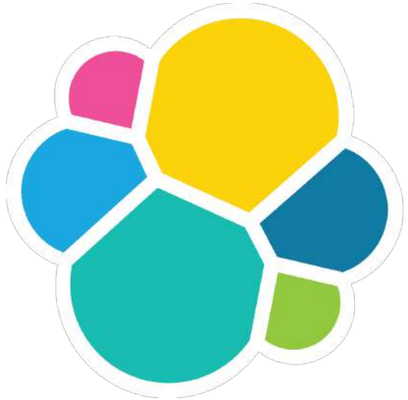
Observability is More than Logs, Metrics & Traces

Philipp Krenn @xeraa



elastic

Developer 🥑

Who is using logs?

Print what happened for each occurence — component level

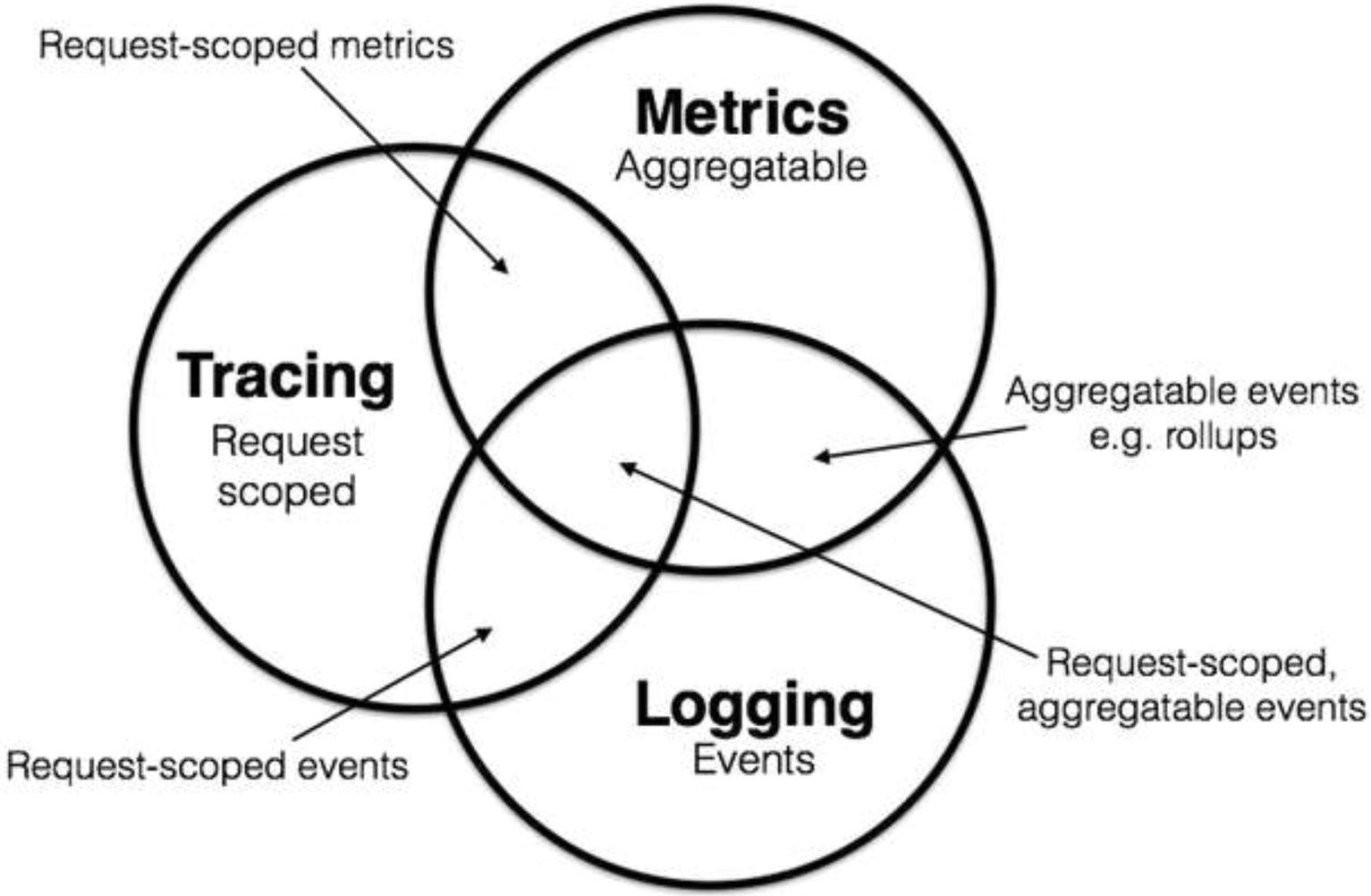
Who is using metrics?

Periodic measurement of some value(s) — aggregateable

Who is using APM / tracing?

(Distributed) traces record activity per request — application level

What is observability?



