Building better data visualisation for information security

Chris Horsley

CSIRT Foundry

CSIRT foundry

Overview

- What do we mean by visualisations?
- Why visualise?
- What should a good visualisation do?
- What type of tech?
- Hands on with D3

Who is this talk for?

- Someone deciding if visualisation will be useful for their team
- Someone who wants to try visualisation after hearing about it
- Someone using visualisation, but looking for new options

Background

- Web dev / development / sys admin background
- AusCERT - Information Security Analyst
- JPCERT - Information Security Analyst
- CSIRT Foundry - Founder, lead developer

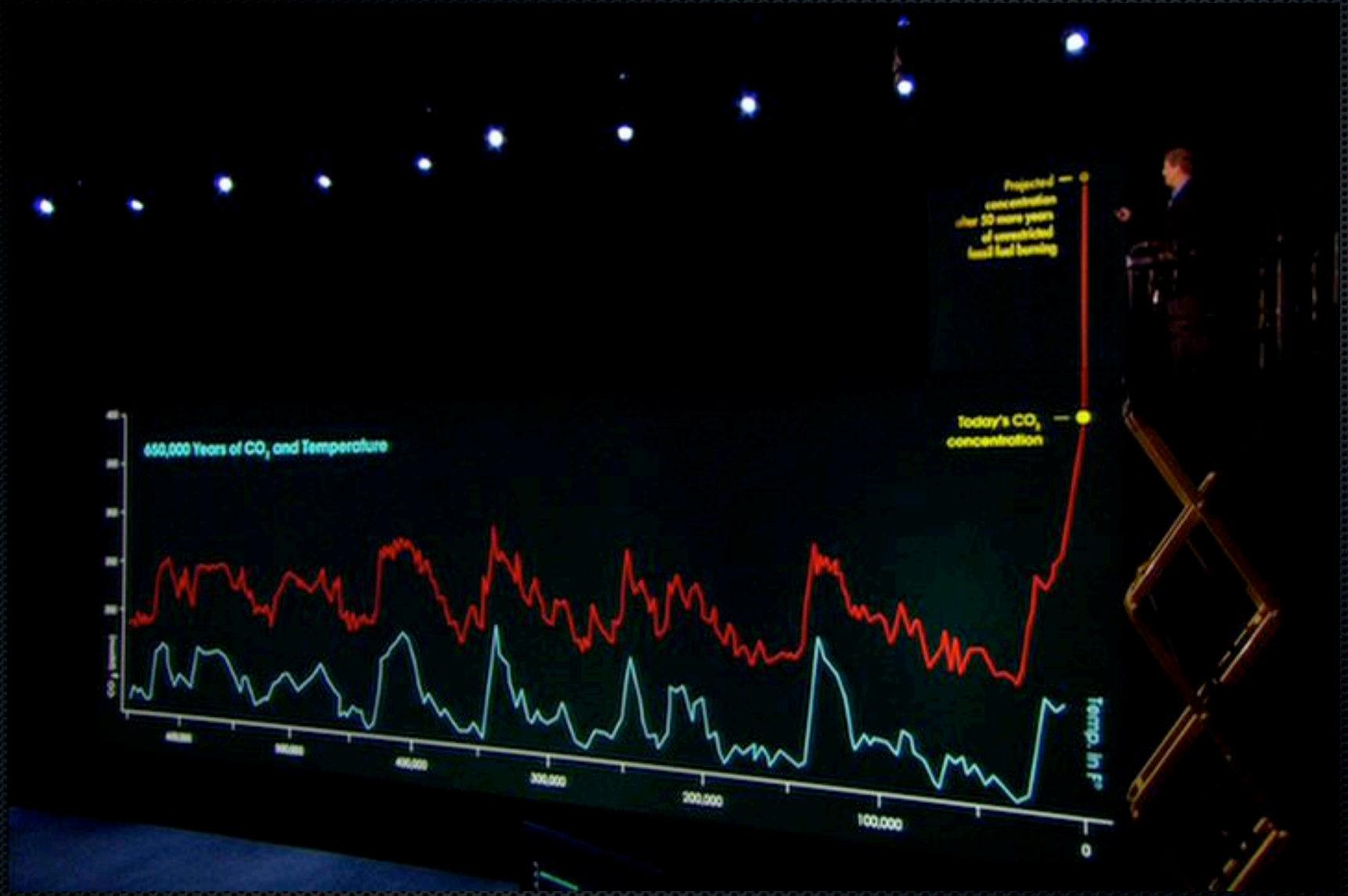
CSIRT foundry

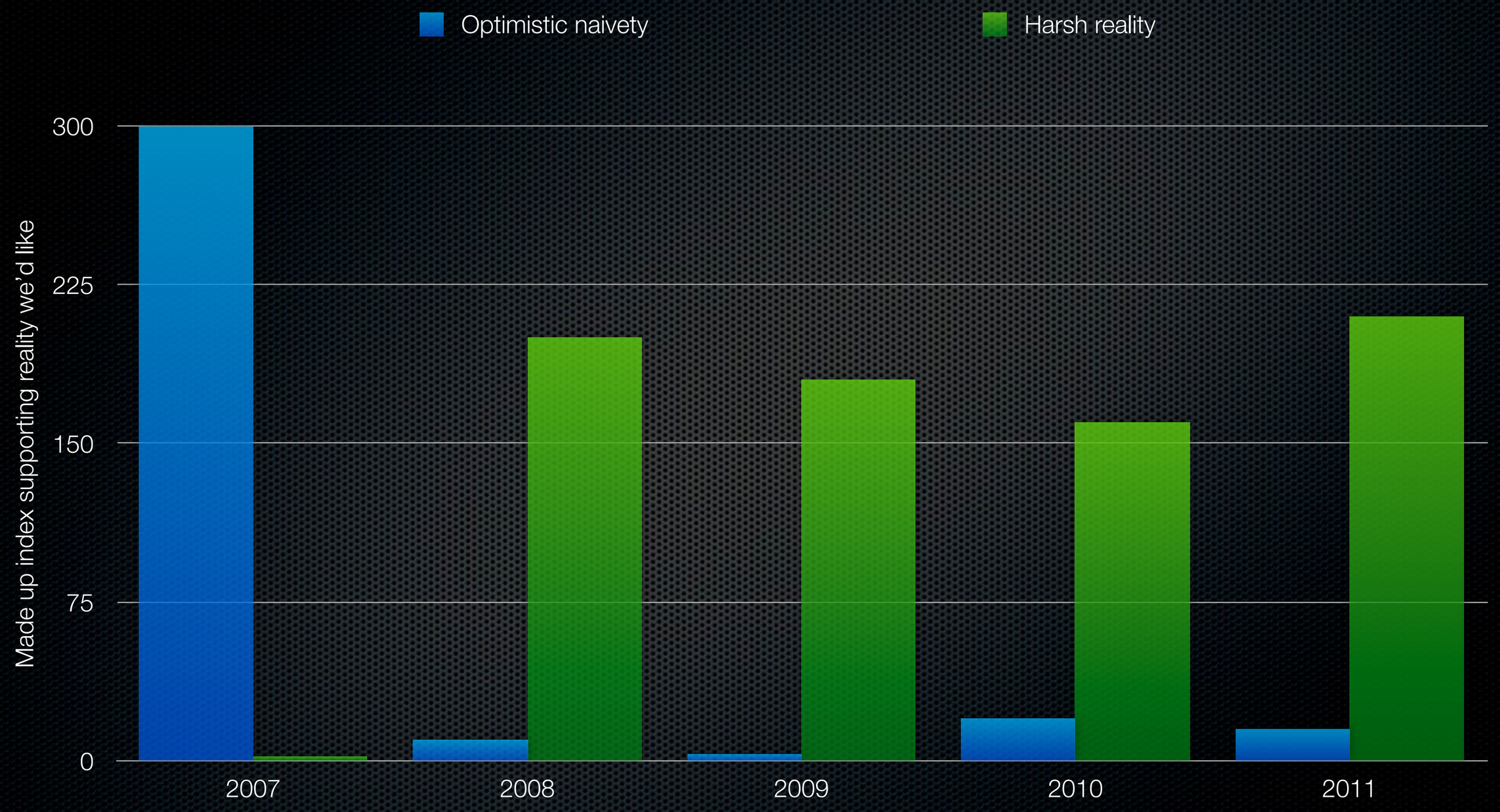
When we talk about “visualisation”...

CSIRT foundry

Data for humans

```
Mar 16 08:12:04 app-1 login[4659]: pam_unix(login:session): session opened for user user3 by LOGIN(uid=0)

Mar 16 08:12:09 app-1 sudo:     user3 : TTY=tty1 ; PWD=/home/user3 ; USER=root ; COMMAND=/bin/su

Mar 16 08:12:09 app-1 sudo: pam_unix(sudo:session): session opened for user root by user3(uid=0)

Mar 16 08:12:09 app-1 sudo: pam_unix(sudo:session): session closed for user root

Mar 16 08:12:09 app-1 su[4679]: Successful su for root by root

Mar 16 08:12:09 app-1 su[4679]: + tty1 root:root

Mar 16 08:12:09 app-1 su[4679]: pam_unix(su:session): session opened for user root by user3(uid=0)

Mar 16 08:12:13 app-1 groupadd[4691]: new group: name=user4, GID=1001

Mar 16 08:12:13 app-1 useradd[4692]: new user: name=user4, UID=1001, GID=1001, home=/home/user4, shell=/bin/
bash

Mar 16 08:12:17 app-1 passwd[4695]: pam_unix(passwd:chauthtok): password changed for user4

Mar 16 08:12:22 app-1 chfn[4696]: changed user `user4' information

Mar 16 08:12:31 app-1 userdel[4700]: delete user `user4'

Mar 16 08:12:31 app-1 userdel[4700]: removed group `user4' owned by `user4'

Mar 16 08:12:38 app-1 groupadd[4702]: new group: name=user1, GID=1001
```

