Bsides Spl22

Innovating in Cyber:

l iplocation for the rest of planet earth

(Starting with Australia)

Ugh… My talk got chosen…
NOW I HAVE TO DO THIS!

Slides and recording will be made available…

BSIDES SPL

We are going to look at

- THE PROBLEM
- THE THOUGHT PROCESS
- THE SOLUTION

But first… where can we get some data?

```
| makeresults count=1
| eval randomIP=(random()%254).".".(random()%254).".".(random()%254).".".(random()%254)
| fields - _time
```

BSIDES SPL

So we got lots of src IP's… but we want AU

FIND THEM…

- who managers the IPs?
- backbone routing tables?
- real data…

Teeeeeo complicated

MAKE THEM…

Who has lots of IP addresses

TELCOS?…? ISP's!!

BIG ISP's

national POP's…

BSplunks$ whois TELCO.AU

Pick a BIG / National ISP…

Get one of their IPs

```
root@SplunkBSides-2022:~# host bigpond.com
bigpond.com has address 61.9.173.37
bigpond.com mail is handled by 10 extmail.bigpond.com.
root@SplunkBSides-2022:~#
```

Get that IP allocation

```
root@SplunkBSides-2022:~# whois 61.9.173.37|grep 'related to'
% Information related to '61.9.128.0 - 61.9.255.255'
% Information related to '61.9.128.0/17AS1221'
root@SplunkBSides-2022:~#
```

@ HOME?

```
curl 'https://api.ipify.org'|xargs
whois|grep 'related to'
```

Pick a BIG / National ISP…

Events Patterns **Statistics (5,023)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 … Next >

City	Country	Region	lat	lon	src
Southport	Australia	Queensland	-27.96870	153.41600	61.9.194.171
Southport	Australia	Queensland	-27.96870	153.41600	61.9.227.92
Hobart	Australia	Tasmania	-42.88210	147.32700	61.9.185.54
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.171.205
Sydney	Australia	New South Wales	-33.86880	151.20900	61.9.161.207
Gold Coast	Australia	Queensland	-28.01670	153.40000	61.9.212.83
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.133.71
Gold Coast	Australia	Queensland	-28.01670	153.40000	61.9.223.124
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.147.192
Melbourne	Australia	Victoria	-37.81360	144.96300	61.9.156.105

BOSIDES SPL

OK - I CAN DO THIS!


WOOF
splunk>enterprise
ASHER LEE
Password
Sign In
Who let the logs out?
splunk
BSIDES SPL
TweetOfAsh
/asherlee/

