7	7	7
(28)	9	9	9	9	9
(29)	5	9	9	7	7
(30)	9	5	7	5	7

Table G.2: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Triage Analysis'

F, SA	F, R	F, A	F, C	SA, R	SA, A	SA, C	R, A	R, C	A, C
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
0.33	0.33	1	0.33	1	3	1	3	1	0.33
3	1	1	3	0.33	0.33	1	1	3	3
0.33	1	1	1	3	3	3	1	1	1
0.33	1	0.33	0.2	3	1	0.33	0.33	0.2	0.33
1	1	1	1	1	1	1	1	1	1
0.33	1	1	3	3	3	5	1	3	3
1	3	5	1	3	5	1	3	0.33	0.2
1	1	1	3	1	1	3	1	3	3
5	3	3	5	0.33	0.33	1	1	3	3
0.33	1	1	1	3	3	3	1	1	1
1	3	3	3	3	3	3	1	1	1
1	5	5	1	5	5	1	1	0.2	0.2
1	0.33	0.33	8	0.33	0.33	8	1	10	10
1	1	1	1	1	1	1	1	1	1
0.2	0.2	0.33	0.33	1	3	3	3	3	1
1	1	1	3	1	1	3	1	3	3
1	3	7	7	3	7	7	5	5	1
3	3	1	5	1	0.33	3	0.33	3	5
1	1	0.33	0.33	1	0.33	0.33	0.33	0.33	1
1	1	1	1	1	1	1	1	1	1
1	1	5	1	1	5	1	5	1	0.2
3	1	3	0.33	0.33	1	0.2	3	0.33	0.2
3	1	1	1	0.33	0.33	0.33	1	1	1
1	1	3	3	1	3	3	3	3	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
0.2	0.2	0.33	0.33	1	3	3	3	3	1
5	3	5	3	0.33	1	0.33	3	1	0.33

G.2 Conversion of Likert Scale to Comparison Matrix for Escalation Analysis

Step 1 The values from the Likert Scale in Table E.3 are converted into numerical values and collated into a tabular format represented in Table G.4.

Step 2 For each participant: The value of each criterion is compared to the value of the all corresponding criteria to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Escalation Analysis is shown in Table G.5.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.6.

Table G.6: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Escalation Analysis'

C, I	C, R	C, P	I, R	I, P	R,P
1.07	0.99	0.77	0.88	0.72	0.76

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Escalation Analysis' is,

$$W_{EA} = \begin{array}{cc} \begin{array}{cccc} \text{EA\_C} & \text{EA\_I} & \text{EA\_R} & \text{EA\_P} \end{array} & \\ \begin{bmatrix} 1.00 & 1.07 & 0.99 & 0.77 \\ 0.93 & 1.00 & 0.88 & 0.72 \\ 1.01 & 1.14 & 1.00 & 0.76 \\ 1.30 & 1.39 & 1.31 & 1.00 \end{bmatrix} & \begin{array}{c} \text{EA\_C} \\ \text{EA\_I} \\ \text{EA\_R} \\ \text{EA\_P} \end{array} \end{array} \tag{G.6}$$

Table G.4: Results of Appropriateness of *Characteristics of Visualisation* for 'Escalation Analysis' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	EA_C	EA_P	EA_I	EA_R
(1)	7	7	7	7
(2)	7	7	7	7
(3)	7	0	3	7
(4)	9	9	7	9
(5)	7	7	9	7
(6)	7	7	9	9
(7)	7	9	9	9
(8)	7	9	7	9
(9)	9	9	9	9
(10)	9	9	9	9
(11)	7	9	3	5
(12)	9	7	7	7
(13)	9	7	7	9
(14)	9	7	9	9
(15)	7	7	7	7
(16)	7	7	7	7
(17)	7	5	7	9
(18)	9	9	9	9
(19)	5	7	7	7
(20)	7	9	9	9
(21)	9	9	9	9
(22)	0	0	9	9
(23)	9	9	9	9
(24)	9	9	9	9
(25)	7	9	9	9
(26)	9	7	7	9
(27)	7	7	7	7
(28)	9	9	9	9
(29)	7	7	7	7
(30)	9	7	7	9

Table G.5: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Escalation Analysis'

C, I	C, R	C, P	I, R	I, P	R,P
1	1	1	1	1	1
1	1	1	1	1	1
8	5	1	0.25	0.13	0.2
1	3	1	3	1	0.33
1	0.33	1	0.33	1	3
1	0.33	0.33	0.33	0.33	1
0.33	0.33	0.33	1	1	1
0.33	1	0.33	3	1	0.33
1	1	1	1	1	1
1	1	1	1	1	1
0.33	5	3	7	5	0.33
3	3	3	1	1	1
3	3	1	1	0.33	0.33
3	1	1	0.33	0.33	1
1	1	1	1	1	1
1	1	1	1	1	1
3	1	0.33	0.33	0.2	0.33
1	1	1	1	1	1
0.33	0.33	0.33	1	1	1
0.33	0.33	0.33	1	1	1
1	1	1	1	1	1
1	0.1	0.1	0.1	0.1	1
1	1	1	1	1	1
1	1	1	1	1	1
0.33	0.33	0.33	1	1	1
3	3	1	1	0.33	0.33
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
3	3	1	1	0.33	0.33

G.3 Conversion of Likert Scale to Comparison Matrix for Correlation Analysis

Step 1 The values from the Likert Scale in Table E.5 are converted into numerical values and collated into a tabular format represented in Table G.7.

Step 2 For each participant: The value of each criterion is compared to the value of the all corresponding criteria to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Correlation Analysis is shown in Table G.8.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.9.

Table G.9: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Correlation Analysis'

C, I	C, R	I, R
0.89	0.94	0.99

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Correlation Analysis' is,

$$W_{CA} = \begin{array}{cccc} \text{CA\_Fl} & \text{CA\_T} & \text{CA\_IC} & \\ \left[\begin{array}{c} 1.00 \\ 1.12 \\ 1.07 \end{array}\right. & \begin{array}{c} 0.89 \\ 1.00 \\ 1.01 \end{array} & \left.\begin{array}{c} 0.94 \\ 0.99 \\ 1.00 \end{array}\right] & \begin{array}{l} \text{CA\_Fl} \\ \text{CA\_T} \\ \text{CA\_IC} \end{array} \end{array} \tag{G.7}$$

Table G.7: Results of Appropriateness of *Characteristics of Visualisation* for 'Correlation Analysis' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	CA_Fl	CA_T	CA_IC
(1)	9	7	9
(2)	7	7	7
(3)	5	3	3
(4)	9	9	9
(5)	7	9	7
(6)	7	9	7
(7)	9	9	9
(8)	9	7	9
(9)	7	9	9
(10)	9	9	9
(11)	5	0	3
(12)	9	7	7
(13)	7	7	9
(14)	9	9	9
(15)	7	9	9
(16)	7	7	7
(17)	7	7	9
(18)	9	9	9
(19)	3	9	9
(20)	7	9	9
(21)	5	9	9
(22)	9	9	9
(23)	9	9	5
(24)	7	7	5
(25)	9	9	9
(26)	5	7	7
(27)	7	7	7
(28)	9	9	9
(29)	9	5	7
(30)	7	9	5

Table G.8: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Correlation Analysis'

C, I	C, R	I, R
3	1	0.33
1	1	1
3	3	1
1	1	1
0.33	1	3
0.33	1	3
1	1	1
3	1	0.33
0.33	0.33	1
1	1	1
6	3	0.25
3	3	1
1	0.33	0.33
1	1	1
0.33	0.33	1
1	1	1
1	0.33	0.33
1	1	1
0.14	0.14	1
0.33	0.33	1
0.2	0.2	1
1	1	1
1	5	5
1	3	3
1	1	1
0.33	0.33	1
1	1	1
1	1	1
5	3	0.33
0.33	3	5

G.4 Conversion of Likert Scale to Comparison Matrix for Threat Analysis

Step 1 The values from the Likert Scale in Table E.7 are converted into numerical values and collated into a tabular format represented in Table G.10.

Step 2 For each participant: The value of each criteria is compared to the value of the all corresponding criterion to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Threat Analysis is shown in Table G.11.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.12.

Table G.12: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Threat Analysis'

Cor, I	Cor, P	Cor, C	I, P	I, C	P,C
1.07	1.13	1.19	1.10	1.15	1.02

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Threat Analysis' is,

$$W_{ThA} = \begin{array}{cccc} \text{ThA\_Cor} & \text{ThA\_I} & \text{ThA\_P} & \text{ThA\_C} \\ \end{array}$$

$$W_{ThA} = \begin{array}{c} \\ \\ \\ \\ \end{array}\begin{array}{cccccc} & \text{ThA\_Cor} & \text{ThA\_I} & \text{ThA\_P} & \text{ThA\_C} & \\ \left[\right. & 1.00 & 1.07 & 1.13 & 1.19 & \left.\right] \text{ThA\_Cor} \\ & 0.94 & 1.00 & 1.10 & 1.15 & \text{ThA\_I} \\ & 0.89 & 0.90 & 1.00 & 1.02 & \text{ThA\_P} \\ & 0.84 & 0.87 & 0.98 & 1.00 & \text{ThA\_C} \end{array} \tag{G.8}$$

Table G.10: Results of Appropriateness of *Characteristics of Visualisation* for 'Threat Analysis' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	ThA_Cor	ThA_I	ThA_P	ThA_C
(1)	9	9	9	7
(2)	7	7	7	7
(3)	9	9	5	7
(4)	7	5	7	7
(5)	9	7	7	7
(6)	7	7	7	9
(7)	5	9	9	9
(8)	9	9	7	7
(9)	9	9	9	9
(10)	5	5	5	5
(11)	5	7	7	5
(12)	9	7	9	9
(13)	7	7	9	9
(14)	9	9	9	7
(15)	7	7	9	9
(16)	7	7	7	7
(17)	9	9	7	7
(18)	9	9	9	9
(19)	3	9	7	7
(20)	9	7	7	9
(21)	9	7	9	7
(22)	9	9	9	9
(23)	9	9	3	3
(24)	9	7	5	7
(25)	9	9	9	9
(26)	7	7	7	5
(27)	7	7	7	7
(28)	9	9	9	9
(29)	9	9	5	9
(30)	7	7	9	7

