EEVi – Framework for Evaluating the Effectiveness of Visualization in Cyber-Security

Aneesha Sethi, Federica Paci, Gary Wills
Electronics and Computer Science, University of Southampton, Southampton, UK
{Aneesha.Sethi, F.M.Paci}@soton.ac.uk, gbw@ecs.soton.ac.uk

Abstract— **Cyber-security visualization is an up-and-coming area which aims to reduce security analysts' workload by presenting information as visual analytics rather than a string of text and characters. But the adoption of the resultant visualizations has not increased. The literature indicates a research gap of a lack of guidelines and standardized evaluation techniques for effective visualization in cyber-security, as a reason for it. Therefore, this research addresses the research gap by developing a framework called EEVi for effective cyber-security visualizations for the performed task. The term 'effective visualization' can be defined as the features of visualization that are crucial to perform a certain task successfully. EEVi has been developed by analyzing qualitative data that leads to the formation of cognitive relationships (called *links*) between data that act as guidelines for effective cyber-security visualization in terms of the performed task. The methodology to develop this framework can be applied to other fields to understand cognitive relationships between data. Additionally, the analysis presents a glimpse into the usage of EEVi in cyber-security visualization.**

Keywords- Cyber-security; Data visualization; Data analysis; Cognition; Human Factors;

I. Introduction

In the field of cyber-security, public and private sectors rely on the expertise and capabilities of security analysts to protect assets and resources connected via computer networks. An area under the umbrella of cyber-security is cyber-security visualization, which provides these analysts with visual data rather than textual data for analysis. The main goal of cyber-security visualization is to provide effective tools [13] that help detect, monitor and mitigate sophisticated technical and social attacks in a timely manner. Thus, it focuses on providing security analysts with a competent tool to prevent and defend against these attacks.

There is an outburst of cyber-security visualization tools, but the visualizations presented by these tools are rarely evaluated for effectiveness in terms of the task they aid in performing [20]. Furthermore, most of the visuals are developed and sometimes evaluated without any involvement of users [20]. The lack of user-involvement could be a result of limited access to security analysts; or due to the nature of their jobs, security analysts cannot make significant time-commitment [16]. This leads to low adoption rate of tools. Rachel King, in The Wall Street Journal, states that only 15% of security analyst are using cyber-security visualizations to aid in performing their tasks [14].

This paper introduces EEVi, a framework for evaluating the effectiveness of visualization in cyber-security. This framework has been developed by qualitatively analyzing requirements of security analysts based on the task they perform. Section II introduces the background literature that led to the identification of the research gap. Section III describes the methodology of qualitative coding that was followed to develop the framework and Section IV introduces the structure of the framework developed as a result. Section V presents the analysis conducted from the framework and Section VI concludes this paper along with an outline of the future work to be undertaken.

II. Background Literature

The authors discovered a research gap, during the review of literature; most cyber-security visualization tools introduced had minimal or no evaluation of the visuals that were displayed. Hence a user could not judge the effectiveness of these visuals for the tasks performed by security analysts. The following section explains the background literature that led to and aided the development of the framework.

In the field of cyber-security, there is an explosion of tools that focus on different aspects of cyber-security visualization ranging from a high level view of the system to a technical low level view. Most of these newly developed tools can be broadly classified into three categories; network analysis, malware analysis and insider threat analysis. Most of these tools provide situational awareness. Situational awareness is a high-level abstraction view [12] of the system which presents an overview of the system and is beneficial to both technical and non-technical people as it aims to bridge the knowledge gap between the two.

- *Network Analysis* tools focus on mapping the physical network of the system to detect possibilities of attack. It includes tools which visually monitor network traffic using intrusion detection techniques [9] or tools which present visualizations of the state of the network for real-time monitoring and network management [4]. Additionally, there exist some proactive tools that display graphs to highlight potential attack vectors [3] based on the state of the network. All of these tools use different kinds of visualizations ranging from the attack-graphs [3] to complicated customized visualizations that look like petri dishes [4].

- *Malware Analysis* tools focus on identifying, detecting and eliminating malware. It includes tools that focus on visually detecting rogue autonomous systems leading to possible malware [19] or tools that detect malware attacks and determine its effects [22]. These tools mainly use different kinds of graphs and charts to present the analysis.
- *Insider Threat Analysis* focuses on analyzing attacks by malicious insiders, people who intentionally try to misuse the legitimate information they have access to. It includes tools that visually detect anomalies and possible attacks through pattern matching [7] or by using machine learning to check for anomalous behavior [1]. Other tools establish acceptable action patterns to easily detect anomalous patterns [17]. These tools use visualizations like color maps [7] and different types of graphs like attack-pattern trees [1] or bipartite graphs [17].