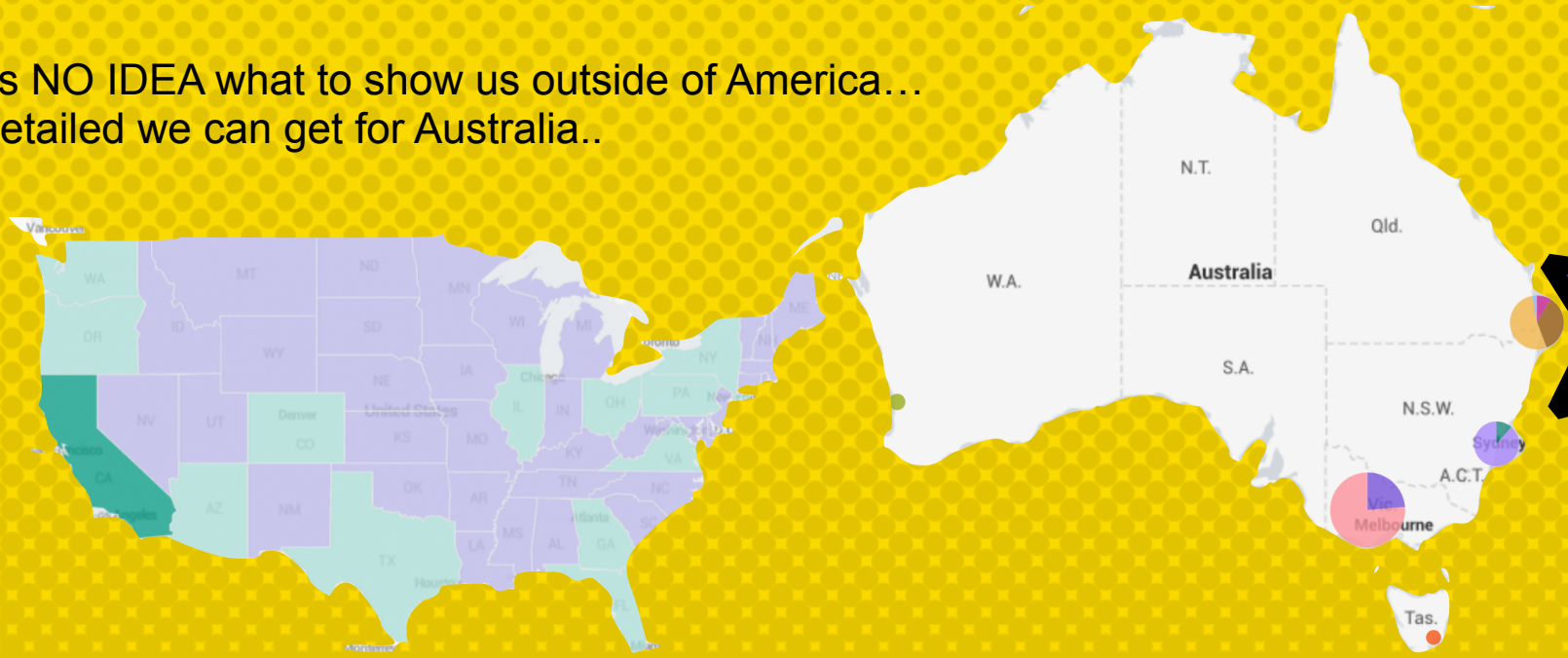
What Problem Are You Solving?

BOSIDES SPL

WHATS WRONG ANYWAY?