Table G.11: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Threat Analysis'

Cor, I	Cor, P	Cor, C	I, P	I, C	P,C
1	1	3	1	3	3
1	1	1	1	1	1
1	5	3	5	3	0.33
3	1	1	0.33	0.33	1
3	3	3	1	1	1
1	1	0.33	1	0.33	0.33
0.2	0.2	0.2	1	1	1
1	3	3	3	3	1
1	1	1	1	1	1
1	1	1	1	1	1
0.33	0.33	1	1	3	3
3	1	1	0.33	0.33	1
1	0.33	0.33	0.33	0.33	1
1	1	3	1	3	3
1	0.33	0.33	0.33	0.33	1
1	1	1	1	1	1
1	3	3	3	3	1
1	1	1	1	1	1
0.14	0.2	0.2	3	3	1
3	3	1	1	0.33	0.33
3	1	3	0.33	1	3
1	1	1	1	1	1
1	7	7	7	7	1
3	5	3	3	1	0.33
1	1	1	1	1	1
1	1	3	1	3	3
1	1	1	1	1	1
1	1	1	1	1	1
1	5	1	5	1	0.2
1	0.33	1	0.33	1	3

G.5 Conversion of Likert Scale to Comparison Matrix for Impact Assessment

Step 1 The values from the Likert Scale in Table E.9 are converted into numerical values and collated into a tabular format represented in Table G.13.

Step 2 For each participant: The value of each criteria is compared to the value of the all corresponding criterion to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Impact Assessment' is shown in Table G.14.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.15.

Table G.15: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Impact Assessment'

II, SA	II, R	SA, R
1.20	1.08	0.93

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Impact Assessment' is,

$$W_{IA} = \begin{array}{c} \begin{array}{ccc} \text{IA\_II} & \text{IA\_SA} & \text{IA\_R} \end{array} \\ \begin{bmatrix} 1.00 & 1.20 & 1.08 \\ 0.83 & 1.00 & 0.93 \\ 0.93 & 1.07 & 1.00 \end{bmatrix} \end{array} \begin{array}{l} \\ \text{IA\_II} \\ \text{IA\_SA} \\ \text{IA\_R} \end{array} \tag{G.9}$$

Table G.13: Results of Appropriateness of *Characteristics of Visualisation* for 'Impact Assessment' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	IA_II	IA_SA	IA_R
(1)	7	9	7
(2)	7	7	7
(3)	5	3	7
(4)	9	9	9
(5)	7	9	9
(6)	9	7	7
(7)	9	9	9
(8)	9	9	7
(9)	0	0	0
(10)	7	7	7
(11)	7	5	9
(12)	7	7	9
(13)	7	9	7
(14)	9	9	9
(15)	9	9	7
(16)	7	7	7
(17)	0	0	0
(18)	9	9	9
(19)	9	9	9
(20)	9	9	9
(21)	9	7	9
(22)	9	9	9
(23)	9	7	7
(24)	7	5	5
(25)	9	9	9
(26)	7	5	7
(27)	7	7	7
(28)	9	9	9
(29)	5	5	5
(30)	9	7	7

Table G.14: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Impact Assessment'

II, SA	II, R	SA, R
0.33	1	3
1	1	1
3	0.33	0.2
1	1	1
0.33	0.33	1
3	3	1
1	1	1
1	3	3
1	1	1
1	1	1
3	0.33	0.2
1	0.33	0.33
0.33	1	3
1	1	1
1	3	3
1	1	1
1	1	1
1	1	1
1	1	1
1	1	1
3	1	0.33
1	1	1
3	3	1
3	3	1
1	1	1
3	1	0.33
1	1	1
1	1	1
1	1	1
3	3	1

G.6 Conversion of Likert Scale to Comparison Matrix for Incident Response Analysis

Step 1 The values from the Likert Scale in Table E.11 are converted into numerical values and collated into a tabular format represented in Table G.16.

Step 2 For each participant: The value of each criteria is compared to the value of the all corresponding criterion to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Incident Response Analysis is shown in Table G.17.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.18.

Table G.18: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Incident Response Analysis'

M, I	M, R	M, SA	M, C	I, R	I, SA	I, C	R, SA	R, C	SA, C
1.10	1.02	1.13	1.05	0.92	0.99	0.97	1.07	0.99	0.97

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Incident Response Analysis' is,

$$W_{IRA} = \begin{array}{cccccc} \text{IRA\_M} & \text{IRA\_I} & \text{IRA\_R} & \text{IRA\_SA} & \text{IRA\_C} & \\ 1.00 & 1.10 & 1.02 & 1.13 & 1.05 & \text{IRA\_M} \\ 0.91 & 1.00 & 0.92 & 0.99 & 0.97 & \text{IRA\_I} \\ 0.98 & 1.09 & 1.00 & 1.07 & 0.99 & \text{IRA\_R} \\ 0.88 & 1.01 & 0.93 & 1.00 & 0.97 & \text{IRA\_SA} \\ 0.96 & 1.03 & 1.01 & 1.03 & 1.00 & \text{IRA\_C} \end{array} \tag{G.10}$$

Table G.16: Results of Appropriateness of *Characteristics of Visualisation* for 'Incident Response Analysis' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	IRA_M	IRA_SA	IRA_I	IRA_C	IRA_R
(1)	7	9	7	7	7
(2)	7	7	7	7	7
(3)	7	9	9	9	7
(4)	9	9	7	9	9
(5)	9	7	9	9	7
(6)	7	7	7	9	9
(7)	7	9	9	9	9
(8)	9	9	7	7	9
(9)	0	0	0	0	0
(10)	0	0	0	0	0
(11)	5	0	7	3	9
(12)	7	9	7	7	7
(13)	5	7	7	9	9
(14)	9	9	9	9	9
(15)	9	7	7	9	9
(16)	7	7	7	7	7
(17)	0	0	0	0	0
(18)	9	9	9	9	9
(19)	9	7	9	9	9
(20)	9	9	9	5	5
(21)	9	9	9	5	5
(22)	9	9	9	9	9
(23)	9	9	9	5	3
(24)	9	9	7	5	5
(25)	9	9	9	9	9
(26)	5	7	7	5	7
(27)	7	7	7	7	7
(28)	9	9	9	9	9
(29)	7	0	7	9	9
(30)	9	0	5	7	7

Table G.17: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Incident Response Analysis'

M, I	M, R	M, SA	M, C	I, R	I, SA	I, C	R, SA	R, C	SA, C
0.33	1	1	1	3	3	3	1	1	1
1	1	1	1	1	1	1	1	1	1
0.33	0.33	0.33	1	1	1	3	1	3	3
1	3	1	1	3	1	1	0.33	0.33	1
3	1	1	3	0.33	0.33	1	1	3	3
1	1	0.33	0.33	1	0.33	0.33	0.33	0.33	1
0.33	0.33	0.33	0.33	1	1	1	1	1	1
1	3	3	1	3	3	1	1	0.33	0.33
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
6	0.33	3	0.2	0.13	0.25	0.1	5	0.33	0.14
0.33	1	1	1	3	3	3	1	1	1
0.33	0.33	0.2	0.2	1	0.33	0.33	0.33	0.33	1
1	1	1	1	1	1	1	1	1	1
3	3	1	1	1	0.33	0.33	0.33	0.33	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
3	1	1	1	0.33	0.33	0.33	1	1	1
1	1	5	5	1	5	5	5	5	1
1	1	5	5	1	5	5	5	5	1
1	1	1	1	1	1	1	1	1	1
1	1	5	7	1	5	7	5	7	3
1	3	5	5	3	5	5	3	3	1
1	1	1	1	1	1	1	1	1	1
0.33	0.33	1	0.33	1	3	1	3	1	0.33
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
8	1	0.33	0.33	0.13	0.1	0.1	0.33	0.33	1
10	5	3	3	0.17	0.13	0.13	0.33	0.33	1

G.7 Conversion of Likert Scale to Comparison Matrix for Forensic Analysis

Step 1 The values from the Likert Scale in Table E.13 are converted into numerical values and collated into a tabular format represented in Table G.19.

Step 2 For each participant: The value of each criteria is compared to the value of the all corresponding criterion to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Forensic Analysis is shown in Table G.20.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.21.

Table G.21: Geometric Means for each list of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Forensic Analysis'

CBC, R	CBC, CoC	CBC, I	R, CoC	R, I	CoC, I
1.02	0.95	1.11	0.90	1.07	1.20

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Forensic Analysis' is,

$$W_{FA} = \begin{array}{cccccc} & \text{FA\_CBC} & \text{FA\_R} & \text{FA\_CoC} & \text{FA\_I} & \\ \left[\begin{array}{c} \\ \\ \\ \\ \end{array}\right. & \begin{array}{c} 1.00 \\ 0.98 \\ 1.06 \\ 0.90 \end{array} & \begin{array}{c} 1.02 \\ 1.00 \\ 1.12 \\ 0.93 \end{array} & \begin{array}{c} 0.95 \\ 0.90 \\ 1.00 \\ 0.84 \end{array} & \begin{array}{c} 1.11 \\ 1.07 \\ 1.20 \\ 1.00 \end{array} & \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right] \begin{array}{l} \text{FA\_CBC} \\ \text{FA\_R} \\ \text{FA\_CoC} \\ \text{FA\_I} \end{array} \end{array} \tag{G.11}$$