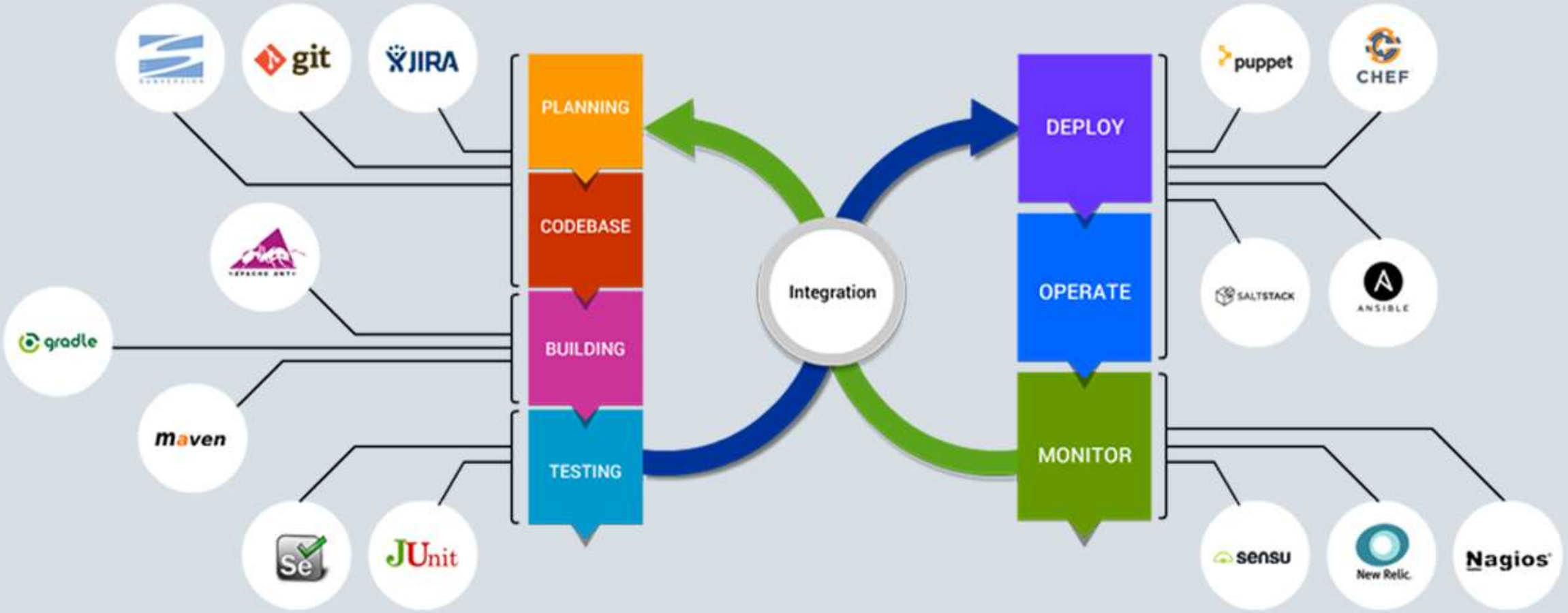
https://peter.bourgon.org/blog/2017/02/21/metrics-tracing-and-logging.html

[...] this seems like calling "gasoline, motor oil, and tires" the three pillars of F1 racing. It's not wrong, precisely, but ...

