DEVELOPMENT OF BUG FREE *MODEL FOR CYBER SECURITY*

(Font-24 and center)

Author:
Araga Babu Rajendra Prasad Reddy

Research Scholar
Hyderabad
India

ABSTRACT

*This paper describes the development process of **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. MODEL 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.*

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 MODEL could be built by forming relationships from the themes that arose.

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. 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.

Keywords: Thematic Analysis, Escalation Analysis, Security Management

1. What is Cognitive Task?

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 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 toform requirements for the cyber-security visualisation tool they were developing. One ofthe 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 *MODEL*.

1. Thematic Analysis

The development of the *MODEL* model used a qualitative *bottom-up* approach, called *Thematic Analysis*, to define the aspects within *MODEL*. A *bottom-up* approach involvesgoing 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 ideasfor 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, anidea 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 thesignificance of the data and represents a patterned response, which is reflectedby 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. Atthis stage, the relationships between the potential candidate themes and codesstarts 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 theyfit 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 ofthematic analysis of the dataset. The cognitive relationships lead to a storyline which presents the narrative of a coherent story through which themes canbe 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).

2. Process of Thematic Analysis

The development of the model was an iterative process using Thematic Analysis. Therewere 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 todevelop the model.

3.1 Familiarising with Data

The research papers that were used for the development of *MODEL* 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”.

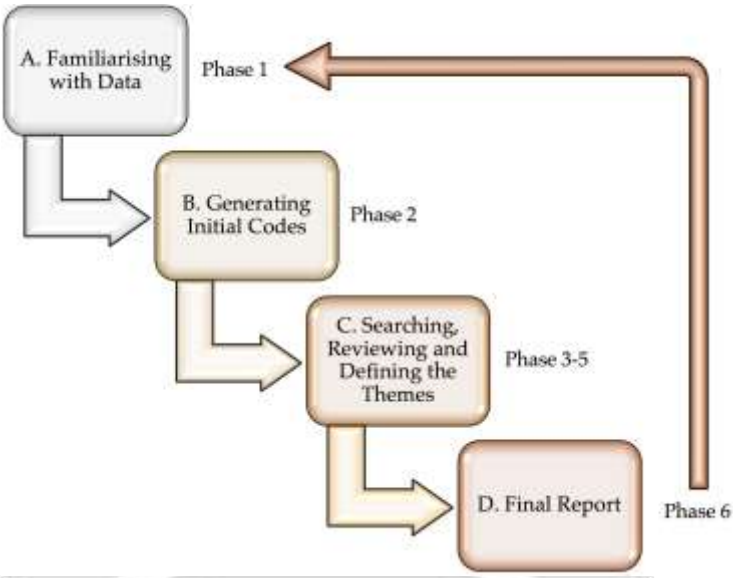

Figure 3.1: Overview of Thematic Analysis, the methodology followed for the development of *MODEL* in four stages.

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 *MODEL*, 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 *MODEL* (Chapter 4) with seven expert cyber-security analysts, followed by a confirmation of *MODEL* (Chapter 5) with analysts, mostly from cyber-security domain. This would make the generalisability of *MODEL* 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 amodel 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 andStuart 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 whichgave insight into the roles, goals, obstacles and activities of the analysts in an organisation.

3.2 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 extractof 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

