

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



DATA DOG

See it all in one place

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

The screenshot displays the DataDog web interface. On the left, there's a sidebar with a red circle highlighting the 'ALERTS' section, which contains a list of critical events like 'Cassandra series dialtone is critical on i-44bb122b'. Below this is the 'CUSTOM METRICS' section. In the center, there are several monitoring dashboards showing time-series data for metrics such as 'Pingdom response times (ms)', 'Points processed per second, by host', 'Average worker wait, by host', 'Postgres rows fetched / returned', 'Disk latency (ms, by device)', and 'Postgres load averages 1-5-15'. A yellow button at the bottom center says 'SIGN UP FOR FREE'. Surrounding the interface are various hand-drawn style callouts representing different integration points: 'CLOUD HOSTING', 'CODE CHANGES', 'ON-PREMISE SERVERS', 'CDN', 'CONFIG. MANAGEMENT', 'ISSUE TRACKING', 'PERFORMANCE MONITORING', and 'USAGE ANALYTICS'.



Pain

A man with short brown hair wearing dark sunglasses and a leather jacket is looking upwards and slightly to his right. He is holding a large, futuristic-looking handgun with both hands, pointing it towards the bottom left of the frame. Red laser beams radiate outwards from behind him, creating a starburst effect against a black background.

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

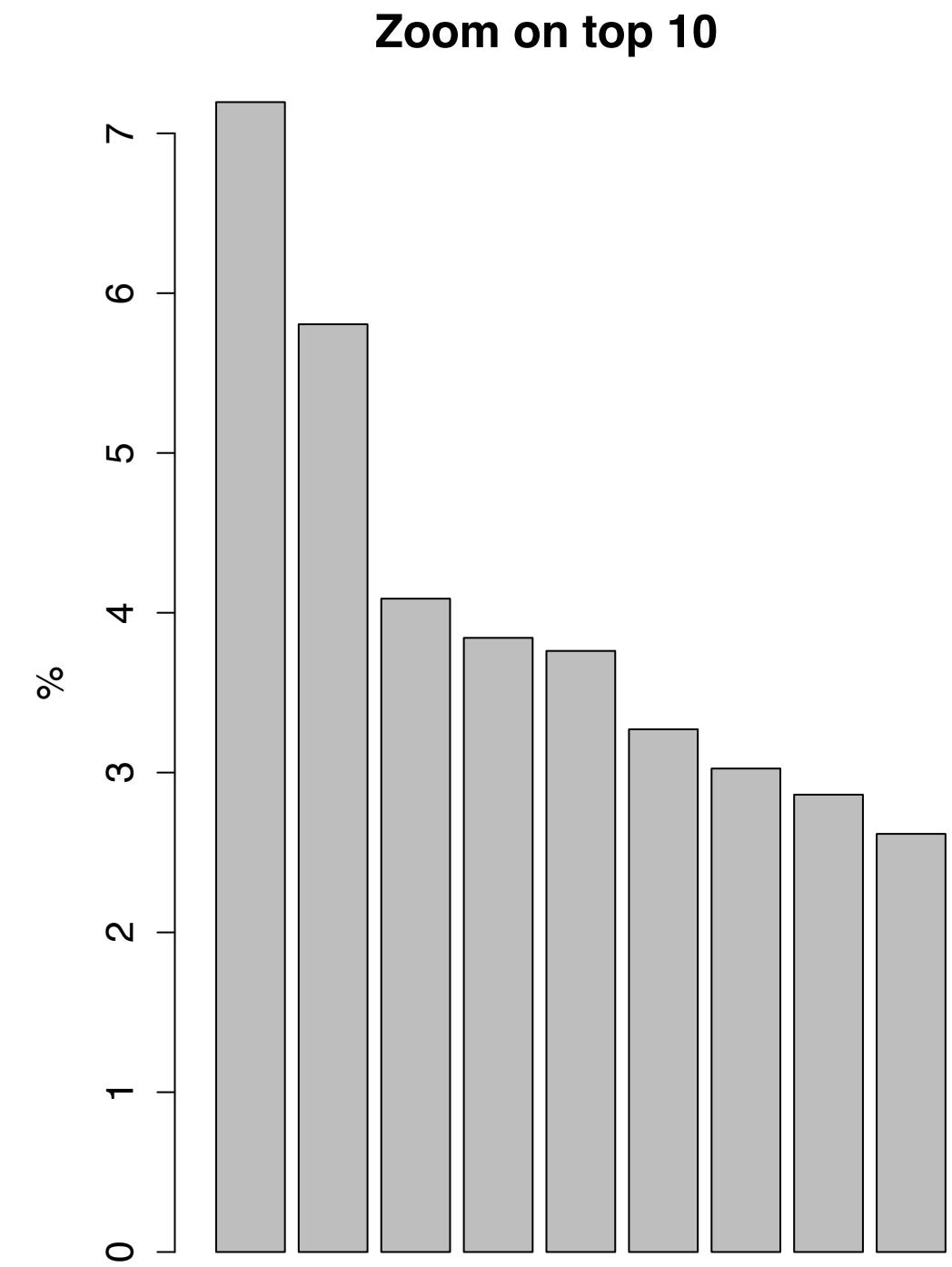
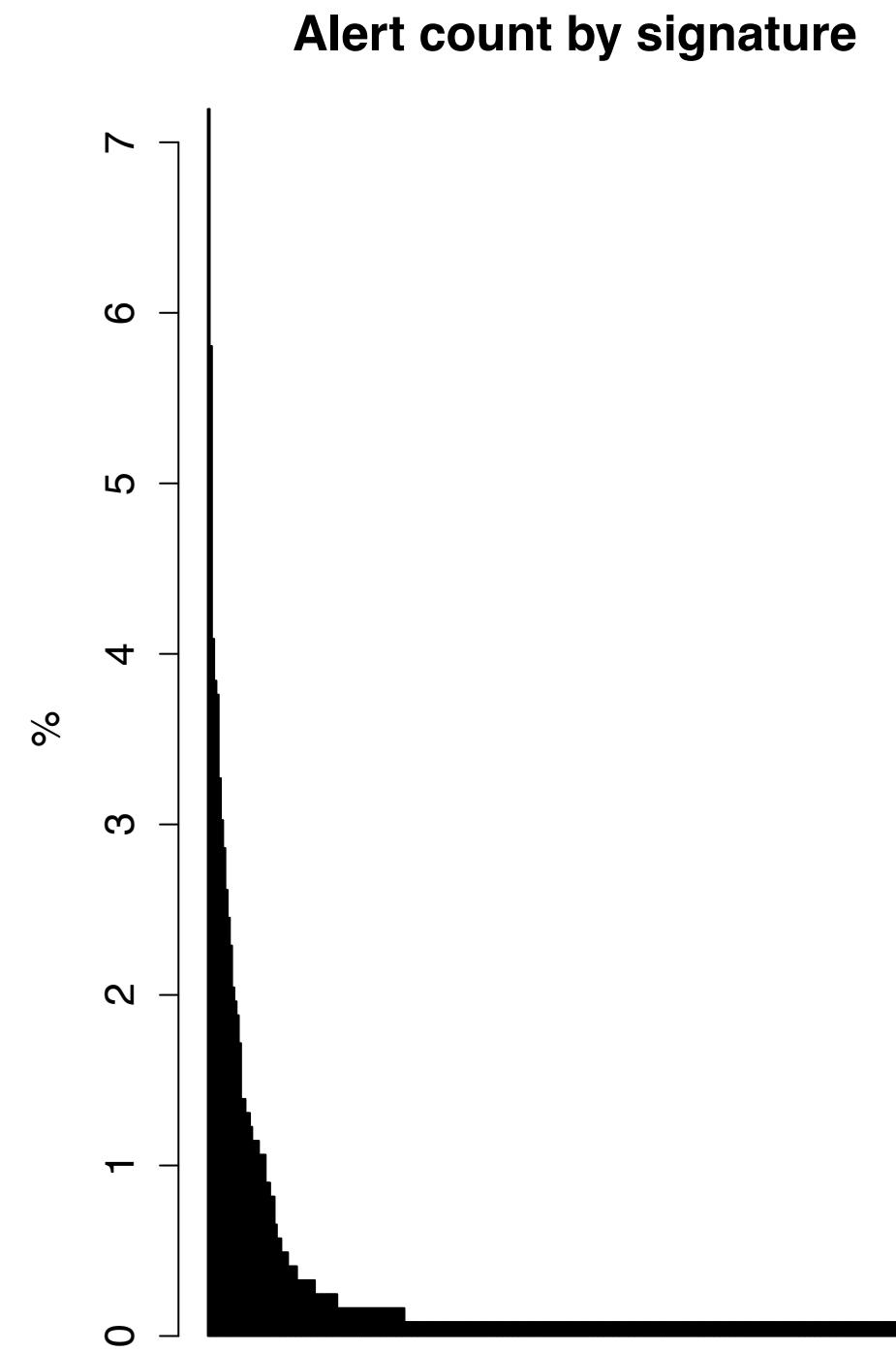
Alert Signatures (example)

