Visual Analysis of Goal-Directed Network Defense Decisions

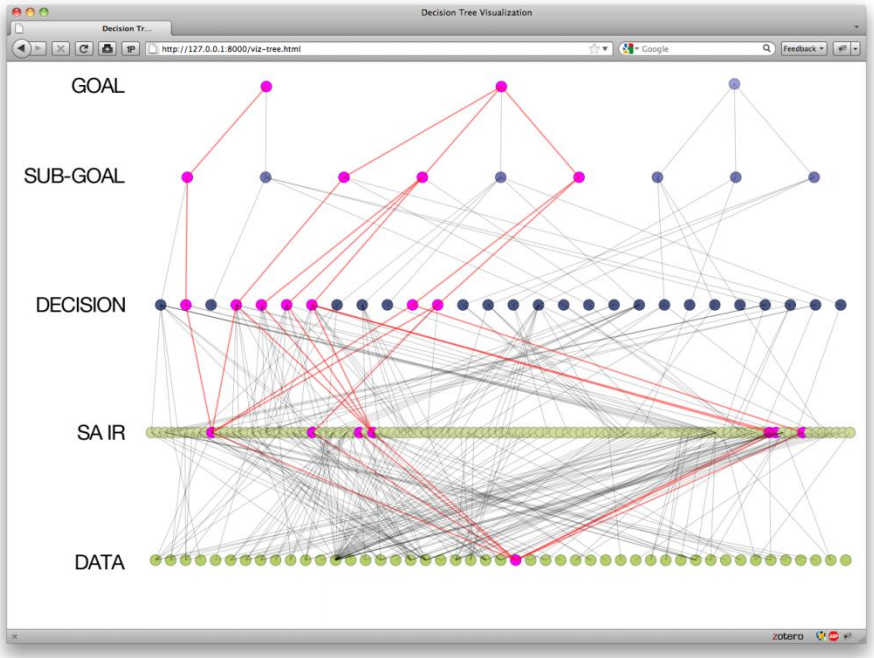
20 July 2011

Chris Horn
Anita D'Amico

VizSec 2011
Pittsburgh, PA

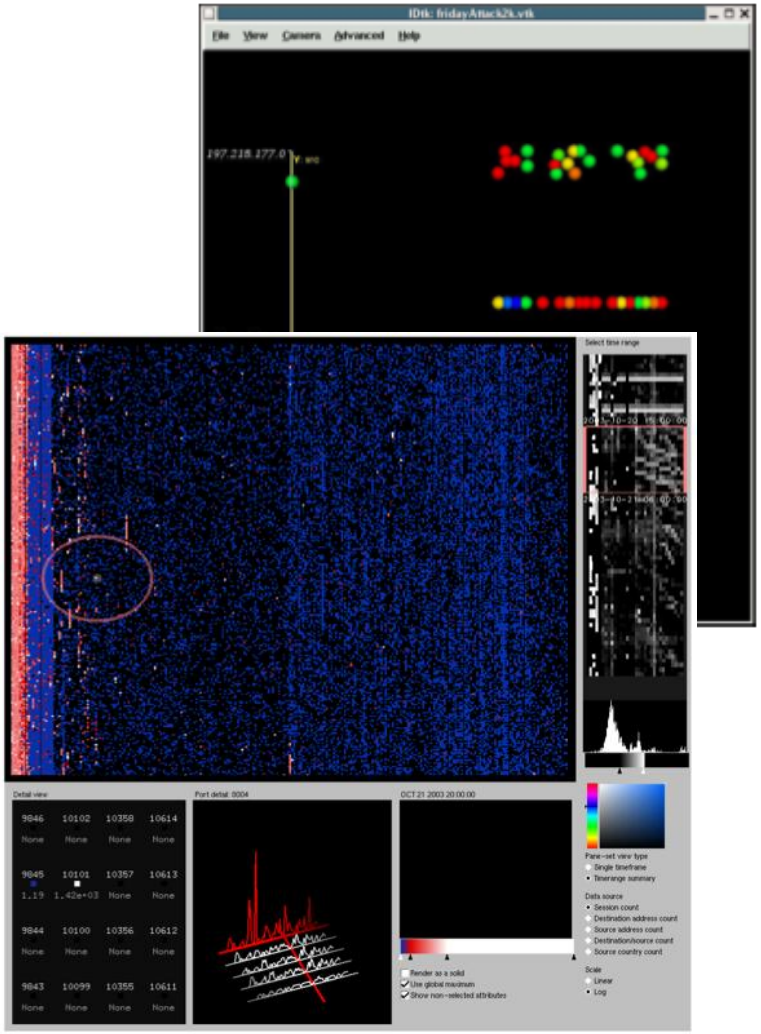
Overview

- Visual analytic system for working with data describing computer network defense
- Prototyped in a few weeks
- Runs everywhere
  - Stand-alone
  - Web-based
  - No network access
  - Unprivileged user
  - Windows, OS X, Linux
- Provided us with valuable insight into our data



