# Let’s go geospatial with Kibana and Elasticsearch

Jorge Sanz
2020-02-08, Kibana, Elastic,
xurxosanz jsanz

https://ela.st/wecode-2020
https://ela.st/wecode-2020-slides

# Workshop objectives

## Elastic and Geo

- Understand the basics of the **Elastic Stack**
- What are the **Elasticsearch** most relevant **geospatial** features
- How **Kibana** can be used to create dashboards with geodata
- What are the basics of a modern **web map application**
- Have a bit of **fun**, if possible 😅

# Agenda

1. Intro to the Elastic stack
2. Lab set up and data import
3. Kibana overview: Dashboards, Lens, Canvas, and Maps
4. Elasticsearch (geo) queries
5. Web mapping 101

# Using your trial cloud account

- Create a 14 days free trial account at **cloud.elastic.co**
- Create a new deployment (**details**)
  - defaults are ok
  - you can disable the APM instance
- To load the flight tracking data:
  - You can stream data from your laptop using the opensky-loader docker image or the node script (**details**)
  - Alternatively you can upload the sample GeoJSON file or generate a new one (**details**)

# Using docker-compose

Start the docker compose services

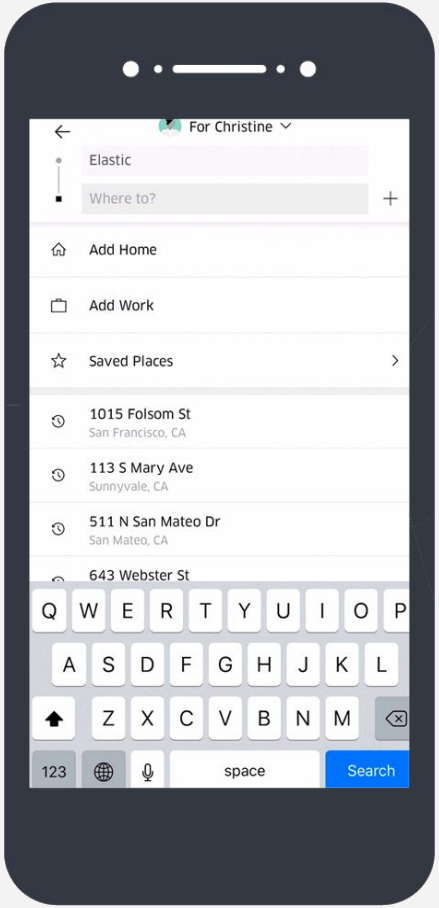
```
$ git clone https://github.com/jsanz/wecode20.git
$ cd wecode20/lab
$ docker-compose up
```

Visit http://localhost:5601

# Agenda

1. Intro to the Elastic stack
2. Lab set up and data import
3. Kibana overview: Dashboards, Lens, Canvas, and Maps
4. Elasticsearch (geo) queries
5. Web mapping 101

