Alerting: More Signal Less Noise Less Pain

Alexis Lê-Quôc (@alq)

Is this talk for me?

- ✓ I am or will be **on-call**
- ✓ I **don't like** being alerted
- ✓ I want the **pain** to go away

The next 40 minutes

1. Alerts == pain?
2. Measure alerts
3. Concrete (& fun) steps

Alleviate the **pain**

When am I on-call next?

↥ Ops

Level 1:
Oct 21, 2013 at 7:00 PM - Oct 22, 2013 at 1:30 AM

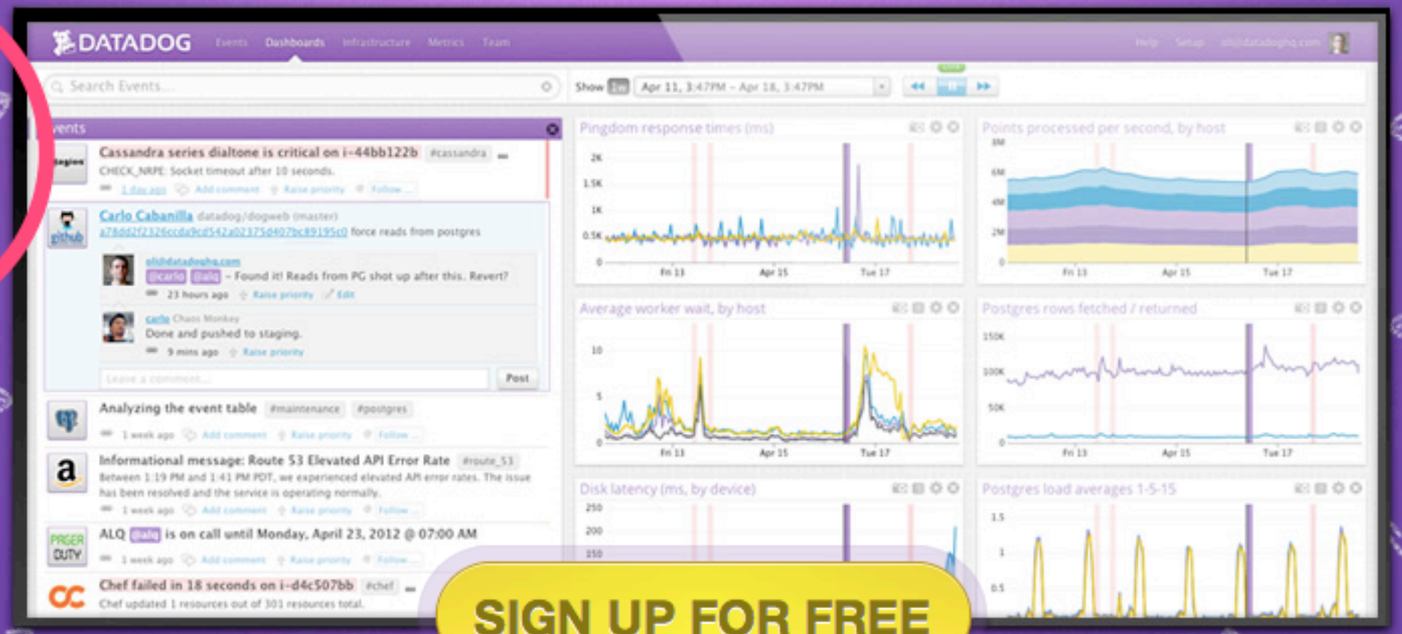
Level 2:
Oct 28, 2013 at 7:00 AM - Nov 4, 2013 at 7:00 AM

Level 3: on-call all the time

DATADOG

See it all in one place

Your servers, your clouds, your metrics, your apps, your team. Together.