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

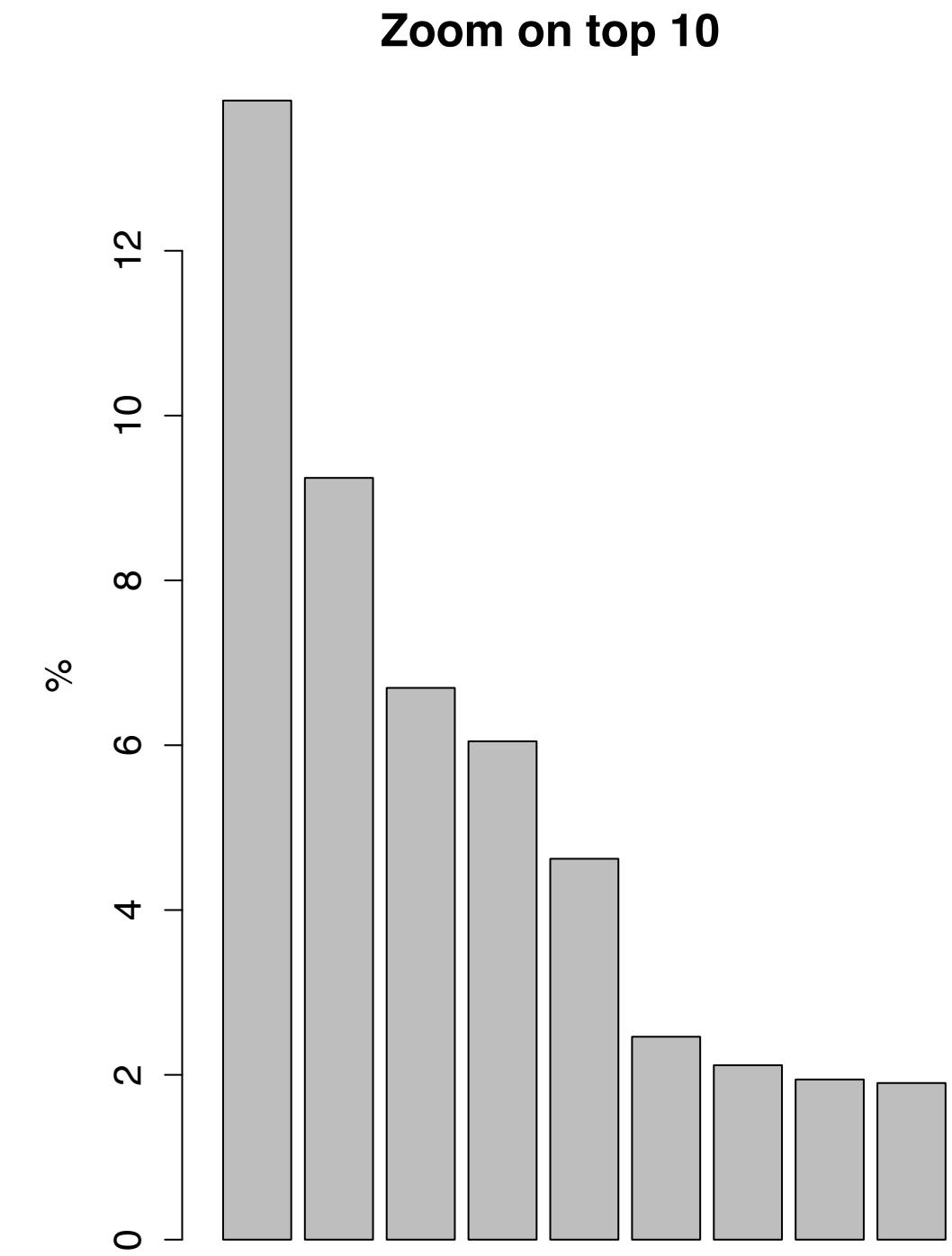
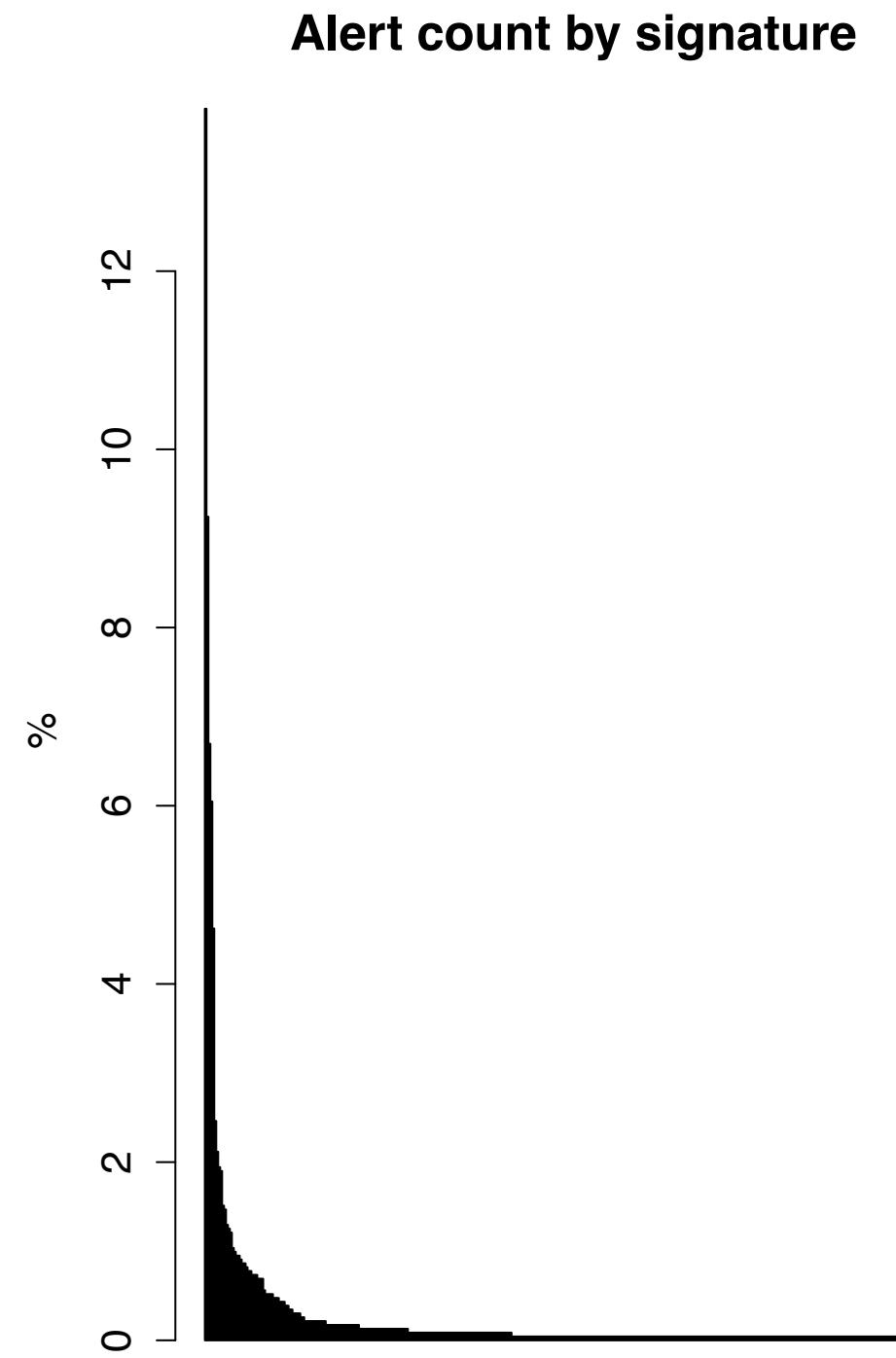
Case I: Top 5 = 25% in volume