Table G.19: Results of Appropriateness of *Characteristics of Visualisation* for 'Forensic Analysis' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	FA_CBC	FA_R	FA_CoC	FA_I
(1)	7	7	7	9
(2)	7	7	7	7
(3)	5	7	5	7
(4)	9	9	9	9
(5)	0	0	0	0
(6)	7	7	7	7
(7)	9	9	9	9
(8)	9	7	7	9
(9)	0	0	0	0
(10)	7	7	7	7
(11)	7	3	5	5
(12)	9	7	9	7
(13)	7	7	9	7
(14)	9	9	9	9
(15)	7	7	9	7
(16)	7	7	7	7
(17)	0	0	0	0
(18)	9	9	9	9
(19)	7	9	7	7
(20)	9	9	9	5
(21)	9	9	9	7
(22)	9	9	9	9
(23)	9	9	9	5
(24)	7	7	7	5
(25)	9	9	9	9
(26)	5	7	7	7
(27)	7	7	7	7
(28)	9	7	9	9
(29)	5	7	9	7
(30)	9	9	7	9

Table G.20: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Forensic Analysis'

CBC, R	CBC, CoC	CBC, I	R, CoC	R, I	CoC, I
1	1	0.33	1	0.33	0.33
1	1	1	1	1	1
0.33	1	0.33	3	1	0.33
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
3	3	1	1	0.33	0.33
1	1	1	1	1	1
1	1	1	1	1	1
5	3	3	0.33	0.33	1
3	1	3	0.33	1	3
1	0.33	1	0.33	1	3
1	1	1	1	1	1
1	0.33	1	0.33	1	3
1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
0.33	1	1	3	3	1
1	1	5	1	5	5
1	1	3	1	3	3
1	1	1	1	1	1
1	1	5	1	5	5
1	1	3	1	3	3
1	1	1	1	1	1
0.33	0.33	0.33	1	1	1
1	1	1	1	1	1
3	1	1	0.33	0.33	1
0.33	0.2	0.33	0.33	1	3
1	3	1	3	1	0.33

G.8 Conversion of Likert Scale to Comparison Matrix for Security Quality Management

Step 1 The values from the Likert Scale in Table E.15 are converted into numerical values and collated into a tabular format represented in Table G.22.

Step 2 For each participant: The value of each criteria is compared to the value of the all corresponding criterion to create $n(n-1)/2$ list of pairwise compared values (PCV), where n is the number of criteria. This list of PCVs for 'Security Quality Management' is shown in Table G.23.

Step 3 Geometric mean of each list of PCV is calculated as shown in Table G.24.

Table G.24: Geometric Mean for the list of PCV (pairwise comparison value) for pair of all criteria (characteristics of visualisation) for 'Security Quality Management'

Fe ,R
0.94

Step 4 Each PCV_{GM} represents the pairwise comparison between criteria and is added to the comparison matrix. The comparison Matrix for 'Security Quality Management' is,

$$W_{SQM} = \begin{array}{c|cc|l} & \text{SQM\_Fe} & \text{SQM\_R} & \\ \hline & 1.00 & 0.94 & \text{SQM\_Fe} \\ & 1.06 & 1.00 & \text{SQM\_R} \end{array} \tag{G.12}$$

Table G.22: Results of Appropriateness of *Characteristics of Visualisation* for 'Security Quality Management' for each questionnaire participant on a scale of 1 (Strongly Disagree) to 9 (Strongly Agree)

Participants	SQM_Fe	SQM_R
(1)	7	7
(2)	7	7
(3)	7	7
(4)	9	7
(5)	0	0
(6)	5	5
(7)	0	9
(8)	9	5
(9)	0	0
(10)	5	5
(11)	7	5
(12)	9	9
(13)	5	7
(14)	9	9
(15)	7	9
(16)	7	7
(17)	0	0
(18)	9	9
(19)	3	5
(20)	9	9
(21)	9	9
(22)	9	9
(23)	9	9
(24)	9	9
(25)	9	9
(26)	7	7
(27)	7	7
(28)	9	9
(29)	9	9
(30)	0	0

Table G.23: List of PCV (pairwise comparison values) for pairs of all criteria (characteristics of visualisation) for 'Security Quality Management'

Fe ,R
1.00
1.00
1.00
3.00
1.00
1.00
0.10
5.00
1.00
1.00
3.00
1.00
0.33
1.00
0.33
1.00
1.00
1.00
0.33
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00
1.00

Appendix H

C-EEVi - Calculation of Priority Weights for Component Tasks

The following chapter shows the calculations of priority weights for all component tasks. Section 7.1.3 already presents the calculations for 'Triage Analysis'. The calculations for the other seven component tasks is demonstrated below.

H.1 Calculation of Priority Weights for Escalation Analysis

To determine the priority weights for 'Escalation Analysis':

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for 'Escalation Analysis' were converted to a comparison matrix (calculations in Section G.2).

Step 2 The Original Matrix (W_{EA}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{EA} = \begin{array}{c|cccc|l} & \text{EA\_C} & \text{EA\_I} & \text{EA\_R} & \text{EA\_P} & \\ \hline & 1.00 & 1.07 & 0.99 & 0.77 & \text{EA\_C} \\ & 0.93 & 1.00 & 0.88 & 0.72 & \text{EA\_I} \\ & 1.01 & 1.14 & 1.00 & 0.76 & \text{EA\_R} \\ & 1.30 & 1.39 & 1.31 & 1.00 & \text{EA\_P} \\ \hline & 4.24 & 4.60 & 4.19 & 3.25 & A_{CSum} \end{array} \tag{H.1}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{cc} \begin{array}{cccc} \text{EA\_C} & \text{EA\_I} & \text{EA\_R} & \text{EA\_P} \end{array} & A_{RAv} \\ \begin{bmatrix} 0.24 & 0.23 & 0.24 & 0.24 \\ 0.22 & 0.22 & 0.21 & 0.22 \\ 0.24 & 0.25 & 0.24 & 0.23 \\ 0.31 & 0.30 & 0.31 & 0.31 \end{bmatrix} & \begin{array}{c} 0.236 \\ 0.217 \\ 0.240 \\ 0.307 \end{array} \end{array} \tag{H.2}$$

Step 4 The priority weights for characteristics of visualisation for 'Escalation Analysis' is given below:

$$Priority\ Weights\ for \begin{bmatrix} \text{EA\_C} \\ \text{EA\_I} \\ \text{EA\_R} \\ \text{EA\_P} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.236} \\ \mathbf{0.217} \\ \mathbf{0.240} \\ \mathbf{0.307} \end{bmatrix} \tag{H.3}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of 'Escalation Analysis' is

$$[W_s] = \begin{bmatrix} 0.236 \\ 0.217 \\ 0.240 \\ 0.307 \end{bmatrix} \begin{bmatrix} 1.00 & 1.07 & 0.99 & 0.77 \\ 0.93 & 1.00 & 0.88 & 0.72 \\ 1.01 & 1.14 & 1.00 & 0.76 \\ 1.30 & 1.39 & 1.31 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 0.94 \\ 0.87 \\ 0.96 \\ 1.23 \end{bmatrix} \tag{H.4}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Escalation Analysis' is

$$[CV] = \begin{bmatrix} 0.94 \\ 0.87 \\ 0.96 \\ 1.23 \end{bmatrix} \cdot \begin{bmatrix} 1/0.236 \\ 1/0.217 \\ 1/0.211 \\ 1/0.240 \end{bmatrix} = \begin{bmatrix} 0.94 \\ 0.87 \\ 0.96 \\ 1.23 \end{bmatrix} \cdot \begin{bmatrix} 4.24 \\ 4.61 \\ 4.17 \\ 3.25 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 4.00061 \\ 4.00047 \\ 4.00056 \\ 4.00066 \end{bmatrix} \tag{H.5}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Escalation Analysis' is

$$\lambda_{max} = (4.00061 + 4.00047 + 4.00056 + 4.00066)/4 = 4.00058 \tag{H.6}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n - 1)$$

Consistency Index (CI) in case of 'Escalation Analysis', where n=4, is

$$CI = (4.00058 - 4)/(4 - 1) = 0.00058/3$$

$$\therefore CI = 0.00019 \tag{H.7}$$

Step 9 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = 0.00019/0.9$$

$$\therefore CR = 0.00021 \tag{H.8}$$

As seen, CR = 0.00021, which is less than 0.1. Thus, consistency is achieved and the priority weights in the pairwise comparison (Equation H.3) do not need to be recalculated as they are consistent.

Therefore, the priority weights for each criterion is determined. Equation H.3 represents the priority weights for the characteristics of visualisation for 'Escalation Analysis'. According to the equation, *Priorities* has the highest priority followed by *Reporting, Collaboration* and finally *Interoperation.*

H.2 Calculation of Priority Weights for Correlation Analysis

To determine the priority weights for 'Correlation Analysis':

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for 'Correlation Analysis' were converted to a comparison matrix (calculations in Section G.3).

Step 2 The Original Matrix (W_{CA}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{CA} = \begin{array}{cccc} \text{CA\_Fl} & \text{CA\_T} & \text{CA\_IC} & \\ \left[\begin{matrix} 1.00 \\ 1.12 \\ 1.07 \end{matrix}\right. & \begin{matrix} 0.89 \\ 1.00 \\ 1.01 \end{matrix} & \left.\begin{matrix} 0.94 \\ 0.99 \\ 1.00 \end{matrix}\right] & \begin{matrix} \text{CA\_Fl} \\ \text{CA\_T} \\ \text{CA\_IC} \end{matrix} \\ 2.12 & 1.89 & 1.93 & A_{CSum} \end{array} \tag{H.9}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{cccc} \text{CA\_Fl} & \text{CA\_T} & \text{CA\_IC} & A_{RAv} \\ \left[\begin{matrix} 0.31 \\ 0.35 \\ 0.34 \end{matrix}\right. & \begin{matrix} 0.31 \\ 0.34 \\ 0.35 \end{matrix} & \left.\begin{matrix} 0.32 \\ 0.34 \\ 0.34 \end{matrix}\right] & \begin{matrix} 0.314 \\ 0.345 \\ 0.342 \end{matrix} \end{array} \tag{H.10}$$