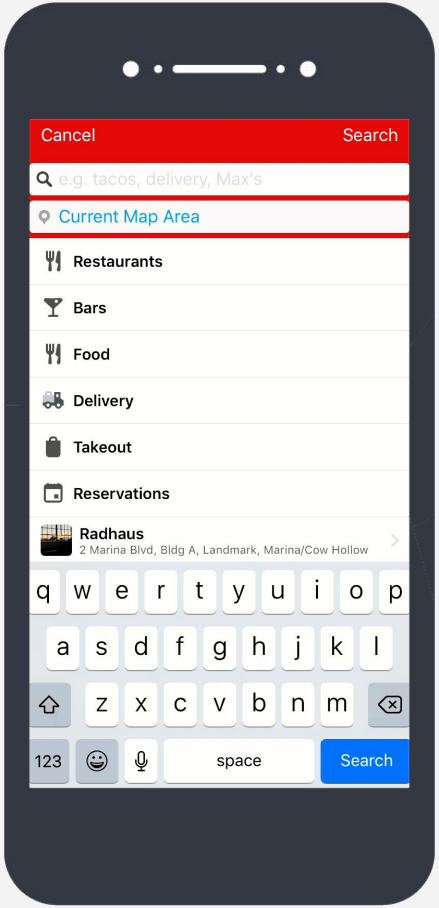
Elastic is a **search company**




Uber

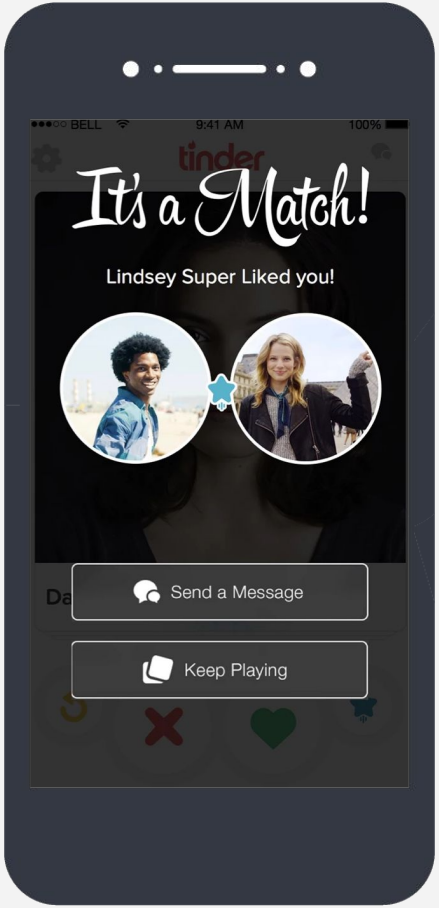
https://eng.uber.com/elk/

elastic




yelp®

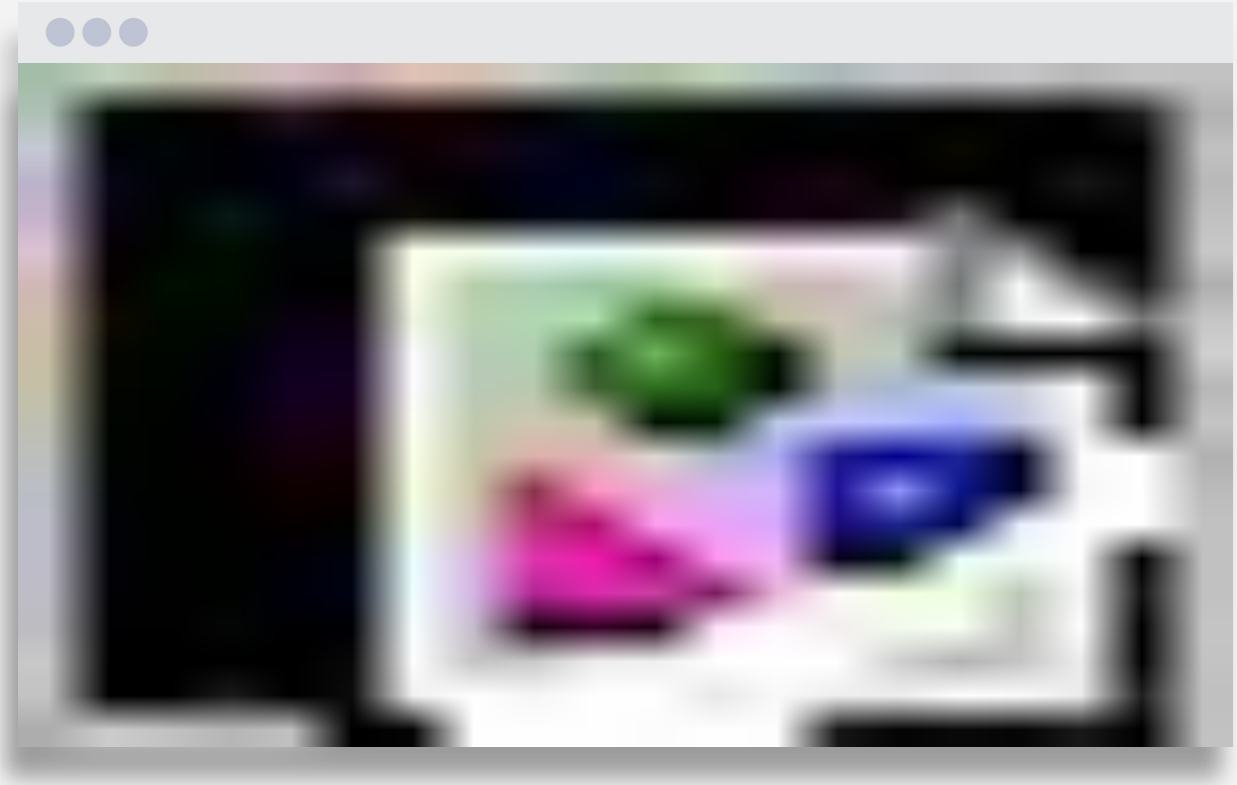
elastic




tinder™

elastic

instacart



ACTIVISION BLIZZARD

elastic

INDIANA UNIVERSITY

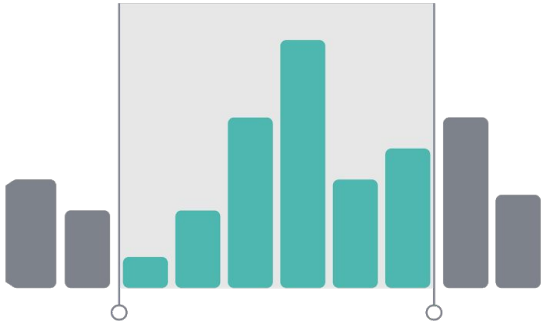
# Customers across various **industries, segments, and geographies**

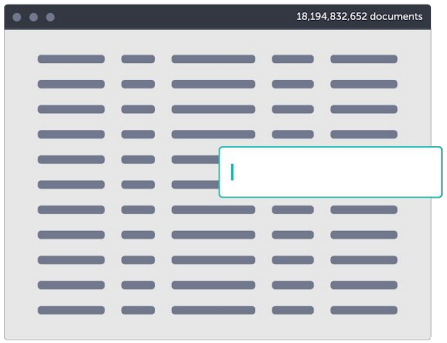
| TECHNOLOGY | FINANCE | TELCO | CONSUMER | PUBLIC SECTOR | AUTOMOTIVE / TRANSPORTATION | RETAIL |
|---|---|---|---|---|---|---|
| LiveChat | BARCLAYS | orange | rightmove | BBC | RENAULT | ebay |
| amadeus | CREDIT SUISSE | LIBERTY GLOBAL | JUST EAT<br>TOMTOM | Department for Work & Pensions | AIRBUS | Argos |
| CDL | BNP PARIBAS | Telefónica | CAR2GO | Liberté • Égalité • Fraternité<br>RÉPUBLIQUE FRANÇAISE<br>MINISTÈRE DE LA DÉFENSE ET DES ANCIENS COMBATTANTS | PSA GROUPE | OTTO |
| SAP Concur | collector bank | kpn | MM KARTON AG | MAG | Audi | Boots |
| TOTANGO | ING | T | PERFORM SPORTS CONTENT & MEDIA | | | |