ALERTS

CUSTOM METRICS

USAGE ANALYTICS

PERFORMANCE MONITORING

ISSUE TRACKING

CONFIG. MANAGEMENT

CDN

ON-PREMISE SERVERS

CODE CHANGES

CLOUD HOSTING

SIGN UP FOR FREE


Pain


Man
vs
Machine

“too frequently”
“odd hours”
“always the same”

3 simple things to measure

“Always the same”

Steps

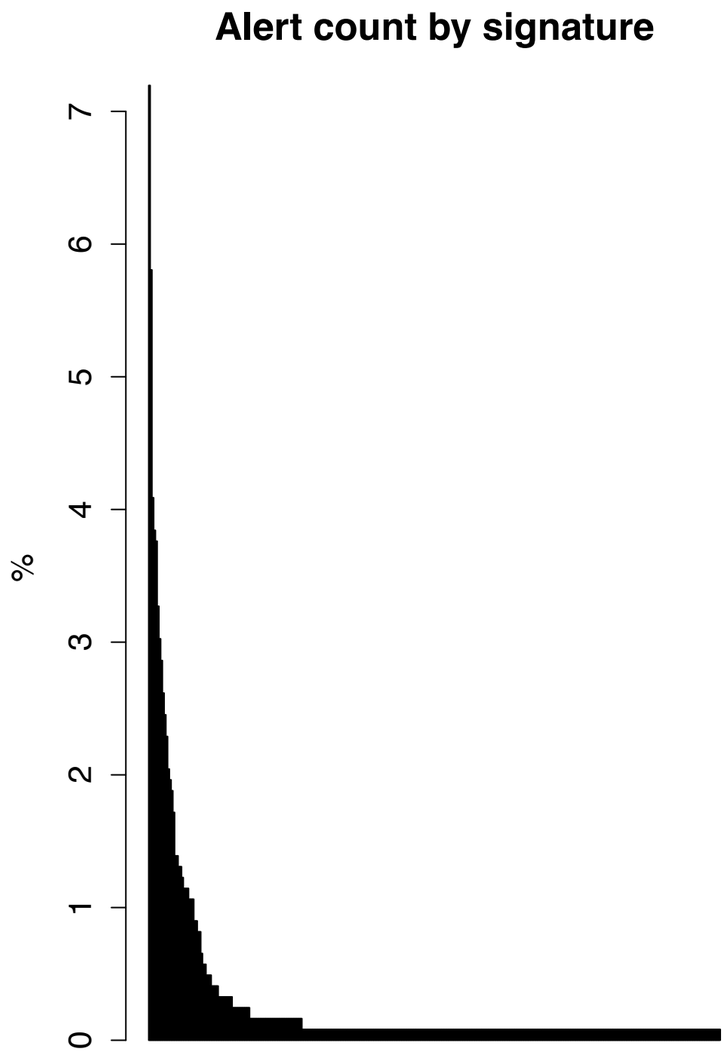
- Group alert stream by “alert signature”
- Rank by occurrences
- Graph

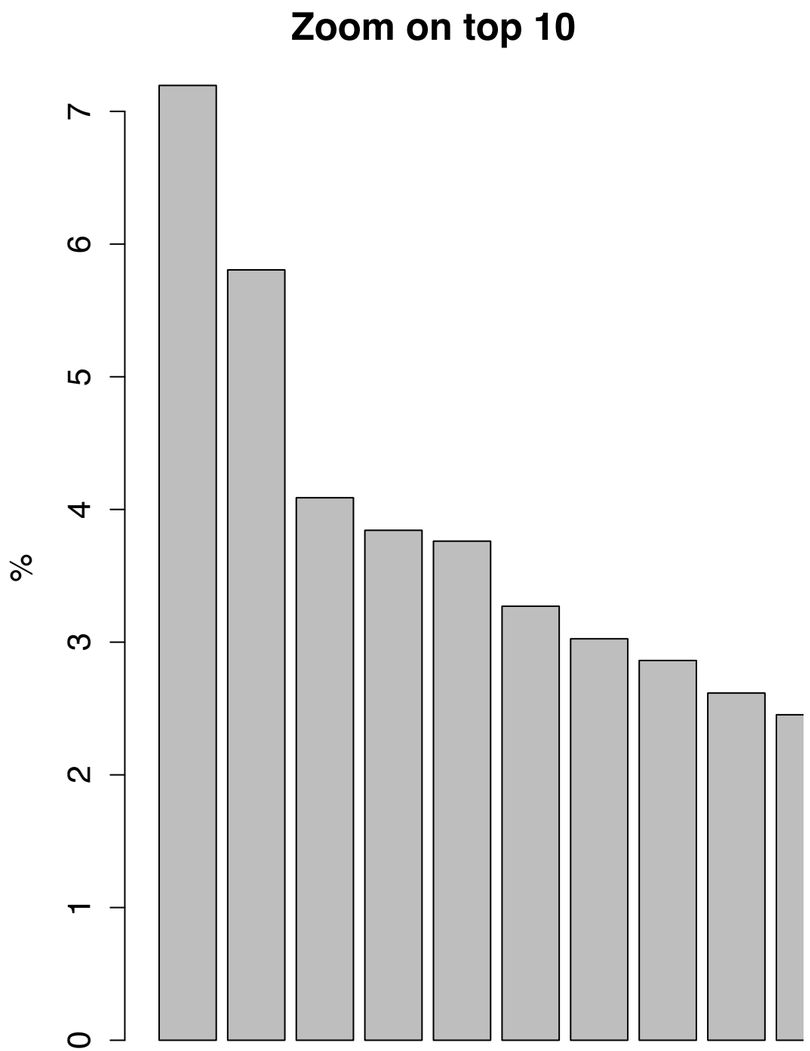
Alert Signatures (example)