However, these tools have not been evaluated to determine their effectiveness in terms of the task they are used to perform. Staheli et al. [20] presented a survey, in 2014, of 130 VizSec (IEEE Symposium on Visualization for Cyber Security) papers which showed that little research had been conducted in determining the effectiveness of cyber-security visualization. It also showed that 46% of these papers did not have any user-involvement in the evaluation phase. To reinforce the results of this survey, the authors conducted a survey of nine papers. It was observed that two of these had no form of evaluation, three did not have any user-involvement and only one allowed complete and unguided interaction with the visualization. Additionally, there was a lack of standardization of evaluation techniques.

The visualizations presented by cyber-security visualization tools were not effective and usually did not take into account the needs of the user or involve them in the evaluation process. This resulted in a low adoption rate of these tools [5]. An assessment of user requirements must be included during the early design phases and later evaluation phases. Additionally, the evaluation techniques used to evaluate most tools were not effective in evaluating the visualizations that were produced based on the performed task nor were the evaluation techniques standardized. The lack of a common framework for standardized evaluation methods [20] has been concluded many times, but there is no research supporting the development of a framework to evaluate the effectiveness of cyber-security visualization tools based on user requirements. Thus, creating a need for guidelines to standardize evaluation techniques and evaluate for effectiveness of performed task.

The main challenge faced in conducting research is this area is a lack of access to experts. One of the goals of D'Amico et al. [10] of the CTA analysis they conducted was having the results used as foundation material for studies with lack of access to security experts or analysts. This led to a need for cognitive task analysis (CTA) papers for cyber-security visualization.

The idea of the use of CTA papers was introduced by Mckenna et al. [16], who used qualitative coding of CTA papers to form requirements for the cyber-security visualization tool they were developing. Additionally, Lam et al. [15] used qualitative coding to describe different evaluation techniques currently used. Vessey's theory of cognitive fit has a classification of spatial tasks, which require problems to be looked at as a whole, and require "...making associations or perceiving relationships in the data" [21] to find effective solutions for the problems. Thus, EEVi is developed on analysis of qualitative papers to form cognitive relationships for effective guidelines for cyber-security visualization.

III. Methodology

The EEVi framework was developed using Thematic Analysis which is a qualitative bottom-up approach. A bottom-up approach means going through the data, without any pre-conceived notions, to completely develop notions or in this case, themes and codes. Thematic Analysis is a qualitative analytic method used to identify, examine and report patterns (or themes) within the data [6].

The four major steps of Thematic Analysis (Fig. 1) which led to the development of the EEVi framework [6]:

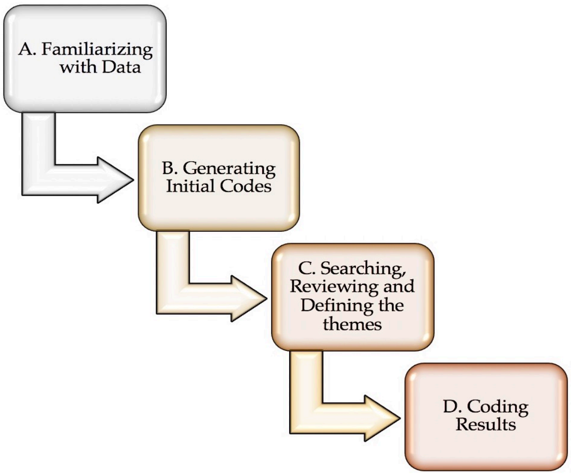

A. Familiarizing with Data
B. Generating Initial Codes
C. Searching, Reviewing and Defining the themes
D. Coding Results

Figure 1: Overview of the methodology followed for Thematic Analysis.