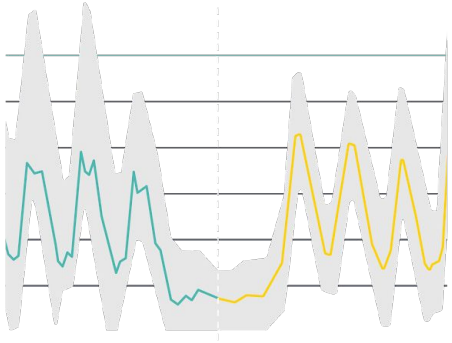


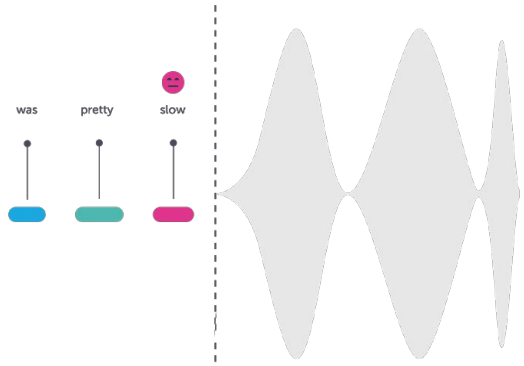
elastic

# Search is the **foundation**





# Technology **differentiation**

## SCALE

Distributed by design

## SPEED

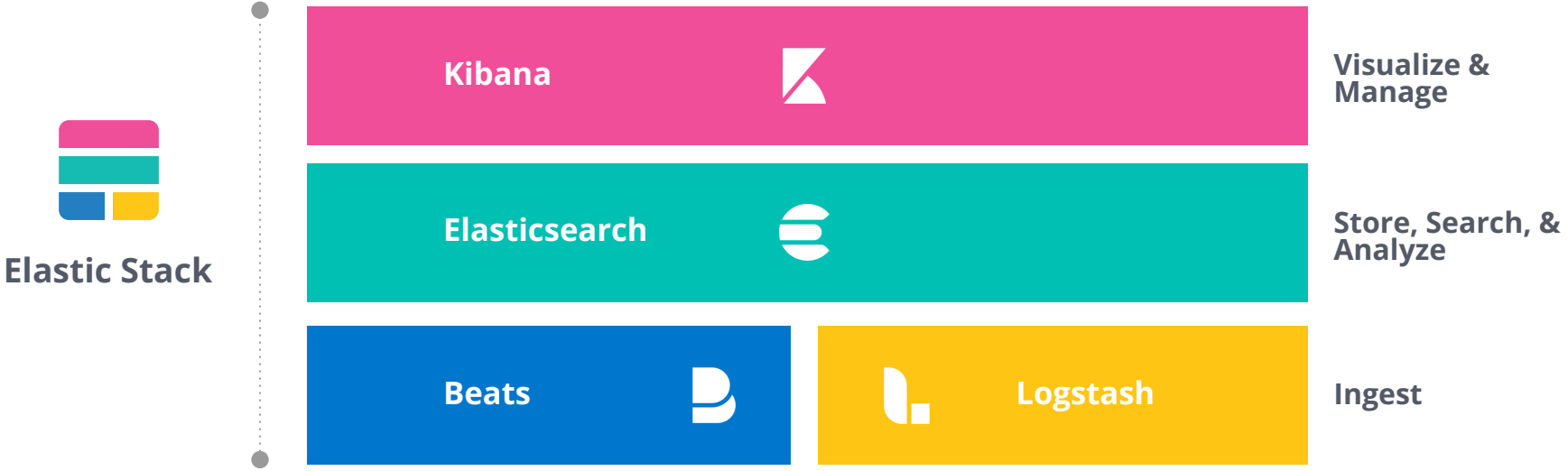
Find matches in milliseconds

## RELEVANCE

Get highly relevant results

# Elastic **Stack**

## What is the stack?






elastic

# Elastic **Stack**

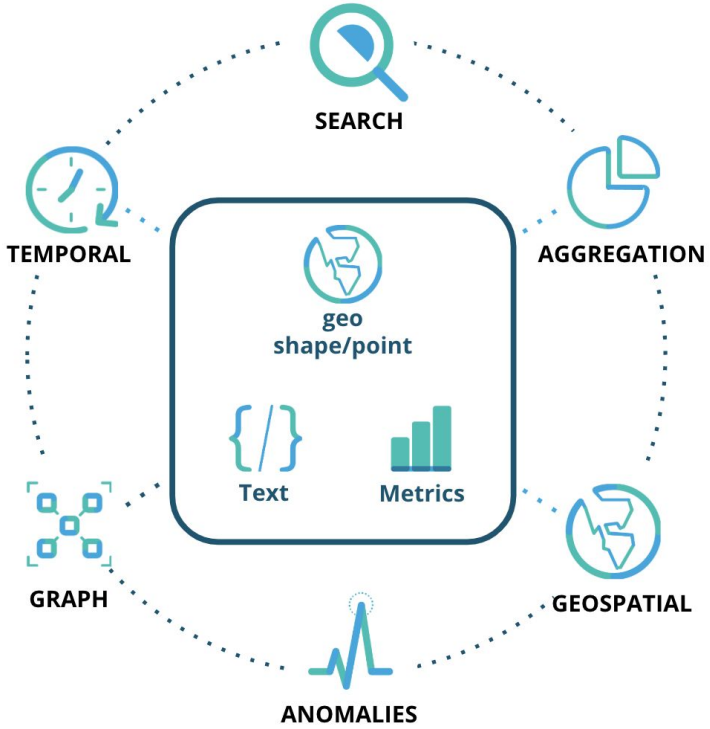



elastic

# Elastic **Stack**

## Elasticsearch

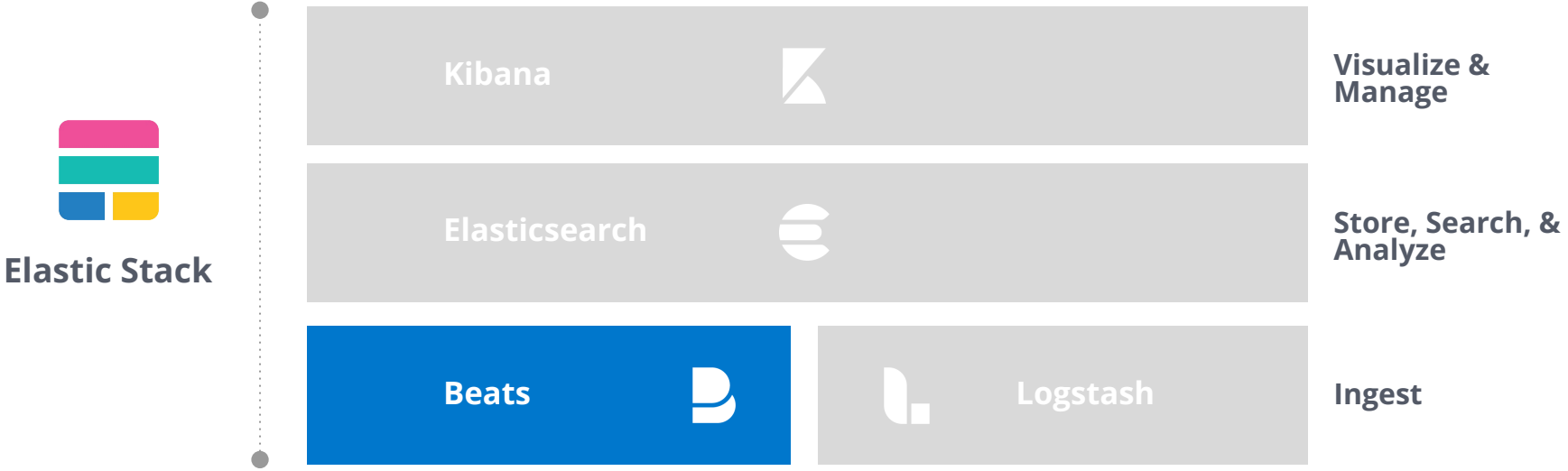
### All data is welcome






elastic

# Elastic **Stack**

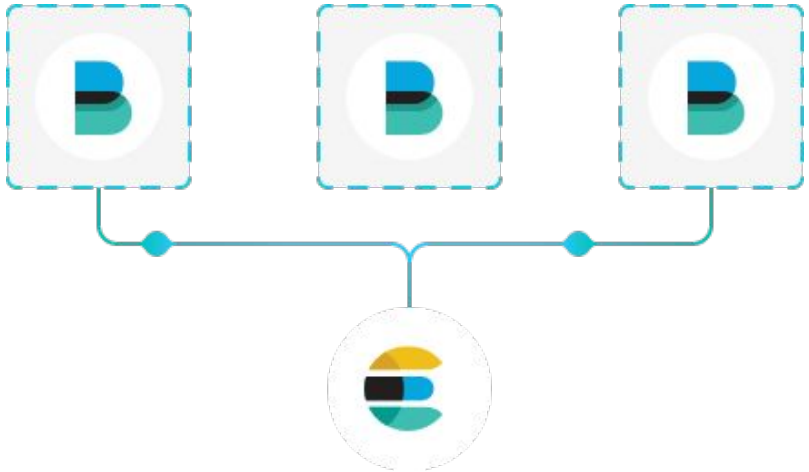





elastic

# Beats

Lightweight data shippers



| | | |
|---|---|---|
| Ship data from the source | Ship and centralize in Elasticsearch | Ship to Logstash for transformation and parsing |
| Ship to Elastic Cloud | Libbeat: API framework to build custom beats | 70+ community Beats |