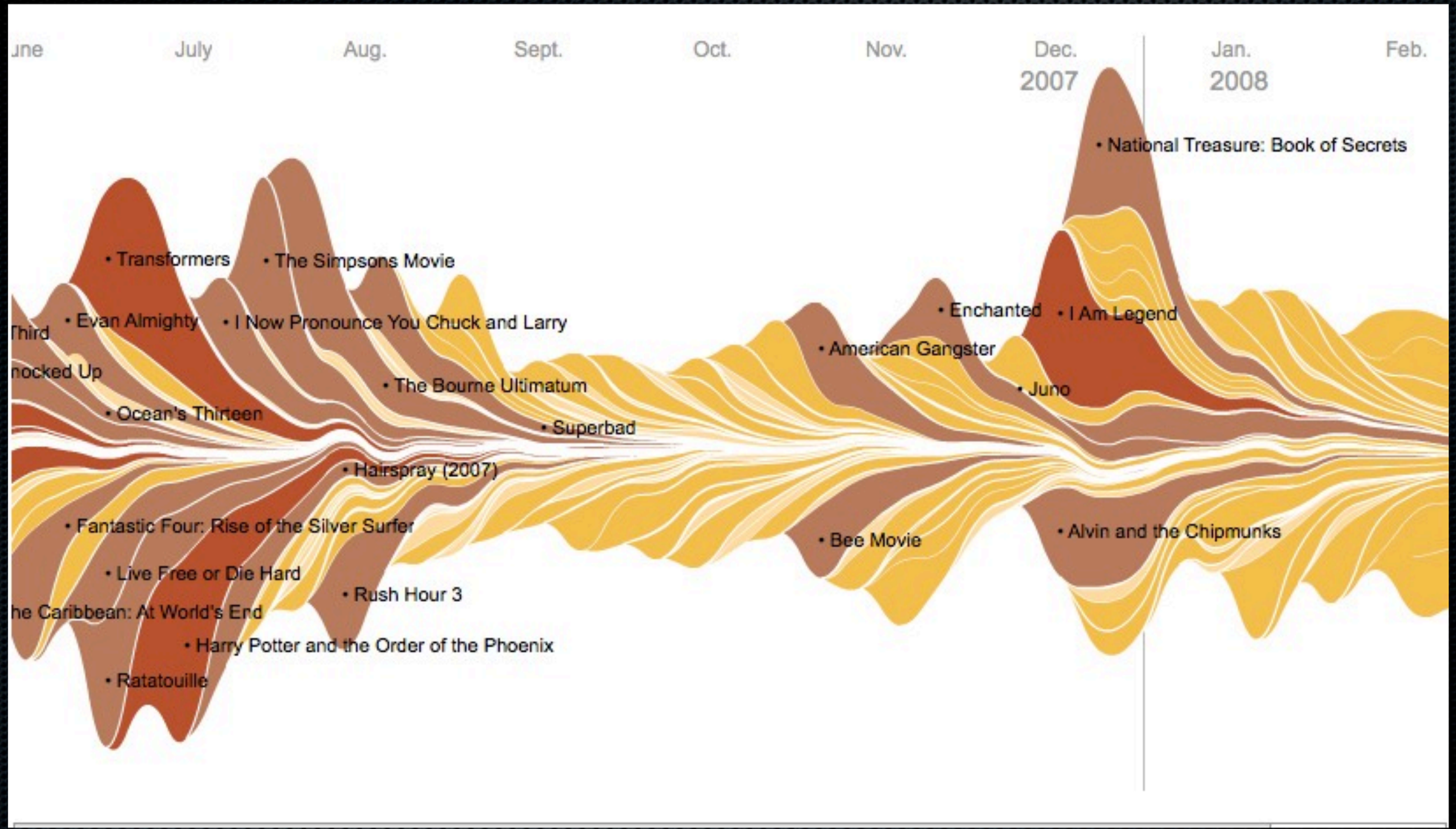

650,000 Years of CO_2 and Temperature
Today's CO_2 concentration
Temp. in F°
400,000
300,000
200,000
100,000
0



CSIRT foundry

```
Beef  ##################
Cake  ######
Tom   ####
Yum   ##################################
Goong #########
```

CSIRT foundry



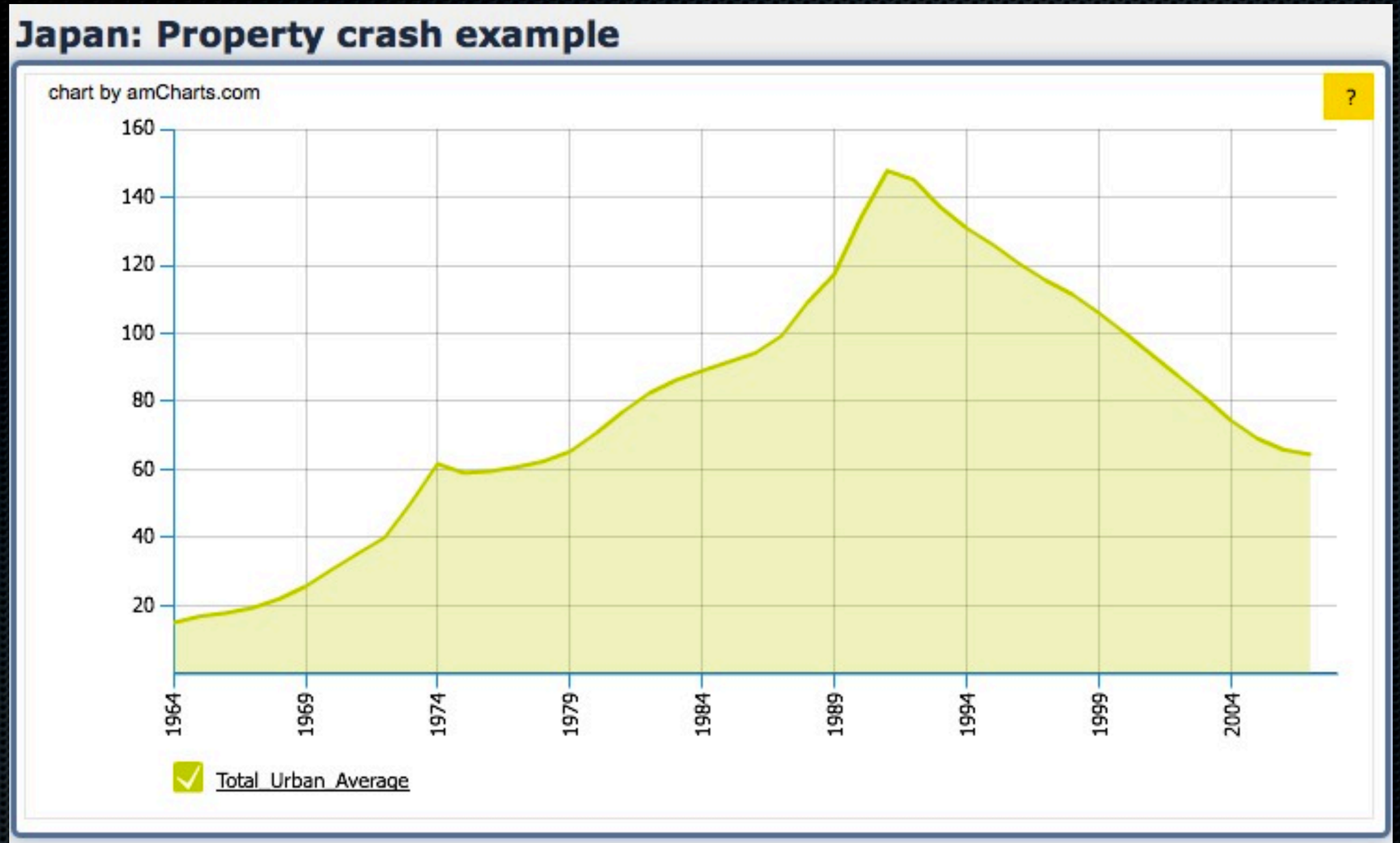
CSIRT foundry

Art + science

What should a good visualisation do?