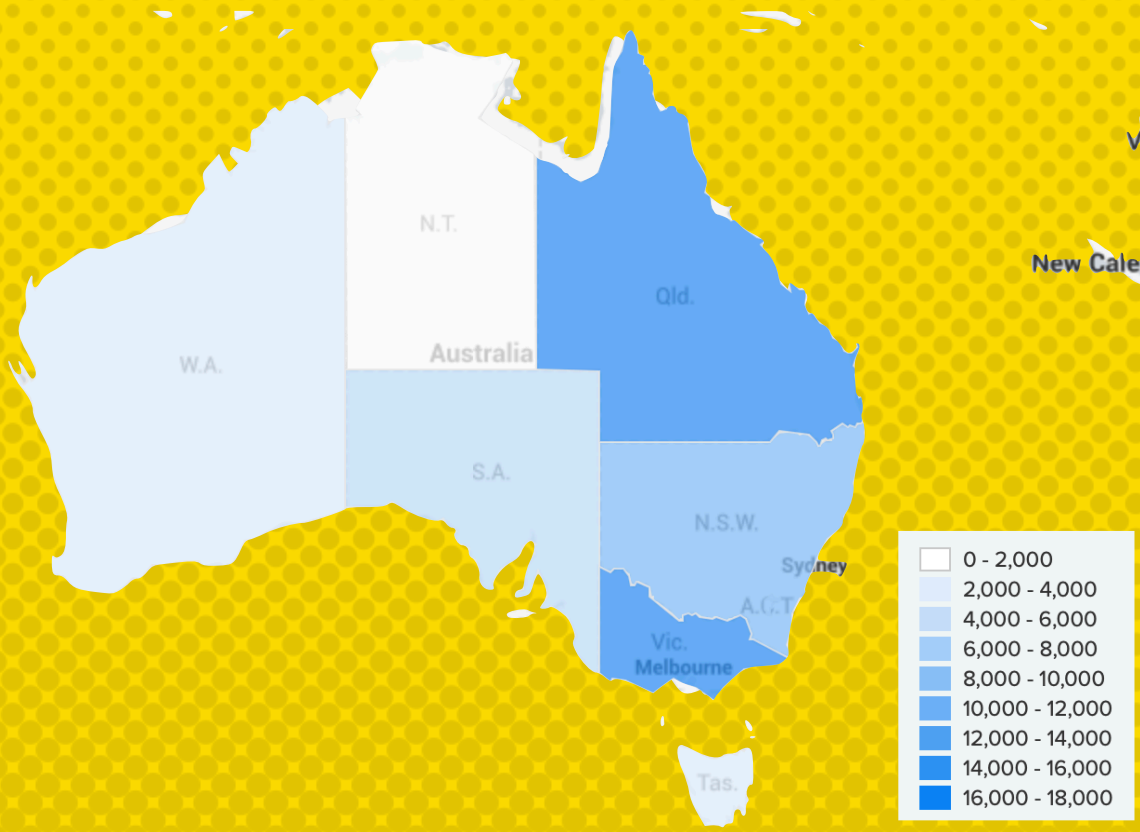
Choropleth vs Cluster Maps

The System has NO IDEA what to show us outside of America…
I wonder how detailed we can get for Australia..
LETS GO

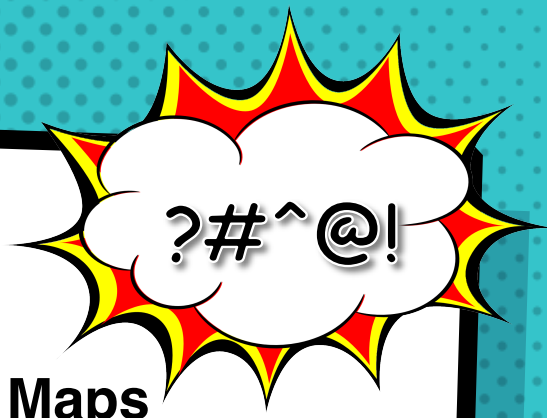


BSIDES SPL

RESULT…?


N.T.
Qld.
W.A.
Australia
S.A.
N.S.W.
Sydney
A.C.T.
Vic.
Melbourne
Tas.
New Cale
0 - 2,000
2,000 - 4,000
4,000 - 6,000
6,000 - 8,000
8,000 - 10,000
10,000 - 12,000
12,000 - 14,000
14,000 - 16,000
16,000 - 18,000

What do we need to know?



iplocation

Lets go maxmind lets go

MAPPING the IP with a Country / City / LGA / Postcode / lat / long

kmz / kml

The important file for geom … how do we know?

Documentation¿

Yes there is splunk docs.. lets search Choropleth & geom

iplocation

geom

Cluster Maps

Used to supply the map bounds for Choropleth maps… this is how I found it!

Choropleth Maps

geom

Lookups:

kmz

- Has an option for GeoIP

Lookup file examples:

- geo_attr_countries.csv
- geo_countries.kmz

Lookups

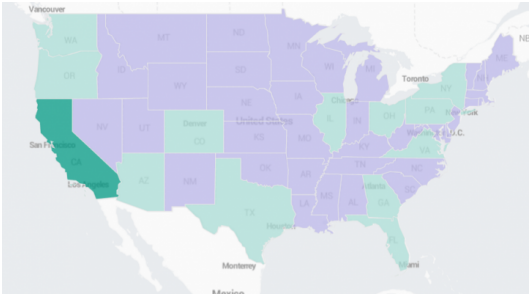
Documentation

Cluster Maps

Working…

Choropleth Maps

DOES NOT WORK FOR AUSTRALIA or anywhere outside the USA really…



BOSIDES SPL

Some more IP Geolocations …

1. ipstack
2. Positionstack
3. ipapi
4. Abstract API
5. ipdata
6. Maxmind
7. IP Geolocation API by WhoisXML
8. IP-API
9. ipgeolocation
10. Ipify
11. IPwhois
12. Ipregistry
13. IP2Location
14. DB-IP
15. IPInfo