# Elastic **Stack**

## Beats

**All the modules**

**FileBeat**
Log Files

**MetricBeat**
Metrics

**PacketBeat**
Network Data

**WinLogBeat**
Window Events

**HeartBeat**
Uptime Monitoring

**AuditBeat**
Audit Data

**FunctionBeat**
Serverless Shipper

**Plus, more than 70 community Beats and growing...**

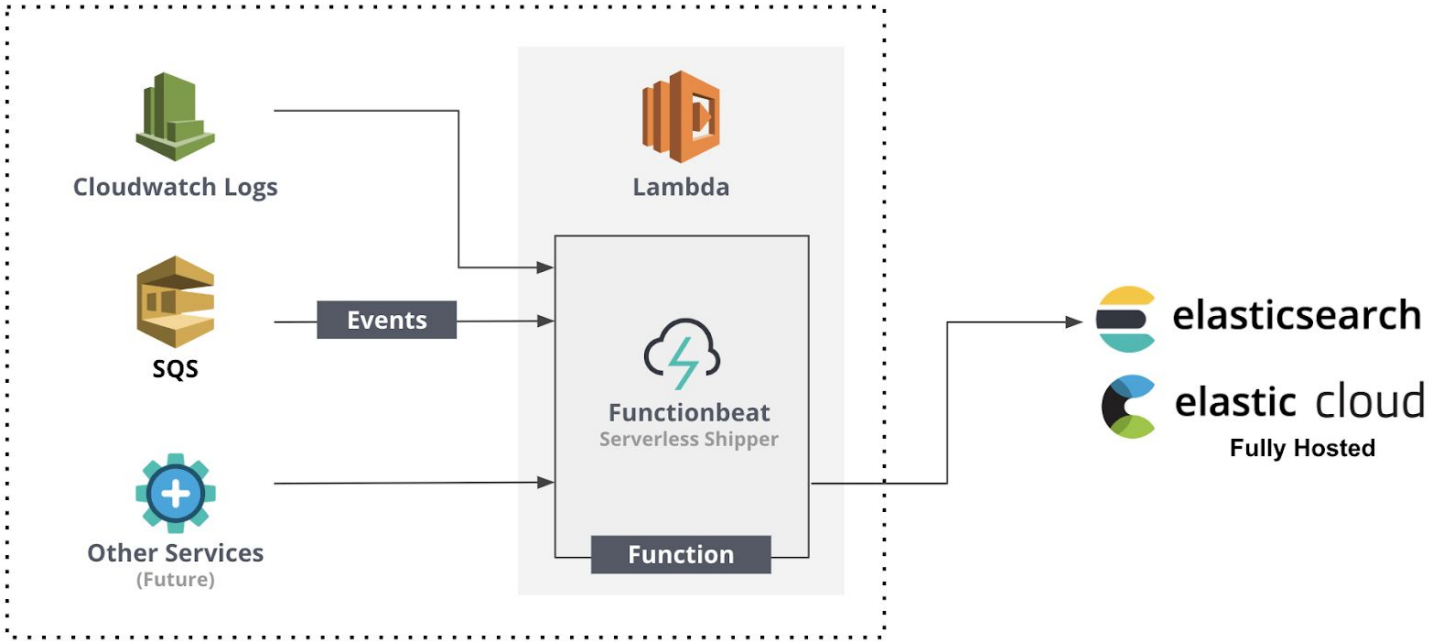


elastic

# Elastic **Stack**

## Beats

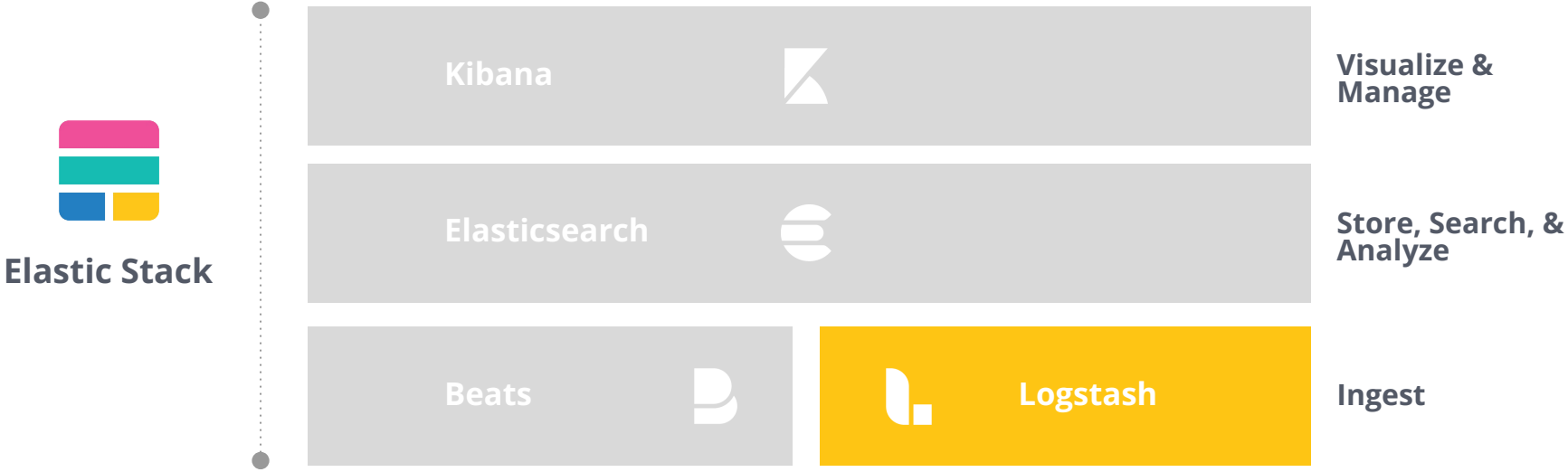
### FunctionBeat - Serverless shipper for Cloud Data






elastic

# Elastic **Stack**

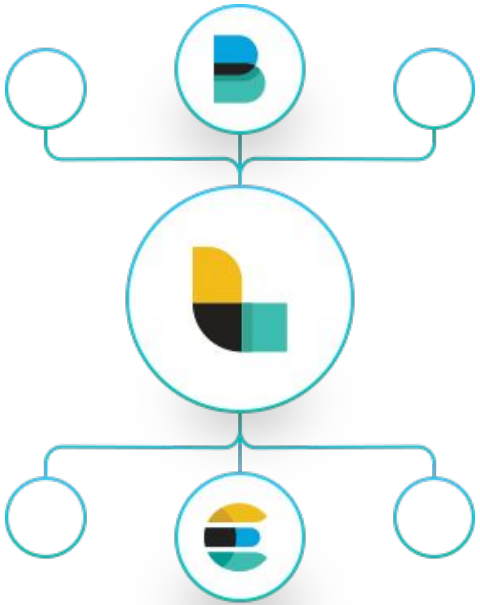





elastic

# Logstash

ETL for Elasticsearch

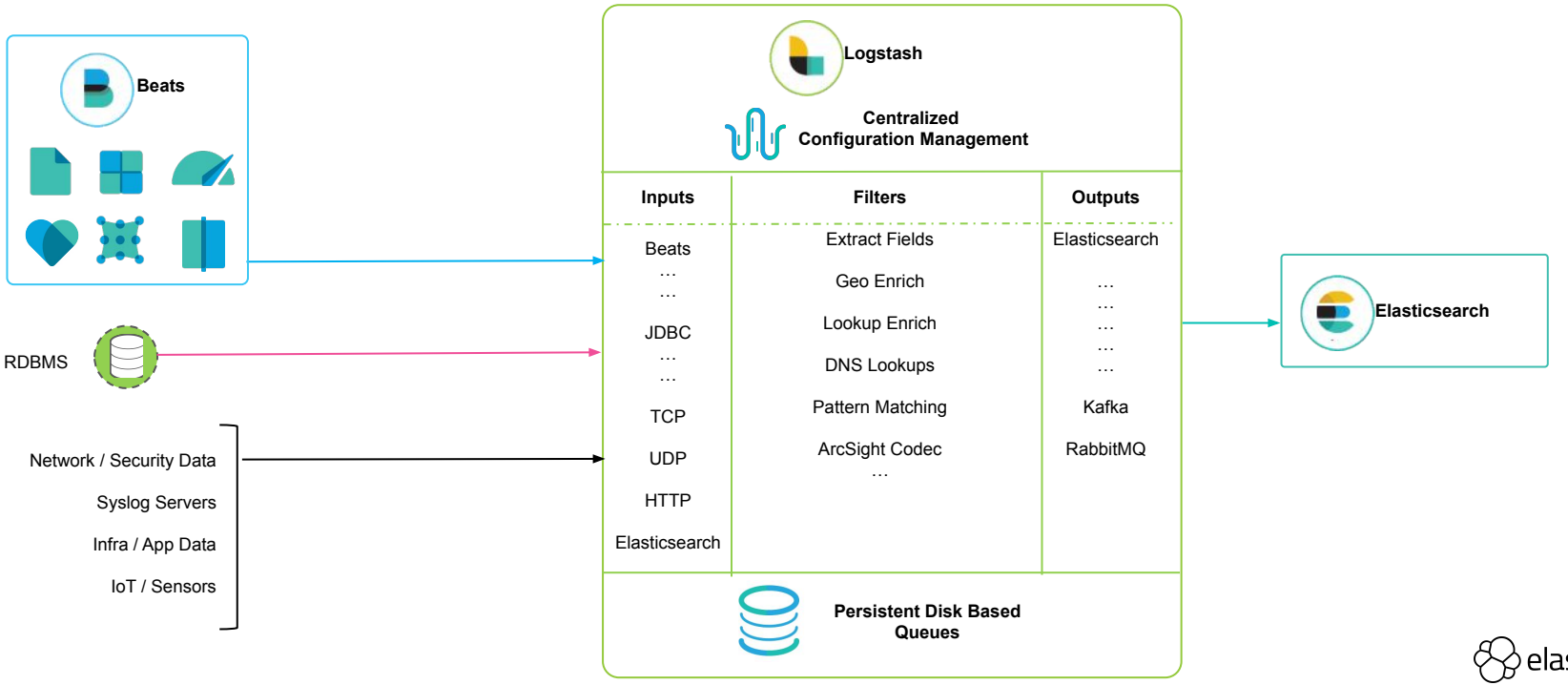


| | | |
|---|---|---|
| Ingest data of all shapes, sizes, and sources | Parse and dynamically transform data | Transport data to any output |
| Secure and encrypt data inputs | Build your own pipelines | Lots of plugins |