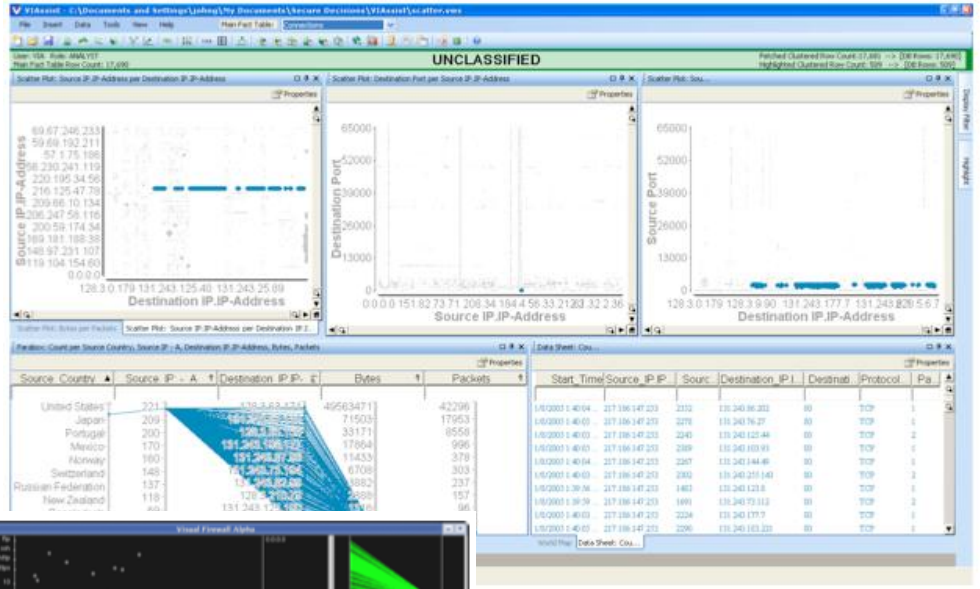
Security visualization has focused on activity data

