UNIVERSITY OF Southampton

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

Aneesha Sethi, Federica Paci, Gary Wills

Aneesha.Sethi@soton.ac.uk

School of Electronics and Computer Science

December 5, 2016

International Conference for Internet Technology and Secured Transactions

Introduction

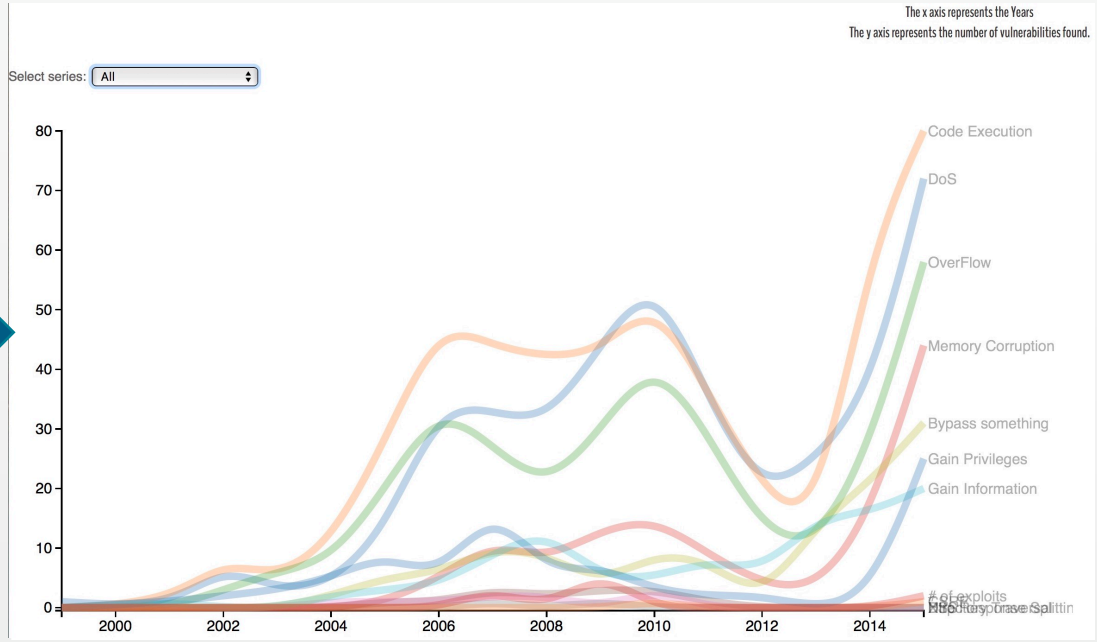
- Visualization in Cyber-Security
  - Presents information as visual analytics rather than string of text and characters for analysis.
  - An effective tool that helps detect, monitor and mitigate sophisticated technical and social attacks in a timely manner[1].
  - There is an outburst of these tools that focus on different aspects of cyber-security visualization ranging from a high level view of the system to a technical low level view.

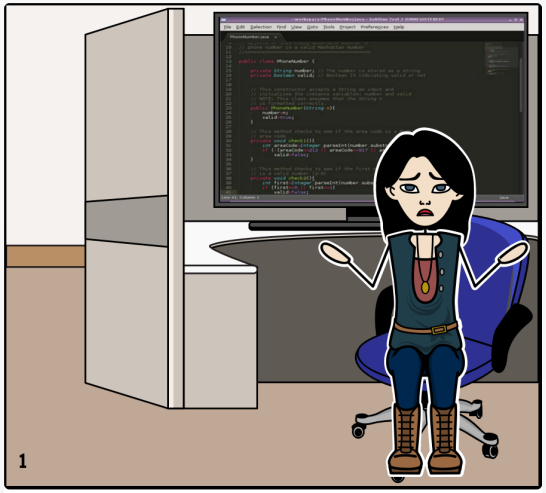
[1] G. Fink, C. North, A. Endert, and S. Rose. Visualizing cyber security: Usable workspaces. In Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on, pages 45–56, Oct 2009.