# Elastic **Stack**

## Logstash

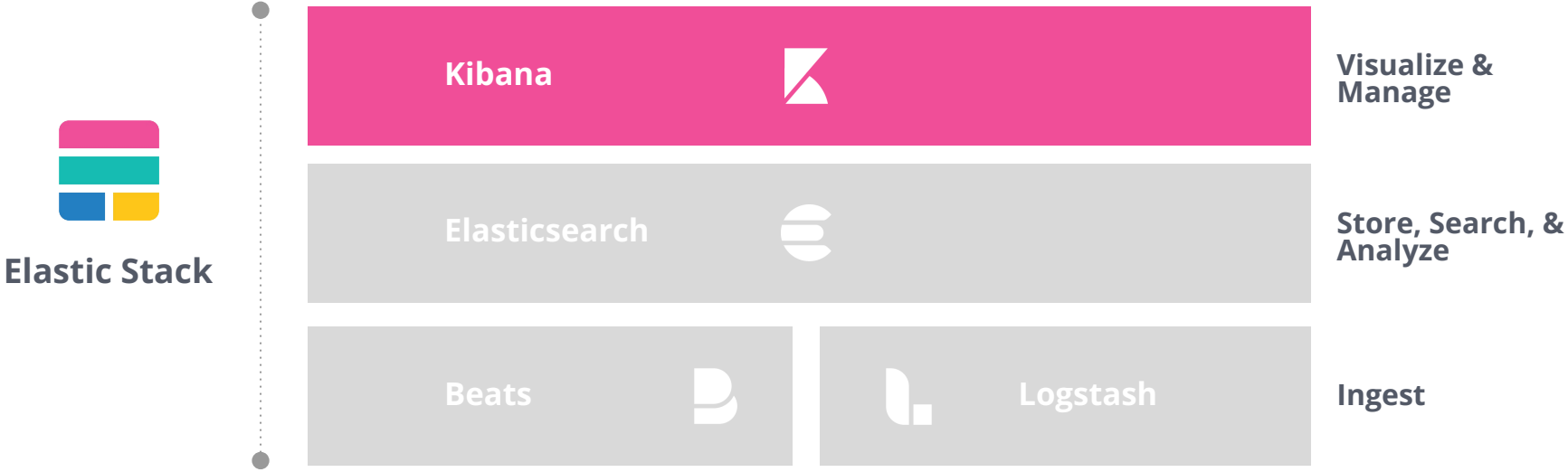
### Normalize and Enrich Data before Indexing