Step 4 The priority weights for characteristics of visualisation for 'Correlation Analysis' is given below:

$$Priority\ Weights\ for \begin{bmatrix} \text{CA\_Fl} \\ \text{CA\_T} \\ \text{CA\_IC} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.314} \\ \mathbf{0.345} \\ \mathbf{0.342} \end{bmatrix} \tag{H.11}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of 'Correlation Analysis' is

$$[W_s] = \begin{bmatrix} 0.314 \\ 0.345 \\ 0.342 \end{bmatrix} \begin{bmatrix} 1.00 & 0.89 & 0.94 \\ 1.12 & 1.00 & 0.99 \\ 1.07 & 1.01 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 0.94 \\ 1.03 \\ 1.03 \end{bmatrix} \tag{H.12}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Correlation Analysis' is

$$[CV] = \begin{bmatrix} 0.94 \\ 1.03 \\ 1.03 \end{bmatrix} \cdot \begin{bmatrix} 1/0.314 \\ 1/0.345 \\ 1/0.342 \end{bmatrix} = \begin{bmatrix} 0.94 \\ 1.03 \\ 1.03 \end{bmatrix} \cdot \begin{bmatrix} 3.19 \\ 2.90 \\ 2.93 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 3.00041 \\ 3.00045 \\ 3.00044 \end{bmatrix} \tag{H.13}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Correlation Analysis' is

$$\lambda_{max} = (3.00041 + 3.00045 + 3.00044)/3 = 3.00043 \tag{H.14}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n - 1)$$

Consistency Index (CI) in case of 'Correlation Analysis', where n=3, is

$$CI = (3.00043 - 3)/(3 - 1) = 0.00043/2$$

$$\therefore CI = 0.00022 \tag{H.15}$$

Step 9 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = 0.00022/0.58$$

$$\therefore CR = 0.00037 \tag{H.16}$$

As seen, CR = 0.00037, which is less than 0.1. Thus, consistency is achieved and the priority weights in the pairwise comparison (Equation H.11) do not need to be recalculated as they are consistent.

Therefore, the priority weights for each criterion is determined. Equation H.11 represents the priority weights for the characteristics of visualisation for 'Correlation Analysis'. According to the equation, *Timeline* has the highest priority followed closely by *Investigatory Capabilities* and finally *Flexibility*.

H.3 Calculation of Priority Weights for Threat Analysis

To determine the priority weights for ‘Threat Analysis’:

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for ‘Threat Analysis’ were converted to a comparison matrix (calculations in Section G.4).

Step 2 The Original Matrix (W_{ThA}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{ThA} = \begin{array}{cccccc} & \text{ThA\_Cor} & \text{ThA\_I} & \text{ThA\_P} & \text{ThA\_C} & \\ & 1.00 & 1.07 & 1.13 & 1.19 & \text{ThA\_Cor} \\ & 0.94 & 1.00 & 1.10 & 1.15 & \text{ThA\_I} \\ & 0.89 & 0.90 & 1.00 & 1.02 & \text{ThA\_P} \\ & 0.84 & 0.87 & 0.98 & 1.00 & \text{ThA\_C} \\ & 3.66 & 3.84 & 4.21 & 4.36 & A_{CSum} \end{array} \tag{H.17}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{ccccc} \text{ThA\_Cor} & \text{ThA\_I} & \text{ThA\_P} & \text{ThA\_C} & A_{RAv} \\ 0.27 & 0.28 & 0.27 & 0.27 & 0.273 \\ 0.26 & 0.26 & 0.26 & 0.26 & 0.260 \\ 0.24 & 0.24 & 0.24 & 0.23 & 0.237 \\ 0.23 & 0.23 & 0.23 & 0.23 & 0.229 \end{array} \tag{H.18}$$

Step 4 The priority weights for characteristics of visualisation for ‘Threat Analysis’ is given below:

$$Priority\ Weights\ for \begin{bmatrix} \text{ThA\_Cor} \\ \text{ThA\_I} \\ \text{ThA\_P} \\ \text{ThA\_C} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.273} \\ \mathbf{0.260} \\ \mathbf{0.237} \\ \mathbf{0.229} \end{bmatrix} \tag{H.19}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of ‘Threat Analysis’ is

$$[W_s] = \begin{bmatrix} 0.273 \\ 0.260 \\ 0.237 \\ 0.229 \end{bmatrix} \begin{bmatrix} 1.00 & 1.07 & 1.13 & 1.19 \\ 0.94 & 1.00 & 1.10 & 1.15 \\ 0.89 & 0.90 & 1.00 & 1.02 \\ 0.84 & 0.87 & 0.98 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 1.09 \\ 1.04 \\ 0.95 \\ 0.92 \end{bmatrix} \tag{H.20}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Threat Analysis' is

$$[CV] = \begin{bmatrix} 1.09 \\ 1.04 \\ 0.95 \\ 0.92 \end{bmatrix} \cdot \begin{bmatrix} 1/0.273 \\ 1/0.260 \\ 1/0.237 \\ 1/0.229 \end{bmatrix} = \begin{bmatrix} 1.09 \\ 1.04 \\ 0.95 \\ 0.92 \end{bmatrix} \cdot \begin{bmatrix} 3.66 \\ 3.84 \\ 4.21 \\ 4.36 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 4.00031 \\ 4.00029 \\ 4.00027 \\ 4.00027 \end{bmatrix} \tag{H.21}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Threat Analysis' is

$$\lambda_{max} = (4.00031 + 4.00029 + 4.00027 + 4.00027)/4 = 4.00029 \tag{H.22}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n - 1)$$

Consistency Index (CI) in case of 'Threat Analysis', where n=4, is

$$CI = (4.00029 - 4)/(4 - 1) = 0.00029/3$$

$$\therefore CI = 0.00010 \tag{H.23}$$

Step 9 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = 0.00010/0.9$$

$$\therefore CR = 0.00011 \tag{H.24}$$

As seen, CR = 0.00011, which is less than 0.1. Thus, consistency is achieved and the priority weights in the pairwise comparison (Equation H.19) do not need to be recalculated as they are consistent.

Therefore, the priority weights for each criterion is determined. Equation H.19 represents the priority weights for the characteristics of visualisation for 'Threat Analysis'. According to the equation, *Correlation* has the highest priority closely followed by *Interoperation, Priorities* and finally *Collaboration.*

H.4 Calculation of Priority Weights for Impact Assessment

To determine the priority weights for 'Impact Assessment':

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for 'Impact Assessment' were converted to a comparison matrix (calculations in Section G.5).

Step 2 The Original Matrix (W_{IA}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{IA} = \begin{array}{cccc} \text{IA\_II} & \text{IA\_SA} & \text{IA\_R} & \\ \left[\begin{array}{c} 1.00 \\ 0.83 \\ 0.93 \end{array}\right. & \begin{array}{c} 1.20 \\ 1.00 \\ 1.07 \end{array} & \left.\begin{array}{c} 1.08 \\ 0.93 \\ 1.00 \end{array}\right] & \begin{array}{c} \text{IA\_II} \\ \text{IA\_SA} \\ \text{IA\_R} \end{array} \\ 2.76 & 3.27 & 3.01 & A_{CSum} \end{array} \tag{H.25}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{cccc} \text{IA\_II} & \text{IA\_SA} & \text{IA\_R} & A_{RAv} \\ \left[\begin{array}{c} 0.36 \\ 0.30 \\ 0.34 \end{array}\right. & \begin{array}{c} 0.37 \\ 0.31 \\ 0.33 \end{array} & \left.\begin{array}{c} 0.36 \\ 0.31 \\ 0.33 \end{array}\right] & \begin{array}{c} 0.362 \\ 0.306 \\ 0.332 \end{array} \end{array} \tag{H.26}$$

Step 4 The priority weights for characteristics of visualisation for 'Impact Assessment' is given below:

$$Priority\ Weights\ for \begin{bmatrix} \text{IA\_II} \\ \text{IA\_SA} \\ \text{IA\_R} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.362} \\ \mathbf{0.306} \\ \mathbf{0.332} \end{bmatrix} \tag{H.27}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of 'Impact Assessment' is

$$[W_s] = \begin{bmatrix} 0.362 \\ 0.306 \\ 0.332 \end{bmatrix} \begin{bmatrix} 1.00 & 1.20 & 1.08 \\ 0.83 & 1.00 & 0.93 \\ 0.93 & 1.07 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 1.09 \\ 0.92 \\ 0.10 \end{bmatrix} \tag{H.28}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Impact Assessment' is

$$[CV] = \begin{bmatrix} 1.09 \\ 0.92 \\ 0.10 \end{bmatrix} \cdot \begin{bmatrix} 1/0.362 \\ 1/0.306 \\ 1/0.332 \end{bmatrix} = \begin{bmatrix} 1.09 \\ 0.92 \\ 0.10 \end{bmatrix} \cdot \begin{bmatrix} 2.76 \\ 3.27 \\ 3.01 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 3.00019 \\ 3.00016 \\ 3.00017 \end{bmatrix} \tag{H.29}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Impact Assessment' is

$$\lambda_{max} = (3.00019 + 3.00016 + 3.00017)/3 = 3.00017 \tag{H.30}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n - 1)$$

Consistency Index (CI) in case of 'Impact Assessment', where n=3, is

$$CI = (3.00017 - 3)/(3 - 1) = 0.00017/2$$

$$\therefore CI = 0.000085 \tag{H.31}$$

Step 9 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = 0.000085/0.58$$

$$\therefore CR = 0.00015 \tag{H.32}$$

As seen, CR = 0.00015, which is less than 0.1. Thus, consistency is achieved and the priority weights in the pairwise comparison (Equation H.27) do not need to be recalculated as they are consistent.

Therefore, the priority weights for each criterion is determined. Equation H.27 represents the priority weights for the characteristics of visualisation for 'Impact Identification'. According to the equation, *Impact Assessment* has the highest priority closely followed by *Reporting* and finally *Situational Awareness*.

H.5 Calculation of Priority Weights for Incident Response Analysis

To determine the priority weights for 'Incident Response Analysis':

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for 'Incident Response Analysis' were converted to a comparison matrix (calculations in Section G.6).