Introduction

- Visualization in Cyber-Security

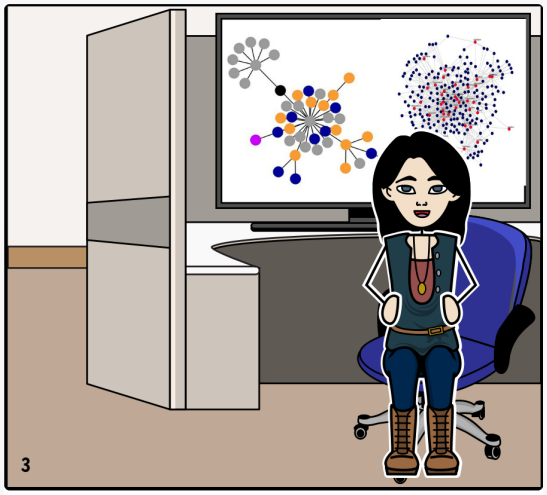
```
indicatorName,indicatorCode,year,yearCode,DoS,Code Execution,OverFlow,Memory Corruption,SQL Injection,XSS,Directory Traversal,Http Response Splitting,Bypass something,Gain Information,Gain Privileges,CSRF,File Inclusion,# of exploits
DoS,DoS,1999,YR1999,1, , , , , , , , , , , ,
DoS,DoS,2001,YR2001,0, , , , , , , , , , , ,
DoS,DoS,2002,YR2002,7, , , , , , , , , , , ,
DoS,DoS,2003,YR2003,3, , , , , , , , , , , ,
DoS,DoS,2004,YR2004,4, , , , , , , , , , , ,
DoS,DoS,2005,YR2005,13, , , , , , , , , , , ,
DoS,DoS,2006,YR2006,34, , , , , , , , , , , ,
DoS,DoS,2007,YR2007,33, , , , , , , , , , , ,
DoS,DoS,2008,YR2008,31, , , , , , , , , , , ,
DoS,DoS,2009,YR2009,44, , , , , , , , , , , ,
DoS,DoS,2010,YR2010,56, , , , , , , , , , , ,
DoS,DoS,2011,YR2011,35, , , , , , , , , , , ,
DoS,DoS,2012,YR2012,19, , , , , , , , , , , ,
DoS,DoS,2013,YR2013,25, , , , , , , , , , , ,
DoS,DoS,2014,YR2014,36, , , , , , , , , , , ,
DoS,DoS,2015,YR2015,72, , , , , , , , , , , ,

All,All,1999,YR1999,1,0,0,0, ,0,0,0,0,0,0,0, ,0,
All,All,2001,YR2001,0,1,0,0, ,0,0,0,0,1,1,0, ,0,
All,All,2002,YR2002,7,8,3,0, ,0,0,0,0,0,2,0, ,0,
All,All,2003,YR2003,3,5,6,0, ,0,0,0,0,0,3,0, ,0,
All,All,2004,YR2004,4,11,8,0, ,0,1,0,2,2,5,0, ,0,
All,All,2005,YR2005,13,28,20,1, ,1,1,0,5,3,9,0, ,0,
All,All,2006,YR2006,34,48,34,5, ,1,1,0,6,4,5,0, ,0,
All,All,2007,YR2007,33,44,27,11, ,3,2,1,10,9,17,0, ,3,
All,All,2008,YR2008,31,42,20,8, ,2,2,0,9,13,6,0, ,0,
All,All,2009,YR2009,44,43,30,13, ,3,0,1,4,5,7,0, ,6,
All,All,2010,YR2010,56,52,42,15, ,3,3,0,9,5,3,1, ,0,
All,All,2011,YR2011,35,36,29,9, ,1,0,0,8,8,2,0, ,0,
All,All,2012,YR2012,19,20,13,4, ,0,0,0,1,6,2,0, ,0,
All,All,2013,YR2013,25,13,10,3, ,0,0,0,14,15,0,0, ,0,
All,All,2014,YR2014,36,60,27,15, ,0,0,0,21,16,2,0, ,0,
All,All,2015,YR2015,72,80,58,44, ,0,0,0,31,20,25,1, ,2,
,,,,,,,,,,,,,,,,,,
```