Sample size:
1123 alerts
6 months



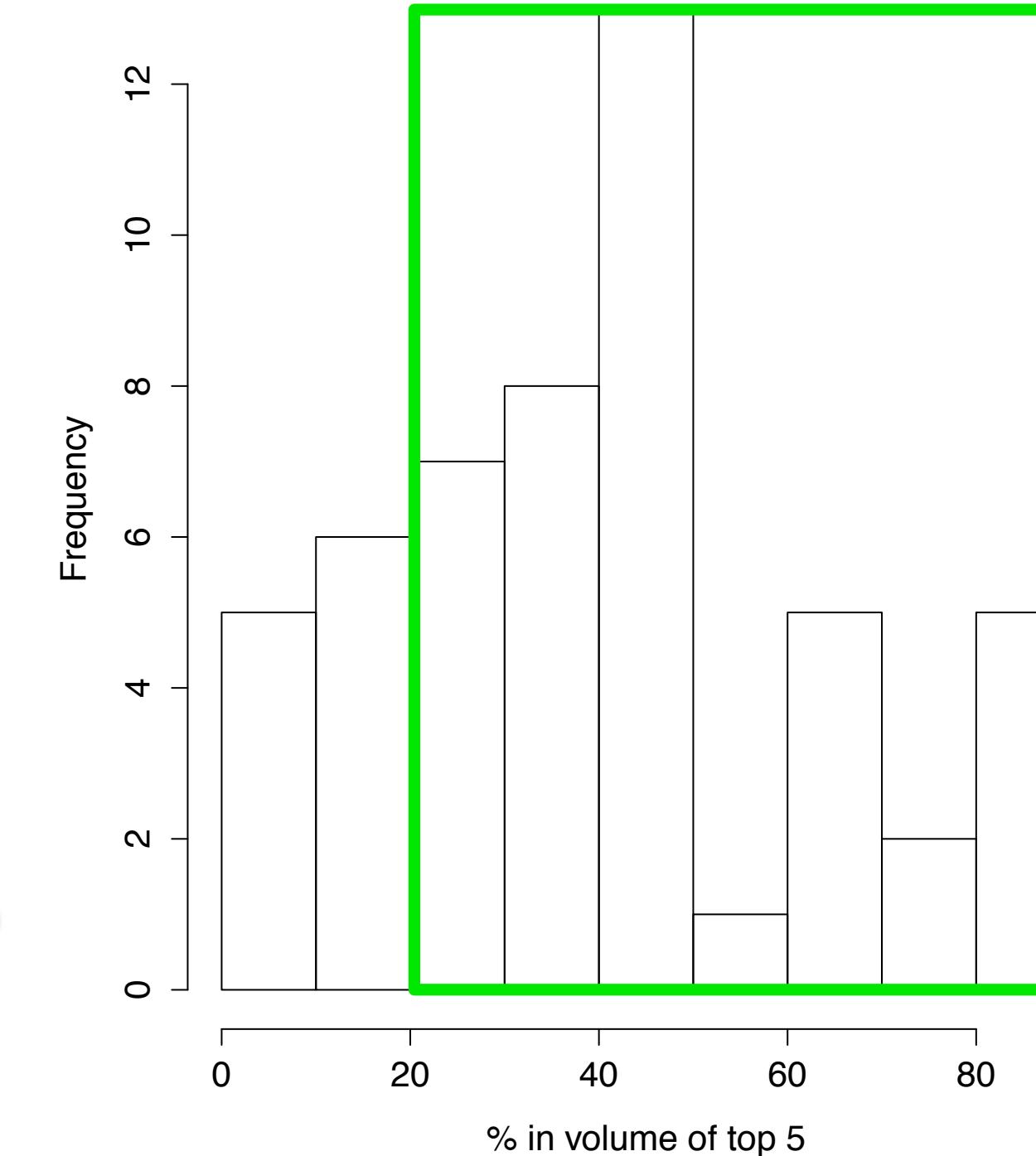