— **https://twitter.com/fuzzychef/status/1186403652124069888**

We've seen this before

DevOps Tools

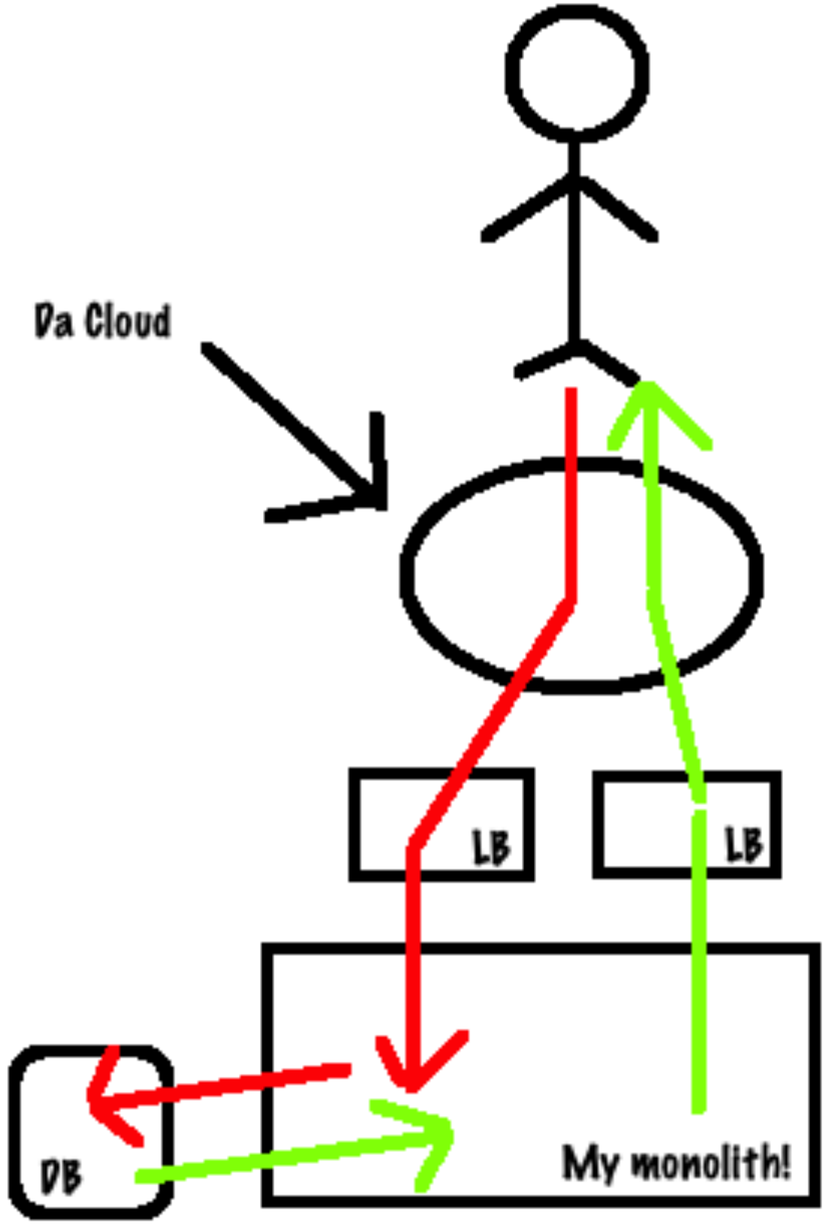


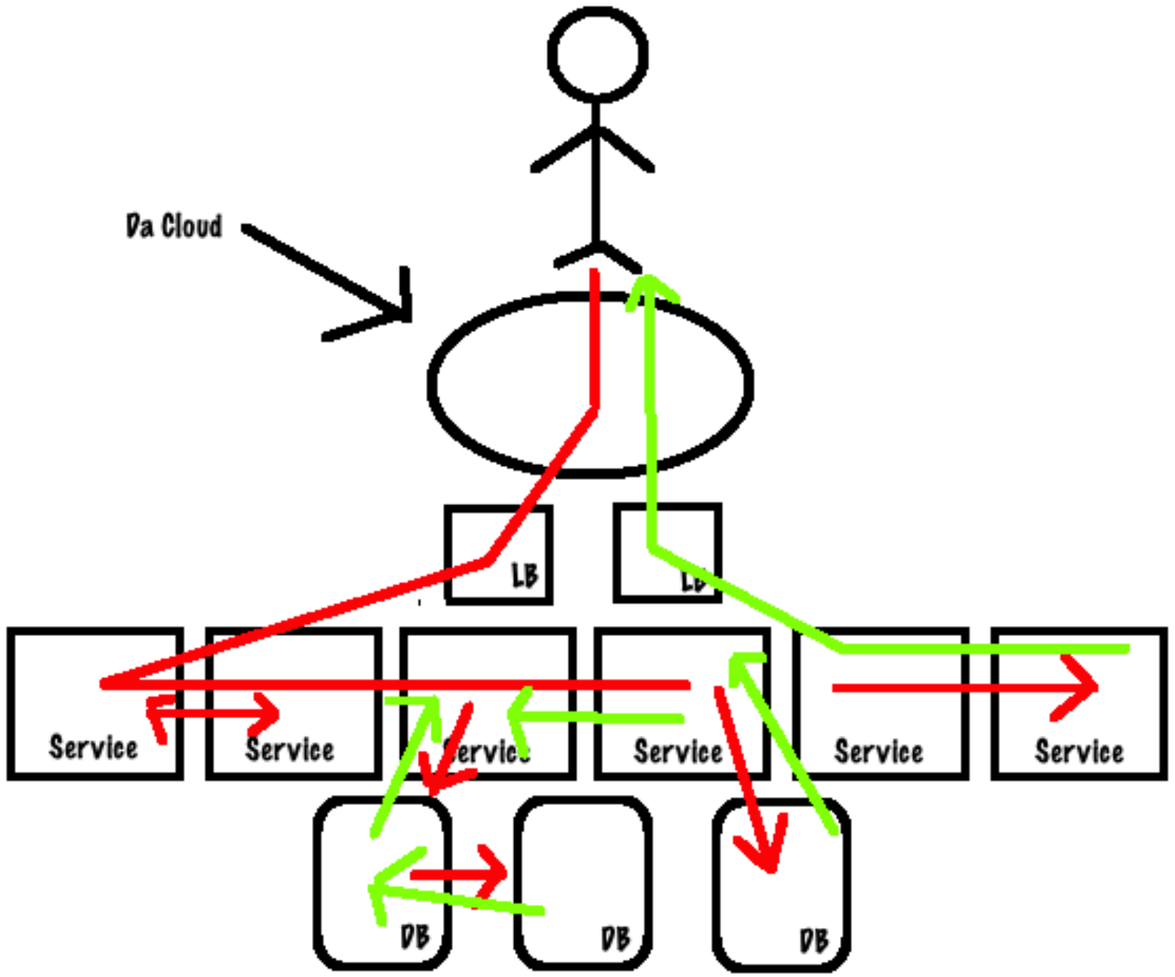
Pets vs Cattle

From **Static Monolithic Architectures**
to **Elastic Microservice Architectures**

Simpler Times