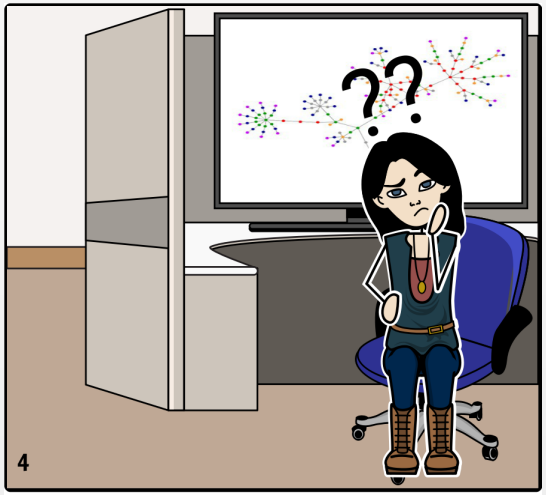


X is a cyber-security analyst. She spends all day looking at log records consisting of text and characters, as part of her job. She is tired and exhausted performing the time-critical monotonous task of reading each log record to find anomalies.

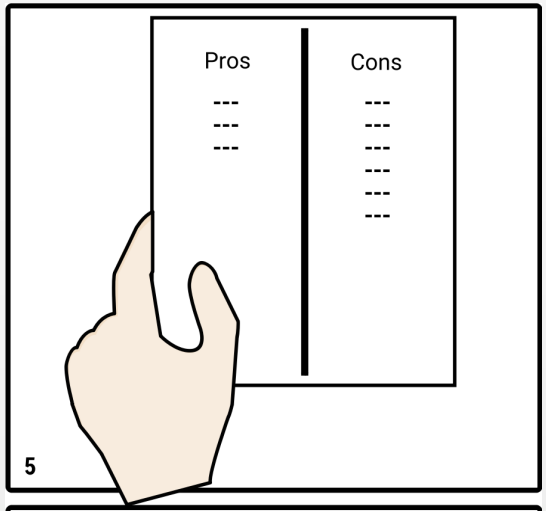
X is in luck, because there is a better and easier way. Visualization in cyber-security can help detect, monitor and mitigate attacks in a timely manner.



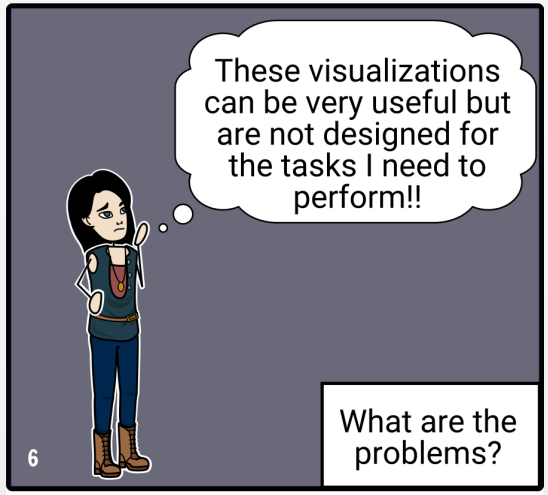
X is happy and excited now that she is introduced to cyber-security visualization. These provide her with a competent tool to prevent and defend against attacks.



Unfortunately, X's excitement was short-lived. Using these cyber-security visualizations for day-to-day tasks was more complicated than she first thought.



She makes a list of the benefits and drawbacks of using these visualizations instead of the textual records. She finally comes to the conclusion...



X is at crossroads now, on one hand the cyber-security visualizations make her job easier but on the other hand they do not support the tasks she needs to perform.

