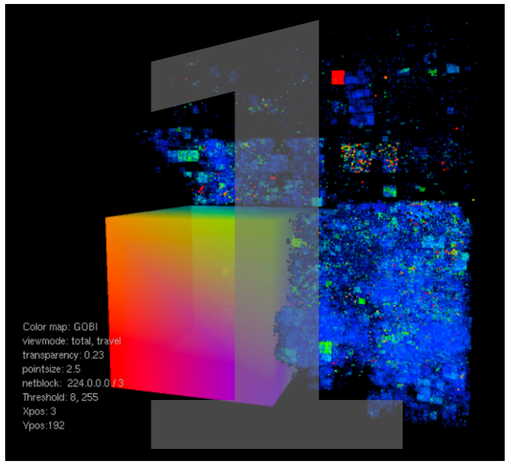
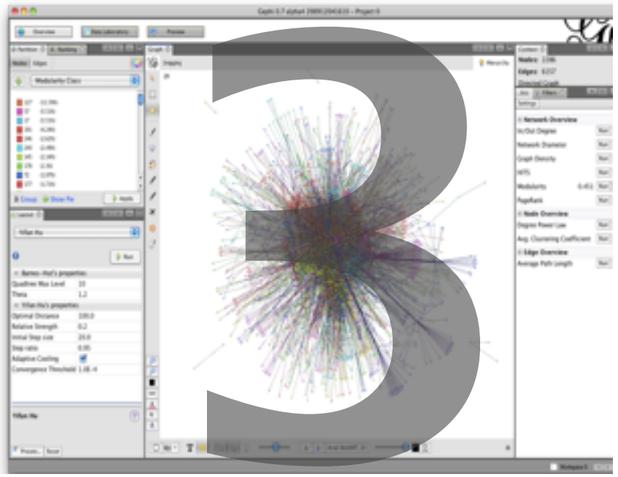
Visualization Trends
And Where We Are Today