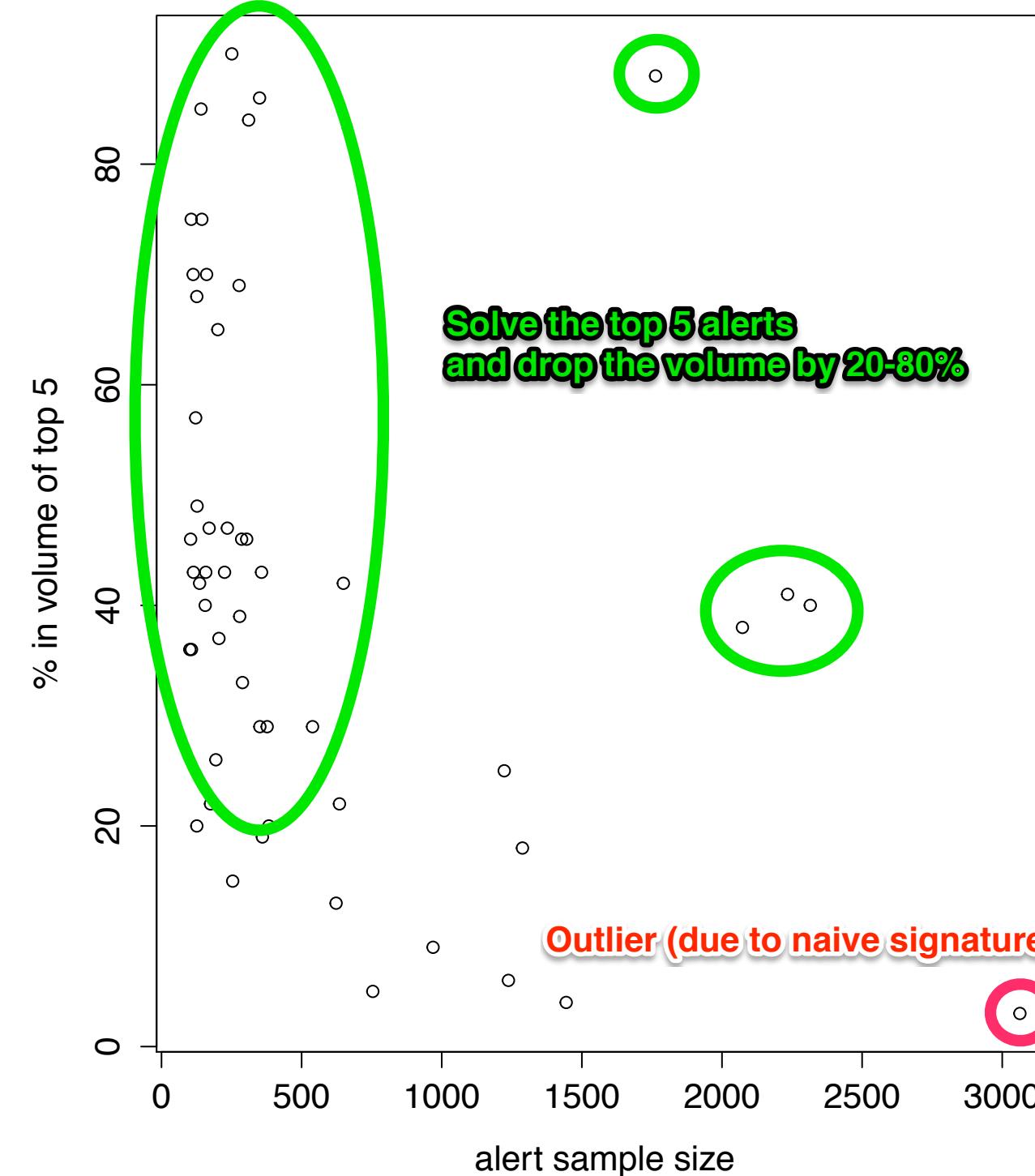
Case 2: Top 5 = 38% in volume