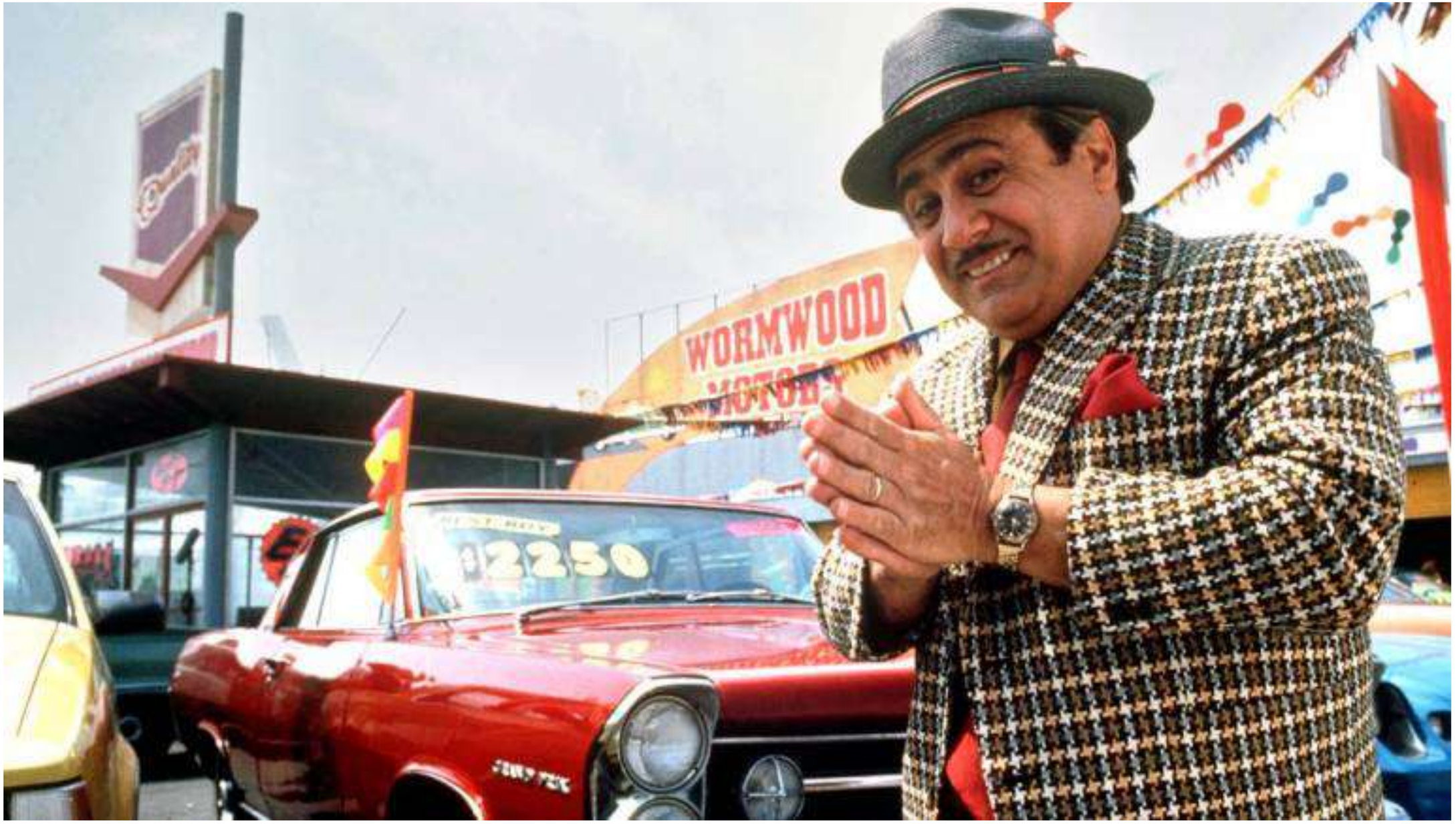
https://www.kartar.net/2019/07/intro-to-distributed-tracing/





Better Times for Vendors

https://www.kartar.net/2019/07/intro-to-distributed-tracing/


WORMWOOD


TOOLS
LIGHTYEAR
TOOLS EVERYWHERE
imgflip.com

DevOps: tools, jobs, departments,...