Komlodi, 2005

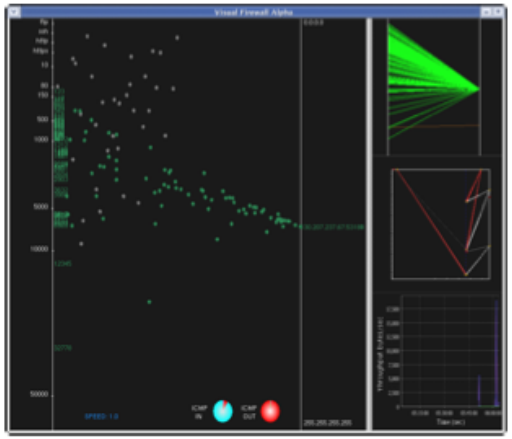


McPherson, 2004

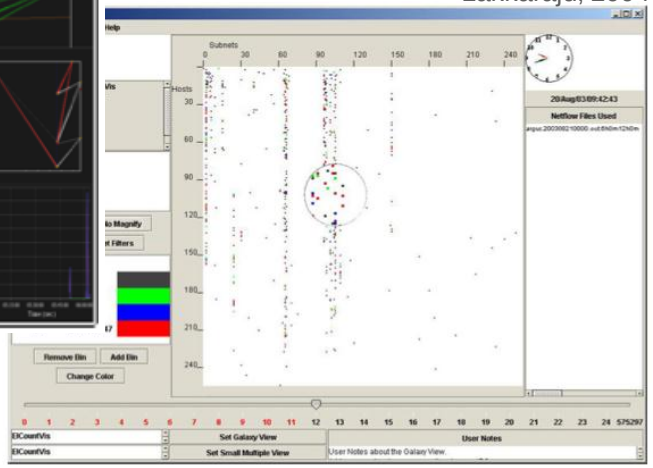
Goodall, 2009



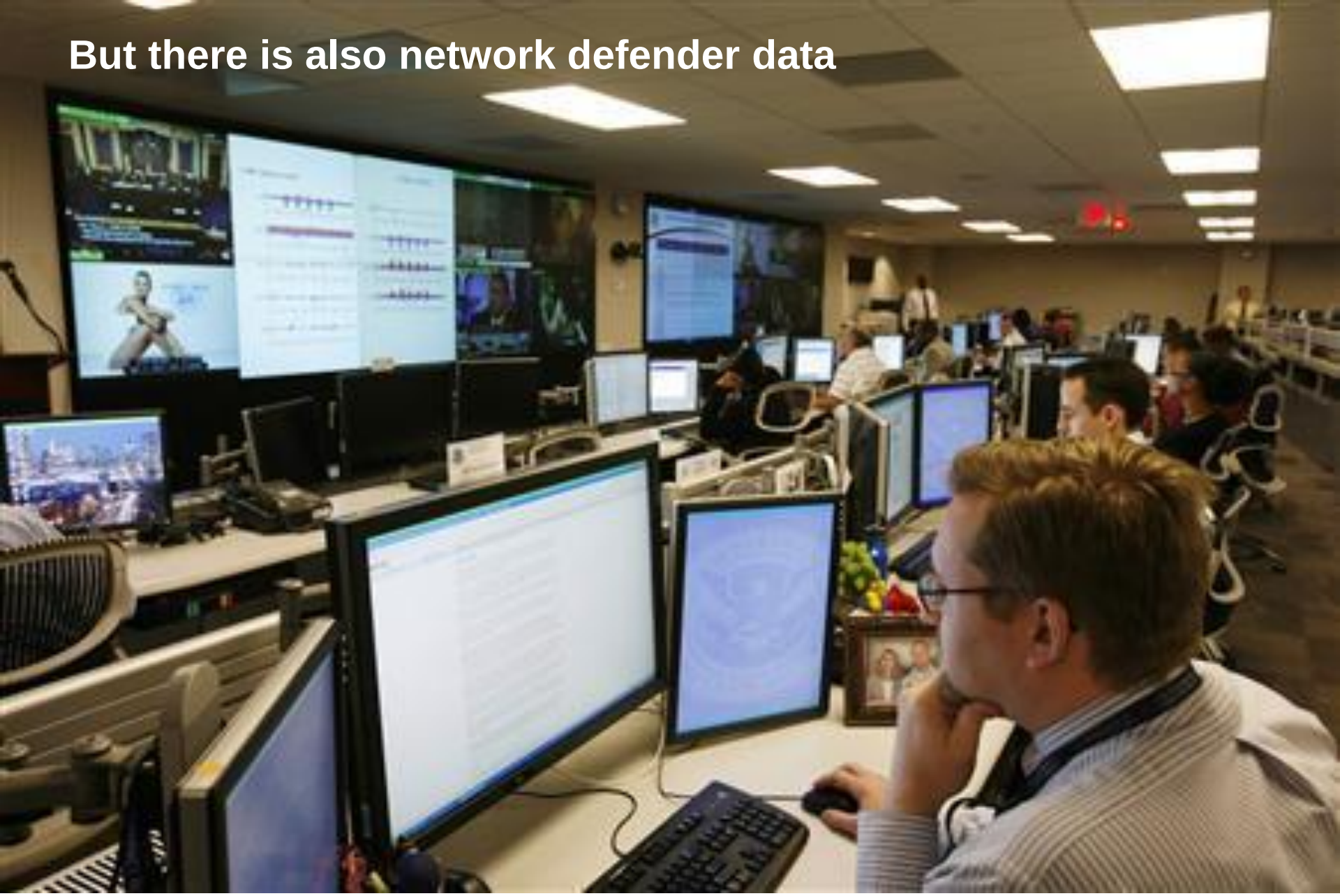
Lee, 2005



Lakkaraju, 2004



But there is also network defender data



Collected data start in the physical world

Data are then commonly transcribed into Microsoft Excel and Visio

Project X

1. What are the CND decisions being made?
2. What information is needed to support these decisions?
3. What data sources are available to provide this information?
4. What are the quality of these data sources?
5. What new technologies and data sources could support better CND decision-making?

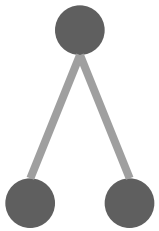
Goal-directed framework

1 An **overarching goal** that orients operations (i.e., an observed practice mission statement)

Goal-directed framework

1. An **overarching goal** that orients operations (i.e., an observed practice mission statement)

2. **Major goals** that decision makers must achieve in pursuing the overarching goal

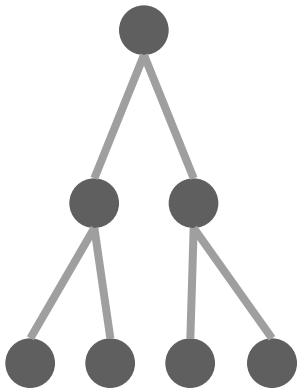


Goal-directed framework

1. An **overarching goal** that orients operations (i.e., an observed practice mission statement)

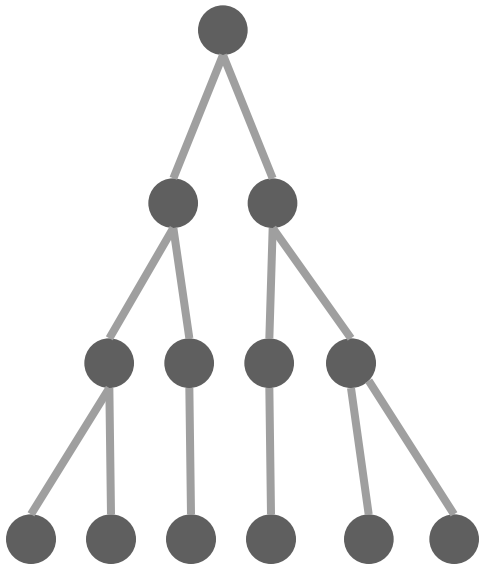
2. **Major goals** that decision makers must achieve in pursuing the overarching goal

3. **Sub-goals** that incrementally contribute to accomplishing the respective major goal



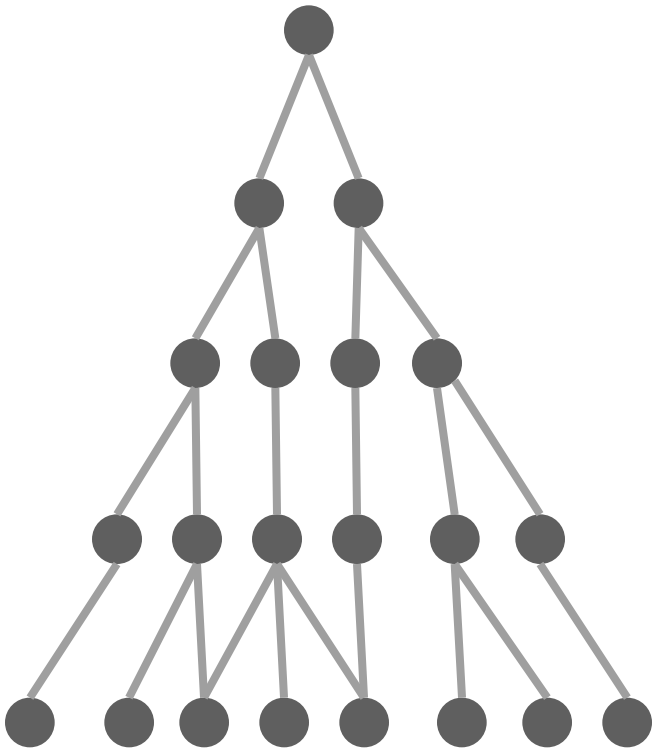
Goal-directed framework

1. An **overarching goal** that orients operations (i.e., an observed practice mission statement)
2. **Major goals** that decision makers must achieve in pursuing the overarching goal
3. **Sub-goals** that incrementally contribute to accomplishing the respective major goal
4. CND **decisions** needed to accomplish the major goals and sub-goals