Step 2 The Original Matrix (W_{IRA}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{IRA} = \begin{array}{c} \begin{array}{ccccc} \text{IRA\_M} & \text{IRA\_I} & \text{IRA\_R} & \text{IRA\_SA} & \text{IRA\_C} \end{array} \\ \left[\begin{array}{ccccc} 1.00 & 1.10 & 1.02 & 1.13 & 1.05 \\ 0.91 & 1.00 & 0.92 & 0.99 & 0.97 \\ 0.98 & 1.09 & 1.00 & 1.07 & 0.99 \\ 0.88 & 1.01 & 0.93 & 1.00 & 0.97 \\ 0.96 & 1.03 & 1.01 & 1.03 & 1.00 \end{array}\right] \begin{array}{l} \text{IRA\_M} \\ \text{IRA\_I} \\ \text{IRA\_R} \\ \text{IRA\_SA} \\ \text{IRA\_C} \end{array} \\ \begin{array}{cccccc} 4.73 & 5.24 & 4.88 & 5.22 & 4.98 & A_{CSum} \end{array} \end{array} \tag{H.33}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{cccccc} \text{IRA\_M} & \text{IRA\_I} & \text{IRA\_R} & \text{IRA\_SA} & \text{IRA\_C} & A_{RAv} \\ 0.21 & 0.21 & 0.21 & 0.22 & 0.21 & 0.211 \\ 0.19 & 0.19 & 0.19 & 0.19 & 0.19 & 0.191 \\ 0.21 & 0.21 & 0.21 & 0.21 & 0.20 & 0.205 \\ 0.19 & 0.19 & 0.19 & 0.19 & 0.20 & 0.192 \\ 0.20 & 0.20 & 0.21 & 0.20 & 0.20 & 0.201 \end{array} \tag{H.34}$$

Step 4 The priority weights for characteristics of visualisation for 'Incident Response Analysis' is given below:

$$Priority\ Weights\ for \begin{bmatrix} \text{IRA\_M} \\ \text{IRA\_I} \\ \text{IRA\_R} \\ \text{IRA\_SA} \\ \text{IRA\_C} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.211} \\ \mathbf{0.191} \\ \mathbf{0.205} \\ \mathbf{0.192} \\ \mathbf{0.201} \end{bmatrix} \tag{H.35}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of 'Incident Response Analysis' is

$$[W_s] = \begin{bmatrix} 0.211 \\ 0.191 \\ 0.205 \\ 0.192 \\ 0.201 \end{bmatrix} \begin{bmatrix} 1.00 & 1.10 & 1.02 & 1.13 & 1.05 \\ 0.91 & 1.00 & 0.92 & 0.99 & 0.97 \\ 0.98 & 1.09 & 1.00 & 1.07 & 0.99 \\ 0.88 & 1.01 & 0.93 & 1.00 & 0.97 \\ 0.96 & 1.03 & 1.01 & 1.03 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 1.06 \\ 0.95 \\ 1.03 \\ 0.96 \\ 1.01 \end{bmatrix} \tag{H.36}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Incident Response Analysis' is

$$[CV] = \begin{bmatrix} 1.06 \\ 0.95 \\ 1.03 \\ 0.96 \\ 1.01 \end{bmatrix} \cdot \begin{bmatrix} 1/0.211 \\ 1/0.191 \\ 1/0.205 \\ 1/0.192 \\ 1/0.201 \end{bmatrix} = \begin{bmatrix} 1.06 \\ 0.95 \\ 1.03 \\ 0.96 \\ 1.01 \end{bmatrix} \cdot \begin{bmatrix} 4.73 \\ 5.24 \\ 4.88 \\ 5.22 \\ 4.98 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 5.00061 \\ 5.00058 \\ 5.00061 \\ 5.00058 \\ 5.00060 \end{bmatrix} \tag{H.37}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Incident Response Analysis' is

$$\lambda_{max} = (5.00061 + 5.00058 + 5.00061 + 5.00058 + 5.00060)/5 = 5.00060 \tag{H.38}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n - 1)$$

Consistency Index (CI) in case of 'Incident Response Analysis', where n=5, is

$$CI = (5.00060 - 5)/(5 - 1) = 0.00060/4$$

$$\therefore CI = 0.00015 \tag{H.39}$$

Step 9 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = 0.00015/1.12$$

$$\therefore CR = 0.00013 \tag{H.40}$$

As seen, CR = 0.00013, which is less than 0.1. Thus, consistency is achieved and the priority weights in the pairwise comparison (Equation H.35) do not need to be recalculated as they are consistent.

Therefore, the priority weights for each criterion is determined. Equation H.35 represents the priority weights for the characteristics of visualisation for 'Incident Response Analysis'. According to the equation, *Mitigation* has the highest priority followed by *Reporting, Collaboration, Situational Awareness* and finally *Interoperation.*

H.6 Calculation of Priority Weights for Forensic Analysis

To determine the priority weights for 'Forensic Analysis':

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for 'Forensic Analysis' were converted to a comparison matrix (calculations in Section G.7).

Step 2 The Original Matrix (W_{FA}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{FA} = \begin{array}{ccccc} \text{FA\_CBC} & \text{FA\_R} & \text{FA\_CoC} & \text{FA\_I} & \\ \left[\begin{array}{c} 1.00 \\ 0.98 \\ 1.06 \\ 0.90 \end{array}\right. & \begin{array}{c} 1.02 \\ 1.00 \\ 1.12 \\ 0.93 \end{array} & \begin{array}{c} 0.95 \\ 0.90 \\ 1.00 \\ 0.84 \end{array} & \left.\begin{array}{c} 1.11 \\ 1.07 \\ 1.20 \\ 1.00 \end{array}\right] & \begin{array}{c} \text{FA\_CBC} \\ \text{FA\_R} \\ \text{FA\_CoC} \\ \text{FA\_I} \end{array} \\ 3.94 & 4.07 & 3.68 & 4.38 & A_{CSum} \end{array} \tag{H.41}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{ccccc} \text{FA\_CBC} & \text{FA\_R} & \text{FA\_CoC} & \text{FA\_I} & A_{RAv} \\ \left[\begin{array}{c} 0.25 \\ 0.25 \\ 0.27 \\ 0.23 \end{array}\right. & \begin{array}{c} 0.25 \\ 0.25 \\ 0.28 \\ 0.23 \end{array} & \begin{array}{c} 0.26 \\ 0.24 \\ 0.27 \\ 0.23 \end{array} & \left.\begin{array}{c} 0.25 \\ 0.25 \\ 0.27 \\ 0.23 \end{array}\right] & \begin{array}{c} 0.254 \\ 0.246 \\ 0.272 \\ 0.228 \end{array} \end{array} \tag{H.42}$$

Step 4 The priority weights for characteristics of visualisation for 'Forensic Analysis' is given below:

$$Priority\ Weights\ for \begin{bmatrix} \text{FA\_CBC} \\ \text{FA\_R} \\ \text{FA\_CoC} \\ \text{FA\_I} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.254} \\ \mathbf{0.246} \\ \mathbf{0.272} \\ \mathbf{0.228} \end{bmatrix} \tag{H.43}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of 'Forensic Analysis' is

$$[W_s] = \begin{bmatrix} 0.254 \\ 0.246 \\ 0.272 \\ 0.228 \end{bmatrix} \begin{bmatrix} 1.00 & 1.02 & 0.95 & 1.11 \\ 0.98 & 1.00 & 0.90 & 1.07 \\ 1.06 & 1.12 & 1.00 & 1.20 \\ 0.90 & 0.93 & 0.84 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 1.02 \\ 0.98 \\ 1.09 \\ 0.91 \end{bmatrix} \tag{H.44}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Forensic Analysis' is

$$[CV] = \begin{bmatrix} 1.02 \\ 0.98 \\ 1.09 \\ 0.91 \end{bmatrix} \cdot \begin{bmatrix} 1/0.254 \\ 1/0.246 \\ 1/0.272 \\ 1/0.228 \end{bmatrix} = \begin{bmatrix} 1.02 \\ 0.98 \\ 1.09 \\ 0.91 \end{bmatrix} \cdot \begin{bmatrix} 3.94 \\ 4.07 \\ 3.68 \\ 4.38 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 4.00015 \\ 4.00014 \\ 4.00015 \\ 4.00014 \end{bmatrix} \tag{H.45}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Forensic Analysis' is

$$\lambda_{max} = (4.00015 + 4.00014 + 4.00015 + 4.00014)/4 = 4.00014 \tag{H.46}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n - 1)$$

Consistency Index (CI) in case of 'Forensic Analysis', where n=4, is

$$CI = (4.00014 - 4)/(4 - 1) = 0.00014/3$$

$$\therefore CI = 0.000053 \tag{H.47}$$

Step 9 Determine the Consistency Ratio (CR), where RI is determined from Table 7.3

$$CR = 0.000048/0.9$$

$$\therefore CR = 0.000053 \tag{H.48}$$

As seen, CR = 0.000053, which is less than 0.1. Thus, consistency is achieved and the priority weights in the pairwise comparison (Equation H.43) do not need to be recalculated as they are consistent.

Therefore, the priority weights for each criterion is determined. Equation H.43 represents the priority weights for the characteristics of visualisation for 'Forensic Analysis'. According to the equation, *Chain of Custody* has the highest priority closely followed by *Case-Building Capabilities, Reporting* and finally *Interoperation.*

H.7 Calculation of Priority Weights for Security Quality Management

To determine the priority weights for 'Security Quality Management':

Step 1 Firstly, the collected responses of *Characteristics of Visualisation* for 'Security Quality Management' were converted to a comparison matrix (calculations in Section G.8).