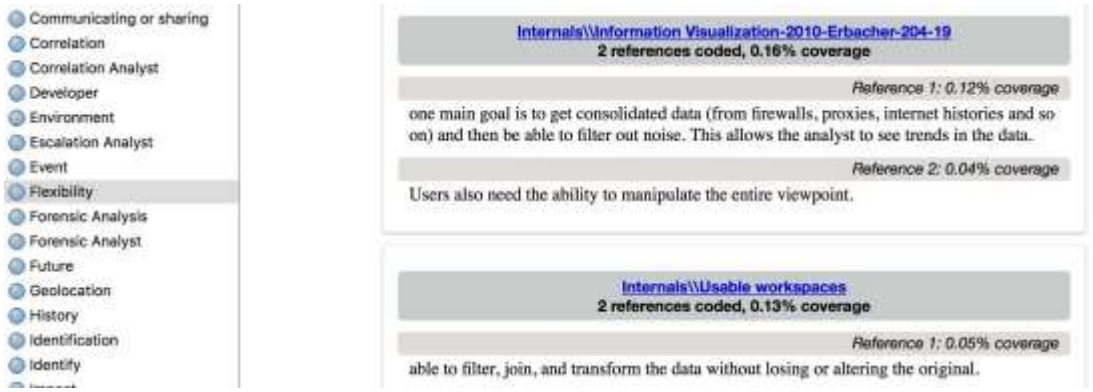

Figure 3.2: Extract of initial codes (on the left), with excerpt of data (on theright), generated in NVivo 11 Software [4].

3.3 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:

Analysis of Data: Task performed by cyber-security analysts;

Data: Type of data used to perform the task;

Features of Visualisation: Features required to perform the t
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.

3.4 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 thename 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 enforcementagencies.	13 occurrences
Security Quality Management (SQM)	The task related to services, such as tutorials or training, that maintain the quality of information security in anorganisation.	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 andarranges 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 thepurpose 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 analyticalprocess.	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 data- sets.	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 (Communicatio n)	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 coordinateall views.	8 occurrences

The cognitive relationships influenced the development of *MODEL* 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 *MODEL*, which is explained in greater detail in the next section.

3.5 Secondary Coder

3. 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 atthe 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. AppendixA presents the results for all identified codes. A visual representation of the cognitiverelationship, is displayed in Figure 3.4.

Table 3.6: Results of Searches in NVivo to find Association between AssociatedCodes 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)

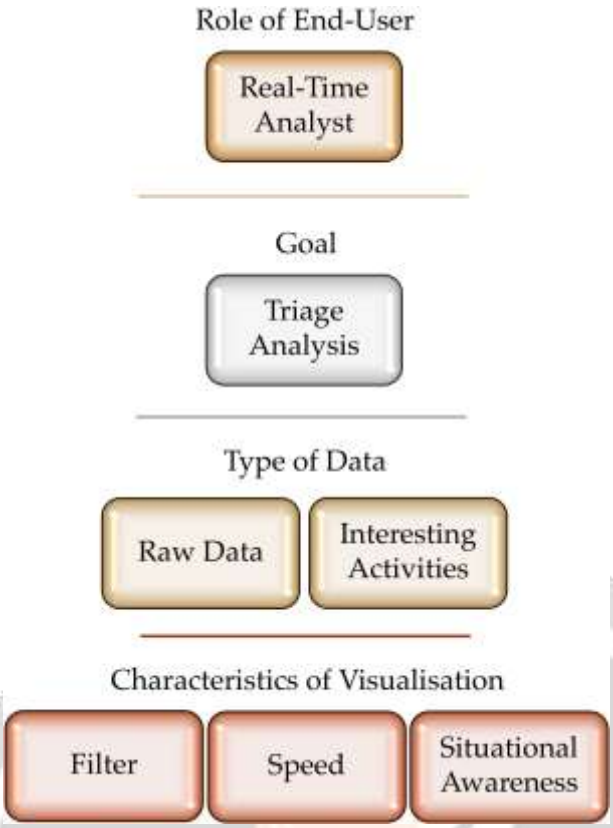

Figure 3.4: Visual representation of cognitive relationship for 'Triage Analysis', with themes and their constituent codes, showing the guidelines for designing the task.

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.

4. 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. Lookingat 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 relationshipis 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 thatis 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 definedat 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.

5. CONCLUSIONS

MODEL was developed to bridge the research gap by standardising design techniques for cyber-security visualisation for the performed task. These guidelines are formedas a result of cognitive relationships associated with the performed task, in the logic sequence derived from *MODEL*'s structure (Figure 3.3). Using 'Thematic Analysis' to develop *MODEL* 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 *MODEL*, as based on the information in this chapter, must consist of *Goal*, *Type of Data*, *Role of End-User* and *Characteristicsof Visualisation*, as outlined for each task.

MODEL 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

6. 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.

1. 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

2. 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

3. 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

4. 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*