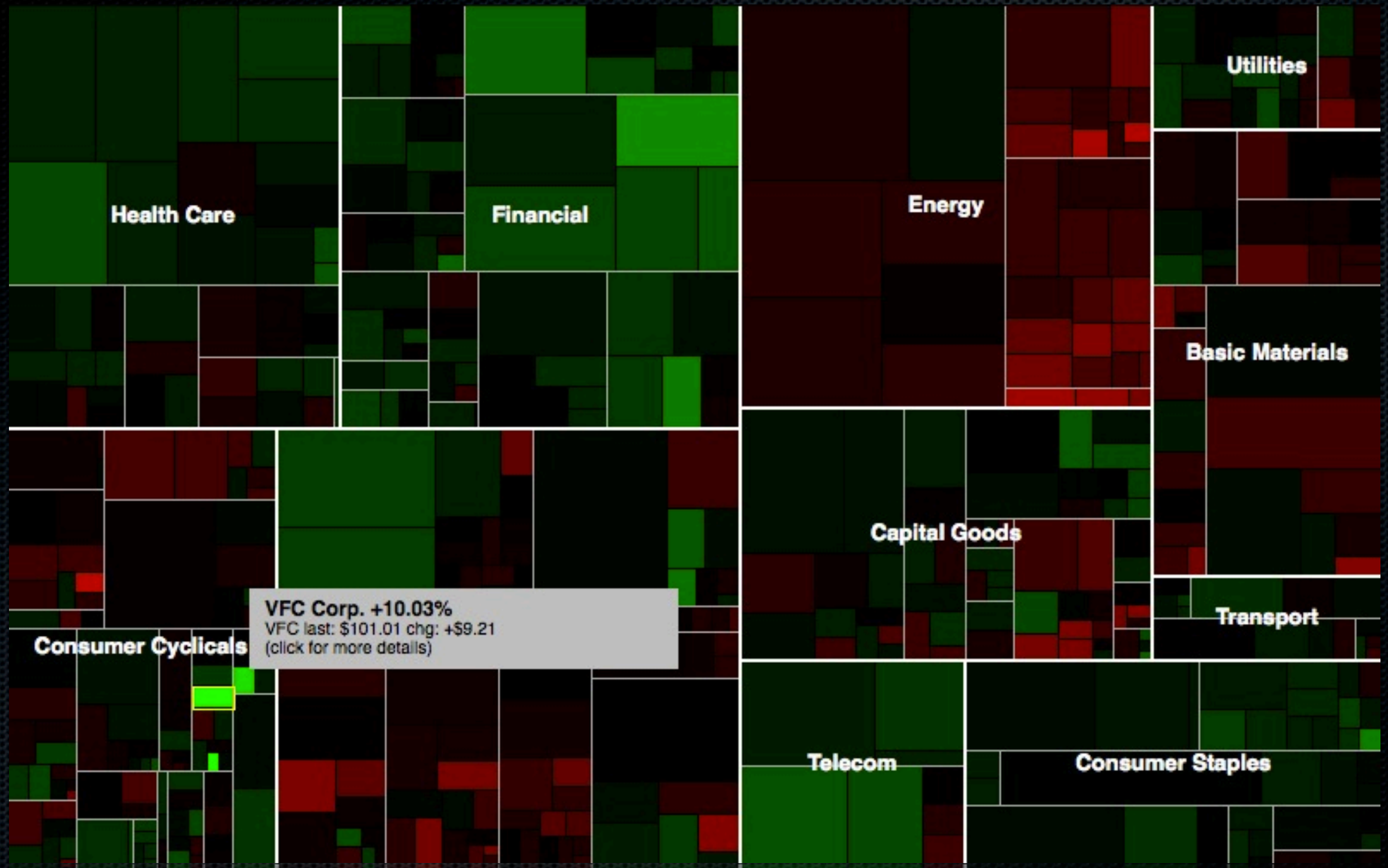
The same as a good photo

CSIRT foundry



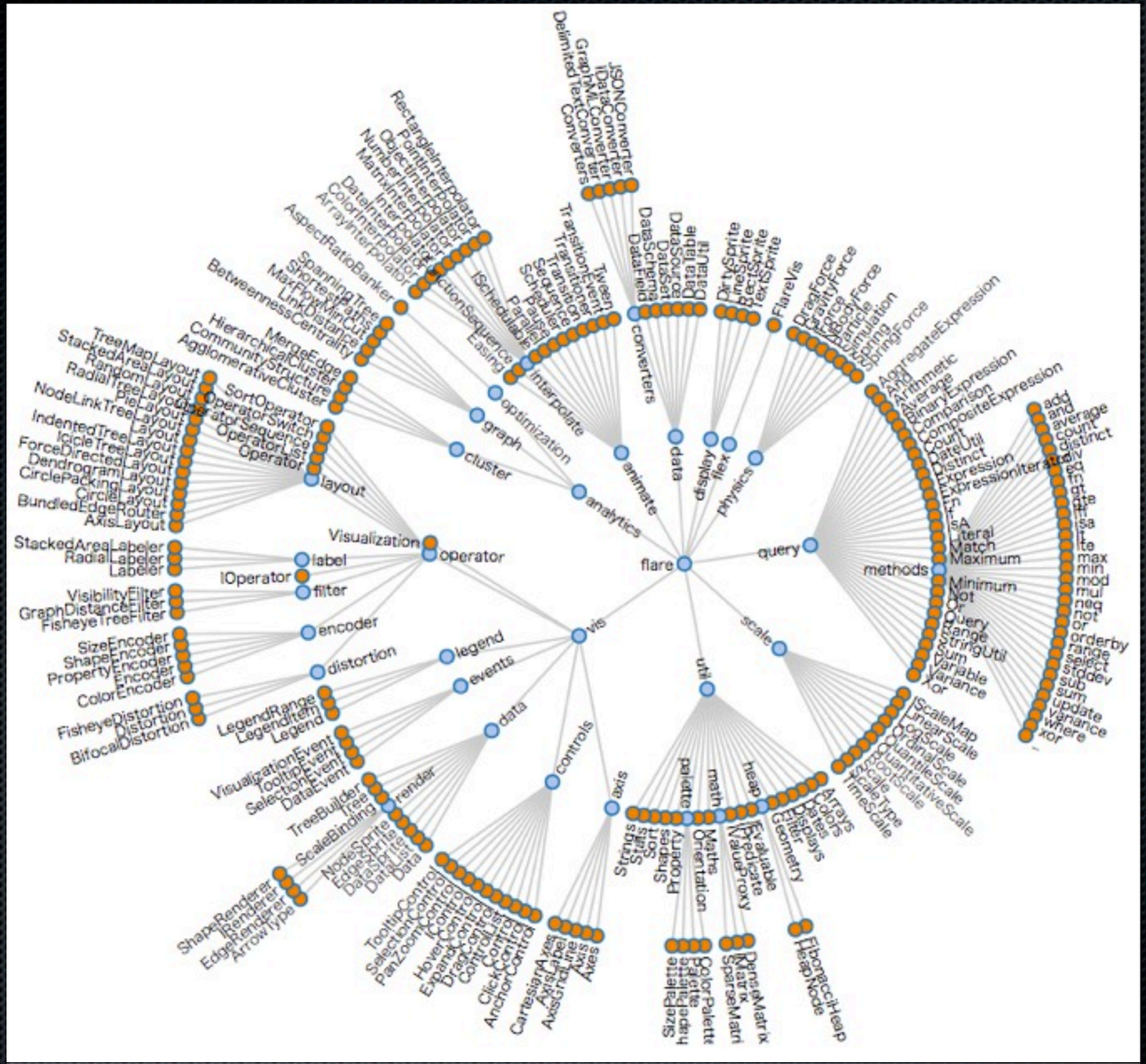
Tell a story

CSIRT foundry

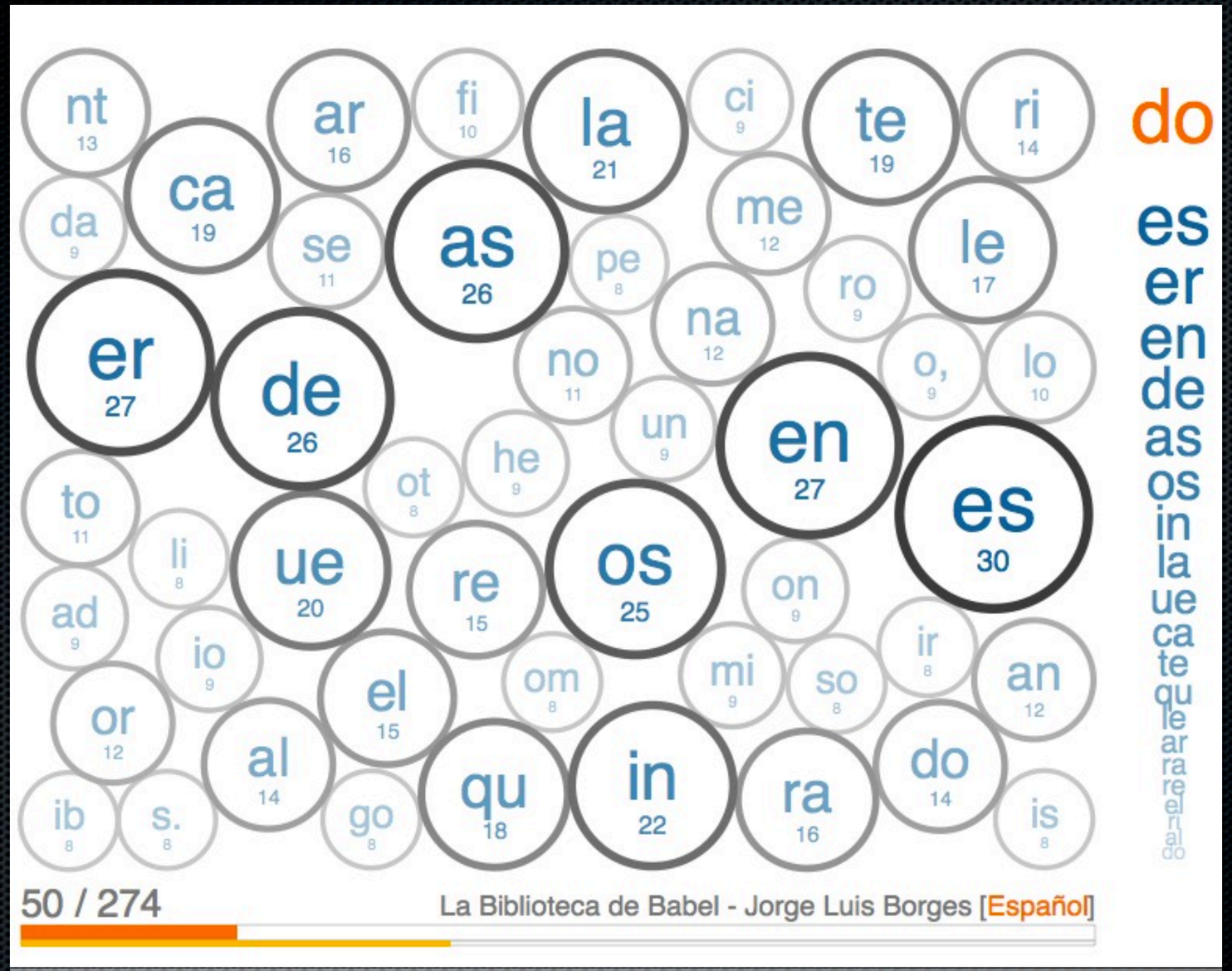


Gives us the next action

CSIRT foundry



Discover new relationships



Be attractive

CSIRT foundry

Think:

Same as writing: what does the reader take away?

