Analysing real-time data with the Elastic Stack

Emanuil Tolev @emanuil_tolev

elastic

Community Engineer

Data and the cognitive problem of

elastic

@emanuil_tolev

Who considers themselves to work with real-time data?

"Real-time"

Deadlines

@emanuil_tolev

Be very careful if you go into making decisions with ms deadlines

and are using a datastore typically used by web devs

So what can you do? A lot.

Make it the destination for data at rest

Have quick guaranteed processing on the fly and store the summary

Let's look at some cars

The VLN


premio
357
302
Sugar Mountain
Money Hill
Uwe Wächtler
BASTUCK
SANDTLER
HANKOOK

Found they were a bit slower. What to do?

Some engineering!

→ gather data

→ analyse it

Alright, what do we have?

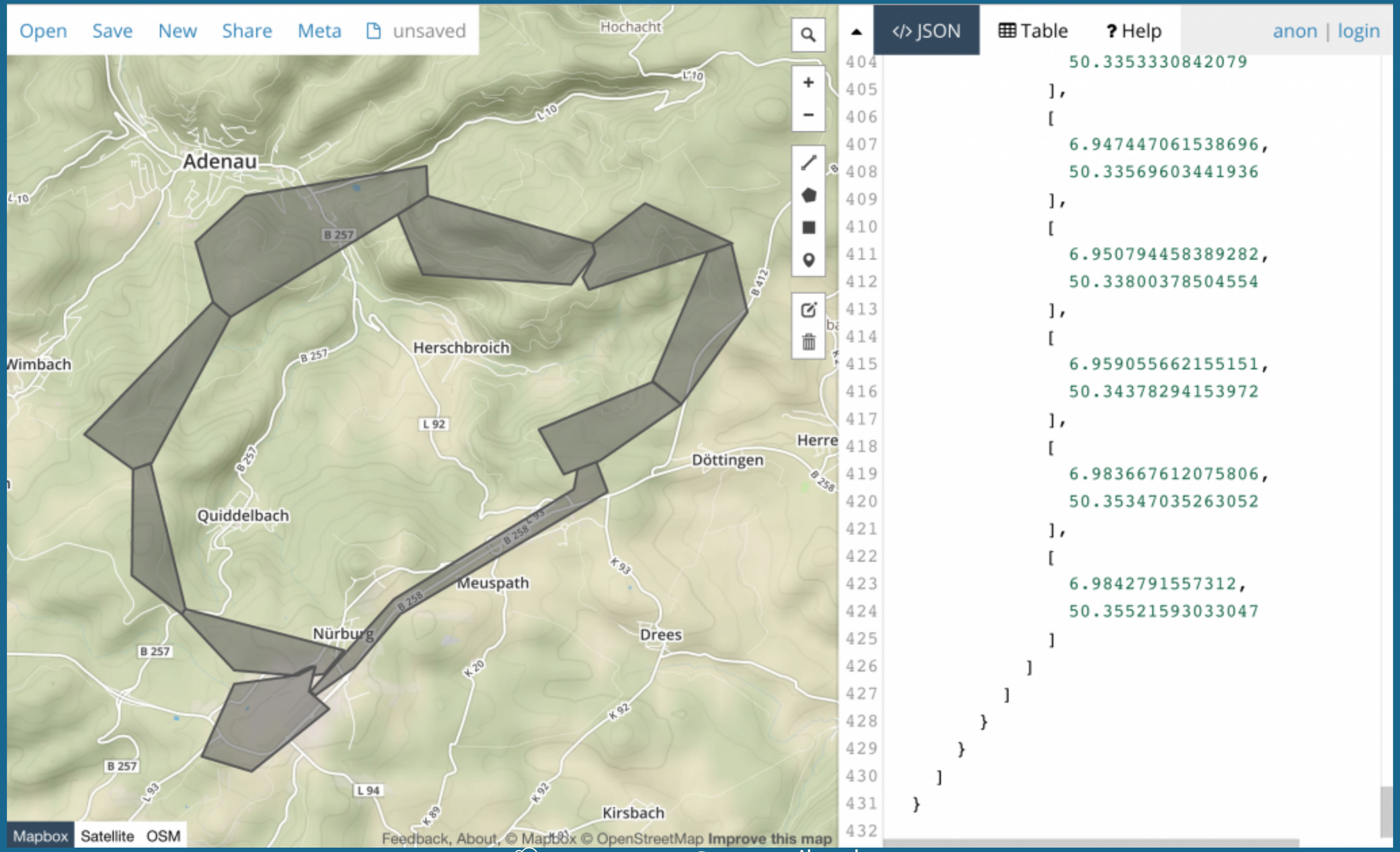
→ location

→ speed

The Racing App

Data source -> proxy -> Elasticsearch

pretty typical



elastic @emanuil_tolev

geo-queries and geo-filters in Elasticsearch to find entry and exit times

each car, every sector

Meplato Racetrack: Analyse zwischen 02.08.2014 12:21:00 und 02.08.2014 16:15:00

Grand Prix Kurs

Runde	344		350		355	357		360	
1.	01:25	+1.0	01:25	+1.0		01:12	-12.0	01:24	
2.	01:24	+2.0	01:26	+4.0		01:22		01:24	+2.0
3.	01:25	+1.0	01:26	+2.0		01:26	+2.0	01:24	
4.	01:24		01:27	+3.0		01:27	+3.0	01:27	+3.0
5.	01:22	+4.0	01:28	+10.0		01:18		01:24	+6.0
6.	01:28	+4.0	01:25	+1.0		01:26	+2.0	01:24	
7.	01:27		01:29	+2.0		01:28	+1.0	01:27	
8.	01:12	-4.0	01:14	-2.0		01:28	+12.0	01:16	
9.	01:25	+5.0	01:26	+6.0		01:20		00:47	-33.0
10.	01:35	+8.0	01:36	+9.0		01:27		01:36	+9.0
11.	01:23		01:24	+1.0		01:26	+3.0	01:32	+9.0
12.	01:24		01:26	+2.0		01:27	+3.0	01:24	
13.	01:26	+1.0	01:25			01:25		01:28	+3.0
14.	01:25		01:26	+1.0		01:26	+1.0	01:26	+1.0
15.	01:27	+1.0	01:08	-18.0		01:26		01:27	+1.0
16.	01:21		01:21			01:27	+6.0	01:25	+4.0