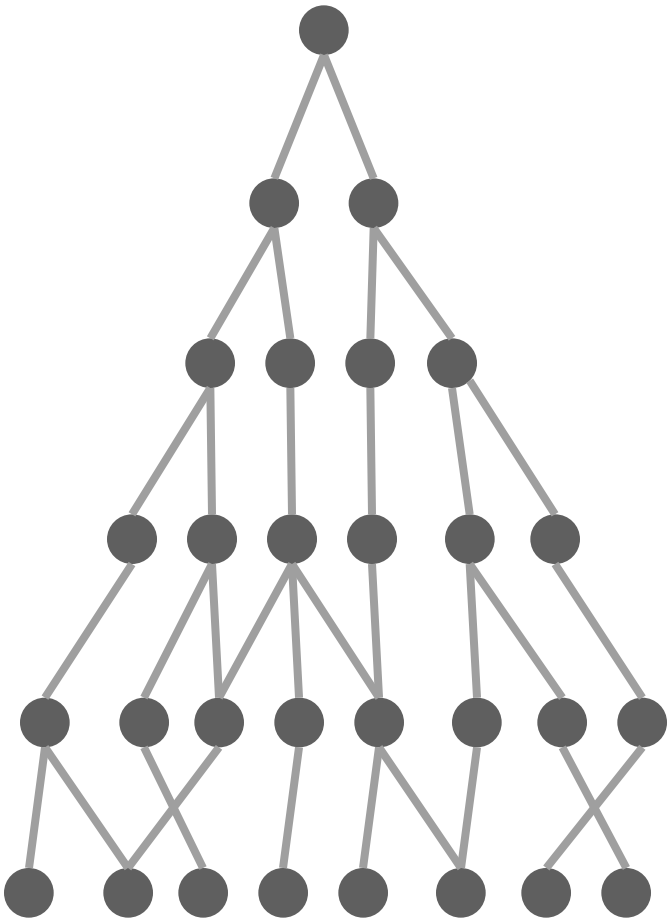
Goal-directed framework

1. An **overarching goal** that orients operations (i.e., an observed practice mission statement)
2. **Major goals** that decision makers must achieve in pursuing the overarching goal
3. **Sub-goals** that incrementally contribute to accomplishing the respective major goal
4. CND **decisions** needed to accomplish the major goals and sub-goals
5. **Situation awareness (SA) information requirements** needed to make decisions (the information needs of a decision)