elastic

# Elastic **Stack**



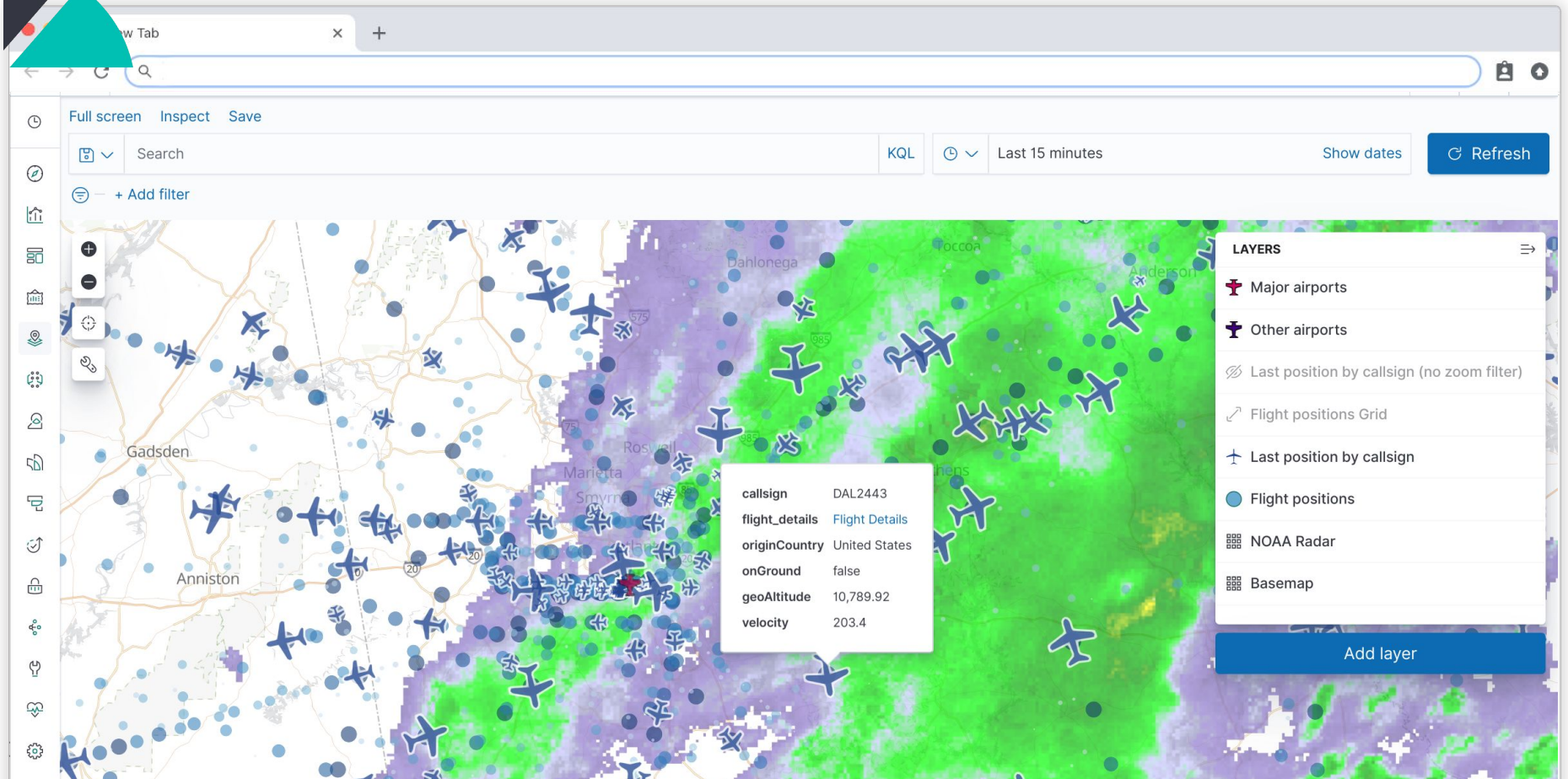



elastic

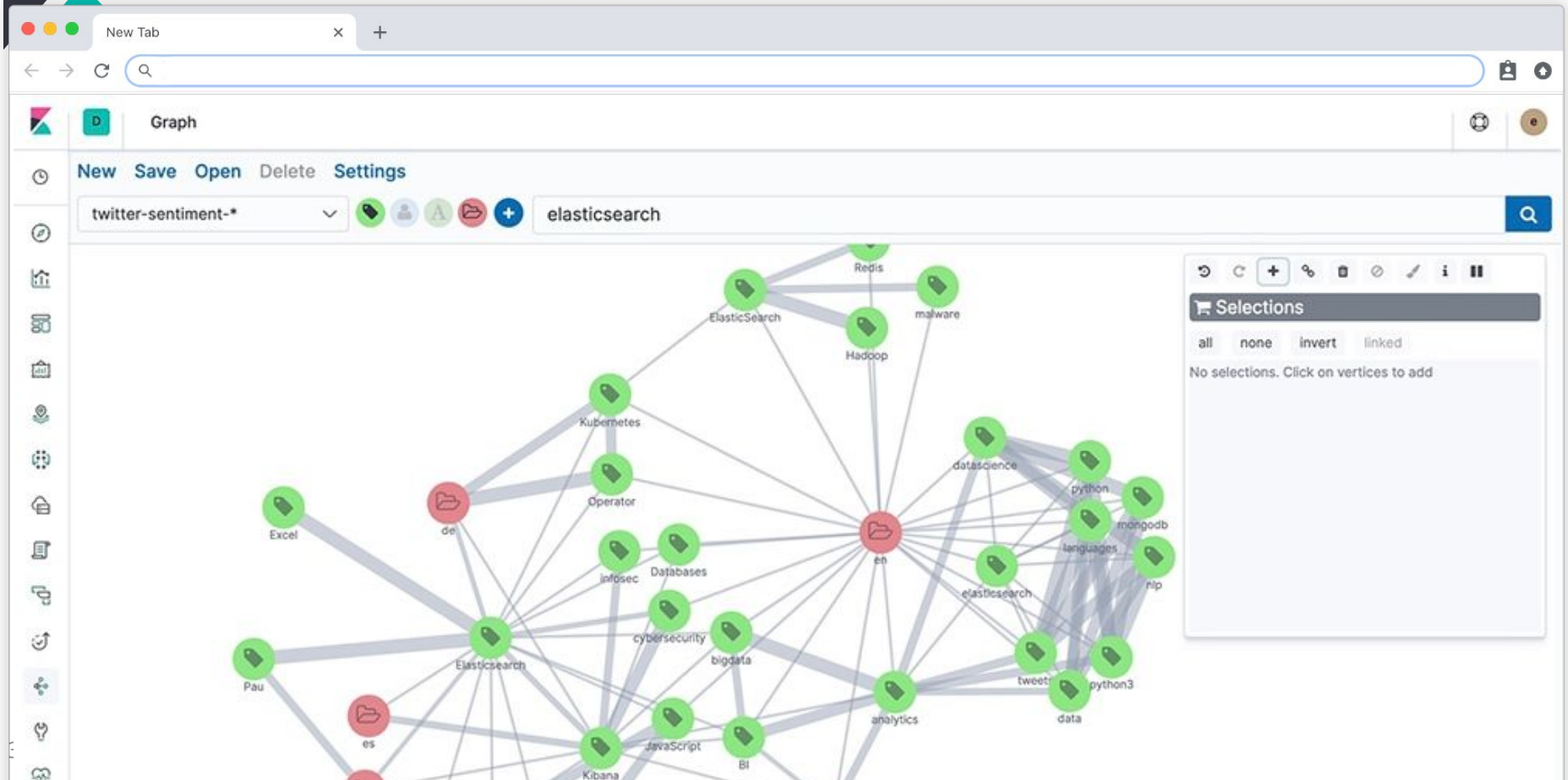
# Kibana: **Dashboards**

# Kibana: **Canvas**

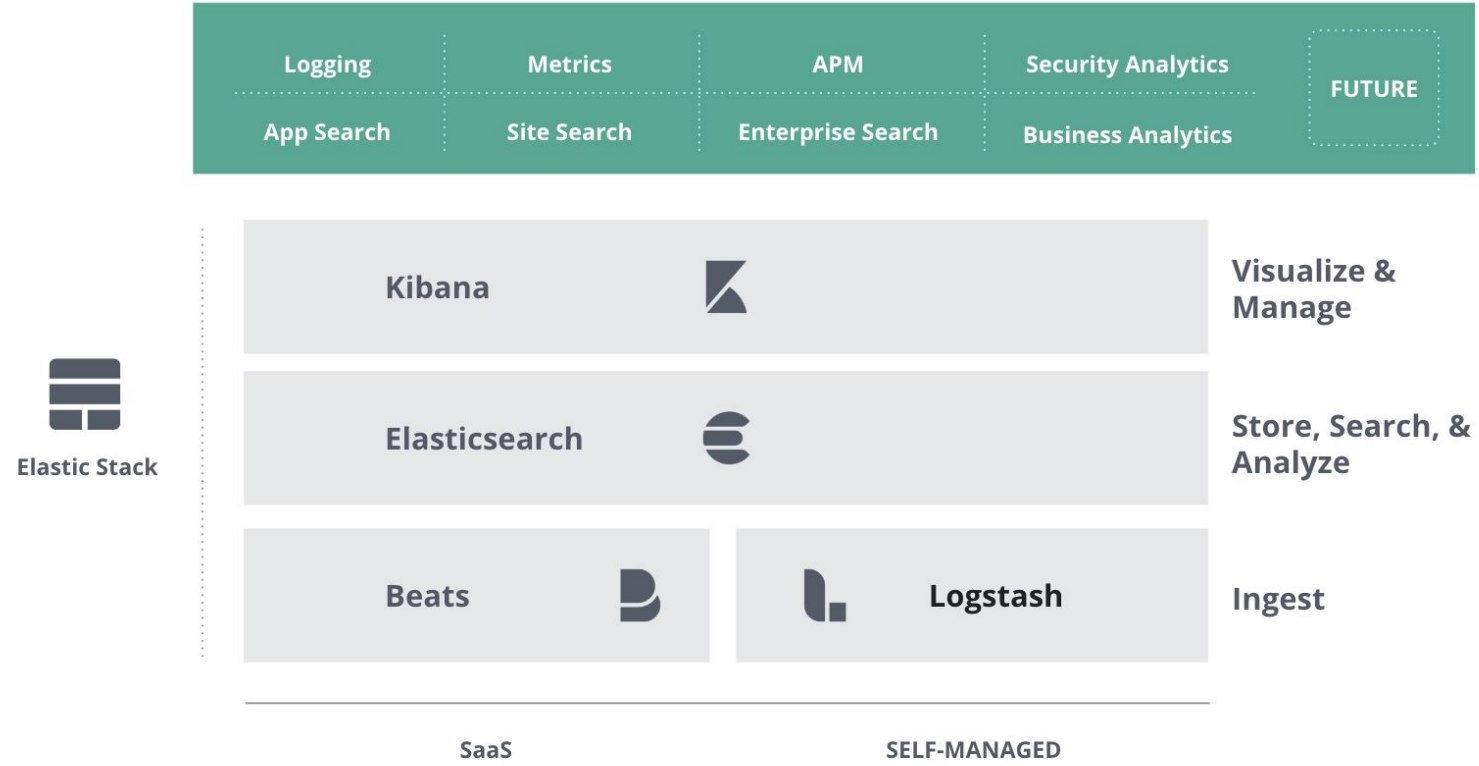
# Kibana: **Elastic Maps**



# Kibana: **Graph**



# Solutions



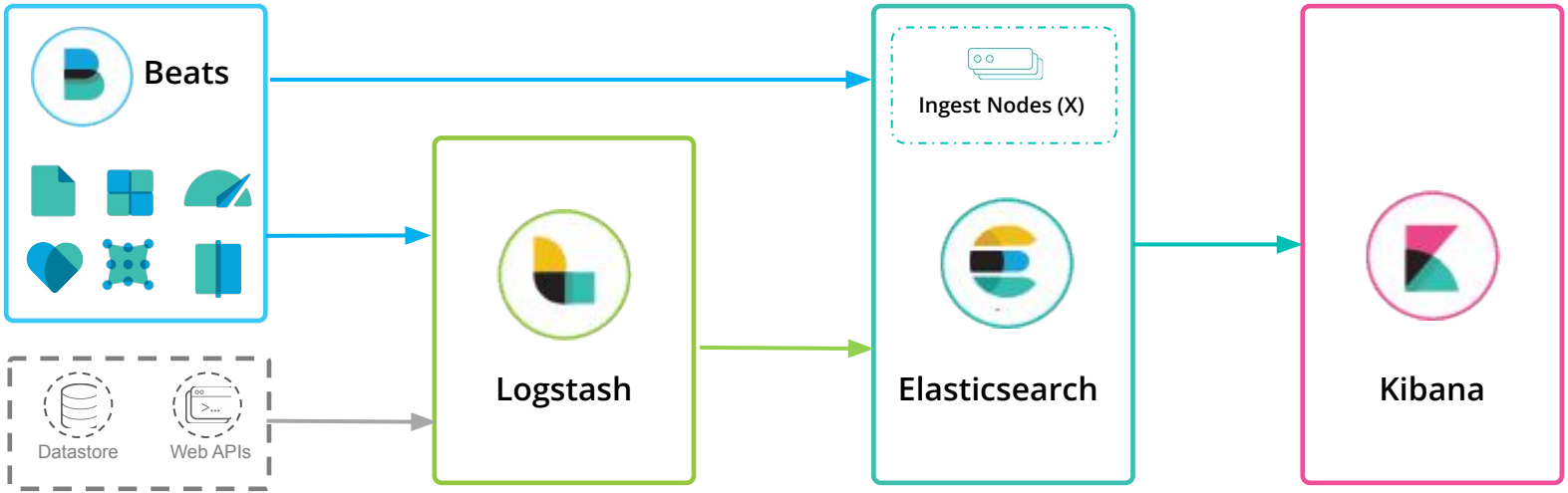



elastic

# Elastic **Stack**

## How does it work together?

### Ingest, Store, Search, Visualise






elastic

# Continue your journey…

## More resources

- Spin up a cluster
  - Hosted: cloud.elastic.co
  - Self managed - elastic.co/downloads
- Explore live examples @ elastic.co/demos
- Watch webinars @ elastic.co/videos
- Chat with us @ ela.st/slack (blog plost)
- Forums : https://discuss.elastic.co/
- Go deeper with documentation @ elastic.co/guide
- Sign up for training @ elastic.co/training
- Attend a local meetup or Elastic{ON}: Madrid 2020-02-18

