Need-to-know metrics

MetriCon 2008

Fred Cohen
CEO – Fred Cohen & Associates
President – California Sciences Institute

Your speaker

- Fred Cohen & Associates
  - Back-end provider for companies who sell strategic security research, analysis, and consulting services – mostly to large enterprises
  - Challenges to digital forensic evidence in legal matters
  - Books, tools, and so forth
- California Sciences Institute
  - Non-profit California Educational Institution
  - Graduate courses in
    - National Security and
    - Advanced Investigation
  - MS degrees
  - PhD. degrees
  - Starting classes 2009-01

These results stem from FCA client work
Client details are confidential – don't ask

Outline

- A data gathering effort and its results
  - The tool and methodology used
  - What they came up with
- Gathering data from the audience
  - Government types
  - Corporate types
  - Other types
- Duty to protect analysis for an actual client
- Summary, Conclusions, and Further Work

Outline

- A data gathering effort and its results
  - The tool and methodology used
  - What they came up with
- Gathering data from the audience
  - Government types
  - Corporate types
  - Other types
- Duty to protect analysis for an actual client
- Summary, Conclusions, and Further Work

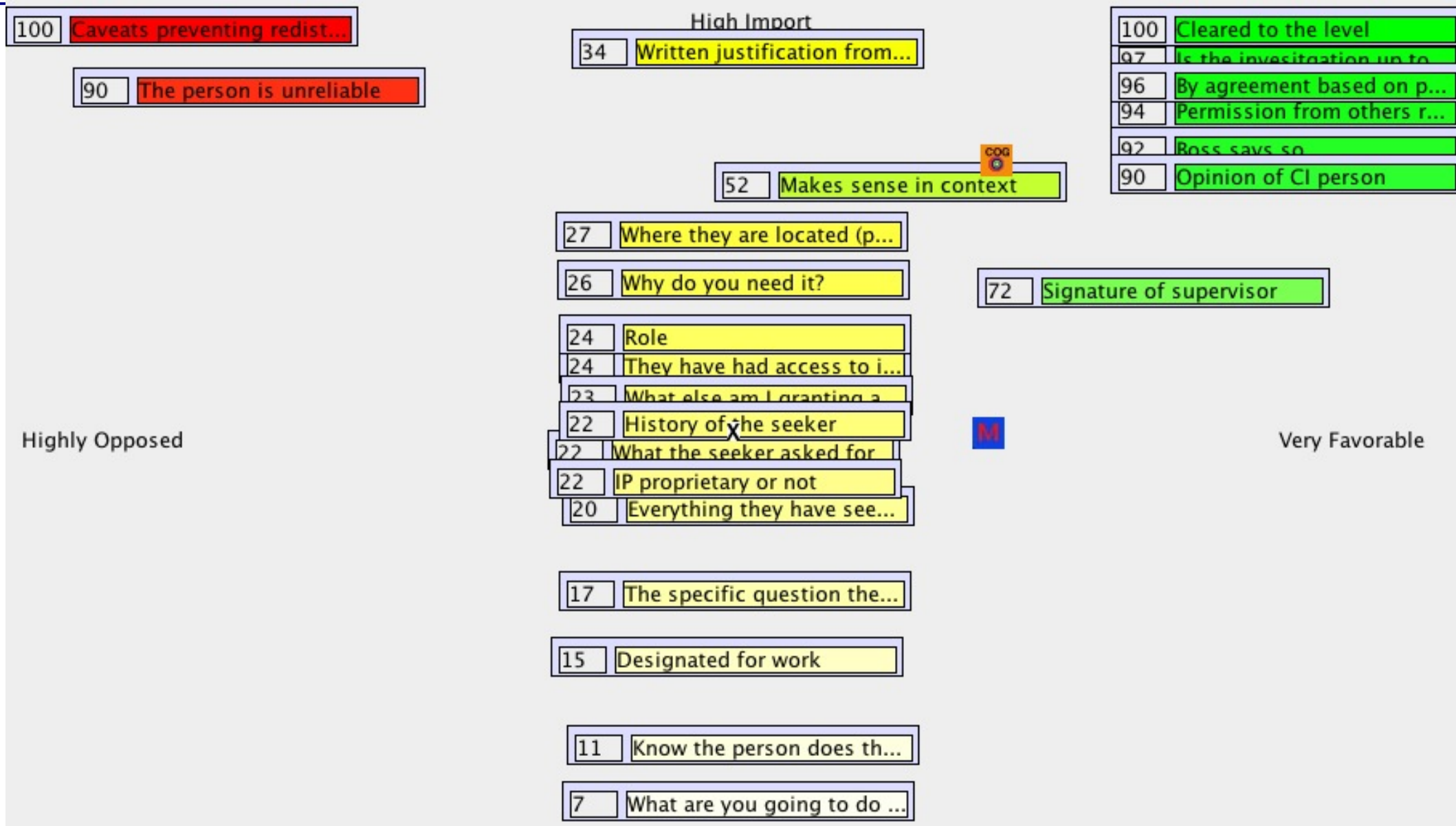
The tool

- Decider
  - The tool used for this part of this effort
  - Also used for experiments on the Metrics list <1 year ago
  - Designed to bring clarity to decisions
    - Not to make decisions for you
    - Not to help make “better” decisions (whatever they are)
    - Not to force you to make decisions one way or another
  - It does this by providing a 2-dimensional mapping
    - Factors (defined by the users)
    - Placed in a space structured by {importance x favorability}
    - Placements are relative to each other, not absolute values
  - This allows large numbers of disparate factors to be compared – apples to oranges