name	count
Root disk space	88
redis-queue	71
Zombies	50
Total Processes	47
dispatcher	37
pgsql backends	35
cassandra JVM Heap	32
SSH	30

Naive: alert headers

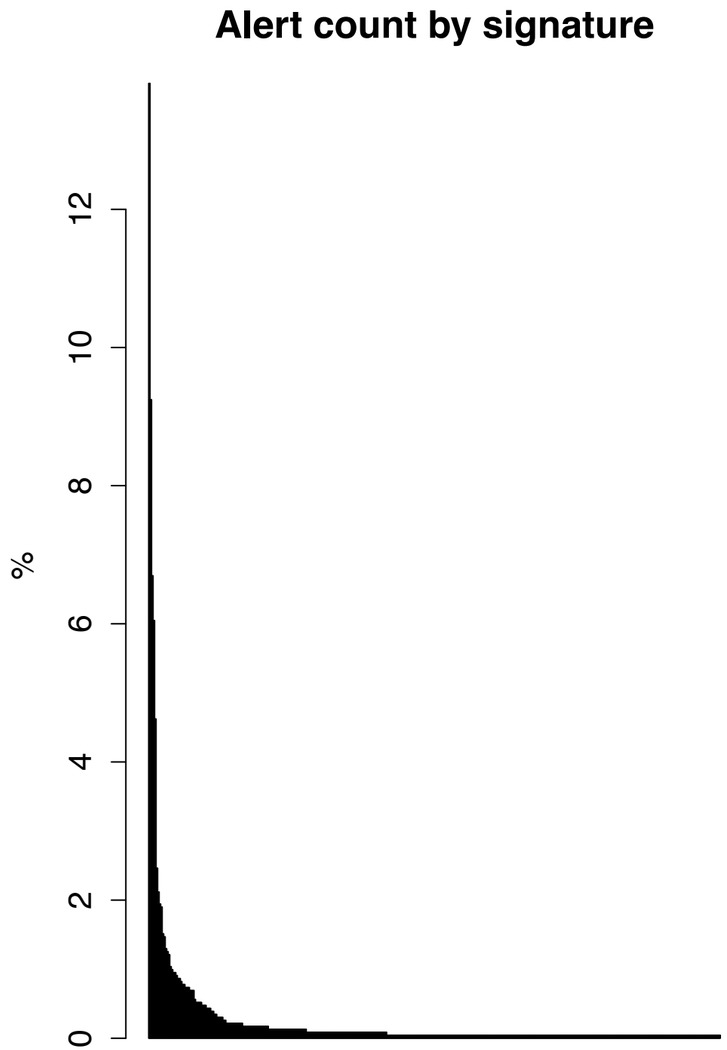
Case 1: Top 5 = 25% in volume

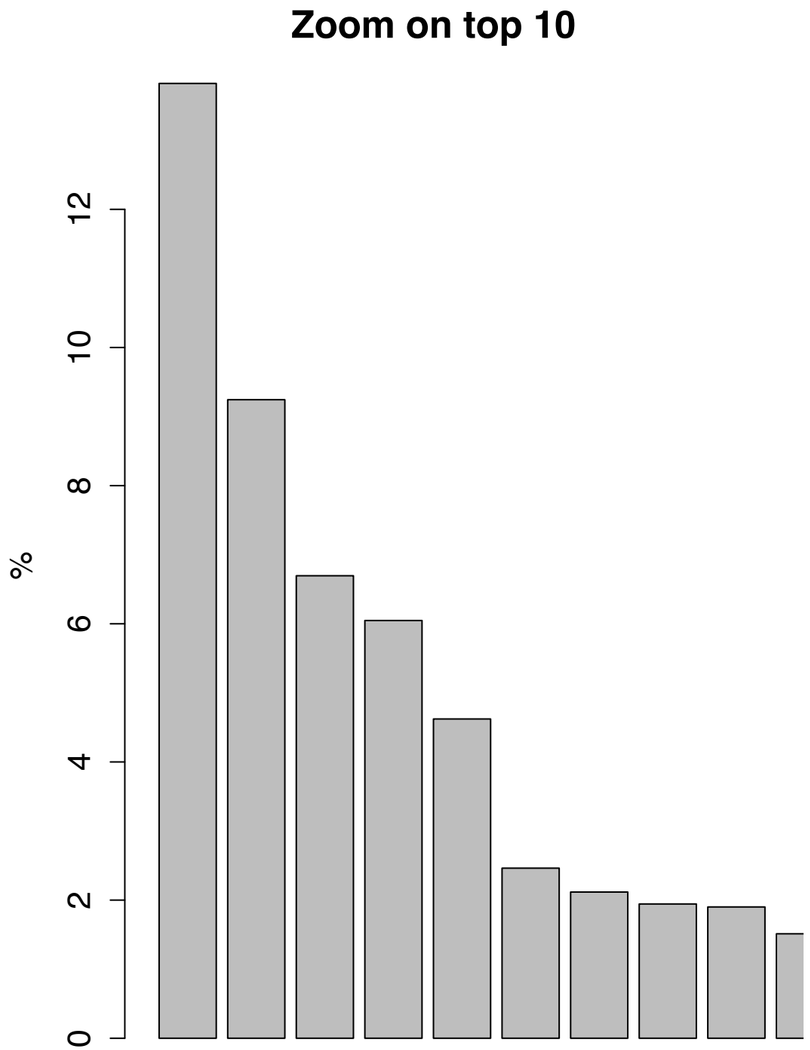




Sample size:
1123 alerts
6 months

Case 2: Top 5 = 38% in volume

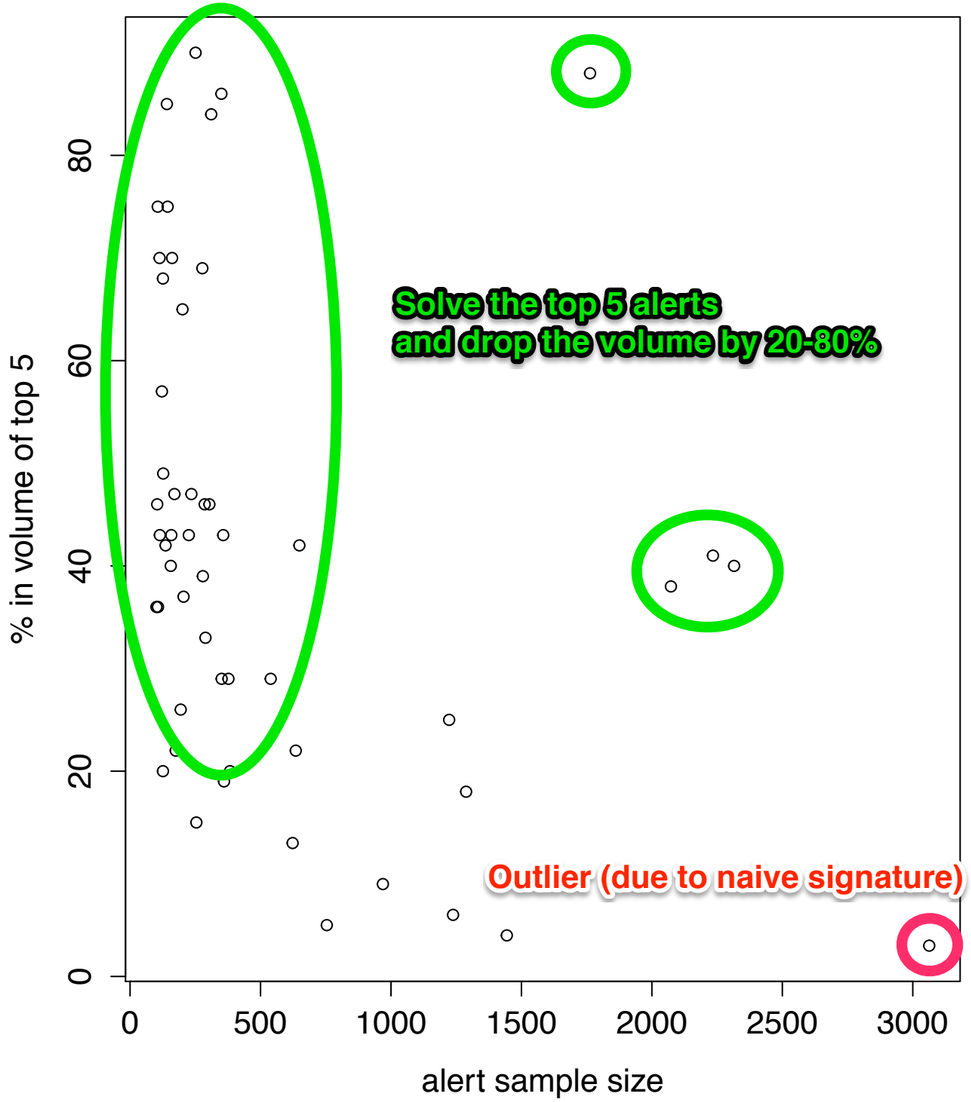


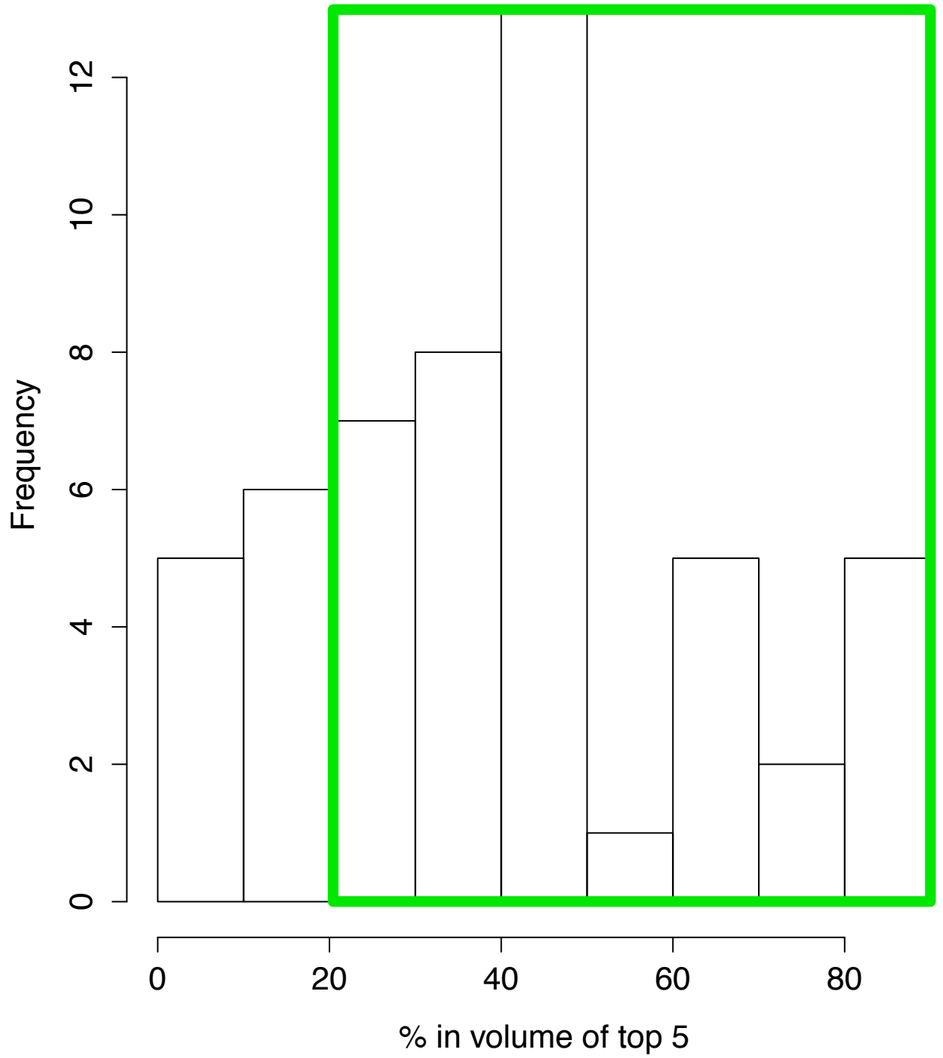