# Agenda

1. Intro to the Elastic stack
2. Lab set up and data import
3. Kibana overview: Dashboards, Lens, Canvas, and Maps
4. Elasticsearch (geo) queries
5. Web mapping 101

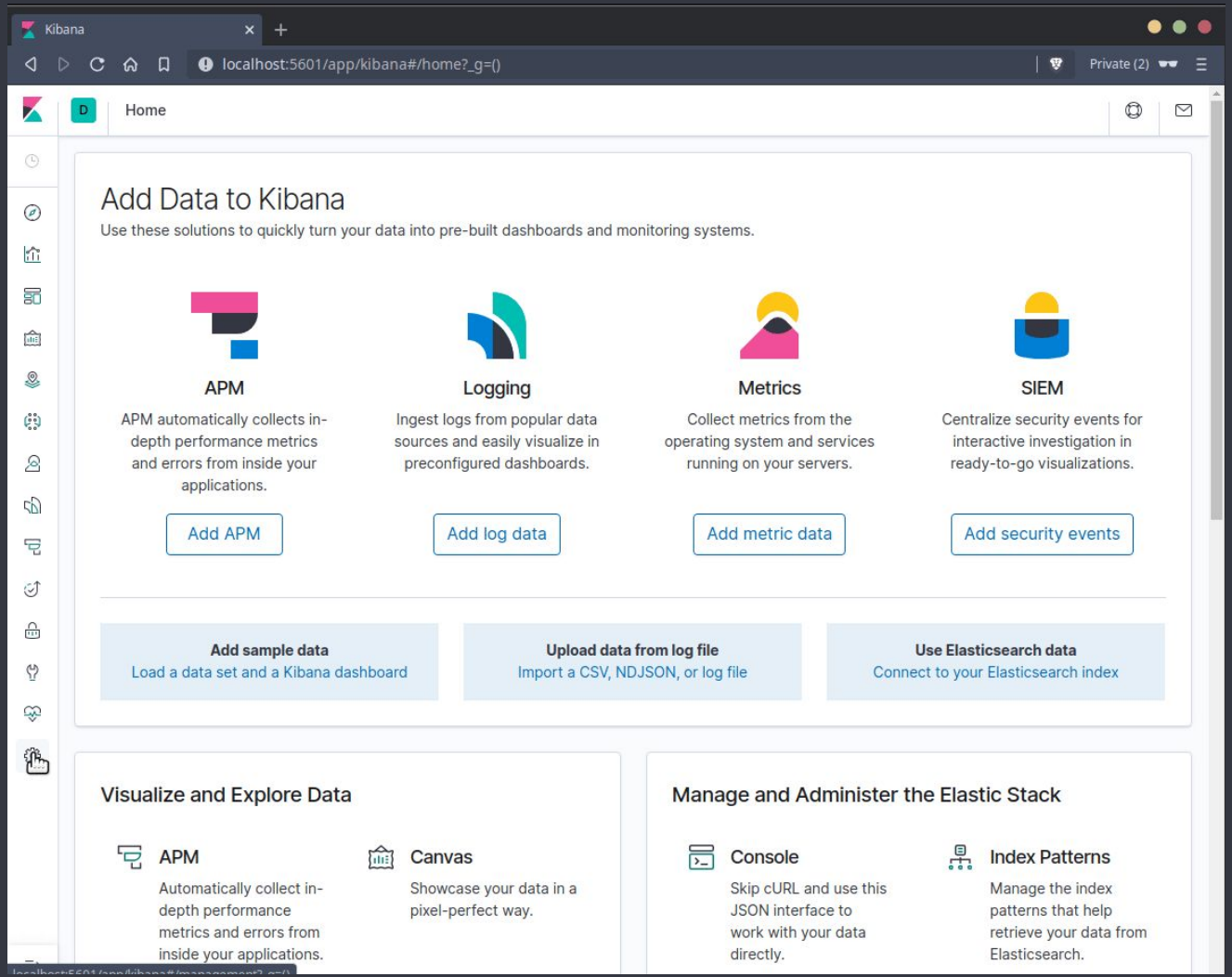
# A few Kibana concepts

elastic

# Index patterns

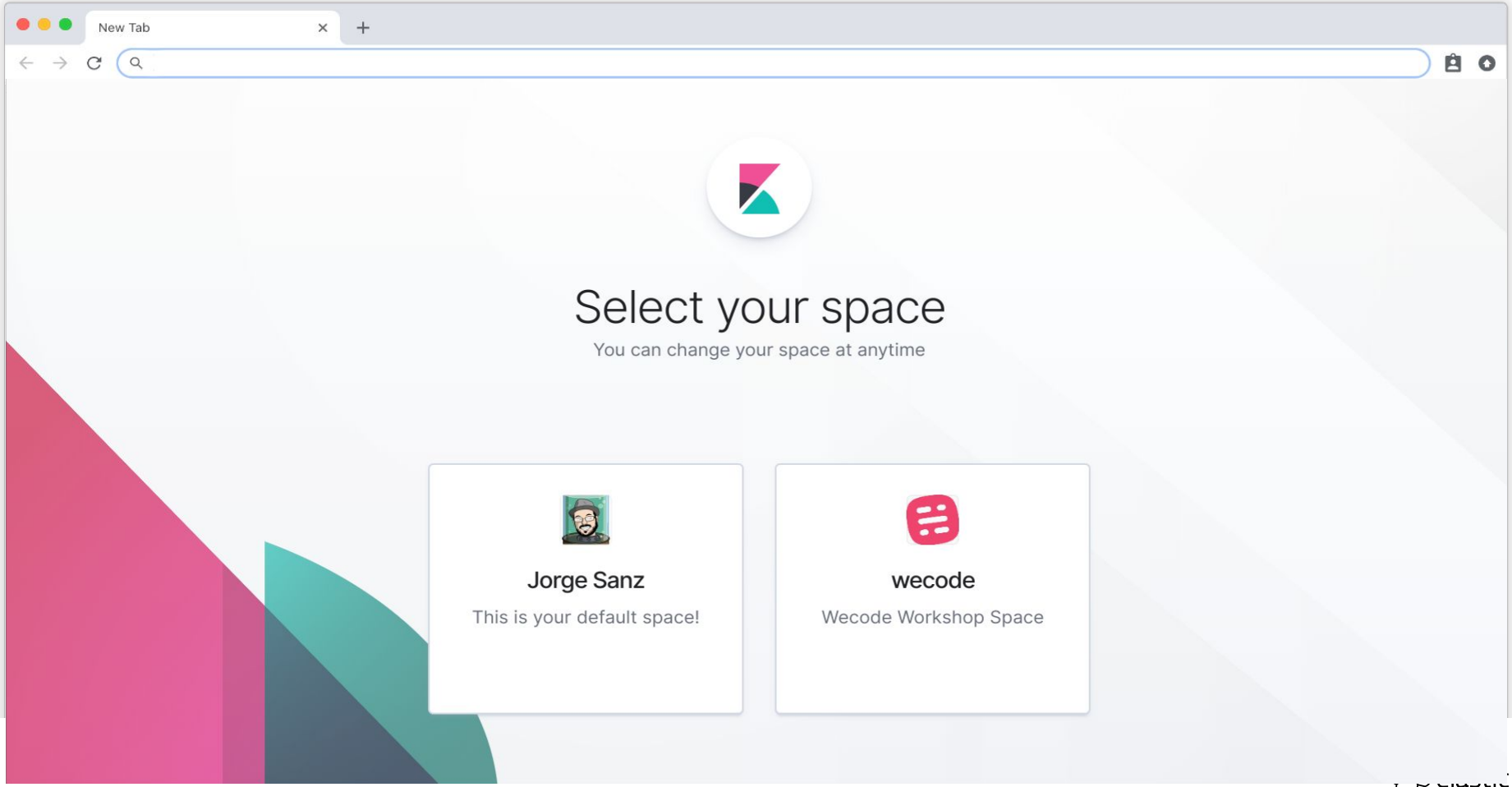
- A logic component to **group** indexes by a string **pattern**
  - `my_application_logs_*`
- Fields can have **custom formatters**: number, currency, url, image,...
- Can have a date field used for **time range selections**
- **Scripted fields** allow custom computations at query time