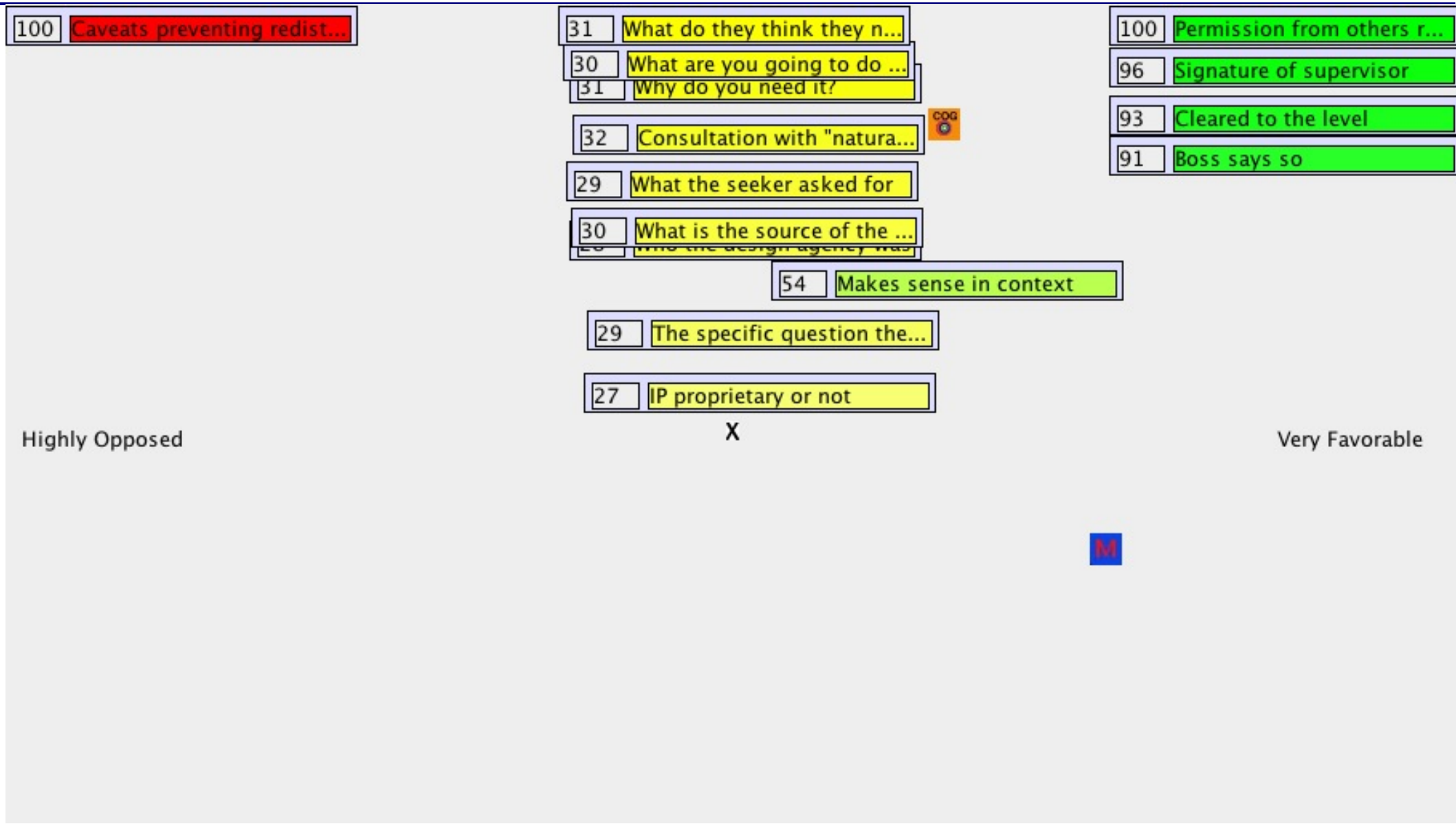
What they came up with

- Several different organizations were involved
  - All part of the same overall enterprise
  - But not the same corporation
- They have all been making NTK decisions
  - For many years
  - Under the same overall governance requirements
  - Independently
- Many individuals make NTK decisions in each
  - Individuals may do different things within each
  - Each has internal standards as well