A. Familiarizing with Data

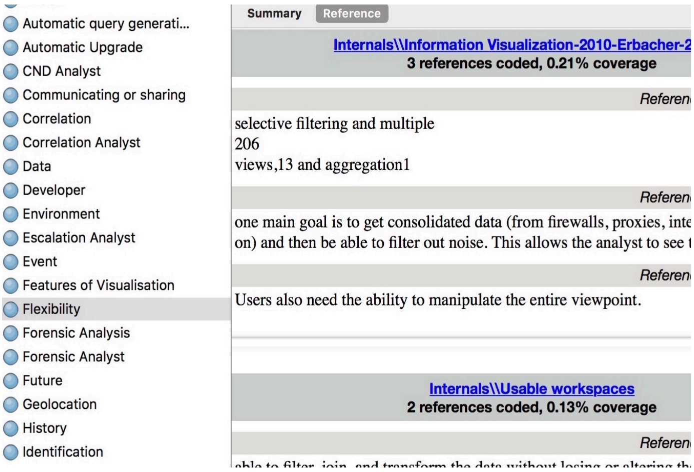
The data that formed the basis of EEVi was mainly derived from papers that presented results of Cognitive Task Analysis (CTA) of security analysts. CTA is borne from the field of applied psychology, which attempts to follow an inductive approach rather than trying to identify predefined data [2]. It has been used in many studies to describe the cognition (or the way the mind works) necessary for task performance and to extract mental models or in this case, how analysts achieve situational awareness for cyber-security [8]. Most studies generally include interviews, observations and hypothetical scenario creation [10].

The papers that were used for the purpose of this research were: D'Amico et al. [10], D'Amico et al. [11], Erbacher et al. [12], Fink et al. [13] and Mckenna et al. [16]. The reasons these papers were chosen was because of the data they presented. These papers gave precise details about analyst roles, the type of data they used, how the analysis were conducted, what the analysts thought about visualization approaches and their experiences, if any, with visualizations. D'Amico et al. [10] and D'Amico et al. [11] gave insight into roles of analysts and the tasks they perform in organizations. Erbacher et al. [12] presents interviews with analysts for the specific purpose of cyber-security visualization. Fink et al. [13] presents a variety of information about how to make visualizations useful for security analysts and Mckenna et al. [16] formed the basis of this study and helped understand how to research these papers and take out the relevant elements from it. Thus, these papers formed the basis of the EEVi framework.

B. Generating Initial Codes

The next step began after the papers were read and an initial list of ideas represented in the papers had been formulated. The list is further analyzed and used to produce the initial set of codes as seen in Fig. 2. These codes represent an extract of data and are thus named accordingly identifying the aspect of the data it represents.

The codes represent the qualitative aspects of the framework which is represented by a *codebook*. A *codebook* includes a collated list of all the initially generated codes. At this stage an idea of the themes start to form but are not yet defined.



Automatic query generati...
Automatic Upgrade
CND Analyst
Communicating or sharing
Correlation
Correlation Analyst
Data
Developer
Environment
Escalation Analyst
Event
Features of Visualisation
Flexibility
Forensic Analysis
Forensic Analyst
Future
Geolocation
History
Identification

Summary | Reference

Internals\\Information Visualization-2010-Erbacher-2
3 references coded, 0.21% coverage

Referen

selective filtering and multiple
206
views,13 and aggregation1

Referen

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

Referen

Users also need the ability to manipulate the entire viewpoint.

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

Referen

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

Figure 2: Snippet of initial codes generated with extract of data using QSR International's NVivo 11 Software [18].

C. Searching, Reviewing and Defining the Themes

The next step is to define the themes based on the codebook that has been generated in the previous step. A theme captures the sigificance of the data and represents a patterned response [6] which is reflected by the group of codes it defines.

The codebook consists of a list of different codes that were identified across the dataset. The next task is to sort the codes and search for potential themes. At this stage the relationships between the potential themes and codes also starts to form.

The potential themes are then reviewed against the codes they represent and further refined. Then the potential themes are reviewed against the dataset and research questions to validate the representation of the theme by reviewing the relationships the themes form against the data.