Sample size:
2324 alerts
6 months

Top 5 over 103 alert streams

Min. 100 alerts per stream

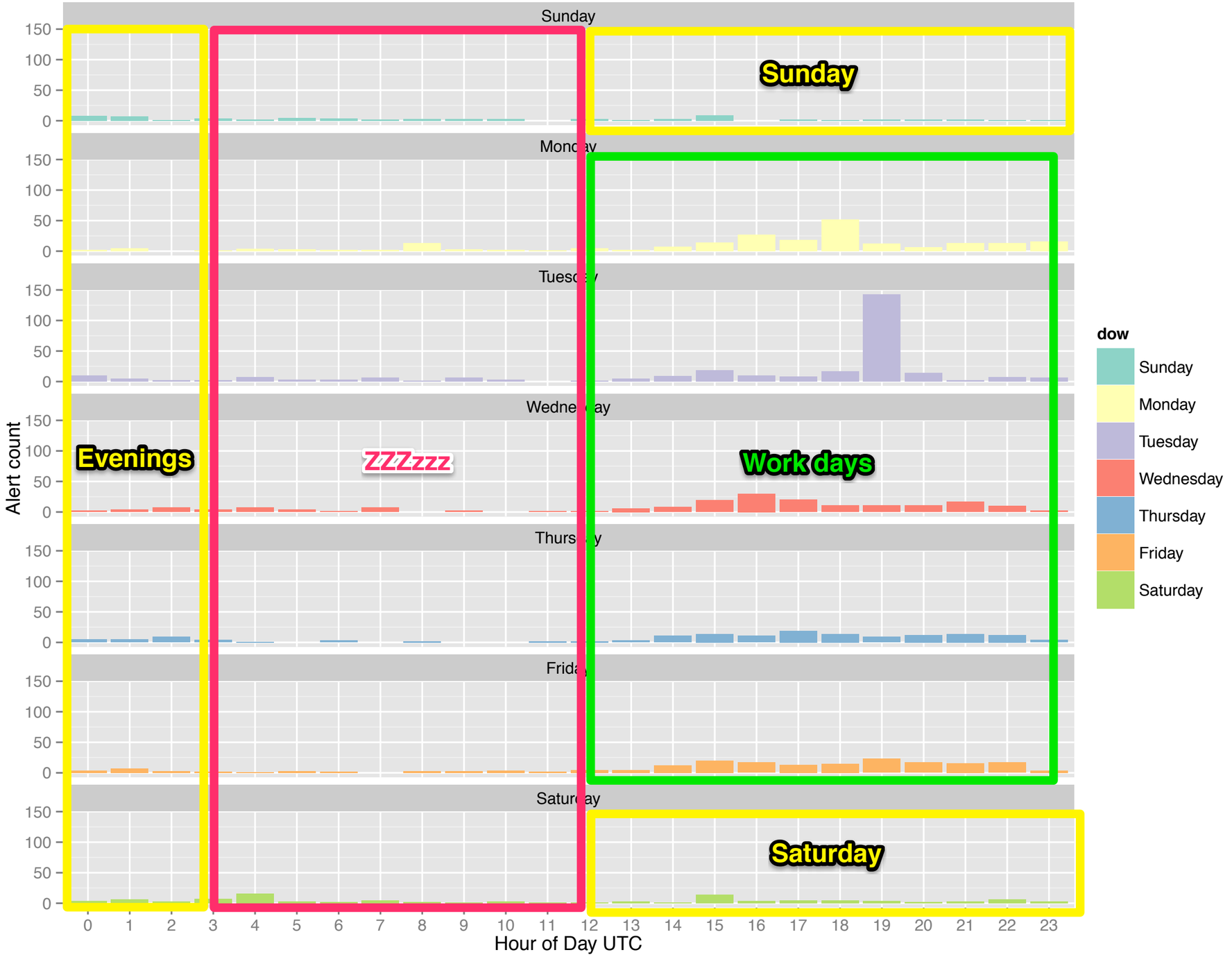




“Odd hours”