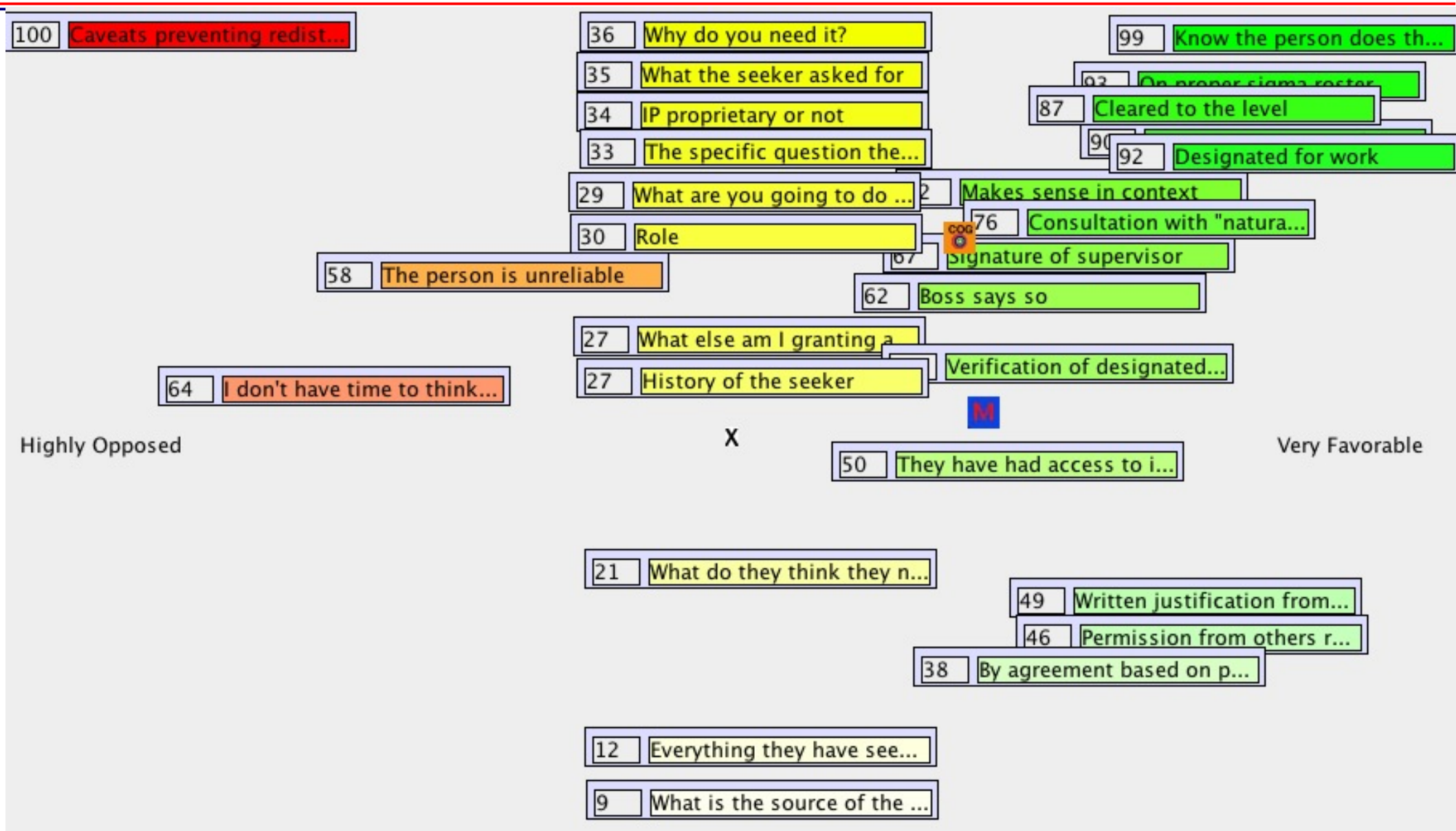
Example results



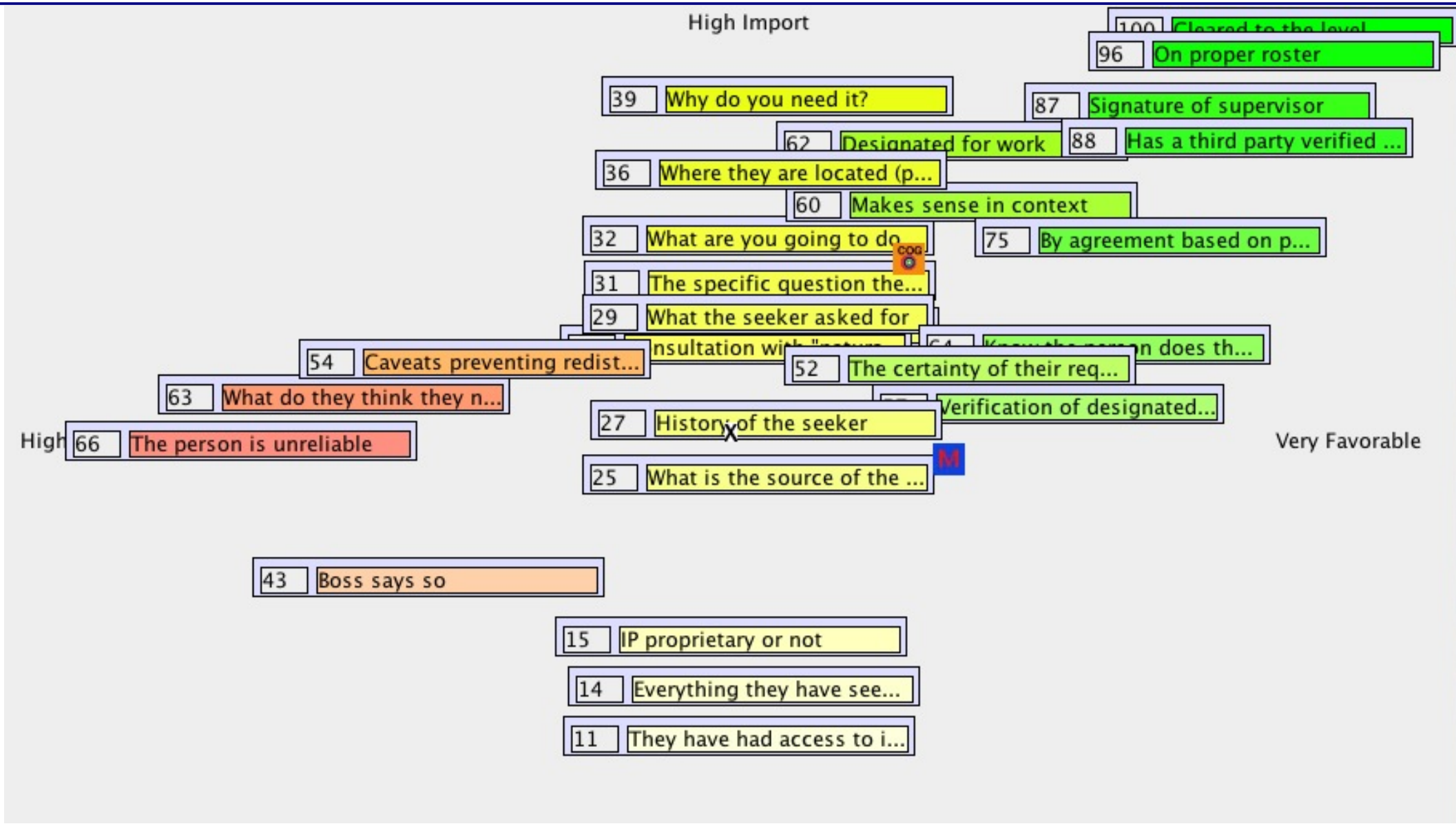
Example results



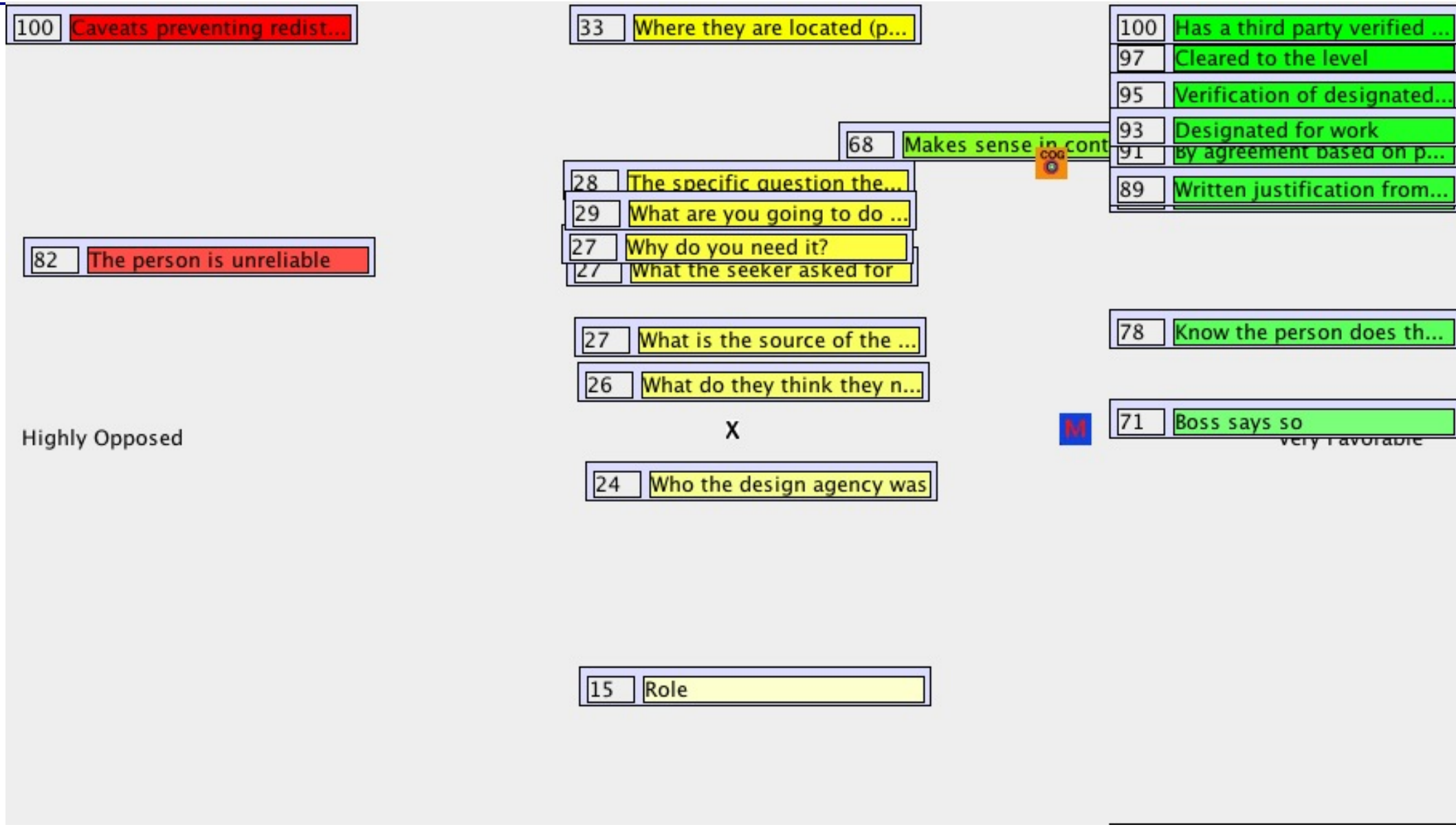