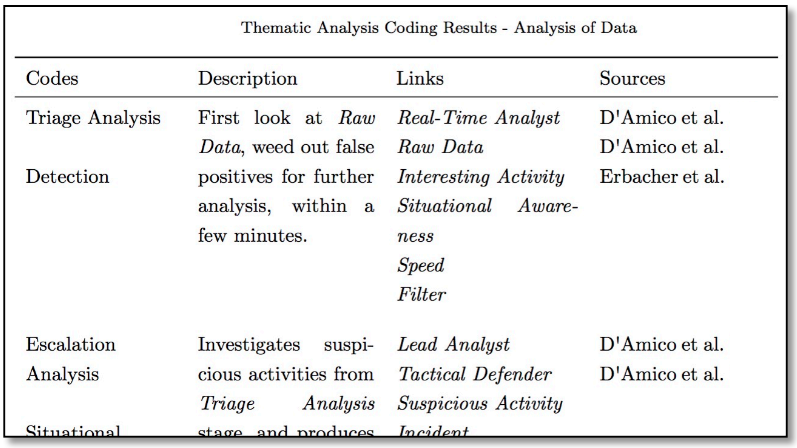
Thus, the themes are defined according to the data it represents and how it fits in relation to the data set and the research questions. The identified themes were:

1. *Analysis of Data* – Task performed by security analysts;
2. *Data* – Type of data used to perform tasks;
3. *Feature of Visualization* – Features of visualization required to perform the tasks;

Role of Analyst – The security analyst that perform the tasks.

D. *Coding Results*

The results identify the themes, codes and relationships or *links* identified as a result of thematic analysis of the dataset. The results formed four tables, one for each theme, with the codes, its description, links to other codes and the sources, as shown below in Fig 3.



Thematic Analysis Coding Results - Analysis of Data

Codes	Description	Links	Sources
Triage Analysis Detection	First look at *Raw Data*, weed out false positives for further analysis, within a few minutes.	*Real-Time Analyst* *Raw Data* *Interesting Activity* *Situational Awareness* *Speed* *Filter*	D'Amico et al. D'Amico et al. Erbacher et al.
Escalation Analysis Situational	Investigates suspicious activities from *Triage Analysis* stage and produces	*Lead Analyst* *Tactical Defender* *Suspicious Activity* *Incident*	D'Amico et al. D'Amico et al.

Figure 3: Snippet of the final results of Thematic Analysis.

The cognitive relationships, defined as *links*, influenced the development of the EEVi framework. The cognitive relationships formed between different codes led to a similar generic structure of themes each time. This structure was refined and formed the structure of the EEVi framework.

IV. Structure of EEVi

The results identified in the previous section were cognitively linked together and led to the EEVi framework to determine the effectiveness of visualization depending on the performed task. The structure of the framework can be seen in Fig. 4.

The framework forms *links* (or cognitive relationships) between the four themes to determine the effectiveness of a tool. These themes are defined by a set of codes. When these codes are cognitively linked together with the data from the qualitative analysis, it forms a cognitive relationship. This relationship defines codes from each theme that would be imperative for an effective visualization for the performed task when linked together cognitively.

Thus the generic structure of the framework can be defined as Role of Analyst *performs* Analysis of Data *using* Data and *requiring* Features of Visualization to create effective cyber-security visualization.

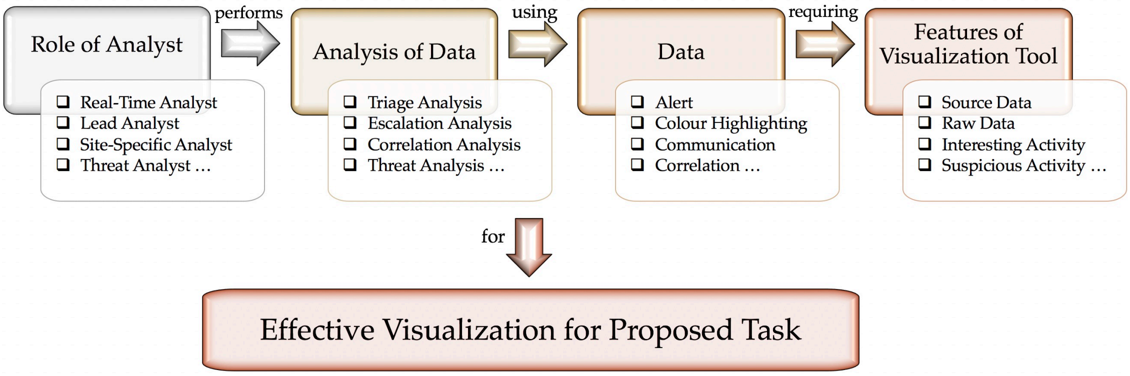


Figure 4: Structure of EEVi Framework for deriving effective visualisation.

V. Analysis

The structure of EEVi led to a generic relationship that required cognitive relationships to form guidelines for effective visualization for the performed task.