The average System Engineer salary in the US is $100K, but the salary range typically falls between $89K and $110K.

https://www.salary.com/research/salary/listing/system-engineer-salary

The average DevOps Engineer salary in the US is $119K, but the salary range typically falls between $107K and $132K.

https://www.salary.com/research/salary/listing/devops-engineer-salary


WE SHOULD DO DEVOPS
imgflip.com


WE SHOULD DO OBSERVABILITY
imgflip.com

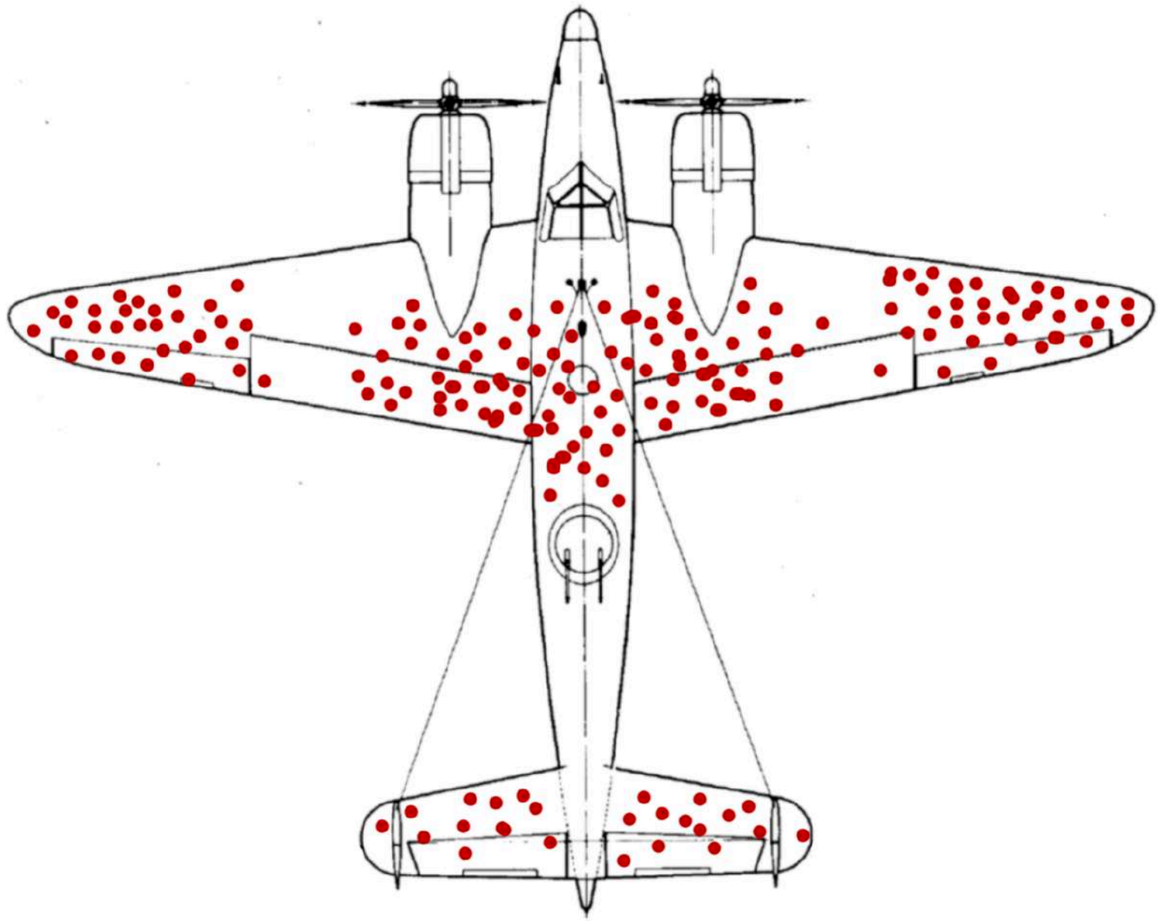
THE MONITOR

So what *is* observability?

A system is observable if the behaviour of the entire system can be determined by only looking at its inputs and outputs.

— Kálmán (1961), On the General Theory of Control Systems

	Knowns	Unknowns
Known	👁️ 🧠 Things we are aware of and understand	👁️ Things we are aware of but **do not** understand
Unknown	🧠 Things we **are not** aware of but understand	Things we **are not** aware of and **do not** understand



https://
de.wikipedia.org/wiki/
Survivorship_Bias

elastic

Exposing state and answer:

What is the status of my system?