Example results



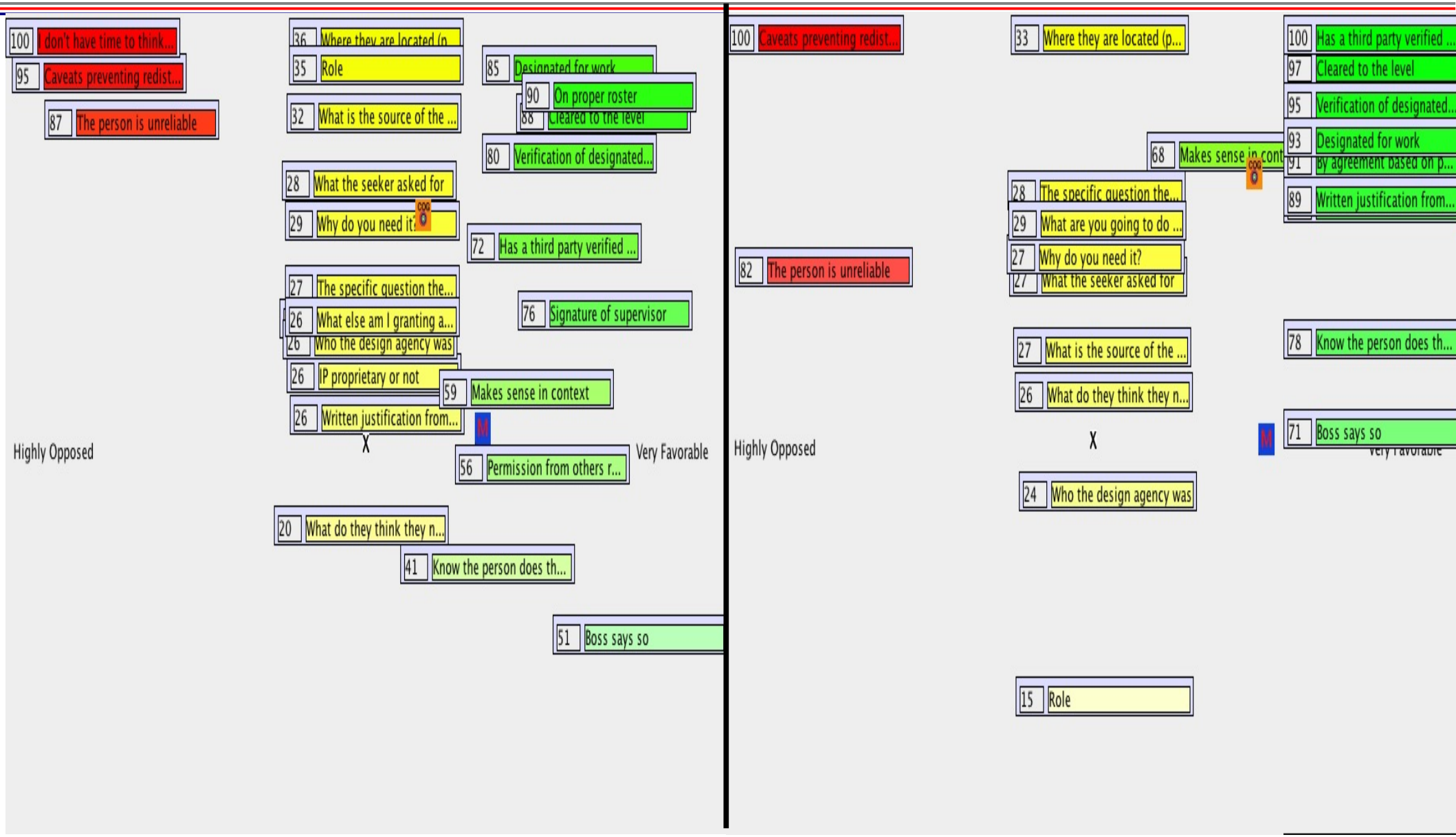
Example results



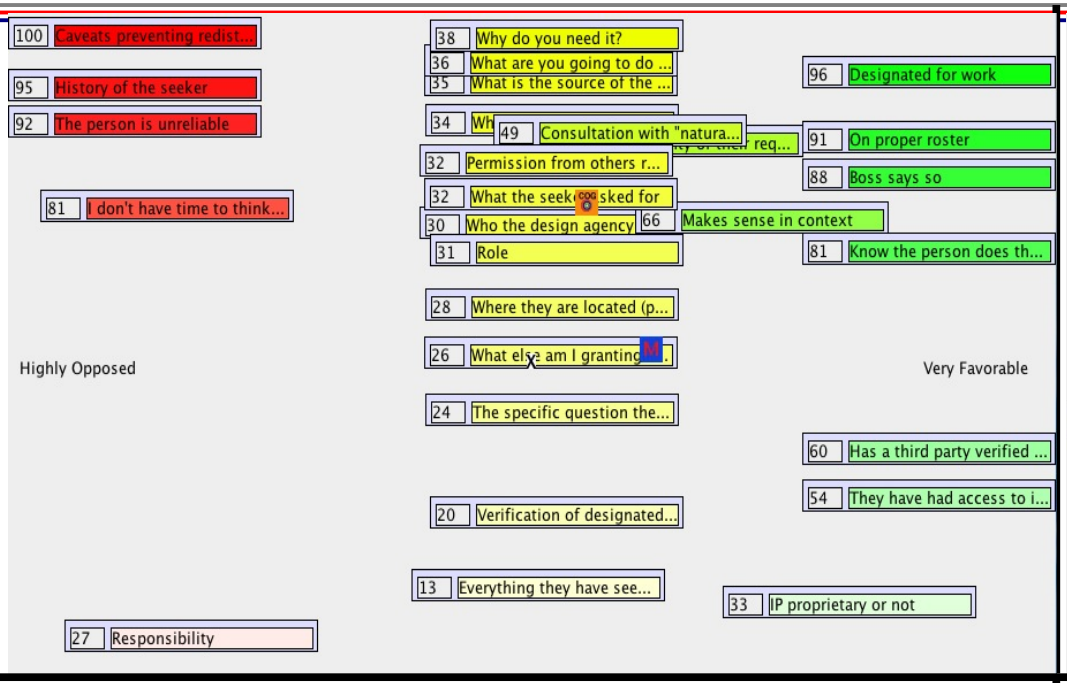
Example results