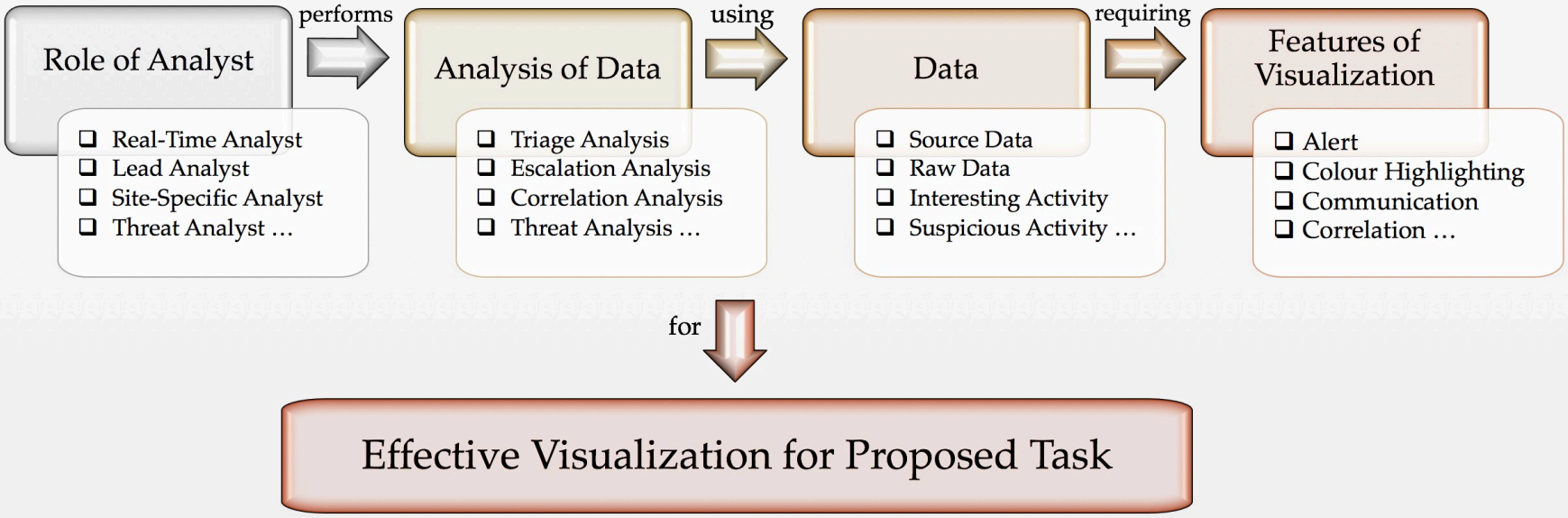
University of Southampton, Aneesha Sethi <Aneesha.Sethi@soton.ac.uk>

What Leads to these Problems?

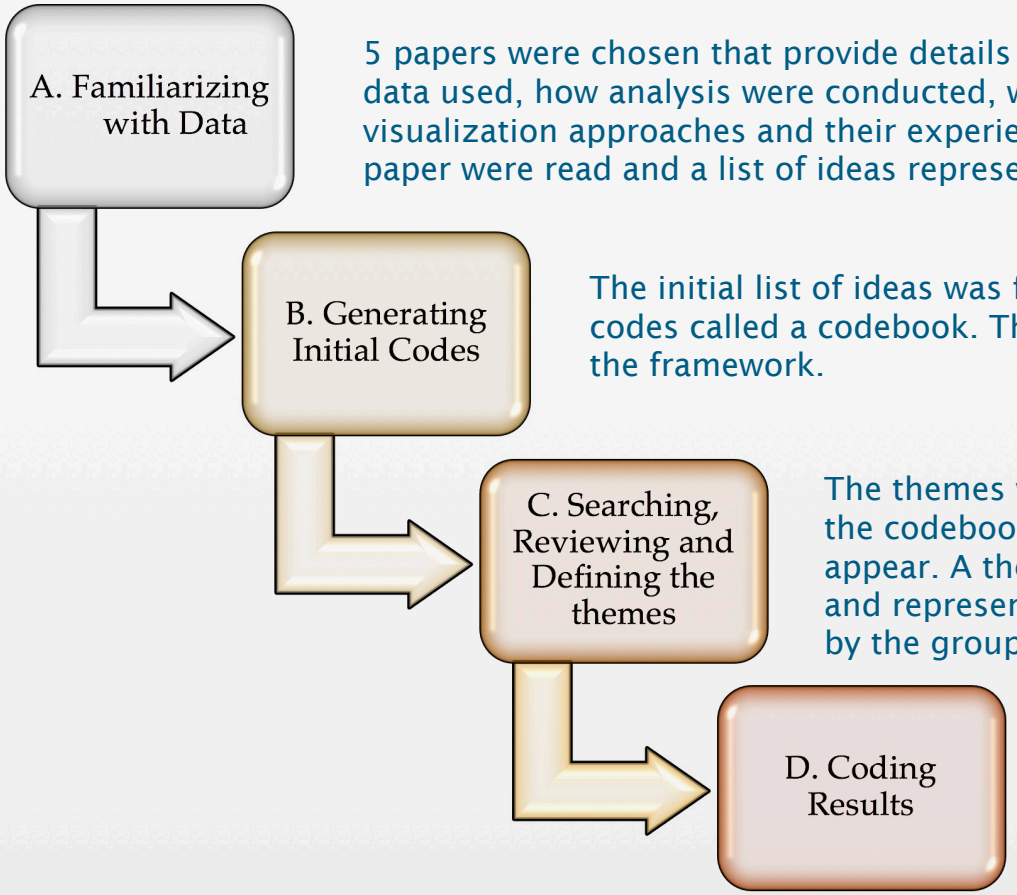
- The visualizations are rarely evaluated for effectiveness in terms of the task they aid in performing.
- Most of the visualizations are developed and often evaluated without any user-involvement.
- The techniques used to evaluate most tools were not standardized.