Step 2 The Original Matrix (W_{SQM}) is presented below with the calculated sums of each column (A_{CSum})

$$W_{SQM} = \begin{array}{cc|c} \text{SQM\_Fe} & \text{SQM\_R} & \\ \hline 1.00 & 0.94 & \text{SQM\_Fe} \\ 1.06 & 1.00 & \text{SQM\_R} \\ \hline 2.06 & 1.94 & A_{CSum} \end{array} \tag{H.49}$$

Step 3 Calculate the normalised matrix and the average of each row (A_{RAv})

$$\begin{array}{cc|c} \text{SQM\_Fe} & \text{SQM\_R} & A_{RAv} \\ \hline 0.49 & 0.49 & 0.485 \\ 0.52 & 0.52 & 0.515 \end{array} \tag{H.50}$$

Step 4 The priority weights for characteristics of visualisation for 'Security Quality Management' is given below:

$$Priority\,Weights\,for \begin{bmatrix} \text{SQM\_Fe} \\ \text{SQM\_R} \end{bmatrix} is\ A_{RAv} = \begin{bmatrix} \mathbf{0.485} \\ \mathbf{0.515} \end{bmatrix} \tag{H.51}$$

Step 5 Determine the Weight Sum Vector $[W_s]$, where $[A_{RAv}]$ represents the calculated priority weights and $[W]$ is the original matrix,

$$[W_s] = [A_{RAv}][W]$$

Weight Sum Vector $[W_s]$ in case of 'Security Quality Management' is

$$[W_s] = \begin{bmatrix} 0.485 \\ 0.515 \end{bmatrix} \begin{bmatrix} 1.00 & 0.94 \\ 1.06 & 1.00 \end{bmatrix}$$

$$\therefore [W_s] = \begin{bmatrix} 0.97 \\ 1.03 \end{bmatrix} \tag{H.52}$$

Step 6 Determine the Consistency Vector [CV]

$$[CV] = [W_s] \cdot [1/A_{RAv}]$$

Consistency Vector [CV] in case of 'Security Quality Management' is

$$[CV] = \begin{bmatrix} 0.97 \\ 1.03 \end{bmatrix} \cdot \begin{bmatrix} 1/0.485 \\ 1/0.515 \end{bmatrix} = \begin{bmatrix} 0.97 \\ 1.03 \end{bmatrix} \cdot \begin{bmatrix} 2.06 \\ 1.94 \end{bmatrix}$$

$$\therefore [CV] = \begin{bmatrix} 2 \\ 2 \end{bmatrix} \tag{H.53}$$

Step 7 Determine the average of all elements of [CV], which is represented by λ_{max}. The value for λ_{max} in case of 'Security Quality Management' is

$$\lambda_{max} = (2+2)/2 = 2 \tag{H.54}$$

Step 8 Determine the Consistency Index (CI), n is number of criteria

$$CI = (\lambda_{max} - n)/(n-1)$$

Consistency Index (CI) in case of 'Security Quality Management', where n=2, is

$$CI = (2-2)/(2-1) = 0/1$$

$$\therefore CI = 0 \tag{H.55}$$

Therefore, the priority weights for each criterion is determined. Equation H.51 represents the priority weights for the characteristics of visualisation for 'Security Quality Management'. According to the equation, *Reporting* has the highest priority closely followed by *Feedback*.

References

Adam, E. C. (1993, Oct). Fighter cockpits of the future. In *Digital avionics systems conference, 1993. 12th dasc., aiaa/ieee* (p. 318-323). doi: 10.1109/DASC.1993.283529

Adams, C. N., & Snider, D. H. (2018). Effective data visualization in cybersecurity. In *Southeastcon 2018* (pp. 1–8). IEEE. doi: 10.1109/SECON.2018.8479113

Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud & Security*, *2015*(7), 9 – 17. doi: 10.1016/S1361-3723(15)30066-X

Albar, F. M., & Jetter, A. J. (2013, July). Uncovering project screening heuristics with cognitive task analysis: How do gatekeepers decide which technologies to promote? In *2013 proceedings of picmet '13: Technology management in the it-driven services (picmet)* (p. 459-467). IEEE.

Angelini, M., Aniello, L., Lenti, S., Santucci, G., & Ucci, D. (2017, Oct). The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics. In *2017 ieee symposium on visualization for cyber security (vizsec)* (pp. 1–8). IEEE. doi: 10.1109/VIZSEC.2017.8062199

Angelini, M., Prigent, N., & Santucci, G. (2015, Oct). Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In *Visualization for cyber security (vizsec), 2015 ieee symposium on.* IEEE. doi: 10.1109/VIZSEC.2015.7312764

Arendt, D. L., Burtner, R., Best, D. M., Bos, N. D., Gersh, J. R., Piatko, C. D., & Paul, C. L. (2015, Oct). Ocelot: user-centered design of a decision support visualization for network quarantine. In *Visualization for cyber security (vizsec), 2015 ieee symposium on* (pp. 1–8). IEEE. doi: 10.1109/VIZSEC.2015.7312763

Battle, L., Angelini, M., Binnig, C., Catarci, T., Eichmann, P., Fekete, J.-D., . . . Willett, W. (2018). Evaluating visual data analysis systems: A discussion report. In *Hilda'18: Workshop on human-in-the- loop data analytics* (pp. 4:1–4:6). ACM. doi: 10.1145/3209900.3209901

Best, D. M., Endert, A., & Kidwell, D. (2014). 7 key challenges for visualization in cyber network defense. In *Proceedings of the eleventh workshop on visualization for cyber security* (pp. 33–40). ACM. doi: 10.1145/2671491.2671497

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices* (2nd ed.). Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

Bogdan, R. C., & Biklen, S. K. (2007). *Qualitative research for education : an introduction to theory and methods* (5th ed.). Pearson A& B.

Borland, D., Wang, W., Gotz, D., & Rhyne, T. (2018, Nov). Contextual visualization. *IEEE Computer Graphics and Applications*, *38*(6), 17–23. doi: 10.1109/MCG.2018.2874782

Bourque, L. B., & Fielder, E. P. (2003). *How to conduct self-administered and mail surveys* (2nd ed.). California: Sage Publications.

Brans, J. (1982). *L'ingénierie de la décision: élaboration d'instruments d'aide à la décision. la méthode promethee.* Presses de l'Université Laval.

Braun, V., & Clarke, V. (2006, Jul). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. doi: 10.1191/1478088706qp063oa

Brunelli, M. (2015). *Introduction to the analytic hierarchy process.* Springer International Publishing.

Burns, C. M., Kuo, J., & Ng, S. (2003, Oct). Ecological interface design: A new approach for visualizing network management. *Computer Networks*, *43*(3), 369–388. doi: 10.1016/S1389-1286(03)00287-1

Card, S. (2012). *Information visualization* (Third ed.; J. A. Jacko, Ed.). CRC Press.

Card, S., Mackinlay, J., & Shneiderman, B. (1999). *Readings in information visualization: Using vision to think.* USA: Morgan Kaufmann Publishers.

Carvalho, V. S., Polidoro, M. J., & es, J. P. M. a. (2016, April). Owlsight: Platform for real-time detection and visualization of cyber threats. In *Proc. bigdatasecurity* (pp. 61–66). IEEE. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.73

Castro, F. G., Kellison, J. G., Boyd, S. J., & Kopak, A. (2010, Dec). A methodology for conducting integrative mixed methods research and data analyses. *Journal of Mixed Methods Research*, *4*(4), 342–360. doi: 10.1177/1558689810382916

Ceballos, B., Lamata, M. T., & Pelta, D. A. (2016, Apr). A comparative analysis of multi-criteria decision-making methods. *Progress in Artificial Intelligence*, *4*. doi: 10.1007/s13748-016-0093-1

Christou, N. (2017). *The central limit theorem.* University of California, Los Angeles Department of Statistics - http://www.stat.ucla.edu/~nchristo/statistics100A/stat100a_clt.pdf. (Accessed: 5 May 2017)

Cohen, J. (1992). Quantitive methods in phycology a power primer. *Psychological Bulletin*, *112*(1), 155–159. doi: 10.1037/0033-2909.112.1.155

Cohen, L., Manion, L., & Morrison, K. (2013). *Research methods in education* (7th ed.). Taylor & Francis.

Coudriau, M., Lahmadi, A., & François, J. (2016, Dec). Topological analysis and visualisation of network monitoring data: Darknet case study. In *Proc. wifs* (pp. 1–6). IEEE. doi: 10.1109/WIFS.2016.7823920

Crandall, B., Klein, G., & Hoffman, R. (2006). *Working minds: A practitioner's guide to cognitive task analysis.* Bradford Book.

Creese, S., Goldsmith, M., Moffat, N., Happa, J., & Agrafiotis, I. (2013, Nov). CyberVis: Visualizing the potential impact of cyber attacks on the wider enterprise. In *13th annual ieee conference on technologies for homeland security (hst'13)* (pp. 73–79). IEEE. doi: 10.1109/THS.2013.6698979

D'Amico, A., & Whitley, K. (2007, Oct). The real work of computer network defense analysts. In *Proc. vizsec* (pp. 19–37). Springer Berlin Heidelberg. doi: 10.1007/978-3-540-78243-8_2

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005, Sep). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *49*(3), 229–233. doi: 10.1177/154193120504900304

Denzin, N., & Lincoln, Y. (2012). *Collecting and interpreting qualitative materials* (4th ed.). SAGE Publications.

Department for Digital, Culture, Media and Sport. (2018, april). *Cyber security breaches survey 2018: Main report.* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf. (Accessed: 19 Dec 2018)

Department of Defense, USA. (1998). *Dod modeling and simulation (m&s) glossary* (Tech. Rep.). Defence Technical Information Centre.

Dori, D. (2002). *Object-process methodology: A holistic systems paradigm* (1st ed.). Springer.

Ellis, G., & Dix, A. (2006). An explorative analysis of user evaluation studies in information visualisation. In *Proceedings of the 2006 avi workshop on beyond time and errors: Novel evaluation methods for information visualization* (pp. 1–7). ACM. doi: 10.1145/1168149.1168152

Endsley, M. (2016). *Designing for situation awareness: An approach to user-centered design* (2nd ed.). CRC Press.

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., & Fink, G. (2010, Jan). A multi-phase network situational awareness cognitive task analysis. *Information Visualization*, *9*(3), 204–219. doi: 10.1057/ivs.2010.5

Fay, D., Stanton, N. A., & Roberts, A. (2019, may). All at sea with user interfaces: from evolutionary to ecological design for submarine combat systems. *Theoretical Issues in Ergonomics Science*, *20*. doi: 10.1080/1463922X.2019.1582115

Fay, D., Stanton, N. A., & Roberts, A. P. J. (2018). Assessing sonar and target motion analysis stations in a submarine control room using cognitive work analysis. In *Advances in human aspects of transportation* (pp. 191–198). Springer International Publishing. doi: 10.1007/978-3-319-60441-1_19

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). London: SAGE.