Sample size:
2324 alerts
6 months



Top 5 over 103 alert streams

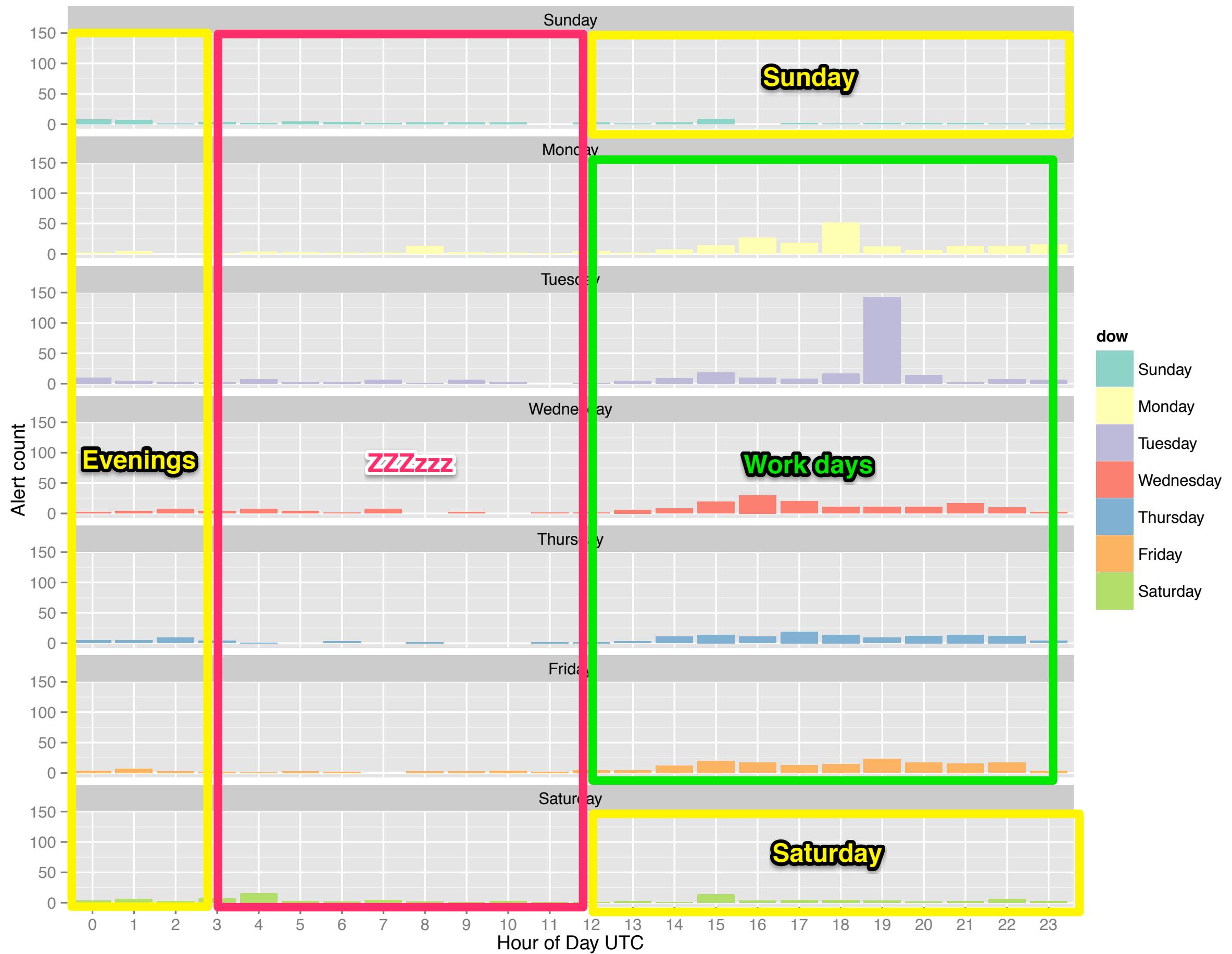
Min. 100 alerts per stream