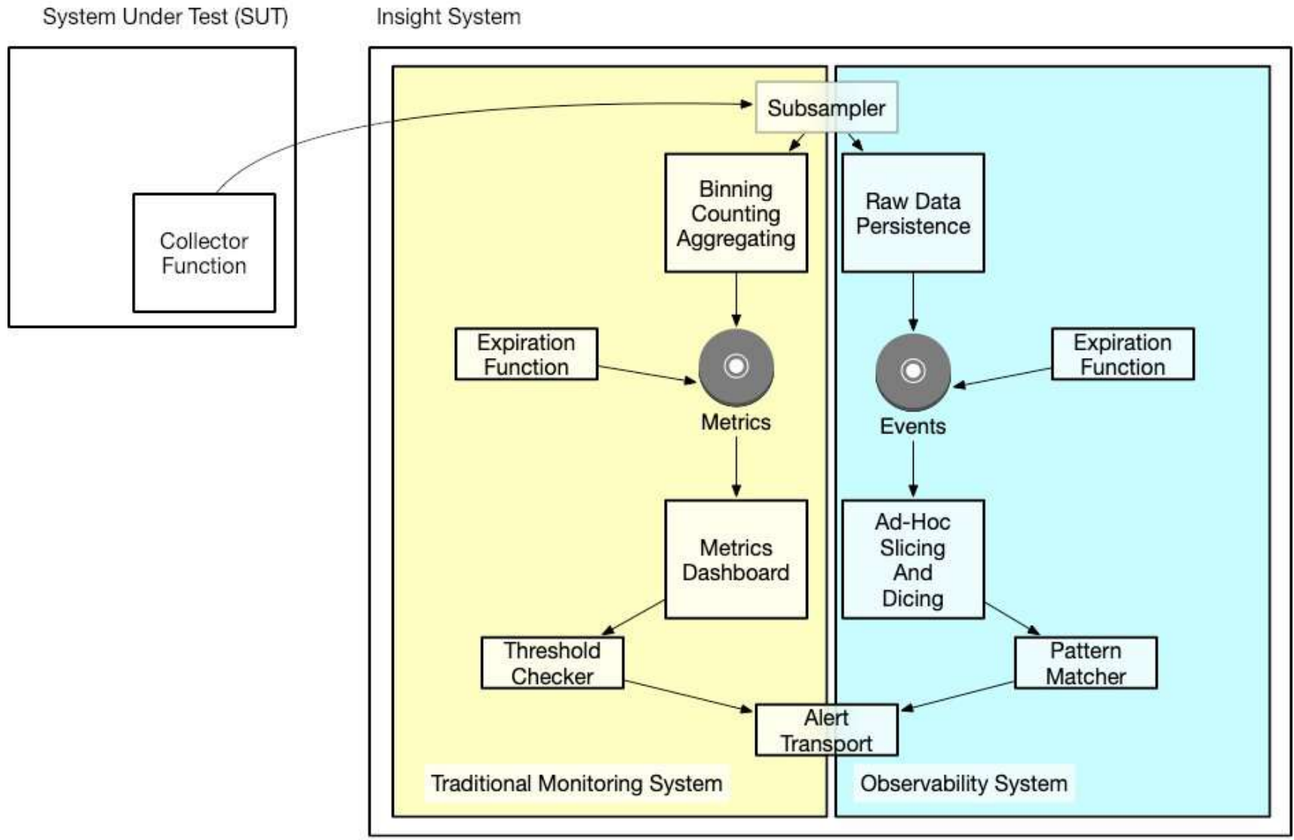
What is not working?

Why is it not working?

Monitoring is your bank telling you you're overdrawn. Observability is the ability to tell you're running out of money because you're spending too much money on chocolates, cakes and sweets because you've recorded data on what you spent your money on throughout the month.