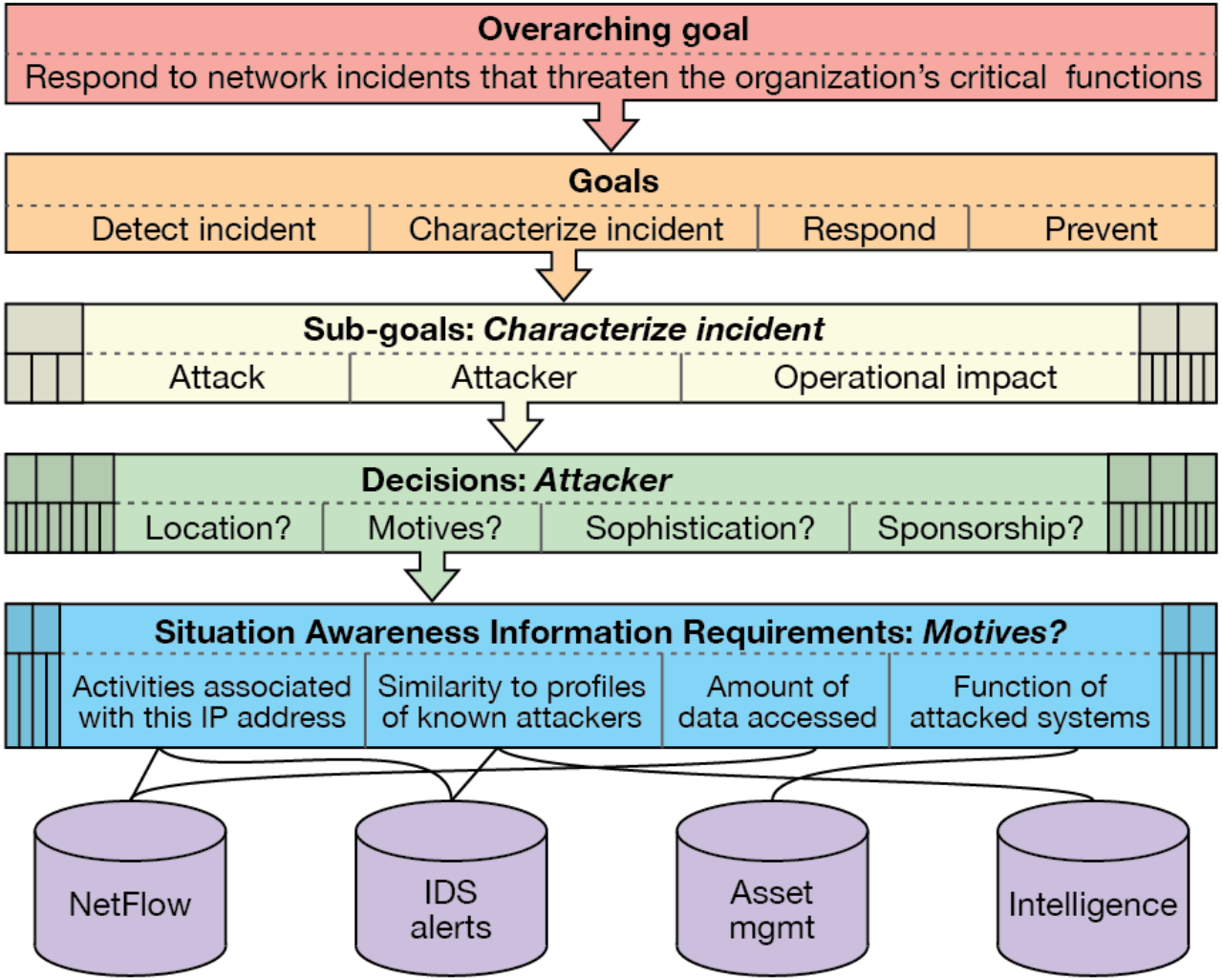


Goal-directed framework

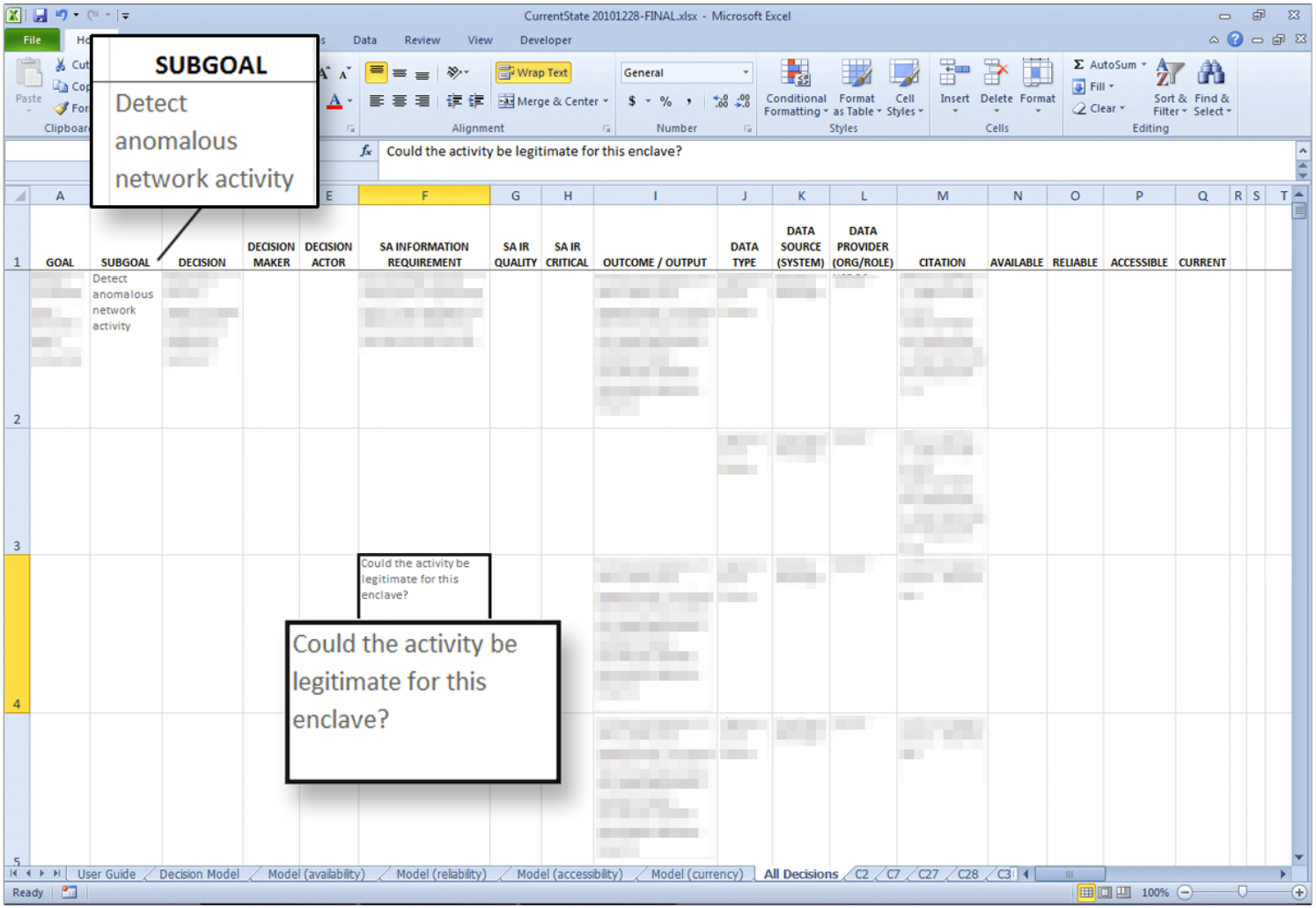
1. An **overarching goal** that orients operations (i.e., an observed practice mission statement)
2. **Major goals** that decision makers must achieve in pursuing the overarching goal
3. **Sub-goals** that incrementally contribute to accomplishing the respective major goal
4. CND **decisions** needed to accomplish the major goals and sub-goals
5. **Situation awareness (SA) information requirements** needed to make decisions (the information needs of a decision)
6. **Data sources** that serve as the foundation for satisfying SA information requirements