Figueiras, A. (2014, July). How to tell stories using visualization. In *International conference on information visualisation* (pp. 18–26). IEEE. doi: 10.1109/IV.2014.78

Fink, G. A., North, C. L., Endert, A., & Rose, S. (2009, Oct). Visualizing cyber security: Usable workspaces. In *Proc. vizsec* (pp. 45–56). IEEE. doi: 10.1109/VIZSEC.2009.5375542

Fischer, F., Fuchs, J., Vervier, P.-A., Mansmann, F., & Thonnard, O. (2012, 10). VisTracer: a visual analytics tool to investigate routing anomalies in traceroutes. In *VIZSEC 2012, 9th International Symposium on Visualization for Cyber Security, October 15, 2012, Seattle, WA, USA.* Seattle, ÉTATS-UNIS. doi: 10.1145/2379690.2379701

Franke, U., & Brynielsson, J. (2014, Oct). Triangulation. *Computers & Security*, *46*, 18–31. doi: 10.1016/j.cose.2014.06.008

Franklin, L., Pirrung, M., Blaha, L., Dowling, M., & Feng, M. (2017). 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)* (pp. 1–8). IEEE. doi: 10.1109/VIZSEC.2017.8062200

Gates, C., & Engle, S. (2013). Reflecting on visualization for cyber security. In *2013 ieee international conference on intelligence and security informatics* (pp. 275–277). IEEE. doi: 10.1109/ISI.2013.6578842

Gatto, M. A. C. (2015). *Making research useful : current challenges and good practices in data visualisation* (Tech. Rep.).

Golafshani, N. (2003, Jan). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597–606.

Gonzalez, V., & Kobsa, A. (2003, July). Benefits of information visualization systems for administrative data analysts. In *Proceedings on seventh international conference on information visualization* (pp. 331–336). IEEE. doi: 10.1109/IV.2003.1217999

Goodall, J. R. (2008). Introduction to visualization for computer security. In *Vizsec 2007: Proceedings of the workshop on visualization for computer security* (pp. 1–17). Springer Berlin Heidelberg. doi: 10.1007/978-3-540-78243-8_1

Gray, J., & Rumpe, B. (2018, Jul). Uml customization versus domain-specific languages. *Software & Systems Modeling*, *17*(3), 713–714. doi: 10.1007/s10270-018-0685-2

Guide to the project management body of knowledge (PMBOK®guide) (Vol. 5; Project Management Institute). (2013). American National Standard Institute.

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016, March). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In *Proc. cogsima* (pp. 14–20). IEEE. doi: 10.1109/COGSIMA.2016.7497780

Harrison, L., Spahn, R., Iannacone, M., Downing, E., & Goodall, J. R. (2012). NV: Nessus vulnerability visualization for the web. In *Proceedings of the ninth international symposium on visualization for cyber security* (pp. 25–32). ACM. doi: 10.1145/2379690.2379694

Hodgett, R. E. (2016, Jul). Comparison of multi-criteria decision-making methods for equipment selection. *The International Journal of Advanced Manufacturing Technology*, *85*(5), 1145–1157. doi: 10.1007/s00170-015-7993-2

Hwang, C.-L., & Yoon, K. (1981). *Multiple attribute decision making: Methods and applications* (1st ed.). Verlag Berlin Heidelberg: Springer.

Jenkins, D. P., Stanton, N. A., Salmon, P. M., & Walker, G. H. (2009). *Cognitive work analysis: Coping with complexity* (1st ed.). Surrey: Ashgate Publishing Ltd.

Kallas, Z. (2011). Butchers' preferences for rabbit meat; AHP pairwise comparisons versus a likert scale valuation. In *Proceedings of the international symposium on the analytic hierarchy process for multicriteria decision making* (pp. 1–6). Creative Decisions Foundation. doi: 978-88-906147-0-5

Karami, A. (2018, May). An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications*, *108*, 36–60. doi: 10.1016/j.eswa.2018.04.038

Keim, D. A., Mansmann, F., Schneidewind, J., & Ziegler, H. (2006). Challenges in visual data analysis. In *Tenth international conference on information visualisation (iv'06)* (pp. 9–16). IEEE. doi: 10.1109/IV.2006.31

Kemal, M. (2019, March). *Data visualization: Methods, types, benefits, and checklist.* https://www.researchgate.net/publication/332101051_Data_Visualization_Methods_Types_Benefits_and_Checklist/stats. doi: 10.13140/RG.2.2.19618.48324

Konidari, P., & Mavrakis, D. (2007). A multi-criteria evaluation method for climate change mitigation policy instruments. *Energy Policy*, *35*(12), 6235–6257. doi: 10.1016/j.enpol.2007.07.007

Lam, H., Bertini, E., Isenberg, P., Plaisant, C., & Carpendale, S. (2012, September). Empirical studies in information visualization: Seven scenarios. *IEEE Transactions on Visualization and Computer Graphics*, *18*(9), 1520–1536. doi: 10.1109/TVCG.2011.279

Legg, P. A. (2016, June). Enhancing cyber situation awareness for non-expert users using visual analytics. In *Proc. cybersa* (pp. 1–8). IEEE. doi: 10.1109/CyberSA.2016.7503278

Linkov, I., Satterstrom, F., Kiker, G., Batchelor, C., Bridges, T., & Ferguson, E. (2006). From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications. *Environment International*, *32*(8), 1072–1093. doi: 10.1016/j.envint.2006.06.013

Lintern, G. (2016). *Tutorial: Work domain analysis.* http://cognitivesystemsdesign.net/Tutorials/Work%20Domain%20Analysis%20Tutorial.pdf. (Accessed: 20

Feb 2019)

Lugmayr, A., Stockleben, B., Scheib, C., & A. Mailaparampil, M. (2017). Cognitive big data: Survey and review on big data research and its implications. what is really "new" in big data? *Journal of Knowledge Management*, *21*(1), 197–212. doi: 10.1108/JKM-07-2016-0307

M E Capstone Design (415/466). (2014). *AHP part 2.* https://www.youtube.com/watch?v=Gl1Wx-8J-to. (Accessed: 22 Feb 2019)

Machuca, J. P., Miller, M. E., & Colombi, J. M. (2012, March). A cognitive task analysis-based evaluation of remotely piloted aircraft situation awareness transfer mechanisms. In *2012 ieee international multi-disciplinary conference on cognitive methods in situation awareness and decision support* (p. 179-182). IEEE. doi: 10.1109/CogSIMA.2012.6188376

Marty, R. (2008). *Applied security visualization* (1st ed.). Addison-Wesley Professional.

Mathison, S. (2005). Triangulation. In *Encyclopedia of evaluation* (p. 424). Thousand Oaks: SAGE Publications, Inc. doi: 10.4135/9781412950558.n555

McIlroy, R. C., & Stanton, N. A. (2015, April). Ecological interface design two decades on: Whatever happened to the srk taxonomy? *IEEE Transactions on Human-Machine Systems*, *45*(2), 145–163. doi: 10.1109/THMS.2014.2369372

McInerny, G. J., Chen, M., Freeman, R., Gavaghan, D., Meyer, M., Rowland, F., ... Hortal, J. (2014, mar). Information visualisation for science and policy: engaging users and avoiding bias. *Trends in Ecology & Evolution*, *29*(3), 148–157. doi: 10.1016/j.tree.2014.01.003

Mckenna, S., Staheli, D., & Meyer, M. (2015, Oct). Unlocking user-centered design methods for building cyber security visualizations. In *Proc. vizsec* (pp. 1–8). IEEE. doi: 10.1109/VIZSEC.2015.7312771

Mu, E., & Pereyra-Rojas, M. (2018). *Practical decision making using super decisions v3 - an introduction to the analytic hierarchy process.* Springer International Publishing.

Mukasa, K. S., & Kaindl, H. (2008). An integration of requirements and user interface specifications. In *2008 16th ieee international requirements engineering conference* (pp. 327–328). IEEE. doi: 110.1109/RE.2008.55

Nance, K., & Marty, R. (2011, Jan). Identifying and visualizing the malicious insider threat using bipartite graphs. In *System sciences (hicss), 2011 44th hawaii international conference on* (pp. 1–9). doi: 10.1109/HICSS.2011.231

Nielsen, J. (1994). *Heuristic evaluation* (J. Nielsen & R. L. Mack, Eds.). New York: John Wiley & Sons.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.

Peterson, E. (2016, Nov). Dagger: Modeling and visualization for mission impact situation awareness. In *Proc. milcom* (pp. 25–30). IEEE. doi: 10.1109/MILCOM.2016.7795296

Pfleeger, C., & Pfleeger, S. (2006). *Security in computing* (4th ed.). Pearson Education.

Plaisant, C. (2004). The challenge of information visualization evaluation. In *Proceedings of the working conference on advanced visual interfaces* (pp. 109–116). ACM. doi: 10.1145/989863.989880

Purwandari, B. (2013). *Developing a model of mobile web uptake in the developing world* (Doctoral dissertation, School of Electronics and Computer Science, University of Southampton, Southampton, UK). Retrieved from https://eprints.soton.ac.uk/358907/

Qin, X., Huang, G., Chakma, A., Nie, X., & Lin, Q. (2008). A mcdm-based expert system for climate-change impact assessment and adaptation planning a case study for the georgia basin, canada. *Expert Systems with Applications*, *34*(3), 2164–2179. doi: 10.1016/j.eswa.2007.02.024

Recker, J. (2013). *Scientific research in information systems : a beginner's guide* (1st ed.). Springer.