These factors led to a low adoption rate of tools presenting cyber-security visualisations. Thus, the need for a common framework, evaluating the effectiveness of cyber-security visualisations for the performed task arose.

EEVi - Framework



Methodology – Thematic Analysis



5 papers were chosen that provide details about security analyst roles, the types of data used, how analysis were conducted, what the analysts thought about visualization approaches and their experiences, if any, with visualizations. These 5 paper were read and a list of ideas represented was formulated.

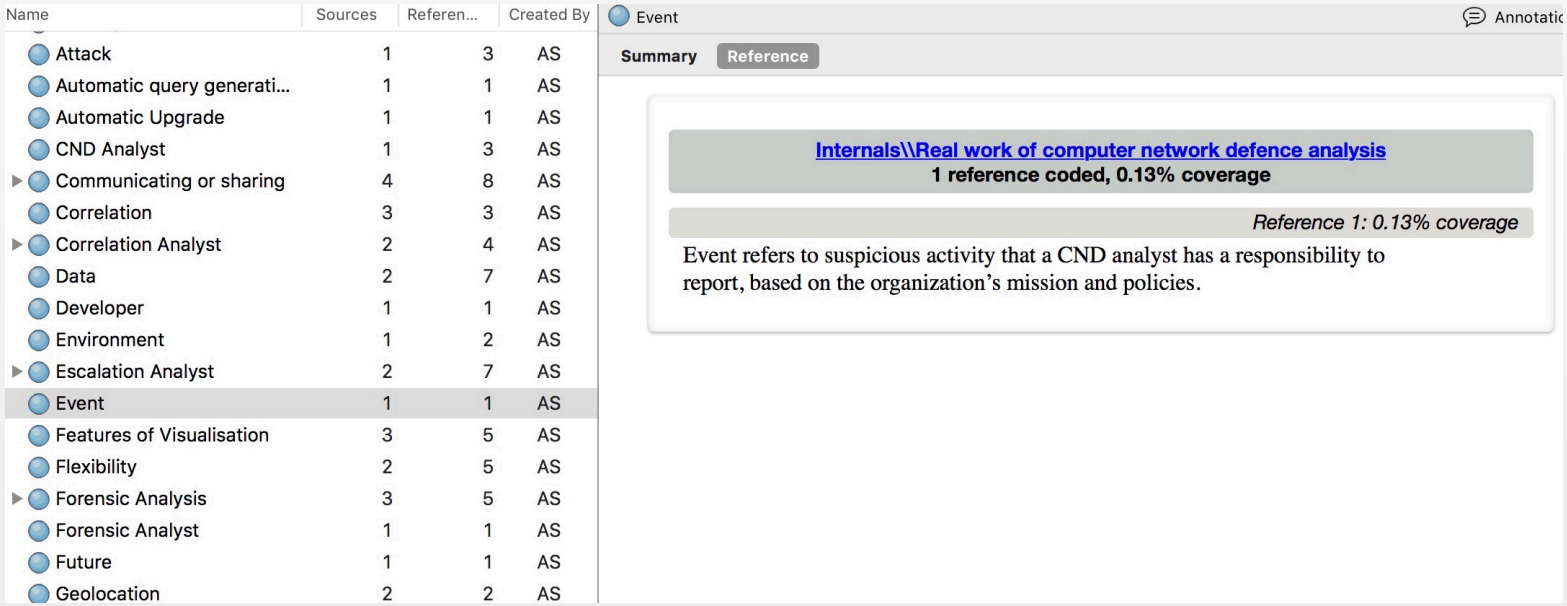
The initial list of ideas was further analysed to produce an initial set of codes called a codebook. The codes represent the qualitative aspects of the framework.

The themes were defined on the basis of the results from the codebook and relationships between themes start to appear. A theme captures the significance of the data and represents a patterned response which is reflected by the group of codes it defines.