Data

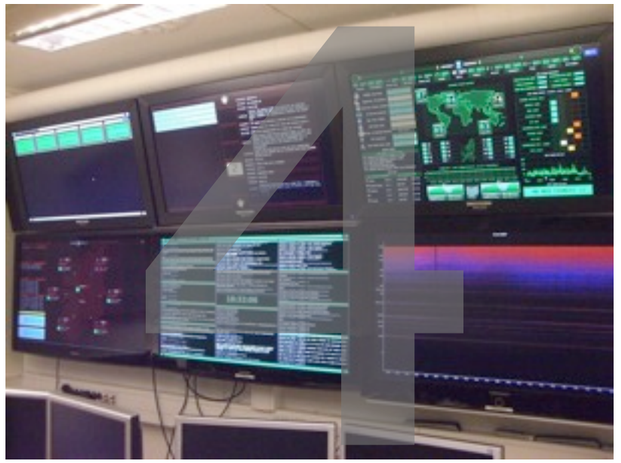


Cloud

Tools



Security

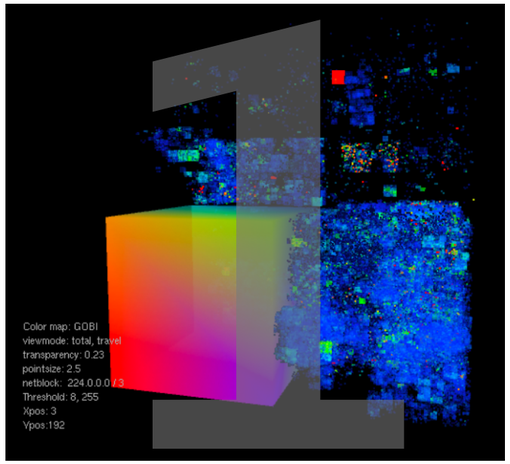


Raffael Marty - @zrlram

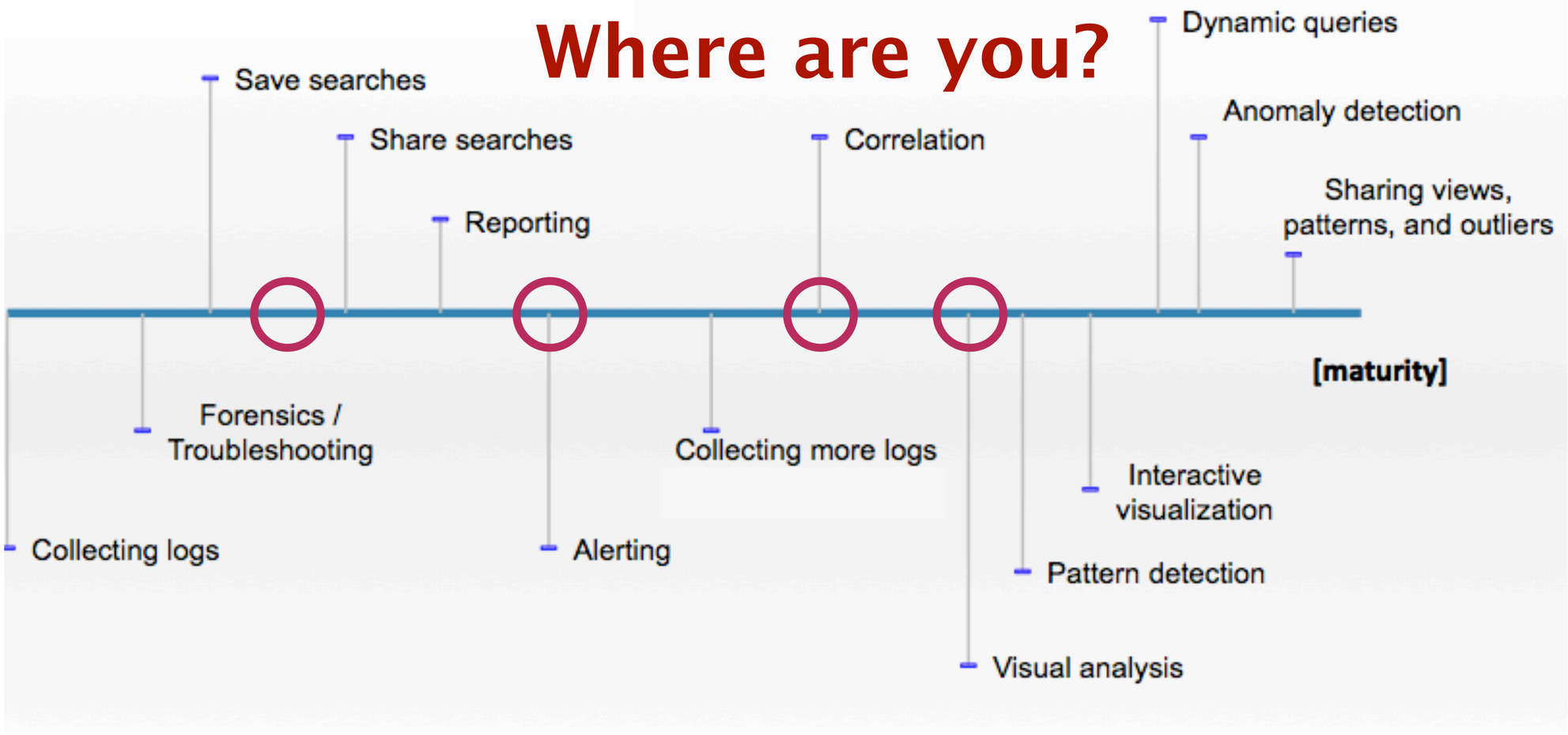
SANS 2010, Washington, D.C.

loggly

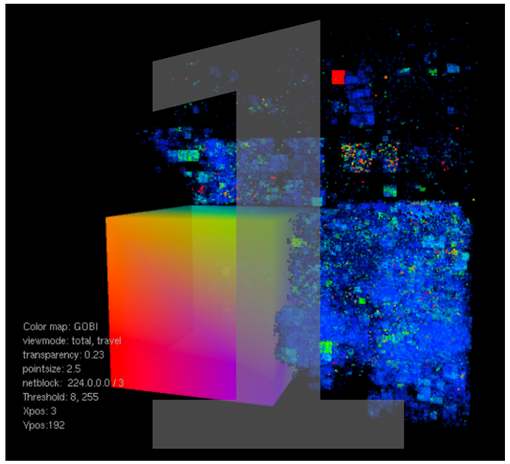
Log Maturity Model



Where are you?