“Odd hours”

Steps

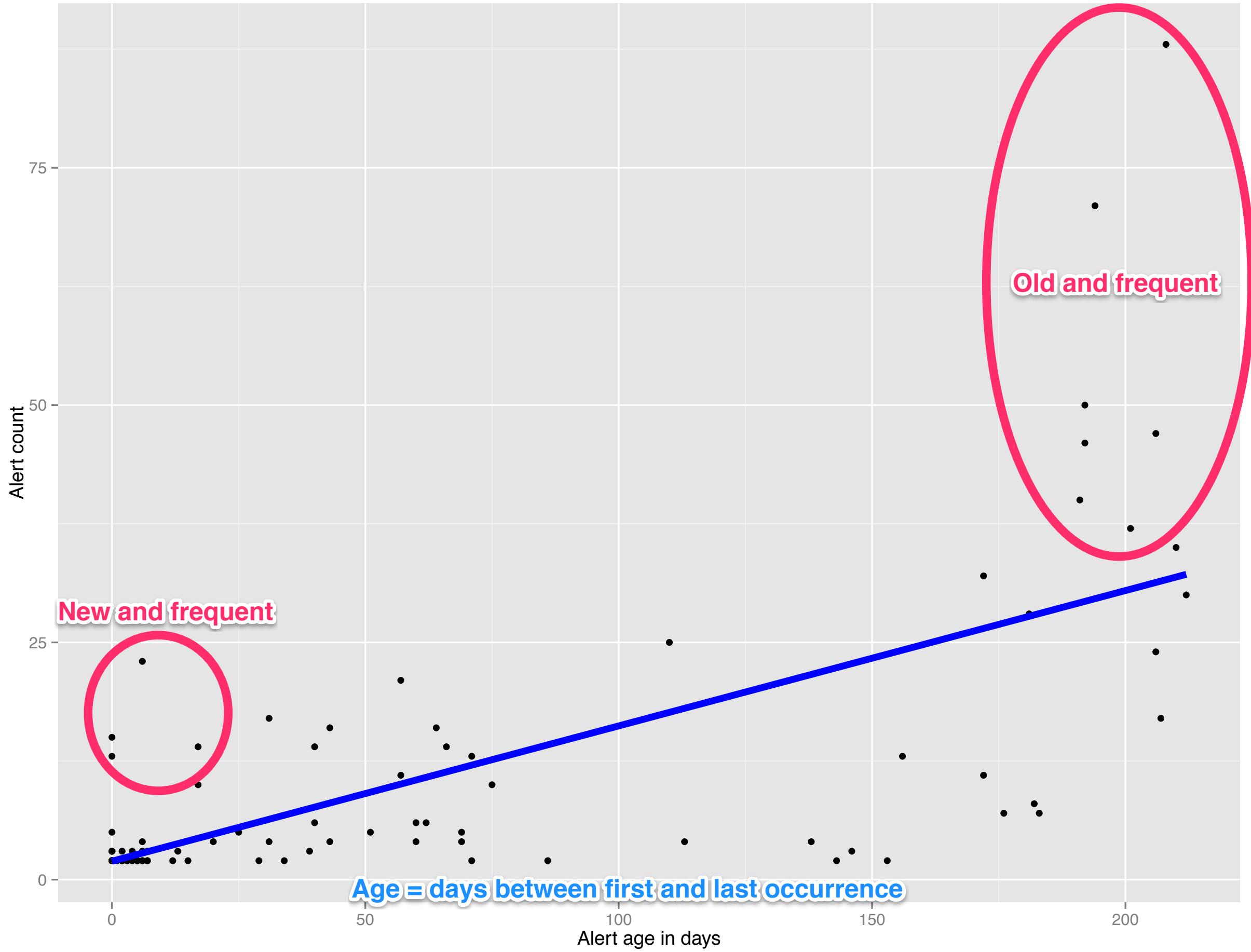
- Group alert stream by signature,
● ... day of week, hour of day
- Graph