The themes, codes and relationships or *links* are identified as a result which were further analysed to design the framework.

Thematic Analysis

1. The first step was to identify the relevant papers and form an initial list of ideas.
2. The next step was to form the **codebook** of initial set of codes based on the list of ideas formulated.



Name	Sources	Referen...	Created By
Attack	1	3	AS
Automatic query generati...	1	1	AS
Automatic Upgrade	1	1	AS
CND Analyst	1	3	AS
Communicating or sharing	4	8	AS
Correlation	3	3	AS
Correlation Analyst	2	4	AS
Data	2	7	AS
Developer	1	1	AS
Environment	1	2	AS
Escalation Analyst	2	7	AS
Event	1	1	AS
Features of Visualisation	3	5	AS
Flexibility	2	5	AS
Forensic Analysis	3	5	AS
Forensic Analyst	1	1	AS
Future	1	1	AS
Geolocation	2	2	AS

Thematic Analysis

1. The first step was to identify the relevant papers and form an initial list of ideas.
2. The next step was to form the **codebook** of initial set of codes based on the list of ideas formulated.
3. The third step was to form **themes** by collating the codes:
    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;
    4. *Role of Analyst* – The security analyst that perform the tasks.
4. Finally, the last step was to record the results along with the **relationships** formed.

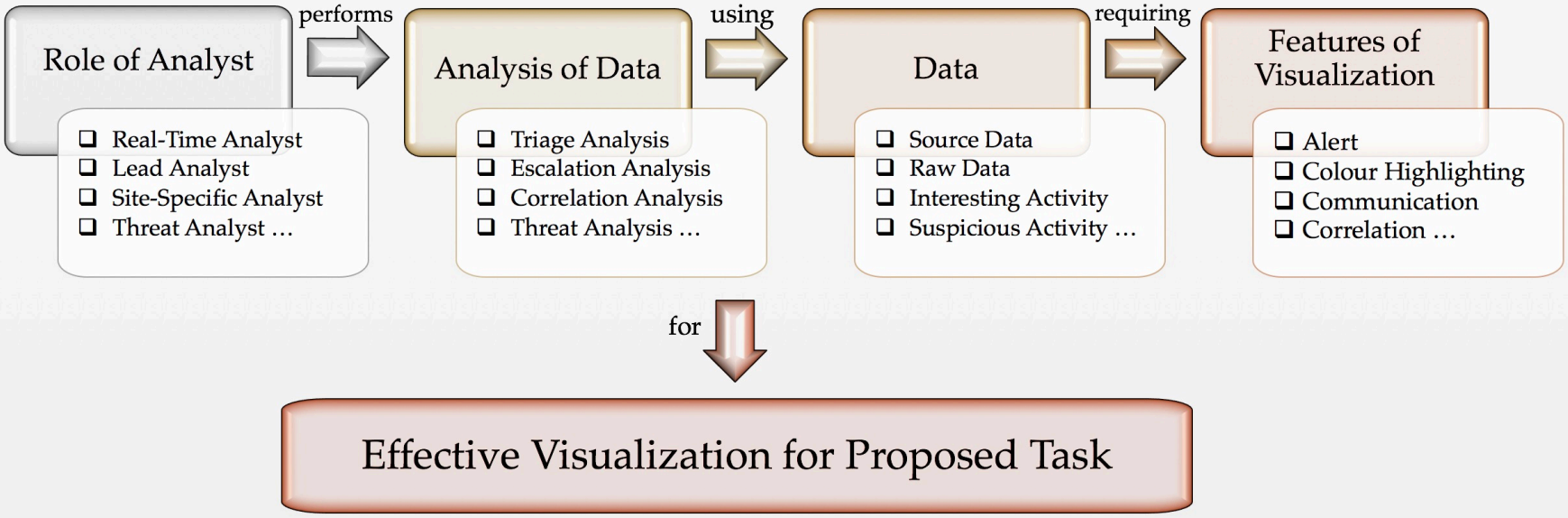
Thematic Analysis

4. Finally, the last step was to record the results along with the **relationships** formed.

Table 3.1: 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. [20] D'Amico et al. [21] Erbacher et al. [30]
Escalation Analysis Situational Assessment	Investigates suspicious activities from *Triage Analysis* stage, and produces reports. May take from hours to weeks to complete.	*Lead Analyst* *Tactical Defender* *Suspicious Activity* *Incident* *Interpolation* *Communication*	D'Amico et al. [20] D'Amico et al. [21]