Data



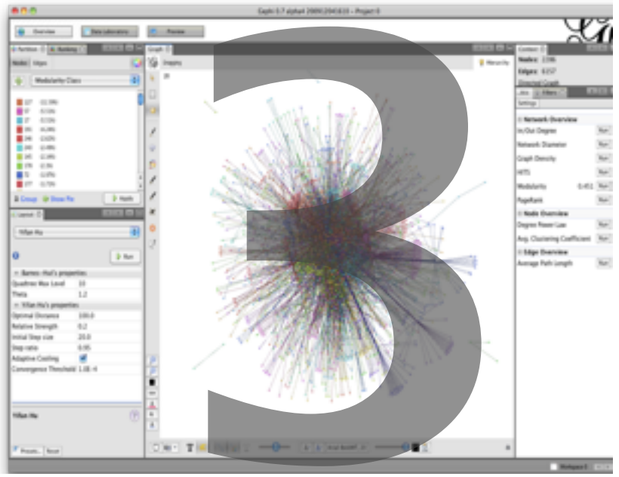
- **No data – no visualization**
- We don't even have / **collect** the data
- It is too **hard** to collect data
- We don't **understand** our data!
- Log management is **expensive**
- **Big data** movement enables large data crunching
- We need data **interoperability** standards – we will get one

Cloud

- A **chance** to build visibility / logging in
- Encourages **open standards** (REST, JSON, etc.)
- Helps advance **Web based** technologies
- Tools are available to **everyone**

- Advancement of **Big Data** tools
- **Build your own**

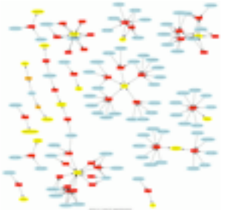
Tools



- We are **nowhere**!
- Same **old** – all over
  - Does your SIEM support <u>real</u> visualization?
- **Missing**: Brushing, Interactivity
- Help the user **understand** the data!

Overview first

Zoom



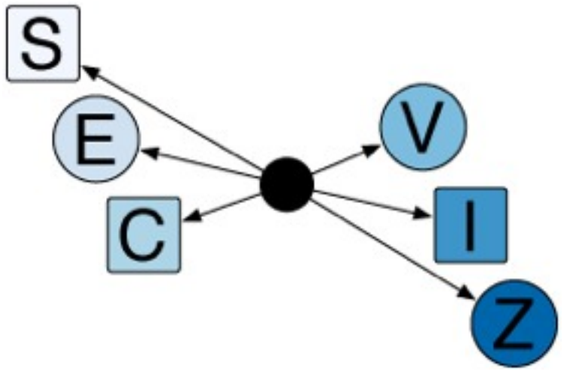
Details on demand

- The move to the **Web** (HTML5)
- **General purpose** tools

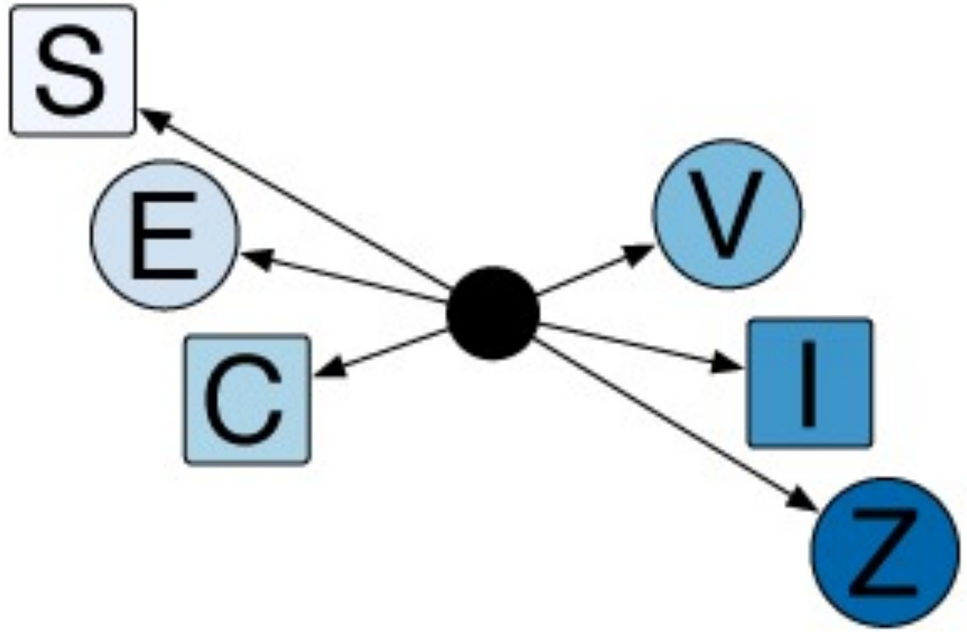
Security

- We **don't have** the data
- Hence, we don't know how to **visualize** it
- Hence, we don't **understand** anything

- We will see more **bad** examples
- Visualization is and will stay an **afterthought**
- More **individual, small** projects



secviz.org



secviz.org - @secviz

about.me/**raffy**

@zrlram