https://geekflare.com/geolocation-ip-api/

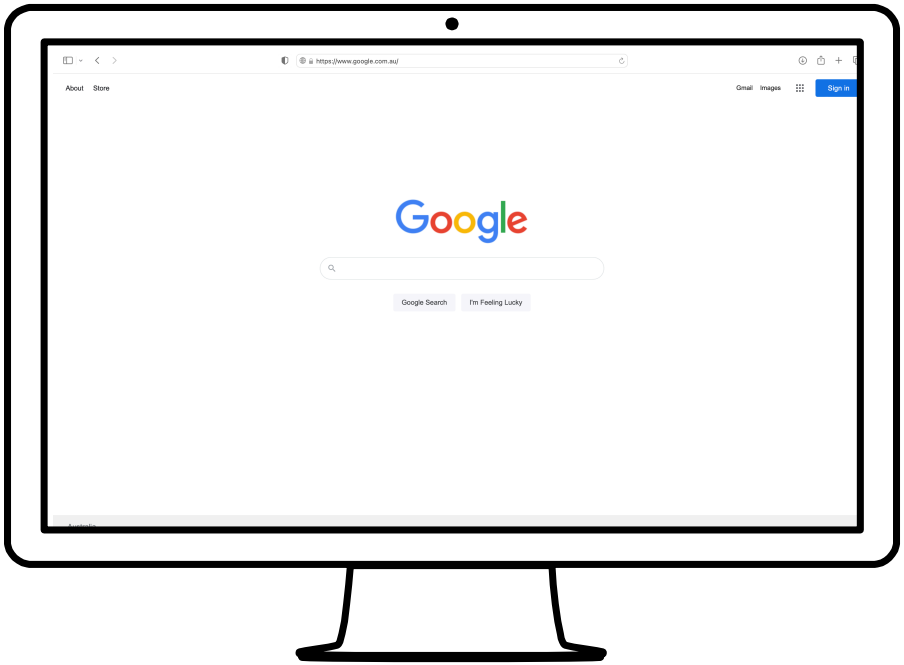
Lets go geom, lets go!

What kind of problem is this?

Why doesn't it populate?

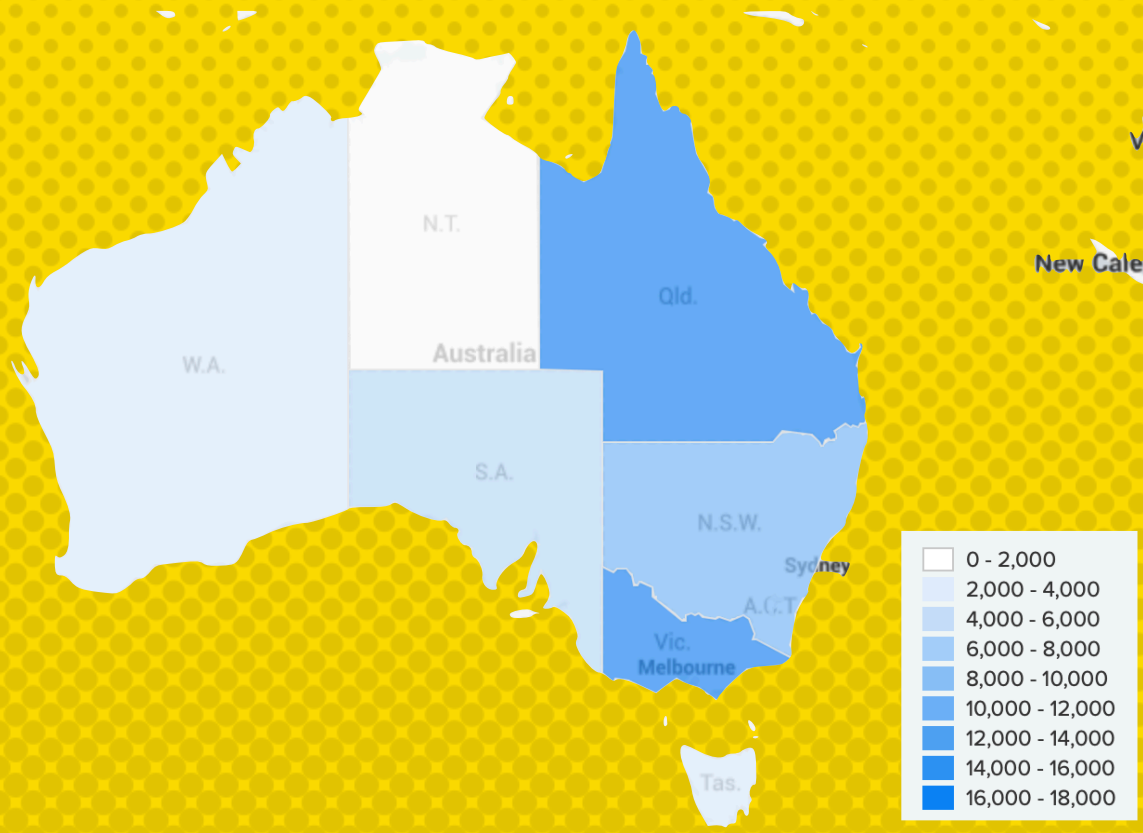
What kind of data is missing?

