AI / ML Won’t Save You

(In Ops)

Julien Goodwin
@laptop006 / jgoodwin@studio442.com.au

Twitter —
16th December

Sebastian Neuner
@neunerseb

Every ddos-detection vendor: "We have AI and machine learning algorithms that detect unwanted traffic patterns!" - Me: "This is the traffic graph for one of our transits and that's legitimate traffic." - Vendor: 😐

♡ 208 9:16 PM - Dec 16, 2019

Twitter — 16th December

Twitter — 16th December

Sebastian Neuner
@neunerseb

Every ddos-detection vendor: "We have AI and machine learning algorithms that detect unwanted traffic patterns!" - Me: "This is the traffic graph for one of our transits and that's legitimate traffic." - Vendor: 😐

♡ 208 9:16 PM - Dec 16, 2019 ⓘ

Julien Goodwin
@LapTop006

I've been tempted to write a "why ML/AI is largely useless in the ops space" talk for a conference, it's easy for me to comment on alerting & network type things, but I do wonder if there are some sensible uses.

♡ 18 2:39 AM - Dec 17, 2019 · Sydney, New South Wales ⓘ

Hi, I’m Julien

Hi, I’m Julien

… and I have opinions

Hi, I’m Julien

… and I have opinions

here’s the short version.

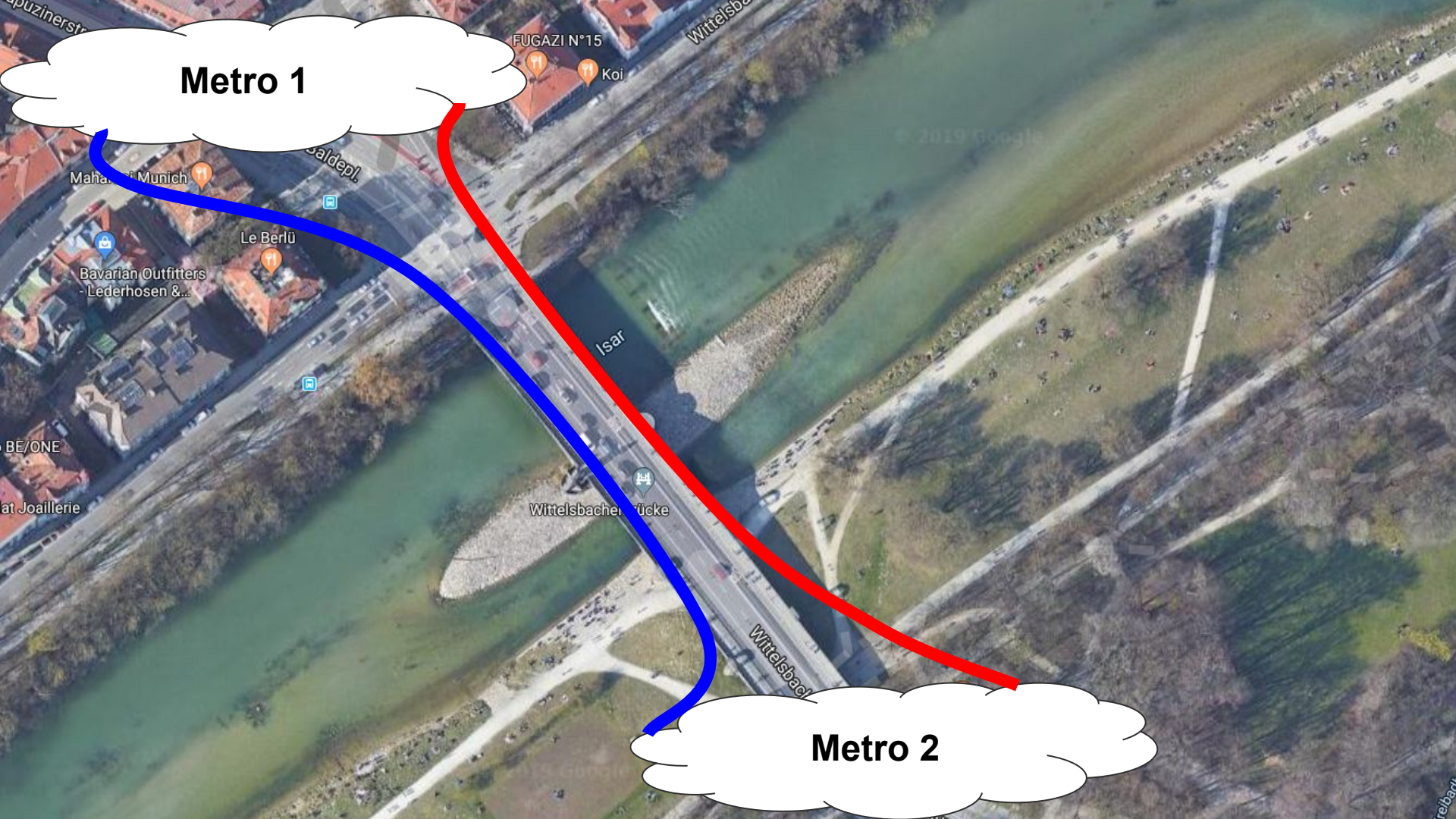
Who am I to rant about this?