— **https://twitter.com/lizthegrey/status/1230979460708499456**

https://twitter.com/isotopp/status/1329087330888470535



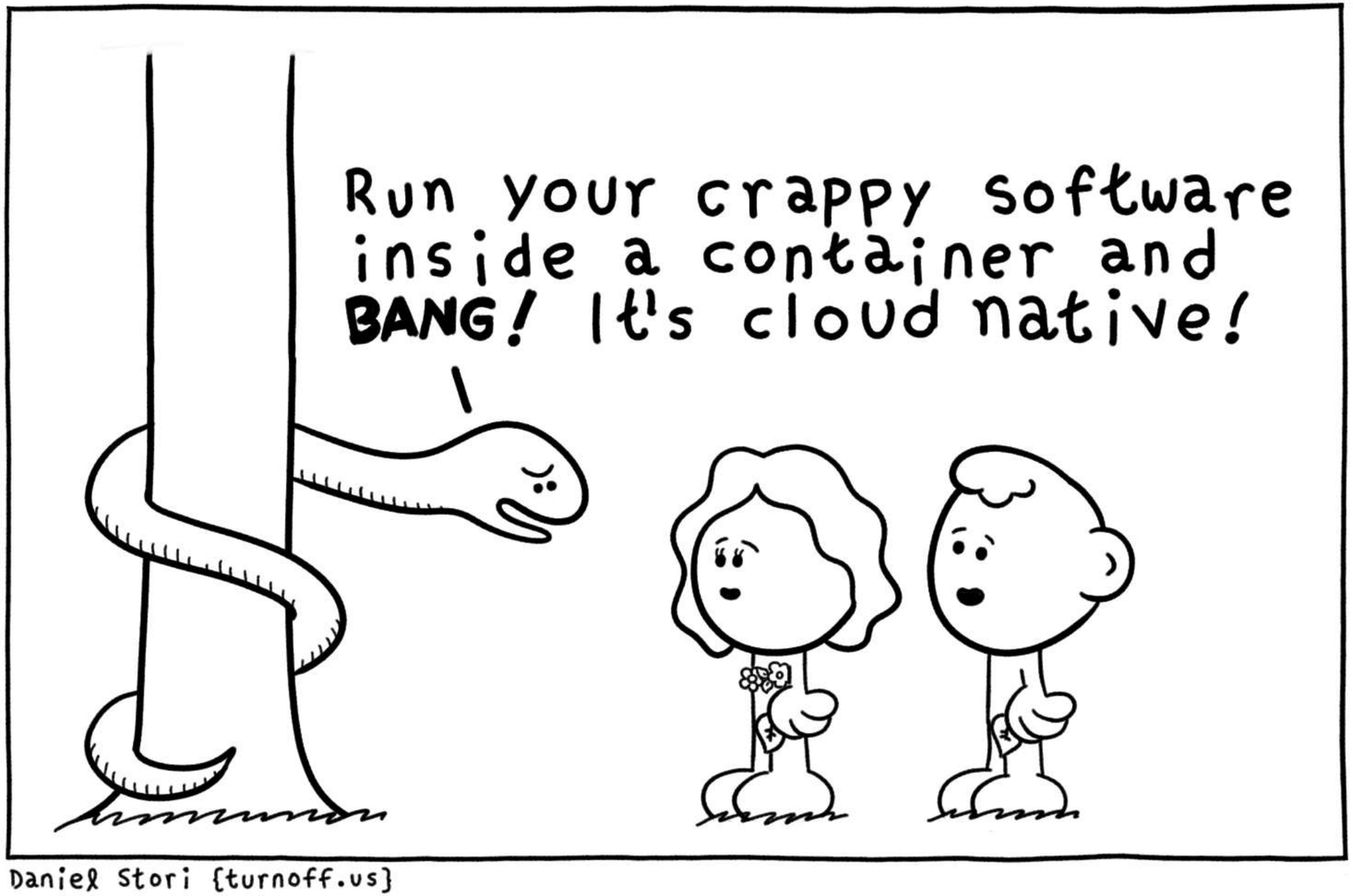
Monitoring:
- Collects numeric metrics
- Aggregates

Used to:
- Validate normal operations (“known known”)
- Detect undesirable system states
- Pinpoint incidents in time and space (interval and components involved)

O11y:
- Non-numeric data
- Non-aggregated data
- Context rich information (“Events”)

Used to:
- Find root causes
- Validate hypotheses on defect causality
- Inspect internal system state