Goal-directed framework



A spreadsheet approach



Spreadsheets are great tools, but not for this job

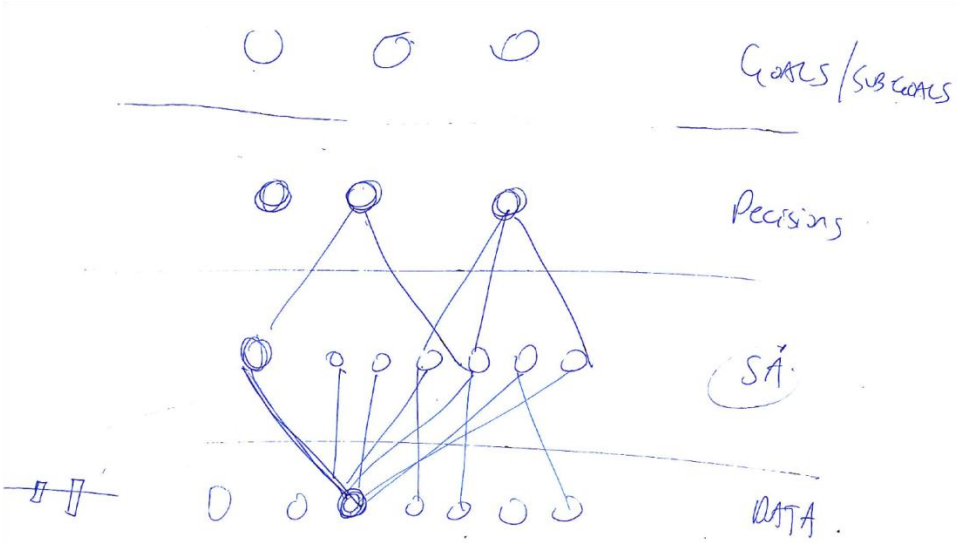
- Spreadsheet proved a very useful discussion tool
- Unfortunately, it has significant limitations
  - Rearranging and inserting elements is laborious
  - Doesn't support many to many relationships
  - Doesn't support automated visualization

Unanswered questions

"What are the most important decisions?"

"What are the most common decisions?"

"On what data sources and systems do these decisions depend?"