EEVi - Framework

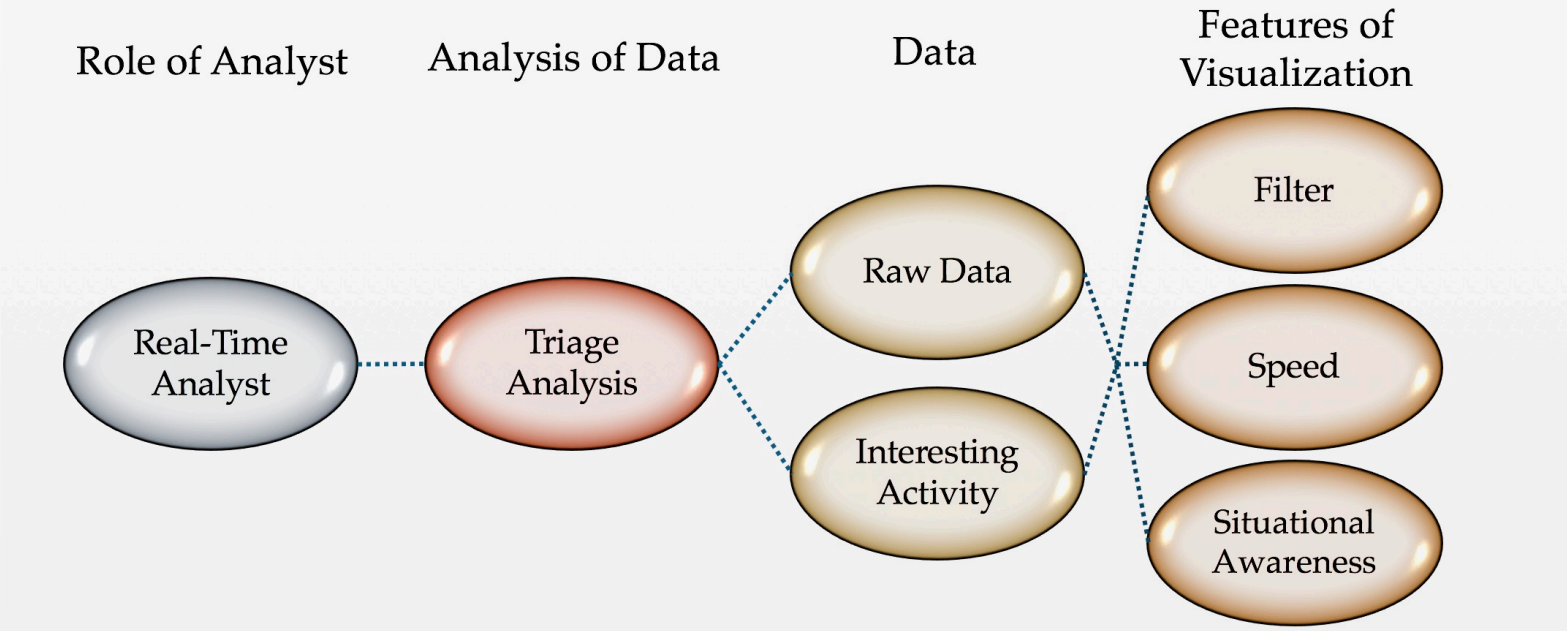


Types of Analysis of Data (Task)

The codes led to the definition of eight type of tasks:

- Triage Analysis
- Escalation Analysis
- Correlation Analysis
- Threat Analysis
- Incident Response Analysis
- Forensic Analysis
- Impact Assessment
- Security Quality Management

Analysis


Role of Analyst
Analysis of Data
Data
Features of Visualization
Real-Time Analyst
Triage Analysis
Raw Data
Interesting Activity
Filter
Speed
Situational Awareness

Summary

- Low user-involvement and not having standardised evaluation lead to low adoption rates of cyber-security visualization tools.
- EEVi presents a common framework, based on user requirements, to standardize evaluation and act as guidelines to develop effective cyber-security visualizations.

Thank you!

Questions?

-Aneesha Sethi
University of Southampton
Aneesha.Sethi@soton.ac.uk