Revilla, M. A., Saris, W. E., & Krosnick, J. A. (2014, Feb). Choosing the number of categories in agree-disagree scales. *Sociological Methods & Research*, *43*(1), 73–97. doi: 10.1177/0049124113509605

Ricca, F., Scanniello, G., Torchiano, M., Reggio, G., & Astesiano, E. (2014, Oct). Assessing the effect of screen mockups on the comprehension of functional requirements. *ACM Transactions on Software Engineering and Methodology*, *24*(1), 1:1–1:38. doi: 10.1145/2629457

Rivero, J. M., Grigera, J., Rossi, G., Luna, E. R., Montero, F., & Gaedke, M. (2014, Jun). Mockup-driven development: Providing agile support for model-driven web engineering. *Information and Software Technology*, *56*(6), 670–687. doi: 10.1016/j.infsof.2014.01.011

Roveta, F., Caviglia, G., Di Mario, L., Zanero, S., Maggi, F., & Ciuccarelli, P. (2011). Burn: Baring unknown rogue networks. In *Proceedings of the 8th international symposium on visualization for cyber security* (pp. 6:1–6:10). ACM. doi: 10.1145/2016904.2016910

Roy, B. (1968). Classement et choix en présence de points de vue multiples. *RAIRO - Operations Research - Recherche Opérationnelle*, *2*(V1), 57–75.

Rutherford, A. (2012). *ANOVA and ANCOVA: A GLM approach* (2nd ed.). New Jersey: John Wiley & Sons.

Saaty, T. L. (1980). *The analytic hierarchy process* (1st ed.). New York: McGraw-Hill.

Saaty, T. L. (2012). *Decision making for leaders: The analytic hierarchy process for decisions in a complex world* (3rd ed.). RWS Publications.

Samant, R., Deshpande, S., & Jadhao, A. (2015, Aug). Survey on multi criteria decision making methods. *International Journal of Innovative Research in Science, Engineering and Technology*, *4*(8), 7175–7178. doi: 10.15680/IJIRSET.2015.0408064

Santhanam, G. R., Holland, B., Kothari, S., & Mathews, J. (2017, Oct). Interactive visualization toolbox to detect sophisticated android malware. In *2017 ieee symposium on visualization for cyber security (vizsec)* (pp. 1–8). IEEE. doi: 10.1109/VIZSEC.2017.8062197

SEBoK. (2019). *Representing systems with models – sebok,.* https://www.sebokwiki.org/w/index.php?title=Representing_Systems_with_Models&oldid=55819. (Accessed: 6 June 2019)

Sethi, A. (2015). *"envision security" – product vulnerability visualisations.* MSc Dissertation, University of Southampton. (unpublished)

Sethi, A., Paci, F., & Wills, G. (2016a, Dec). EEVi - framework and guidelines to evaluate the effectiveness of cyber-security visualization. *International Journal of Intelligent Computing Research*, *7*(4), 761–770. doi: ijicr.2042.4655.2016.0094

Sethi, A., Paci, F., & Wills, G. (2016b, Dec). EEVi - framework for evaluating the effectiveness of visualization in cyber-security. In *Proc. icitst* (pp. 340–345). IEEE. doi: 10.1109/ICITST.2016.7856726

Sethi, A., & Wills, G. (2017, Oct). Expert-interviews led analysis of eevi - a model for effective visualization in cyber-security. In *2017 ieee symposium on visualization for cyber security (vizsec)* (pp. 1–8). IEEE. doi: 10.1109/VIZSEC.2017.8062195

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2019, July). An evaluation framework for network security visualizations. *Computers & Security*, *84*, 70–92. doi: 10.1016/j.cose.2019.03.005

Shiravi, H., Shiravi, A., & Ghorbani, A. A. (2012, Aug). A survey of visualization systems for network security. *IEEE Transactions on Visualization and Computer Graphics*, *18*(8), 1313–1329. doi: 10.1109/TVCG.2011.144

Shneiderman, B. (1996). The eyes have it: a task by data type taxonomy for information visualizations. In *Proceedings 1996 ieee symposium on visual languages* (pp. 336–343). IEEE. doi: 10.1109/VL.1996.545307

Smart, W. (2018, February). *Lessons learned review of the wannacry ransomware cyber attack.* https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf. (Accessed: 8 March 2019)

Staheli, D., Yu, T., Crouser, R. J., Damodaran, S., Nam, K., O'Gwynn, D., . . . Harrison, L. (2014). Visualization evaluation for cyber security: Trends and future directions. In *Proceedings of the eleventh workshop on visualization for cyber security* (pp. 49–56). ACM. doi: 10.1145/2671491.2671492

Stanton, N., Roberts, A., & Fay, D. (2017). Up periscope: understanding submarine command and control teamwork during a simulated return to periscope depth. *Cognition, Technology & Work*, *19*, 399–417. doi: 10.1007/s10111-017-0413-7

Stanton, N., Salmon, P., Jenkins, D., & Walker, G. (2009). *Human factors in the design and evaluation of central control room operations.* CRC Press.

SWEBOK: Guide to the software engineering body of knowledge (Vol. 2; IEEE Computer Society). (2015, October). International Organization for Standardization.

Szafir, D. A. (2018, Jun). The good, the bad, and the biased: Five ways visualizations can mislead (and how to fix them). *Interactions*, *25*(4), 26–33. doi: 10.1145/3231772

Teets, J. M., Tegarden, D. P., & Russell, R. S. (2010). Using cognitive fit theory to evaluate the effectiveness of information visualizations: An example using quality assurance data. *IEEE Transactions on Visualization and Computer Graphics*, *16*(5), 841–853. doi: 10.1109/TVCG.2010.21

The Interaction Design Foundation. (2019). *The glossary of human computer interaction.* https://www.interaction-design.org/literature/book/the-glossary-of-human-computer-interaction/mock-ups#toc_0_1. (Accessed: 15 Feb 2019)

The National Cyber Security Centre. (2018, Jan). *National cyber security centre glossary.* https://www.ncsc.gov.uk/glossary. (Accessed: 04 Feb 2019)

Tory, M., & Moller, T. (2005, Sept). Evaluating visualizations: do expert reviews work? *IEEE Computer Graphics and Applications*, *25*(5), 8–11. doi: 10.1109/MCG.2005.102

Triantaphyllou, E., Shu, B., Sanchez, S. N., & Ray, T. (1998). Multi-criteria decision making: An operations research approach. *Encyclopedia of Electrical and Electronics Engineering*, *15*, 175–186.

Ulmer, A., Schufrin, M., Sessler, D., & Kohlhamme, J. (2018, Oct). Visual-interactive identification of anomalous ip-block behavior using geo-ip data. In *2018 ieee symposium on visualization for cyber security (vizsec).*

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5), 100–110. doi: 10.5430/jnep.v6n5p100

Varga, S., Brynielsson, J., & Franke, U. (2018, Aug). Information requirements for national level cyber situational awareness. In *2018 ieee/acm international conference on advances in social networks analysis and mining (asonam)* (pp. 774–781). IEEE Computer Society. doi: 10.1109/ASONAM.2018.8508410

Velasquez, M., & Hester, P. T. (2013, May). An analysis of multi-criteria decision making methods. *International Journal of Operations Research*, *10*(2), 56–66.

Vessey, I. (2015). The theory of cognitive fit: One aspect of a general theory of problem-solving. In Y. Zhang, P. Zhang, & D. Galletta (Eds.), *Human-computer interaction and management information systems: Foundations* (pp. 141–183). Taylor & Francis.

Vicente, K. J. (2002, Mar). Ecological interface design: Progress and challenges. *Human Factors*, *44*(1), 62–78. doi: 10.1518/0018720024494829

Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., & Wickens, C. (2016, Sep). Addressing human factors gaps in cyber defense. *Proceedings of the Human*

Factors and Ergonomics Society Annual Meeting, *60*(1), 770–773. doi: 10.1177/1541931213601176

von Solms, R., & van Niekerk, J. (2013, Oct). From information security to cyber security. *Computers & Security*, *38*, 97–102. doi: 10.1016/j.cose.2013.04.004

Ware, C. (2013). *Information visualization: Perception for design* (3rd ed.). Morgan Kaufmann Publishers.

Watson, S., & Lipford, H. R. (2017, July). A proposed visualization for vulnerability scan data. In *Thirteenth symposium on usable privacy and security (SOUPS 2017).* USENIX Association.

World Economic Forum. (2018, January). *The global risks report.* https://www.weforum.org/reports/the-global-risks-report-2018. (Accessed: 19 Dec 2018)

World Economic Forum. (2019, January). *The global risks report.* https://www.weforum.org/reports/the-global-risks-report-2019. (Accessed: 8 Mar 2019)

Wüchner, T., Pretschner, A., & Ochoa, M. (2014). Davast: Data-centric system level activity visualization. In *Proceedings of the eleventh workshop on visualization for cyber security* (pp. 25–32). ACM. doi: 10.1145/2671491.2671499

Yuen, J., Turnbull, B., & Hernandez, J. (2015, Oct). Visual analytics for cyber red teaming. In *Visualization for cyber security (vizsec), 2015 ieee symposium on.* IEEE. doi: 10.1109/VIZSEC.2015.7312765

Zage, D., & Zage, W. (2010). *Intrusion detection system visualization of network alerts* (Tech. Rep.). Defence Technical Information Centre.

Zage, W., Zage, D., Gaw, T., & Mast, T. (2011, November). *Exploring 3-dimensional visual intrusion detection systems of network alerts* (Tech. Rep.). Army Research Labs.

Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information Security Journal: A Global Perspective*, *21*(4), 183–192. doi: 10.1080/19393555.2011.654318

Zhao, H., Tang, W., Zou, X., Wang, Y., & Zu, Y. (2019, Aug). Analysis of visualization systems for cyber security. In *Recent developments in intelligent computing, communication and devices* (pp. 1051–1061). Springer. doi: 10.1007/978-981-10-8944-2_122

Zhong, Z., Zhao, Y., Shi, R., Sheng, Y., Liu, J., Meng, H., & Lin, D. (2018, Sep). A user-centered multi-space collaborative visual analysis for cyber security. *Chinese Journal of Electronics*, *27*(5), 910–919. doi: 10.1049/cje.2017.09.021