Steps

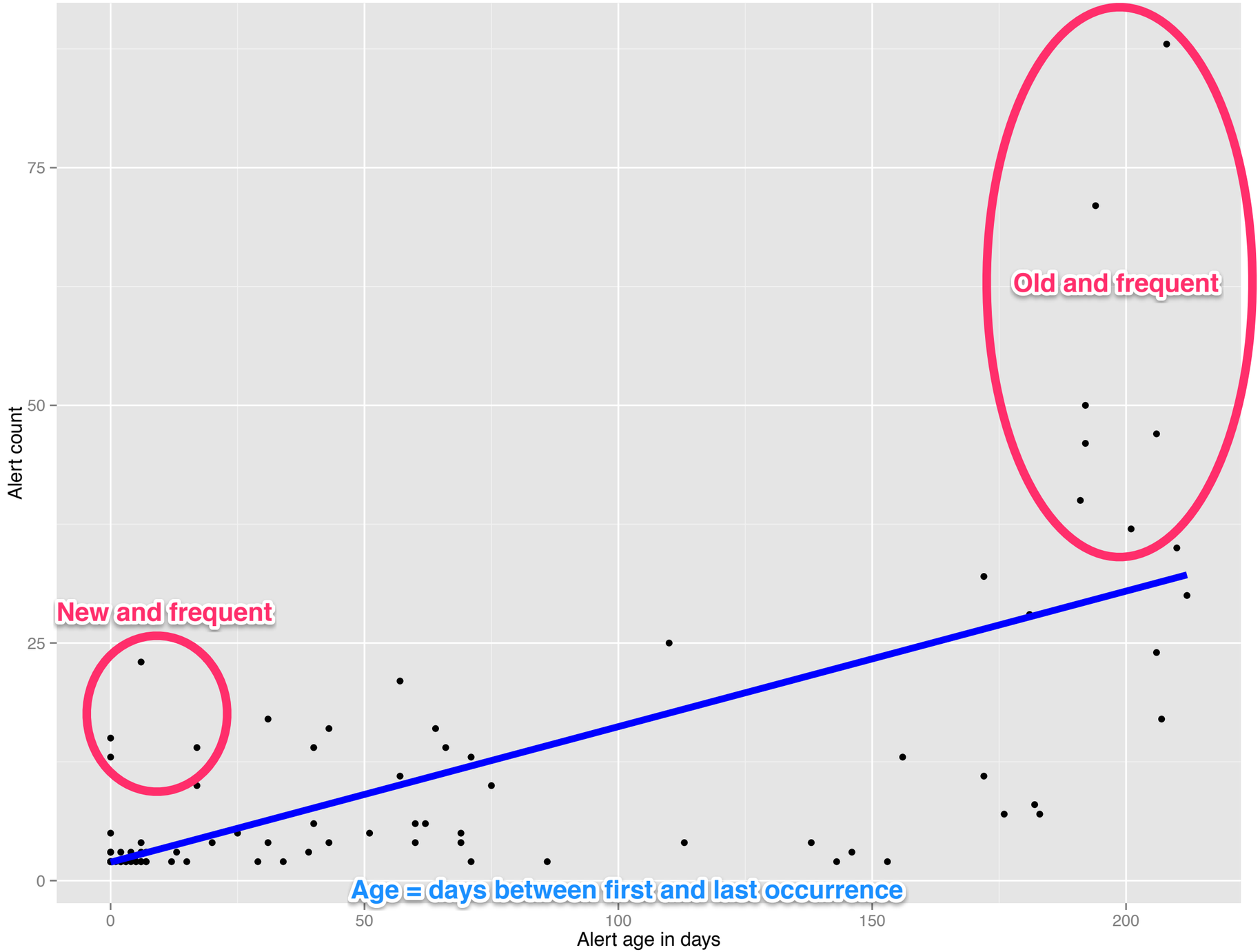
- Group alert stream by signature,
- ... day of week, hour of day
- Graph