The results of the qualitative coding led to the identification of eight tasks that are performed by security analysts. The framework develops cognitive relationships for each of these tasks to determine the crucial features of visualization that are required to successfully perform the task. These tasks are:

1. *Triage Analysis* 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.
2. *Escalation Analysis* is investigation of suspicious activities from the previous stage and production of reports. It may take from hours to a few weeks to complete.
3. *Correlation Analysis* is the search for patterns and trends in data, which may be previously unrecognized. It may take from weeks to a few months to complete.
4. *Threat Analysis* is an intelligent analysis using additional data sources to profile attackers and their motivations.
5. *Incident Response Analysis* is when the analyst recommends or implements actions against a confirmed incident.
6. *Forensic Analysis* is gathering and preservation of data to support law enforcement agencies. It may take from hours to a few weeks to complete.
7. *Impact Assessment* is the task of identification of impact, damage and potential critical nodes that may be reachable after a breach.
8. *Security Quality Management* is the task related to services that support information security in an organization like tutorials or training.

An example of the cognitive relationship can be seen below. It defines the task, identifies the analyst, data source and features of visualization that are crucial for the performed task. The codes are represented along with a snippet of the data that leads to the guidelines for effective visualization.

Triage Analysis is usually performed by Real- Time Analyst [10]. It is the "...first look at the raw data and interesting activity" [10] and hence uses Raw Data and Interesting Activities as types of Data. Visualization for Triage Analysis requires abilities to Filter for "...initial filtering" [10] and for "...weeding out false positives..." [11]. It also requires Speed of data access as "...triage period should be on the order of minutes" [12] and a "...relatively fast decision..." [10] 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" [12]. This would lead to an effective visualization for Real-Time Analyst performing Triage Analysis.

A visual representation of this relationship is displayed in Fig. 5.

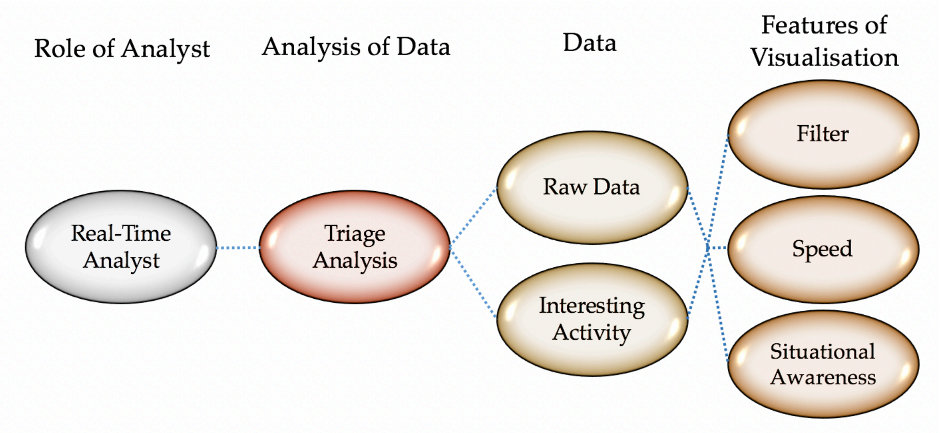


Figure 5: Visual representation of cognitive relationship for Triage Analysis, as derived from the framework.

VI. Conclusion and Future Work

The literature review draws attention to a major issue in the field of cyber-security visualization vis-à-vis the lack of standardized evaluation techniques for effective visualization. The current evaluation techniques are neither standardized nor inclusive of user-validation. This leads to a cloud of uncertainty regarding the effectiveness of visualizations for cyber-security. Hence, there arose the need for a framework which appreciates the requirements of users (security analysts) and evaluates the effectiveness of cyber-security visualization for the performed task.

EEVi bridges the research gap by standardizing evaluation techniques using guidelines for effective cyber-security visualization for the performed task. These guidelines are formed as a result of the cognitive relationships or *links* formed for the performed task (Fig. 5) in the logic sequence derived from the structure of the framework (Fig. 4).

The future work for this research is to use the results of qualitative coding (Fig. 3) to develop guidelines for effective visualization for cyber-security for all tasks performed by security analysts. These guidelines will be used for evaluating the effectiveness of cyber-security visualizations. Thus, this would present a useful solution to the research gap of a lack of guidelines and standardized evaluation techniques for effective visualization in cyber-security.