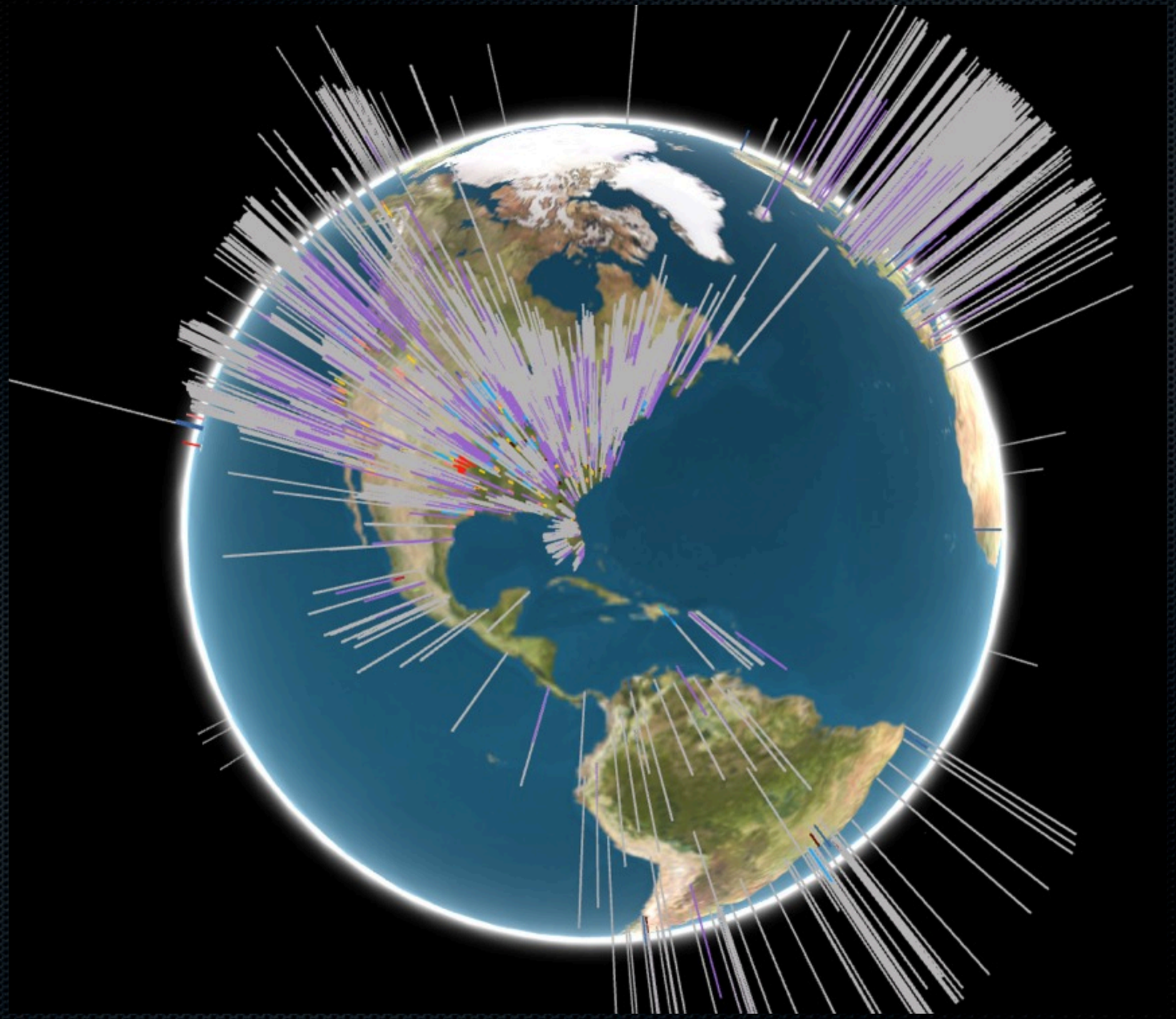
Two broad types of visualisations

Insight

vs

high-level (*a.k.a. management porn)*

CSIRT foundry



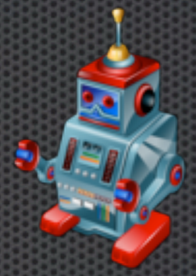
CSIRT foundry

Both can be useful for your team!

- Analyst awareness
- Manager awareness
- Workflow analysis
- Incident trend analysis
- Public education and awareness

What types of visualisations are we talking about today?

Reusable



Automated

Interactive

Animation capable

CSIRT foundry

What kind of visualisation are we **not** talking about today?

CSIRT foundry

- ★ “Infographics”
- ★ One-off visualisations made manually
- ★ Static images
- ★ Flash
- ★ Desktop tools

So, the best toolkit?