What is geom?



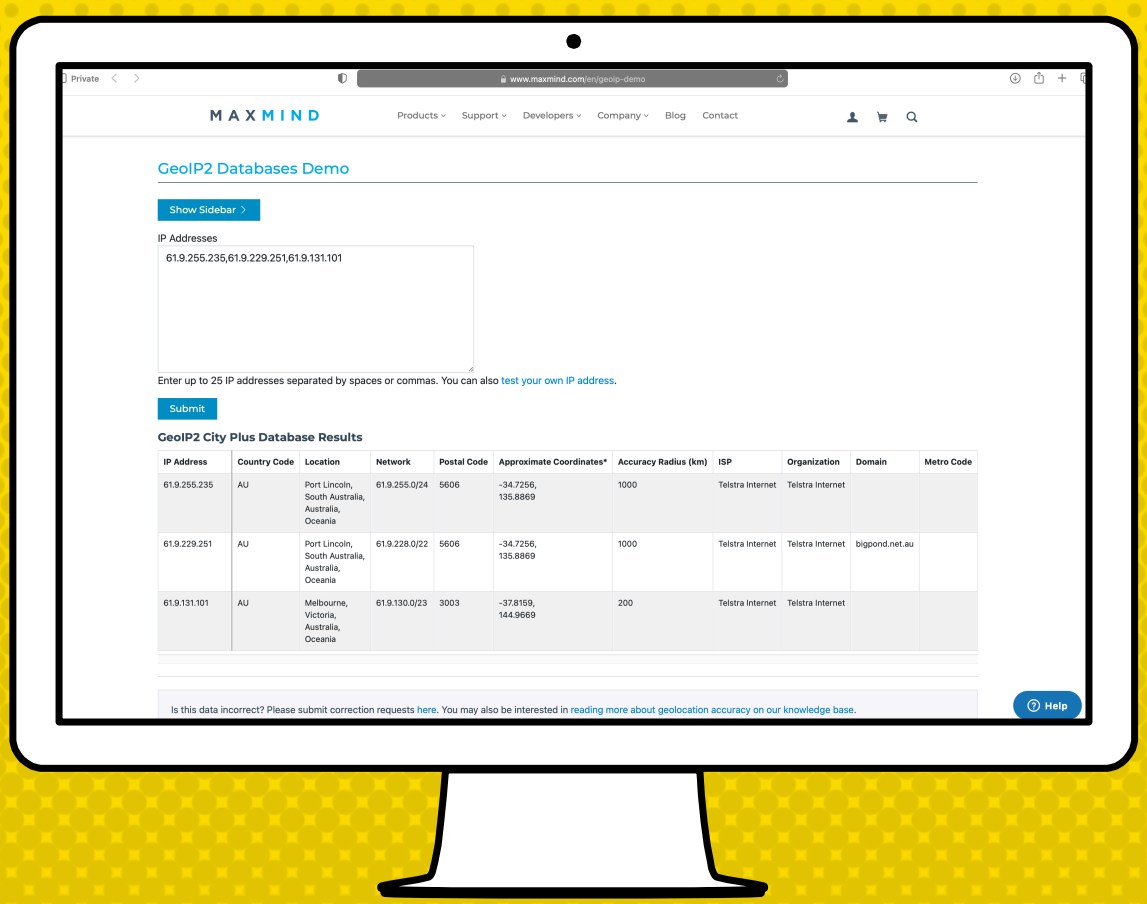
BOSIDES SPL

That’s our AU State Borders…



GEOM Maxmind extra

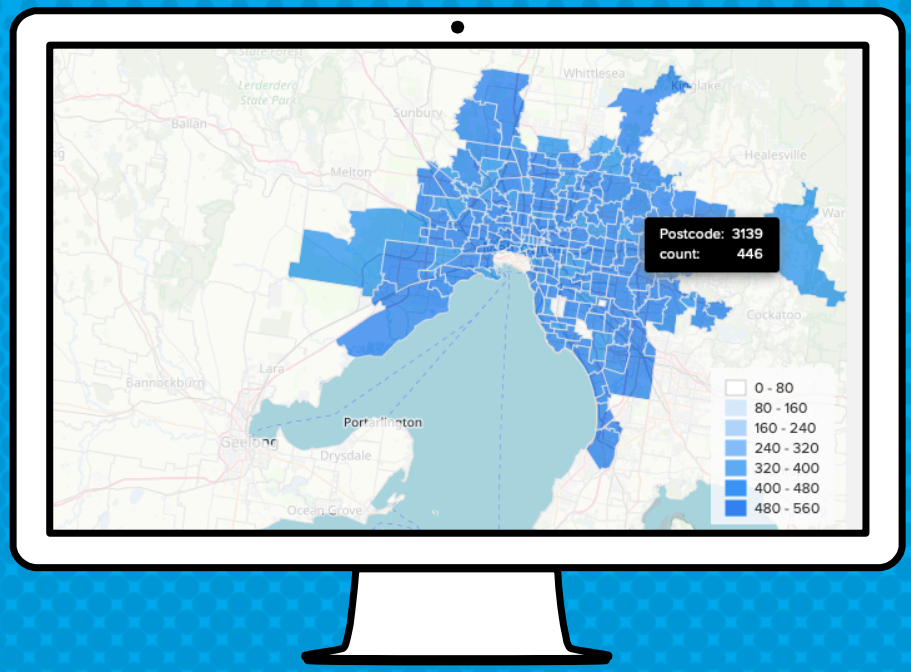
Continent
Country (Inc EU Country)
Country of Registration
Subdivisions (regions)
City Name
Postal Code (Outside USA)
Latitude / Longitude
Accuracy Radius (km)
Metro Code (USA only)
Time zone