17.	01:23	+6.0	01:13	-4.0		01:11	-6.0	01:17	
18.	01:24	+5.0	01:08	-11.0		01:28	+9.0	01:19	
19.	01:05	-15.0	01:20			01:27	+7.0	01:27	+7.0
20.	01:25	+6.0	01:21	+2.0		01:26	+7.0	01:19	
21.	01:26	+2.0	01:26	+2.0		01:27	+3.0	01:24	
22.	01:26	+5.0	01:21			01:27	+6.0	01:26	+5.0
Schnitt	01:25	+4.0	01:25	+8.0	n/a	01:26	+8.0	01:24	+8.0

elastic @emanuil_tolev

Wake up :)
before demo.

Who's done analytics on a real-time data stream? What was it?

One more cool thing - airport security

Crimson Macaw for Manchester Airport Group (MAG)

real-time dashboards for Airport Security Operations at London's Stansted Airport

elastic

@emanuil_tolev

National rail data

STOMP input -> Logstash -> Elasticsearch

NEXT ARRIVAL

London Liverpool Street

Arrives 16:27

Status On Time

TRAINS ARRIVED

2 Trains
in the last 15 minutes

4 Trains
in the last 30 minutes

7 Trains
in the last hour

ARRIVALS

16:14	On Time	Estimated	London Liverpool Street
16:18	On Time	Estimated	Stansted Airport
16:27	On Time	Estimated	London Liverpool Street
16:33	On Time	Estimated	Stansted Airport
16:36	On Time	Estimated	Stansted Airport
16:38	On Time	Estimated	Stansted Airport
16:40	On Time	Estimated	Birmingham New Street
16:44	On Time	Estimated	London Liverpool Street
16:47	On Time	Estimated	Stansted Airport
16:58	Early: 3 Minutes	Arrived	London Liverpool Street
17:02	On Time	Estimated	Stansted Airport
17:11	Early: 6 Minutes	Arrived	London Liverpool Street
17:18	On Time	Estimated	Stansted Airport
17:29	On Time	Estimated	London Liverpool Street
17:32	On Time	Estimated	Stansted Airport
17:38	On Time	Estimated	Stansted Airport
17:40	On Time	Estimated	Birmingham New Street
17:47	On Time	Estimated	London Liverpool Street
17:48	On Time	Estimated	Stansted Airport
18:01	On Time	Estimated	London Liverpool Street

National Rail

MyMAG

Questions?

Emanuil Tolev @emanuil_tolev

etolev@elastic.co