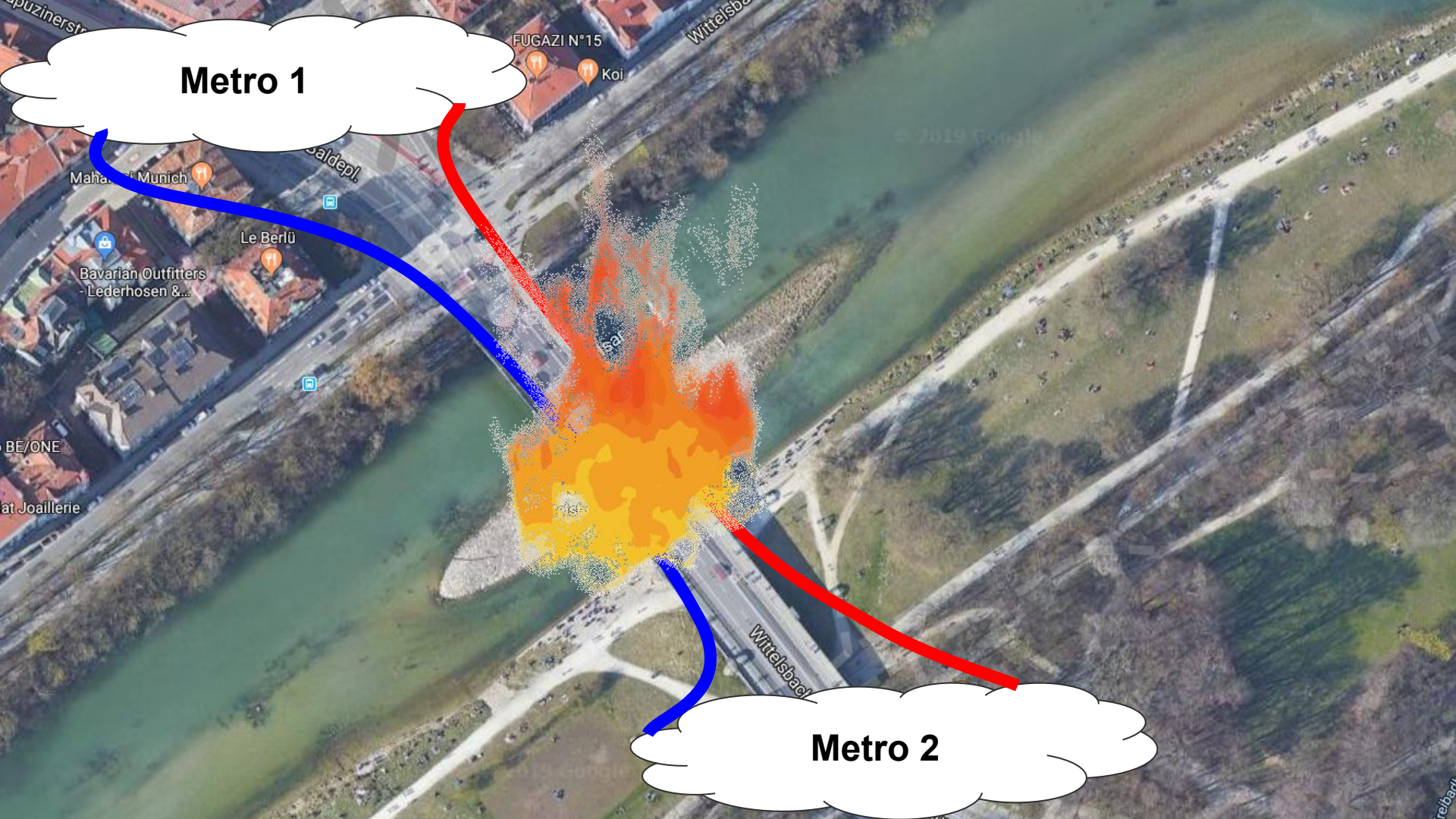
- Professional IT operations since 2000
- NetOps then SRE at Google since 2011
  - Everything from tiny toy services to the world's largest network backbones & CDNs
  - These days a lot of large scale incident management
  - (And low level code yak shaving)

Alert Correlation

Alert Correlation

- X is broken
- Y is broken
- Are they the same underlying incident?


Metro 1
Metro 2
FUGAZI N°15
Koi
Le Berlü
Bavarian Outfitters - Lederhosen &...
Isar
Wittelsbacher Brücke
Wittelsbach
BE/ONE


Metro 1
FUGAZI N°15
Koi
Le Berlü
Bavarian Outfitters - Lederhosen &...
Wittelsbach
Metro 2

Alert Correlation

- Yes?
  - Technically correct.
  - If I have enough redundancy I might not notice that what I thought was a diverse path isn’t.
- No
  - Sure I get two alerts.
  - Because there’s two problems.

Useful Alert Correlation

Basic rule engines can give the vast majority of value using data you already have.

- Inhibit low optical power on link down
- Inhibit link down on bundle down
- Inhibit bundle down on optical span down

Some of this can be autodetected when you don’t have a full intent data store.

Advanced Alert Correlation

Combine a prober mesh with a linear programming engine to find subtle (loss < 0.01%) breakages in a network.

No machine learning required.

Presentation: http://s442.net/pl-deck http://s442.net/pl-vid

Anomaly Detection

Anomaly Detection

1. Here’s a firehose of information
2. Find the interesting things.

Anomaly Detection

1. Here’s a firehose of information
2. Find the ~~interesting~~ things.

Anomaly Detection

1. Here’s a firehose of information
2. Find the unusual things.

Anomaly Detection

1. Here’s a firehose of information
2. Find the unusual things.

But do they matter?

Anomaly Detection

- Here’s a firehose of information
- Find the unusual things.
- But do they matter?
- At even small scale there’s *always* weird things in logs.
- Just storing for later grepping is more useful.
- (Do alert on things you *know* are bad though)

The End.

Counterexamples / Want this as a full talk somewhere?

@laptop006 / jgoodwin@studio442.com.au