GeoNames IDs



BSIDES SPL

ZOOM ZOOM … (Not the chat kind)

- Zoom only goes so deep…
- What are Map Tiles?
- How do I get some?



ZOOM ZOOM ZOOM (EVEN MORE ZOOM...)

- More detail than google?
- Lets consider…
- SVG - An office layout?
- WiFi Usage / Density ?

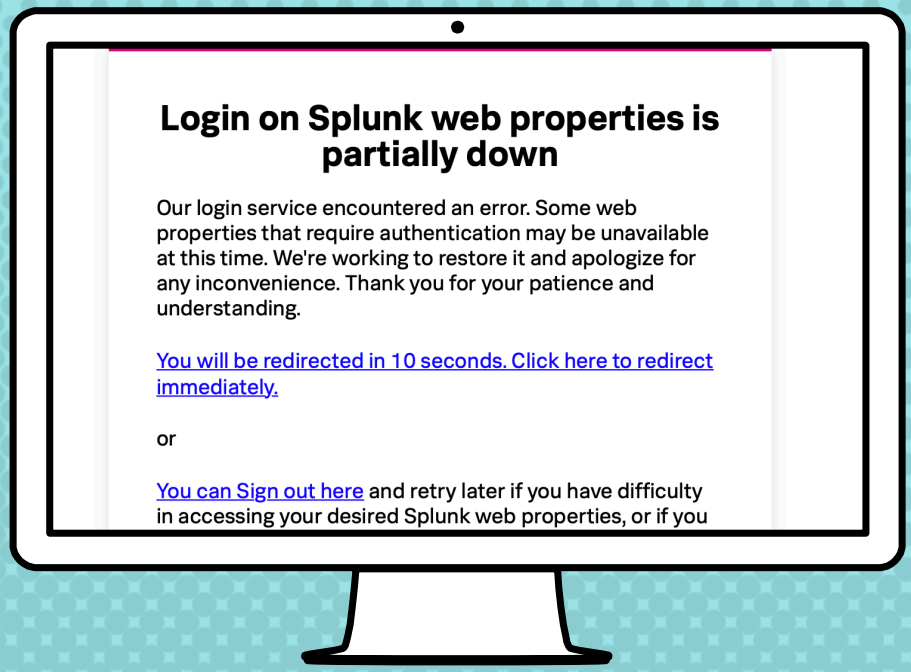
BO SPL SIDES

ZOOM ZOOM ZOOM (EVEN MORE ZOOM...)