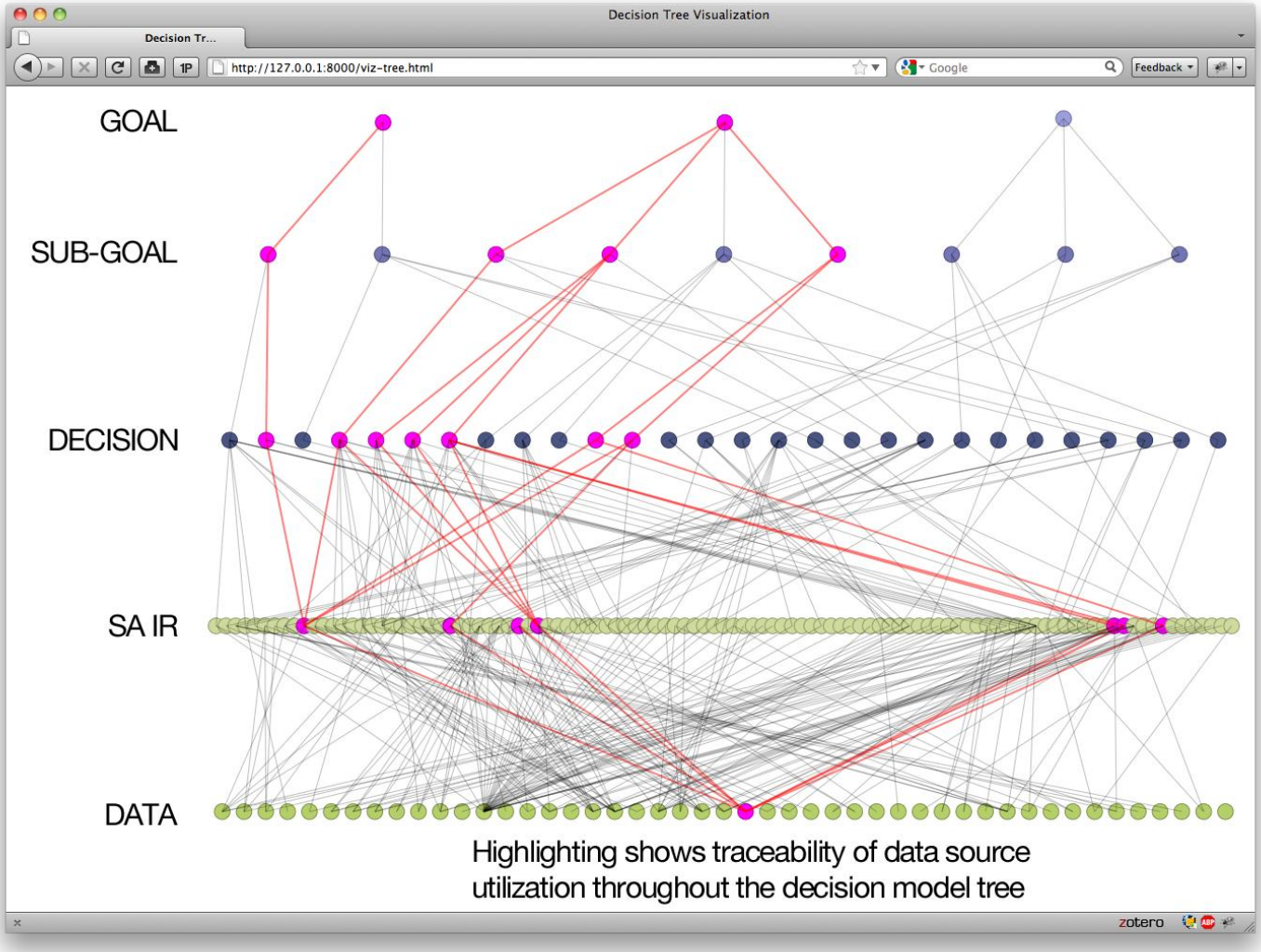
Goals/sub-goals

Decisions

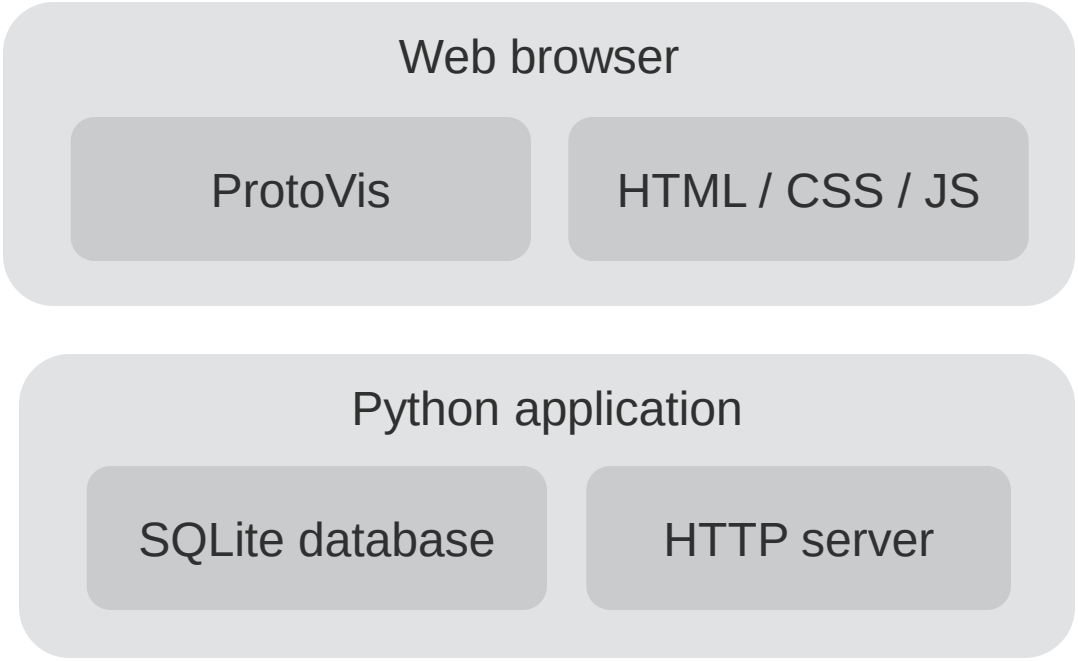
SA requirements

Data

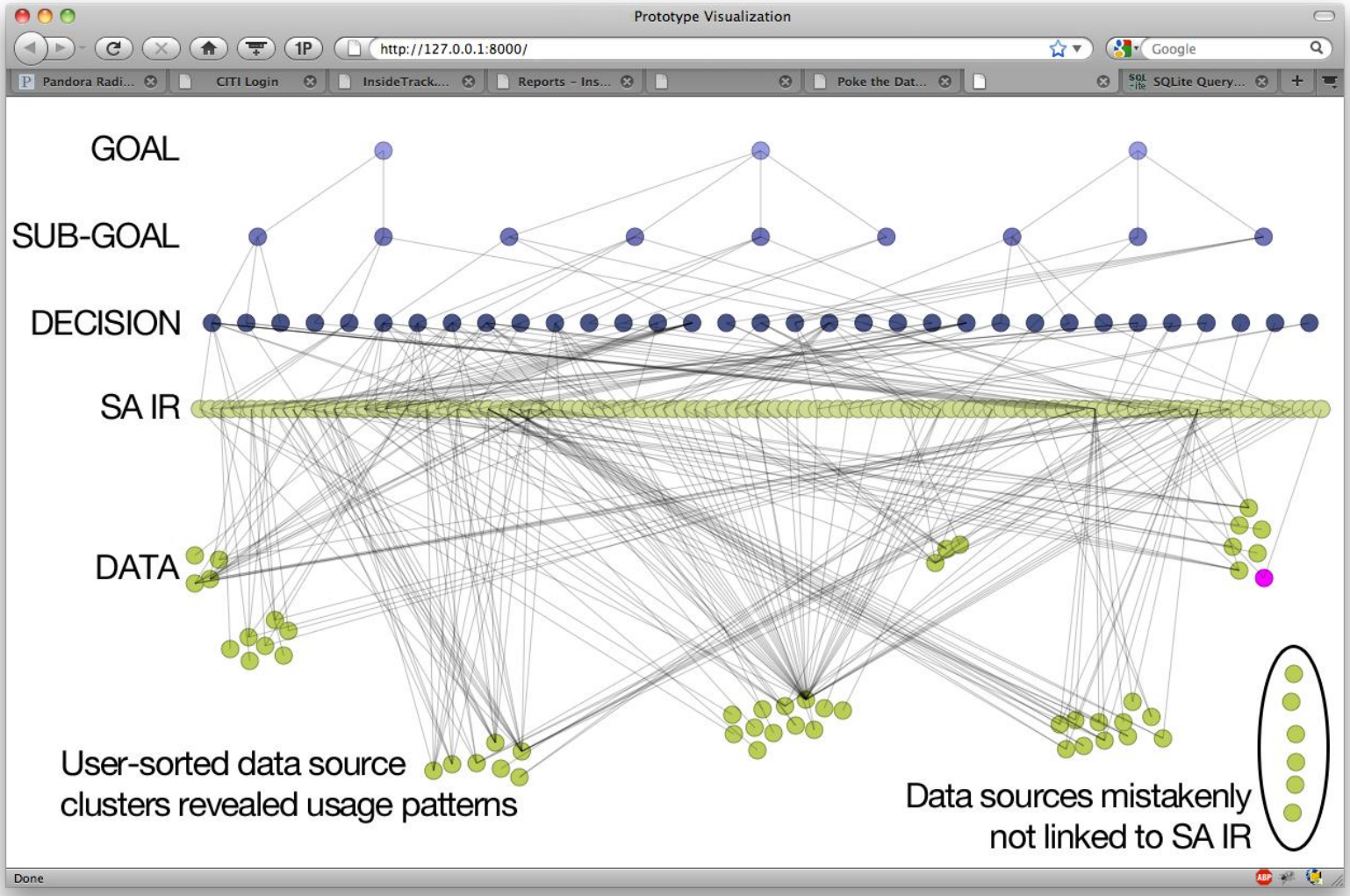
The decision tree model, visualized



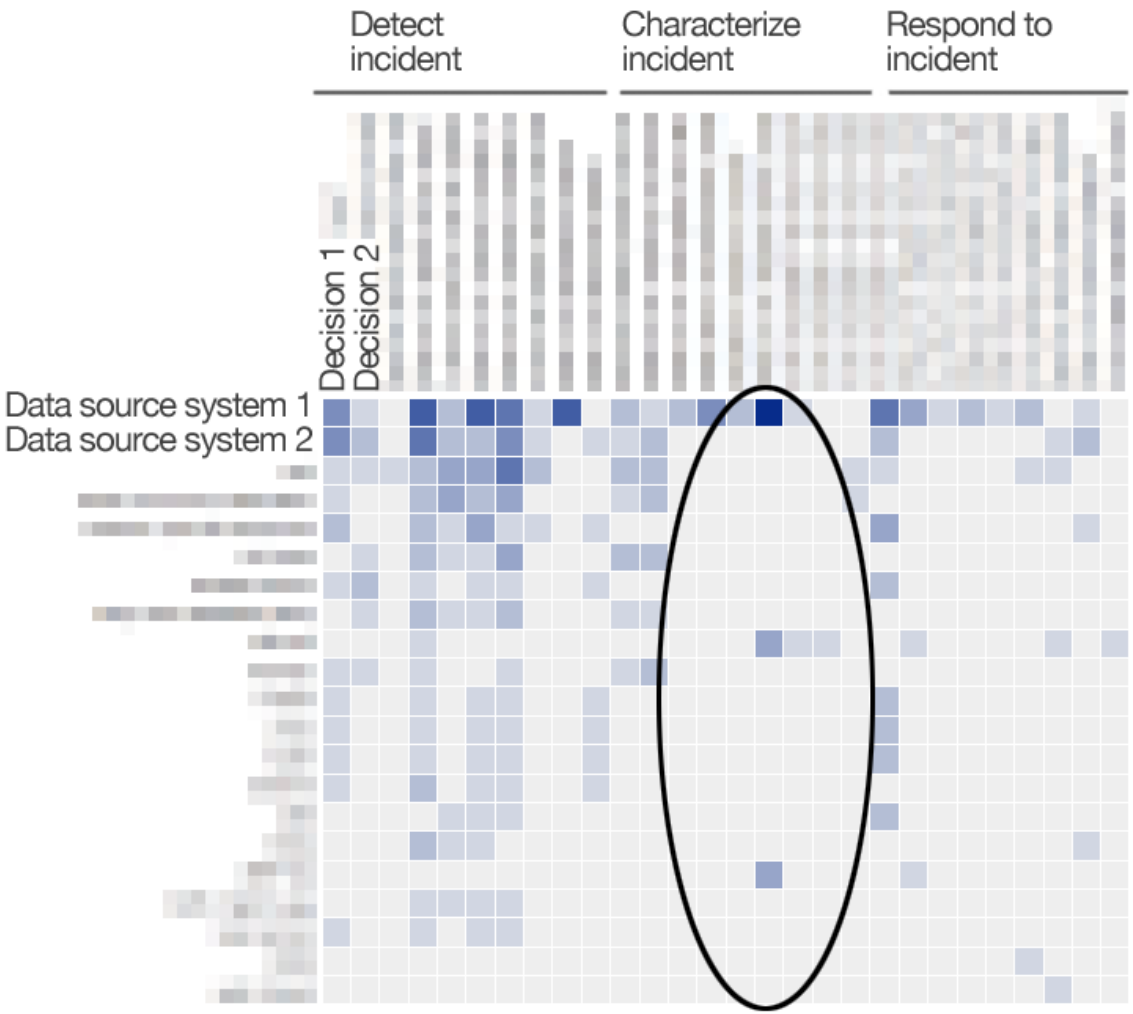
System architecture



Decision tree visualization, in action



Flexibility afforded by a database



Quick demonstration

Room for improvement

- Database editor
  - Workflows for setting per-link meta-data is repetitive and tedious
  - Editor doesn't afford smooth navigation up the decision model structure; when revising links and verifying data entry, this imposes a significant burden
- Tree visualization
  - Lack of labels on the interactive tree view impairs analysis of the model
  - Lack of automated sorting in the interactive tree view made visual analysis of the model more difficult
- Current visualizations
  - Do not convey the full depth of information stored in the database