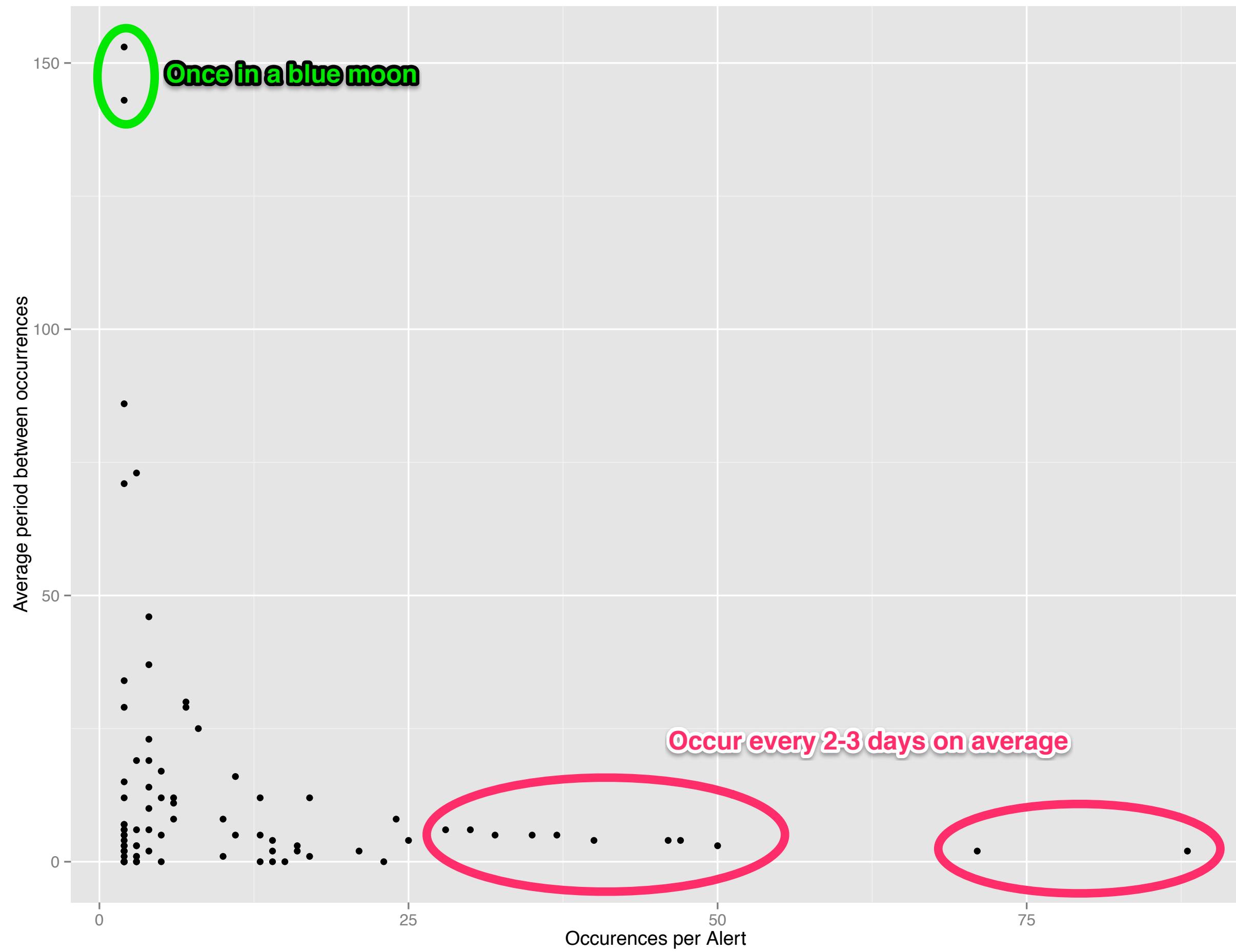


“Too frequently”

Steps

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





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

Quantified

“**too much**”

“**same**”

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