More detail than google?

Lets consider…

SVG - People Finder?



BSIDES SPL

Management…

Your data can come from a lot of places…

GEOIP & Shipping Address are popular

Chlorpleth Maps make data visual.
Visualisation make a story.

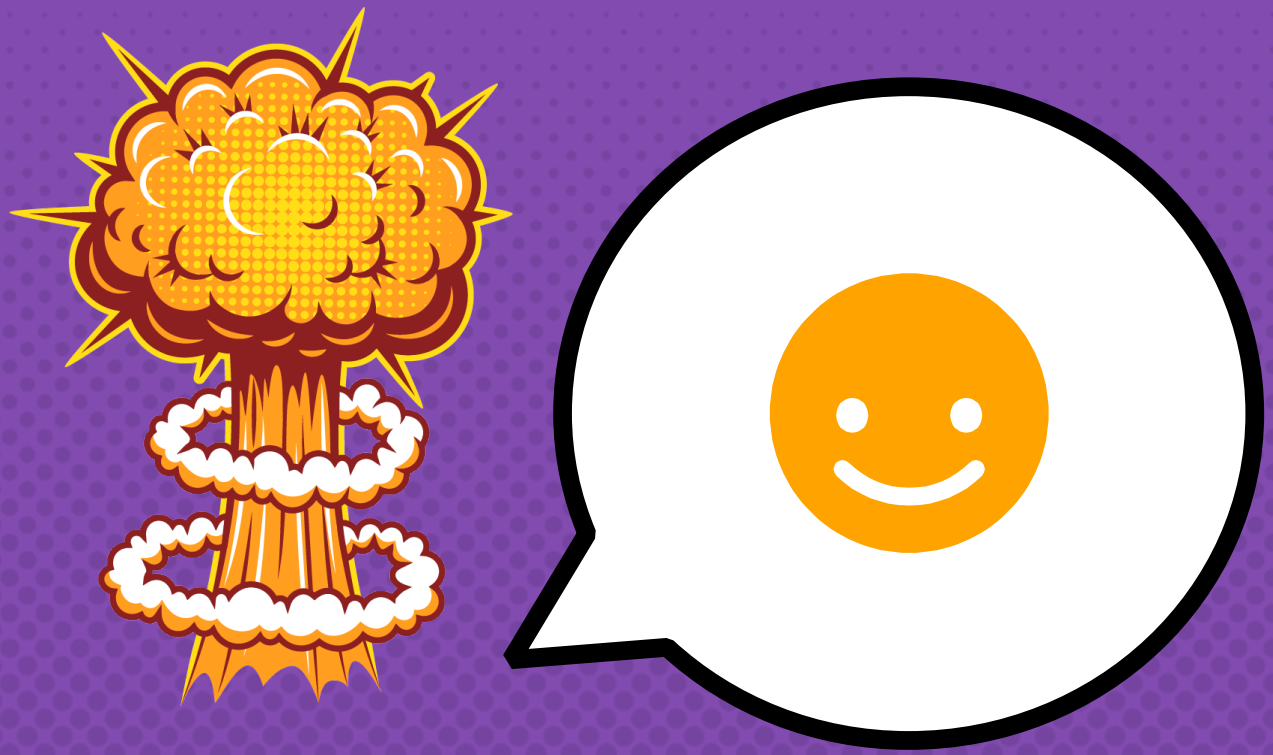
Managers like visual stories.

Good story telling can increase budgets
Better budgets mean more toys for us!

Be-ware the toxic workplace and the toxic manager

BSIDES SPL

BOSIDES SPL



THANKS!

BSIDES SPL