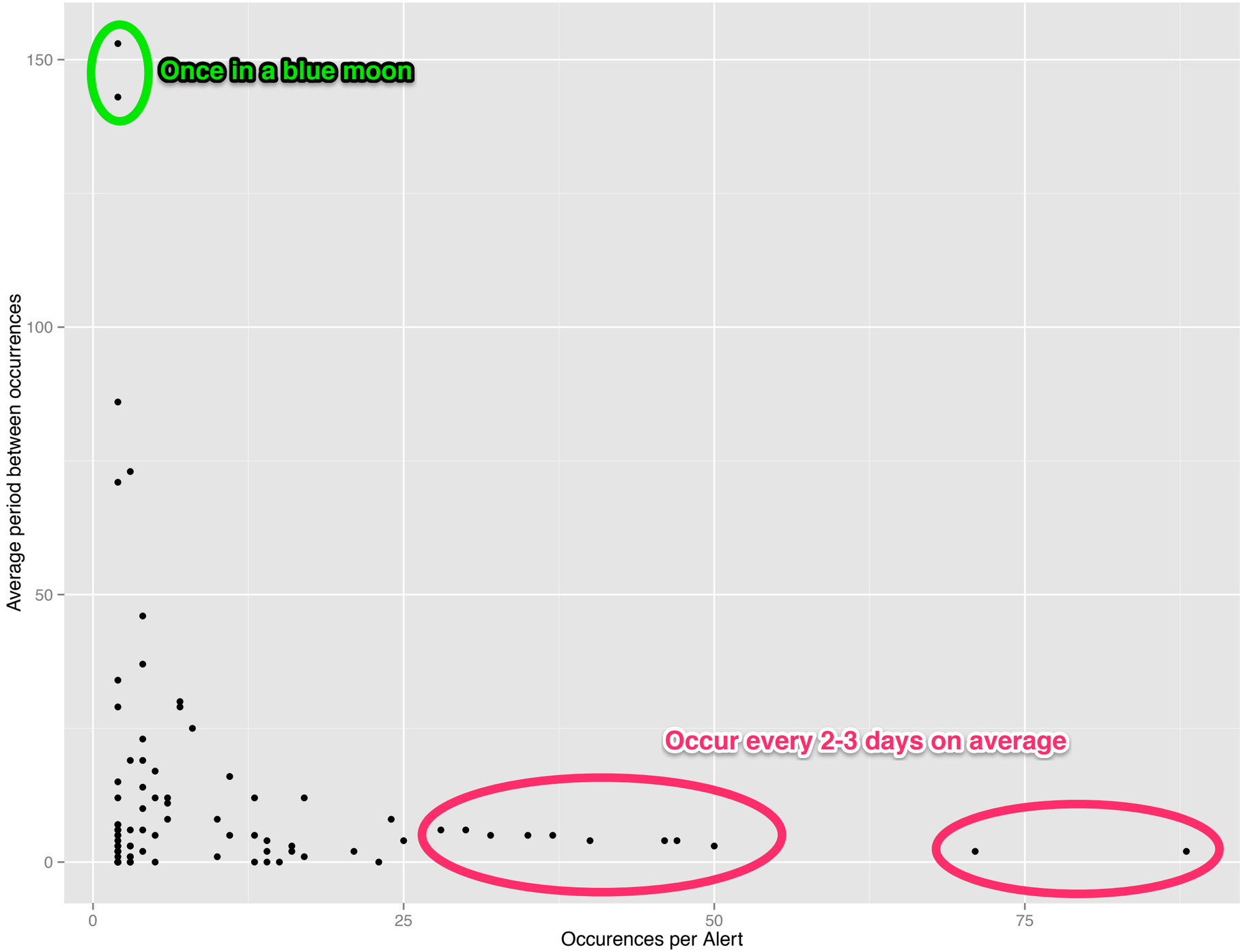

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Alert count
Hour of Day UTC
Sunday
Evenings
ZZZzzz
Work days
Saturday
dow

“Too frequently”

Steps

- Group alerts by signature
- Measure time elapsed between first and last occurrence & average/%-ile time elapsed between occurrences
- Graph


Old and frequent
New and frequent
Age = days between first and last occurrence
Alert count
75
50
25
0
0
50
100
150
200
Alert age in days


Once in a blue moon
Occur every 2-3 days on average
Average period between occurrences
150
100
50
0
0
25
50
75
Occurences per Alert

“too frequently”
“odd hours”
“always the same”


“too f
“
“ same”
Quantified

Concrete steps

Measure your alerts

1. Collect
2. Massage
3. Visualize
4. Learn

Collect your alerts

- From PagerDuty (OpsGenie, Nagios, etc.)
- Import with Python (pygerduty)
- Store in PostgreSQL

Massage your alerts

- Use any of
  - SQL (windowing functions)
  - R (reshape)
  - Python (pandas)

Visualize

- R (or d3.js, excel, etc.)
- Key is quick feedback

Slides, Code & Data

https://github.com/alq666/velocity-ny-2013

Enjoyed it? Hated it? Don’t care?

Let me know **@alq**