ACKNOWLEDGMENT

We thank the University of Southampton for sponsoring and providing the necessary resources and guidance to perform this research. We also thank Toby Wilkinson, Nawfal Fadhel and Giles Howard for their careful proof reading and useful advice.

REFERENCES

[1] I. Agrafiotis, J. R. Nurse, O. Buckley, P. Legg, S. Creese, and M. Goldsmith. Identifying attack patterns for insider threat detection. Computer Fraud & Security, 2015(7):9 – 17, 2015.

[2] F. M. Albar and A. J. Jetter. 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), pages 459–467, July 2013.

[3] M. Angelini, N. Prigent, and G. Santucci. Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on, pages 1–8, Oct 2015.

[4] D. L. Arendt, R. Burtner, D. M. Best, N. D. Bos, J. R. Gersh, C. D. Piatko, and C. L. Paul. Ocelot: user-centered design of a decision support visualization for network quarantine. In Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on, pages 1–8, Oct 2015.

[5] D. M. Best, A. Endert, and D. Kidwell. 7 key challenges for visualization in cyber network defense. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security, VizSec '14, pages 33–40, New York, NY, USA, 2014. ACM.

[6] V. Braun and V. Clarke. Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2):77–101, 2006.

[7] J. B. Colombe and G. Stephens. Statistical profiling and visualization for detection of malicious insider attacks on computer networks. In Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, VizSEC/DMSEC '04, pages 138–142, New York, NY, USA, 2004. ACM.

[8] B. Crandall, G. Klein, and R. Hoffman. Working Minds: A Practitioner's Guide to Cognitive Task Analysis. A Bradford Book. Bradford Book, 2006.

[9] S. Creese, M. Goldsmith, N. Moffat, J. Happa, and I. Agrafiotis. CyberVis: Visualizing the potential impact of cyber attacks on the wider enterprise. In 13th annual IEEE Conference on Technologies for Homeland Security (HST'13), 2013.

[10] A. D'Amico and K. Whitley. The Real Work of Computer Network Defense Analysts, pages 19–37. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[11] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth. 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, 2005.

[12] R. F. Erbacher, D. A. Frincke, P. C. Wong, S. Moody, and G. Fink. A multi-phase network situational awareness cognitive task analysis. Information Visualization, 9(3):204–219, June 2010.

[13] G. Fink, C. North, A. Endert, and S. Rose. Visualizing cyber security: Usable workspaces. In Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on, pages 45–56, Oct 2009.

[14] R. King. Security professionals stymied by outdated visualization tools. The Wall Street Journal, April 2015. Accessed:2016-5-19.

[15] H. Lam, E. Bertini, P. Isenberg, C. Plaisant, and S. Carpendale. Seven Guiding Scenarios for Information Visualization Evaluation. Research Report 2011-992-04, 2011. Superseded by and improved in a follow-up journal article.

[16] S. Mckenna, D. Staheli, and M. Meyer. Unlocking user-centered design methods for building cyber security visualizations. In Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on, pages 1–8, Oct 2015.

[17] K. Nance and R. Marty. Identifying and visualizing the malicious insider threat us- ing bipartite graphs. In System Sciences (HICSS), 2011 44th Hawaii International Conference on, pages 1–9, Jan 2011.

[18] NVivo qualitative data analysis Software; QSR International Pty Ltd. Version 11, 2015.

[19] F. Roveta, G. Caviglia, L. Di Mario, S. Zanero, F. Maggi, and P. Ciuccarelli. Burn: Baring unknown rogue networks. In Proceedings of the 8th International Symposium on Visualization for Cyber Security, VizSec '11, pages 6:1–6:10, New York, NY, USA, 2011. ACM.

[20] D. Staheli, T. Yu, R. J. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, S. McKenna, and L. Harrison. Visualization evaluation for cyber security: Trends and future directions. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security, VizSec '14, pages 49–56, New York, NY, USA, 2014. ACM.

[21] I. Vessey. The theory of cognitive fit: One aspect of a general theory of problem- solving. In Y. Zhang, P. Zhang, and D. Galletta, editors, Human-computer Interaction and Management Information Systems: Foundations, chapter 8, pages 141–183. Taylor & Francis, 2015.

[22] T. Wüchner, A. Pretschner, and M. Ochoa. Davast: Data-centric system level activity visualization. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security, VizSec '14, pages 25–32, New York, NY, USA, 2014. ACM.