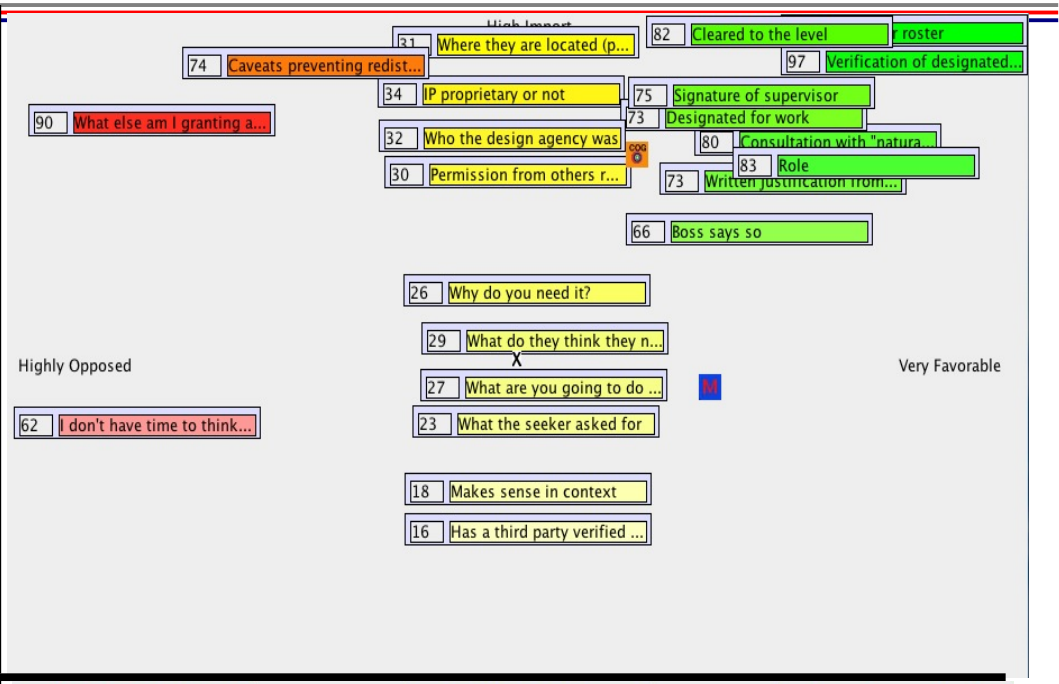


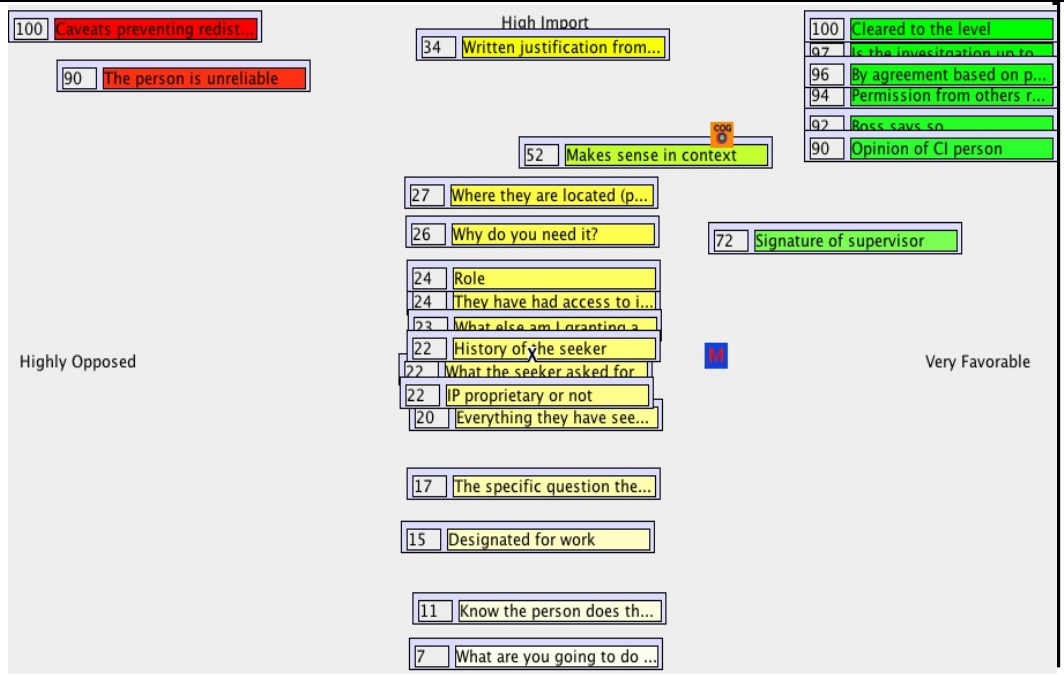
Comparison results

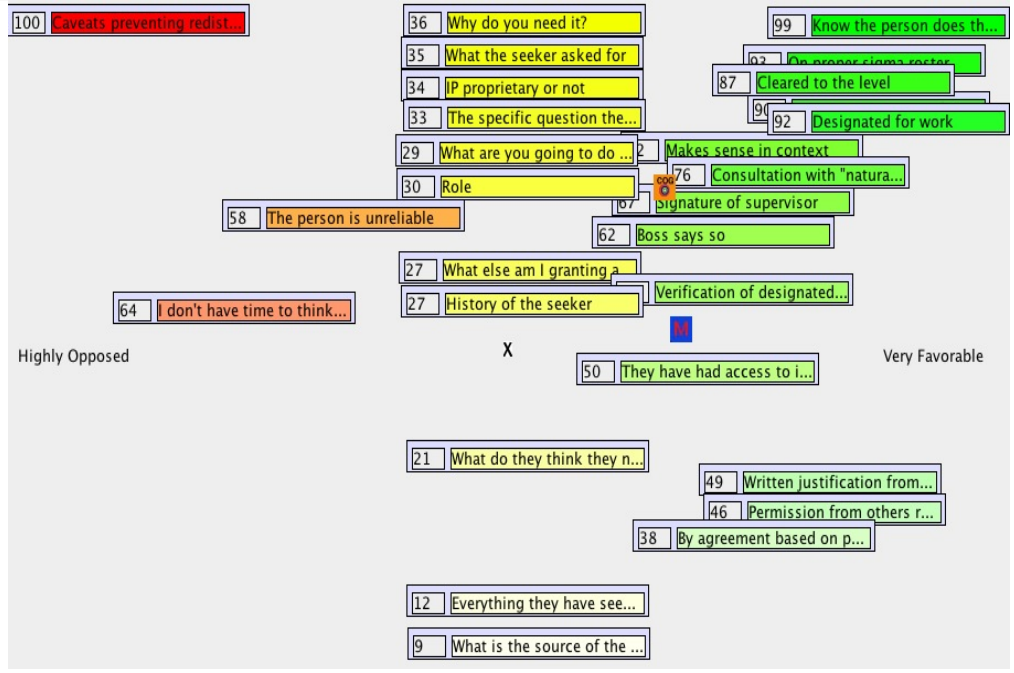


Comparison results









Outline

- A data gathering effort and its results
  - The tool and methodology used
  - What they came up with
- Gathering data from the audience
  - Government types
  - Corporate types
  - Other types
- Duty to protect analysis for an actual client
- Summary, Conclusions, and Further Work

What's the point?