So, the best toolkit?

HTML + Javascript

CSIRT foundry

Why web tech?

- Reusable - programmable, code driven
- Automated - pre-generated code or load data realtime
- Interactive - SVG, events
- Animation - SVG, DOM manipulation
- Lots of helper libraries available
- Data format in wide use - JSON
- Cross-platform

Getting started with web visualisations

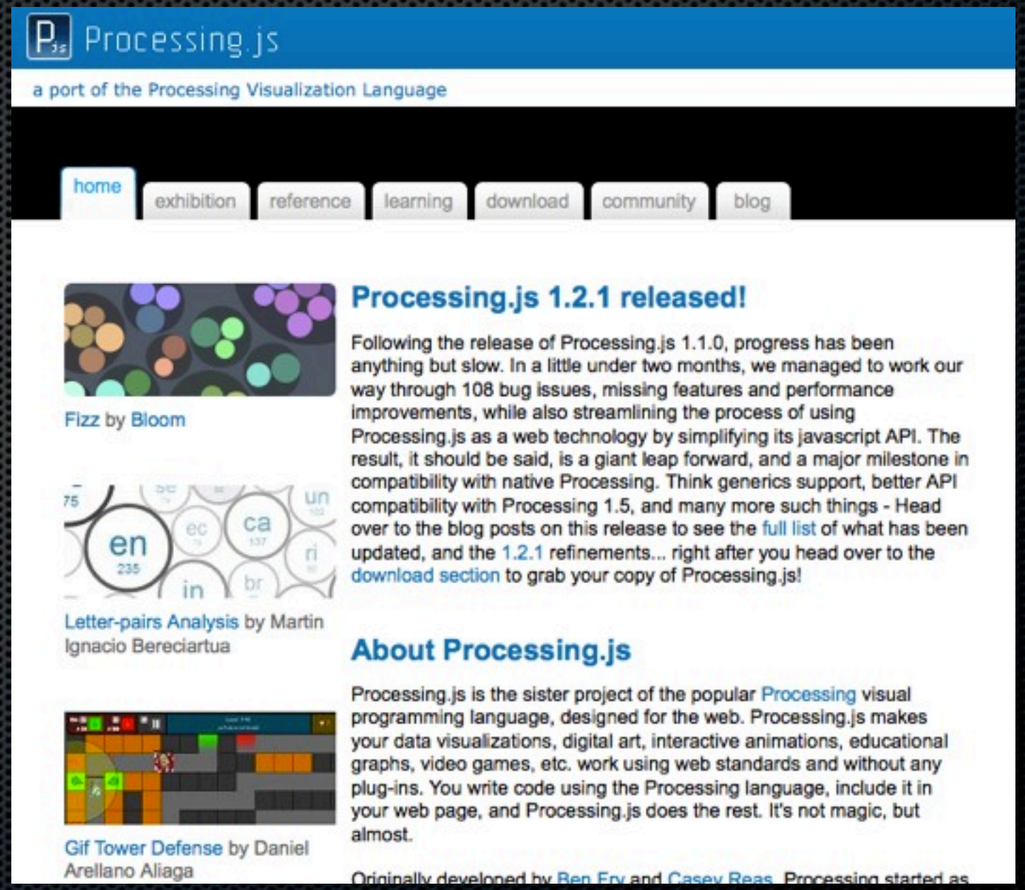
Toolkits

- ProcessingJS
- JIT
- D3

CSIRT foundry

Toolkits - ProcessingJS

- Lower level, broad purpose
- Port from Java to JS
- Wide use by non-techs and artists
- Very flexible
- http://processingjs.org/