- Record (partial) system state snapshots



Monitoring Vendors

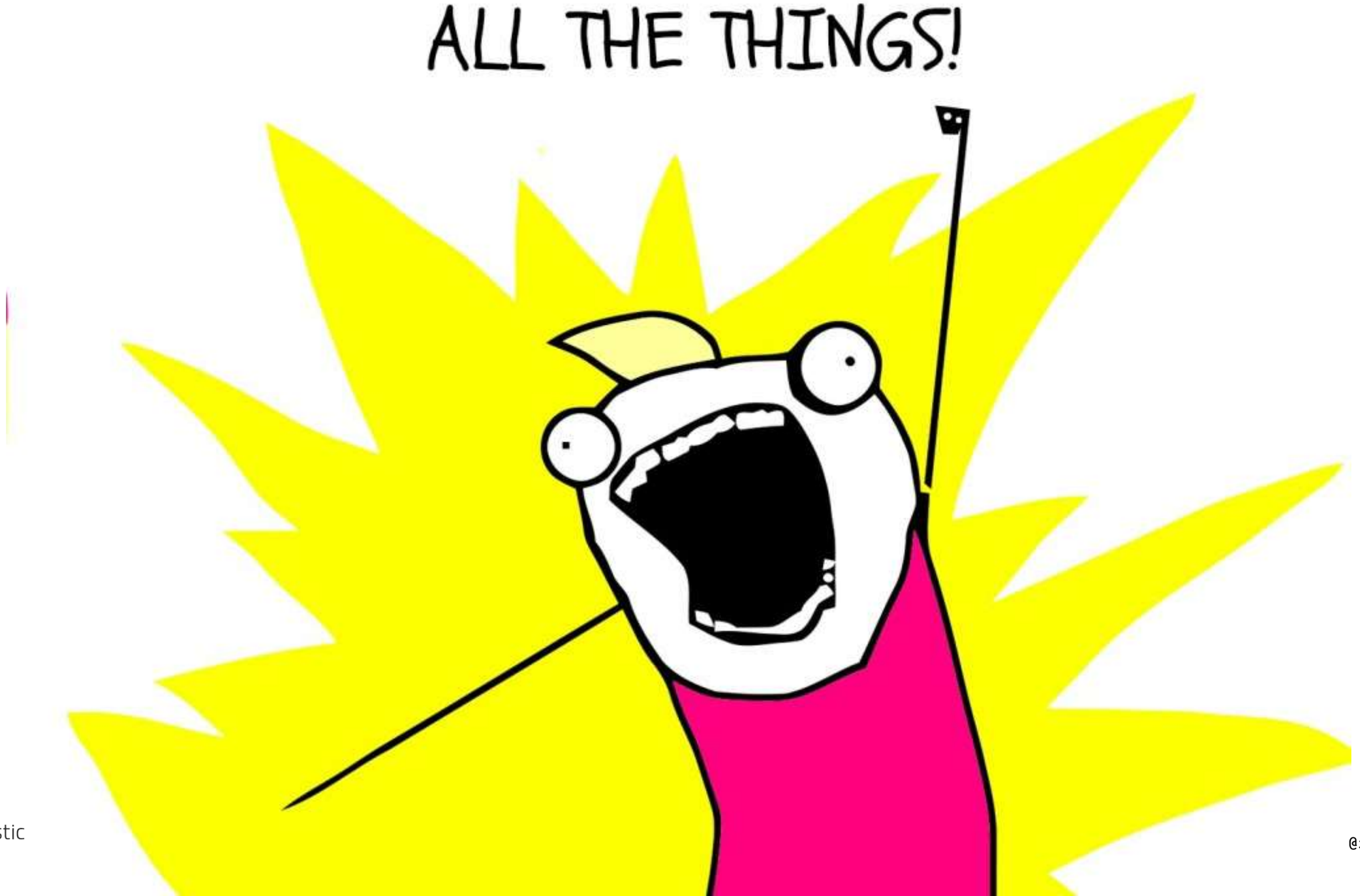
Instrumentation

Understand without shipping new code

Know your system

Trying to summarize a few things I've heard:
Trying to learn how to keep your system healthy by only studying its failures is like trying to learn how to keep your marriage healthy by only studying divorces.

— **https://twitter.com/relix42/status/1199871657696849921**


ALL THE THINGS!

Not all signals are equal

👍 Working log in, successful transaction, performant search, consistent shopping cart

👎 API uptime, error rates, DB query latency

Service Level

Indicator (SLI) — eg. uptime

Objective (SLO) — eg. 99%

Agreement (SLA) — eg. <99% uptime you owe me 

Every time I hear someone say they need five 9's of uptime, I think of GitHub. Everybody relies on them, they have maybe 99.9% uptime, and they got bought for $7.5B by Microsoft. Unless you're making pacemakers, ease up on your crazy uptime requirements.

– **https://twitter.com/benbjohnson/status/1232351432105324544**

You cannot buy observability

Example: From log...


```
{
  "@timestamp":"2020-09-27T19:36:16.872Z",
  "log.level": "WARN",
  "message":"[philipp] failed to log in with password [***]",
  "service.name":"gs-securing-web",
  "process.thread.name":"http-nio-8080-exec-5",
  "log.logger":"hello.AuthenticationEventListener"
}
```

Example: ...to event


```
{
  "@timestamp":"2020-09-27T19:36:16.872Z",
  "log.level": "WARN",
  "message":"[philipp] failed to log in with password [***]",
  "service.name":"gs-securing-web",
  "process.thread.name":"http-nio-8080-exec-5",
  "log.logger":"hello.AuthenticationEventListener",
  "labels.event.category": "LOGIN_FAILURE",
  "labels.user.name": "philipp",
  "labels.source.ip": "0:0:0:0:0:0:0:1",
  "labels.url.full": "/login"
}
```

Beyond logs, metrics & traces

(Synthetic) health checks

Security

Alerting

What is the goal?

Business value — always

REMEMBER M&E INFORMATION IS USEFUL ONLY IF IT IS USED!

Conclusion

Monitoring

Something you do to know *if* the system is not working

Observability

A property of a system to know *why* it is not working

Repeat after me:

You cannot buy DevOps or observability*

* Though I can totally sell it to you

Observability is More

than Logs, Metrics & Traces

Philipp Krenn @xeraa