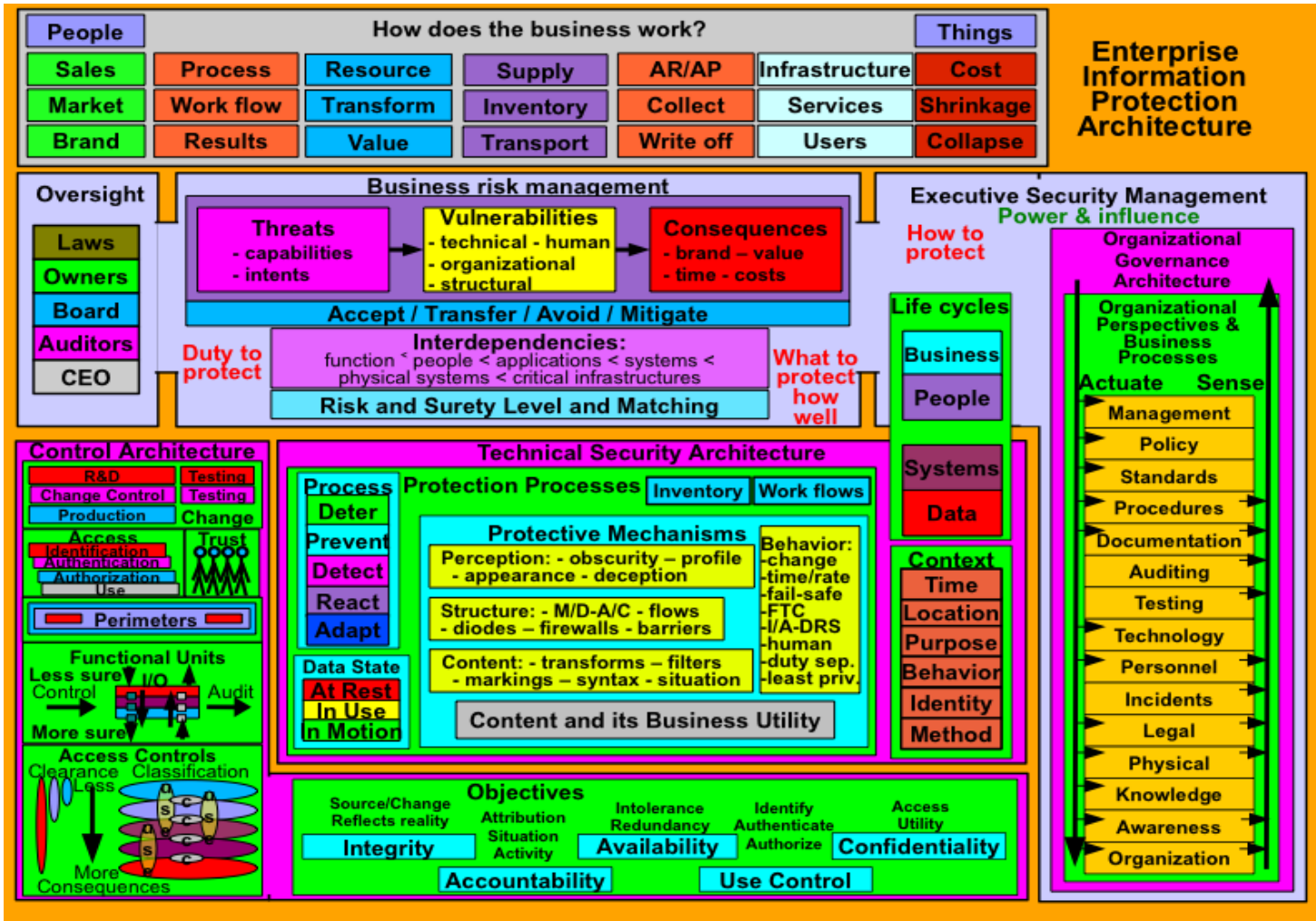
- They were all over the place
  - They disagreed about what was how important and how much so
  - They disagreed about what was favorable and how much so
  - They came up with different orderings for the same factors
  - They used different factors in making their decisions
  - The decisions were very complicated involving more than 20 factors
- And you did the same thing?

Outline

- A data gathering effort and its results
  - The tool and methodology used
  - What they came up with
- Gathering data from the audience
  - Government types
  - Corporate types
  - Other types
- Duty to protect analysis for an actual client
- Summary, Conclusions, and Further Work

Duty to protect analysis

- Duties are derived from oversight
  - Executive decisions
  - Laws
  - Owners
  - Board
  - Auditors



DTP analysis

- In this particular case, factors identified and prioritized included;
  - More than 20 commonly used criteria - Designated for work, On proper roster, Boss says so, Know the person does that work, Makes sense in context, The certainty of their request, Has a third party verified clearance? They have had access to it before, IP proprietary, Caveats preventing redistribution, History of the seeker, The person is unreliable, I don't have time to think it through, Responsibility, Consultation with "natural owner", Why do you need it? What are you going to do with it? What is the source of the data? What do they think they need? Permission from others

Analysis results

- DTP showed that the following are the ONLY factors that may legitimately be considered:
  - Clearance
  - On category access list
  - Is it reasonably required in order to carry out the task they are legally assigned to do?
- All true: grant access
- Otherwise: deny access

Outline

- A data gathering effort and its results
  - The tool and methodology used
  - What they came up with
- Gathering data from the audience
  - Government types
  - Corporate types
  - Other types
- Duty to protect analysis for an actual client
- Summary, Conclusions, and Further Work

What does this all mean?

- It means that the people making the decisions were undertaking a complex metric evaluation
  - It was complicated and time consuming
  - It was involved and data intensive
  - It was causing false denials
  - It was stressing people
  - It was slowing activities
  - It was preventing success
- What good did the metrics do?
  - They showed clearly that the process was broken
  - To all of the people making the decisions

So what happened

- They decided to change the way they did it
  - They simplified their decision processes by a lot
  - They are able to automate much of the process
    - Which doesn't mean that they automated much of it
- How well does this apply elsewhere?
  - The process seems to me to be particularly useful in that the application of these metrics result in changes in organizational security behavior
  - The fact that these are apples and oranges comparisons is particularly useful because it deals with risk management and not risk analysis

Thank You

Questions?
Discussion?!

Dr.Cohen at Mac.Com
http://all.net/