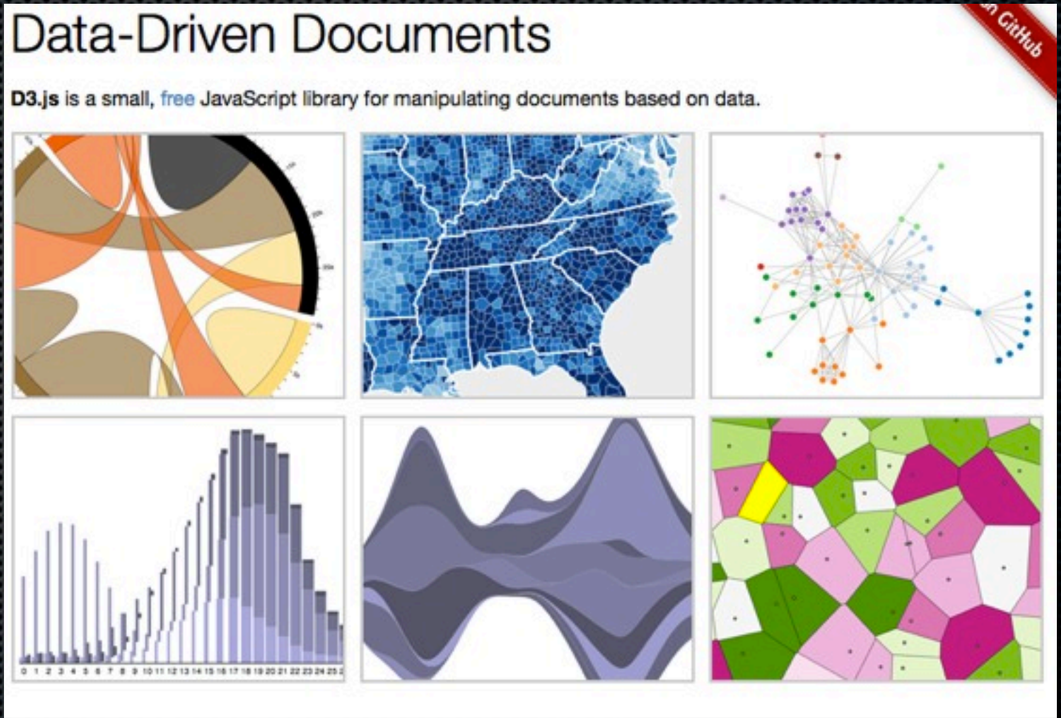
Toolkits - JIT

- Javascript InfoVis Toolkit
- Lots of baked-in layouts
- http://thejit.org/

CSIRT foundry

Toolkits - D3

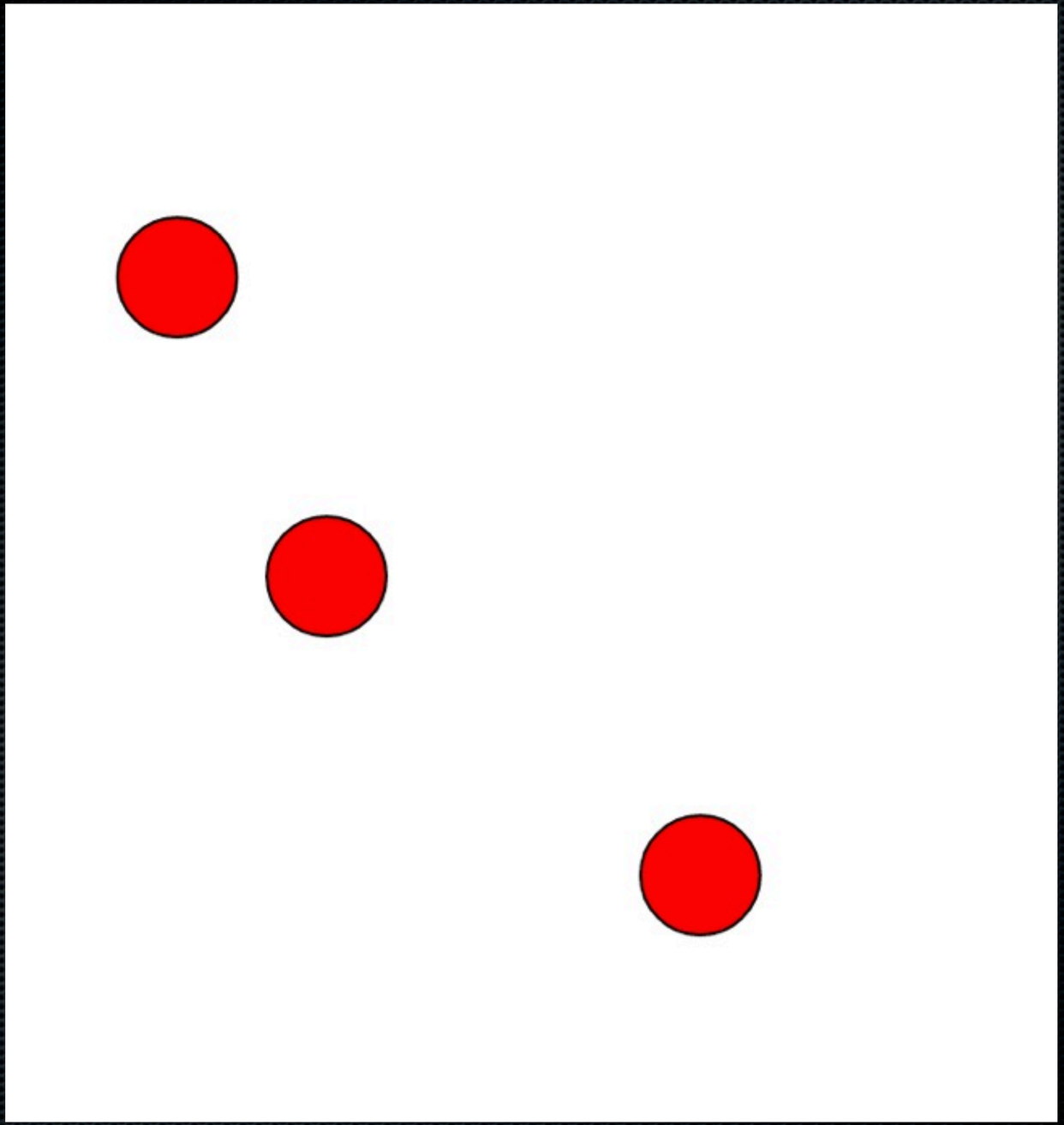
- Bind your data to the document
- Lower level, more flexible
- SVG + DOM manipulation
- Designed for smooth transitions
- http://d3js.org/



D3 in action

Building a D3 vis from scratch

CSIRT foundry



CSIRT foundry

The HTML

```
<HTML>
<HEAD>
  <TITLE>Getting started with D3</TITLE>
  <SCRIPT language="Javascript" src="lib/d3.v2.js"></SCRIPT>
</HEAD>
<BODY>
  <div id="viz"></div>
</BODY>
</HTML>
```

CSIRT foundry

The code

```
var dataset = [10,20,45];

var canvas = d3.select("#viz")
                    .append("svg:svg")
                    .attr("width", 500)
                    .attr("height", 500);

draw();

var mycirc = canvas.selectAll(".mycirc")
    .data(dataset)
    .enter()
    .append("svg:circle")
    .attr("class", "mycirc")
    .attr("fill", "red")
    .attr("stroke", "black")
    .attr("r", 20)
    .attr("cx", function(d){ console.log(d); return d * 5 })
    .attr("cy", function(d, i) { return i * 100 + 100 })
```

CSIRT foundry

Summary

- Tell stories about data
- HTML + JS is a very flexible option for visualisation
- Lots of mature and emerging toolkits
  - D3 is great! http://d3js.org/

Thank you!

- chris.horsley@csirtfoundry.com
- http://csirtfoundry.com
- Twitter: @Parsify and @CSIRTFoundry

CSIRT foundry