# Creating a new index pattern



# Saved Objects

- Kibana **state** is stored in Elasticsearch indexes
- Application **configuration** is stored in saved objects
  - An index pattern, dashboard, map, …
- Saved objects define **dependencies** between them
  - Index pattern >> Map >> Dashboard
- Saved objects can be **exported** and **imported** (JSON)


New Tab
Select your space
You can change your space at anytime
Jorge Sanz
This is your default space!
wecode
Wecode Workshop Space

# Spaces

- Separate Kibana objects by **functional groups**
- Objects can only be stored at a **single** space
- **Roles** can get access to spaces
- **Applications** can be disabled per space **and** role

# Discover

- Quick **exploration** tool
- **Time** range (!!) and auto **update***
- **Search bar** using Kibana Query Language or Lucene syntax*
- **Filters***
- Fields as **columns**
- Index pattern **formatters** are used
- **Inspect** tool: statistics, full request, and response
- **Save** your search for dashboards

* common to many Kibana elements

Discover

New Save Open Share Inspect

RYR* KQL Jan 31, 2020 @ 14:10:26.4 → Jan 31, 2020 @ 19:05:40.7 Refresh

+ Add filter

flight_trackin... (change)

Search field names

Filter by type 0

**Selected fields**

- t callsign
- # geoAltitude
- onGround
- t originCountry
- # velocity
- t flight_details

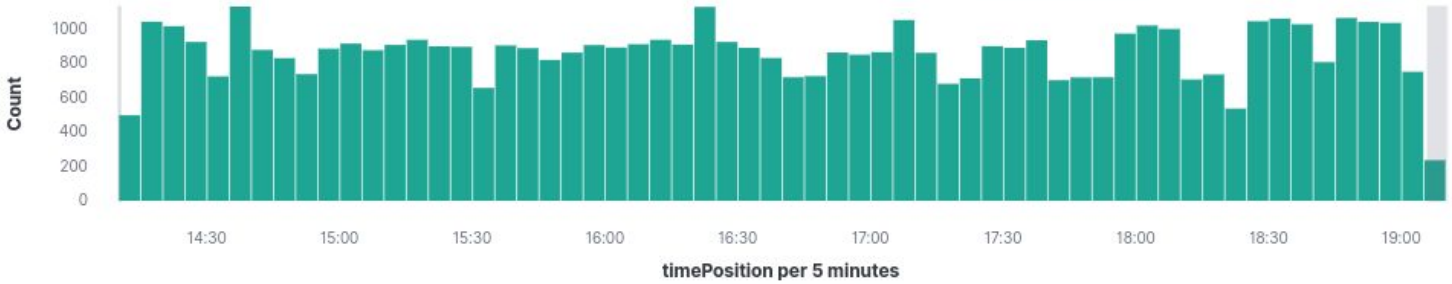
**Available fields**

Popular

- t icao24
- lastContact
- t transponderCode
- @timestamp

**51,724** hits

Jan 31, 2020 @ 14:10:26.480 - Jan 31, 2020 @ 19:05:40.766 — Auto




| Time | callsign | originCountry | onGround | velocity | geoAltitude | flight_details |
|---|---|---|---|---|---|---|
| Jan 31, 2020 @ 14:56:59.000 | RYR64VD | Ireland | false | 247.79 | 11,239.5 | Flight Details |
| Jan 31, 2020 @ 14:55:32.000 | RYR92ZH | Ireland | true | - | - | Flight Details |
| Jan 31, 2020 @ 14:56:59.000 | RYR20TA | Ireland | false | 193.39 | 9,121.14 | Flight Details |
| Jan 31, 2020 @ 14:56:59.000 | RYR7UQ | Ireland | false | 98.15 | 1,211.58 | Flight Details |
| Jan 31, 2020 @ 14:56:59.000 | RYR7NV | Ireland | false | 190.21 | 11,506.2 | Flight Details |
| Jan 31, 2020 @ 14:56:59.000 | RYR6924 | Ireland | false | 225.59 | 11,574.78 | Flight Details |

# Developer Tools

## Console

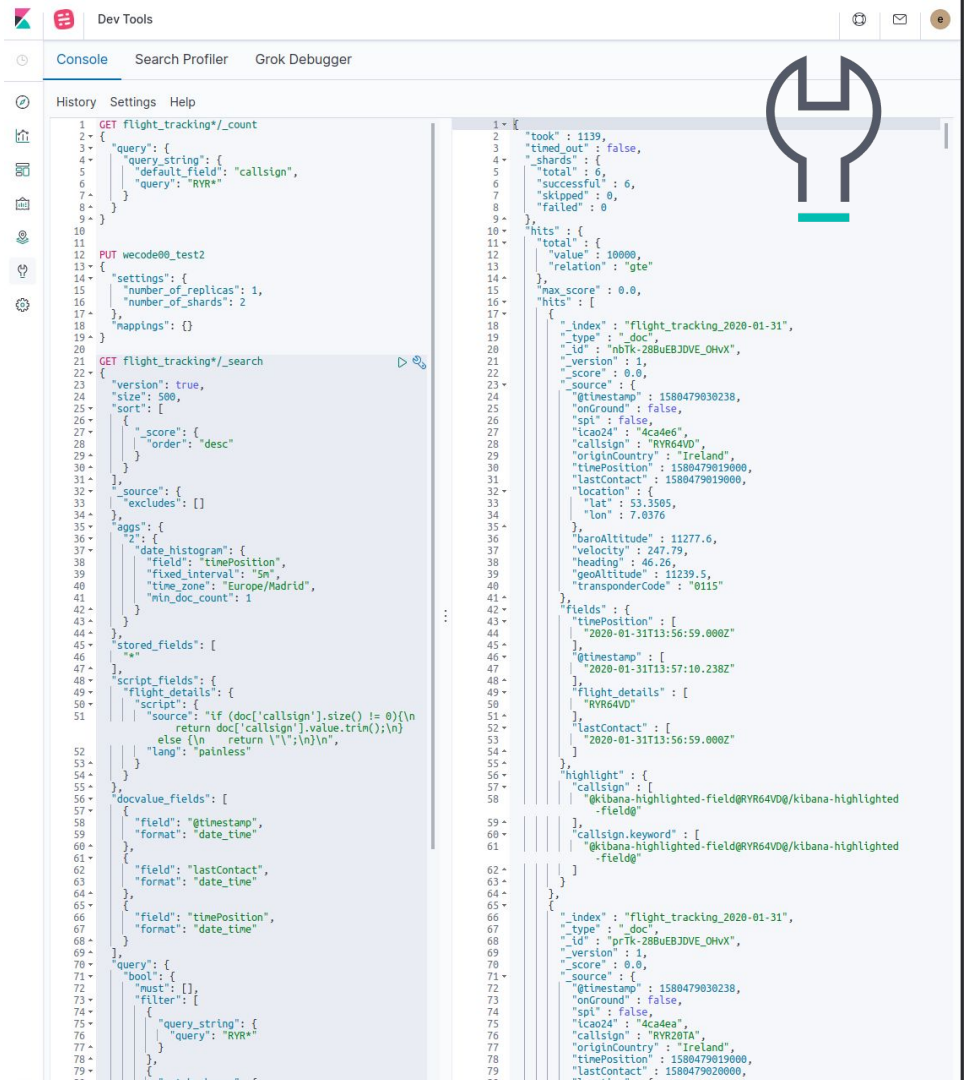
Make any Elasticsearch query with autocompletion, autoindentation, history, etc.

## Search profiler

Get insights of yor query performance

## Grok debugger

Help creating grok expressions for Logstash and other ingestion tools

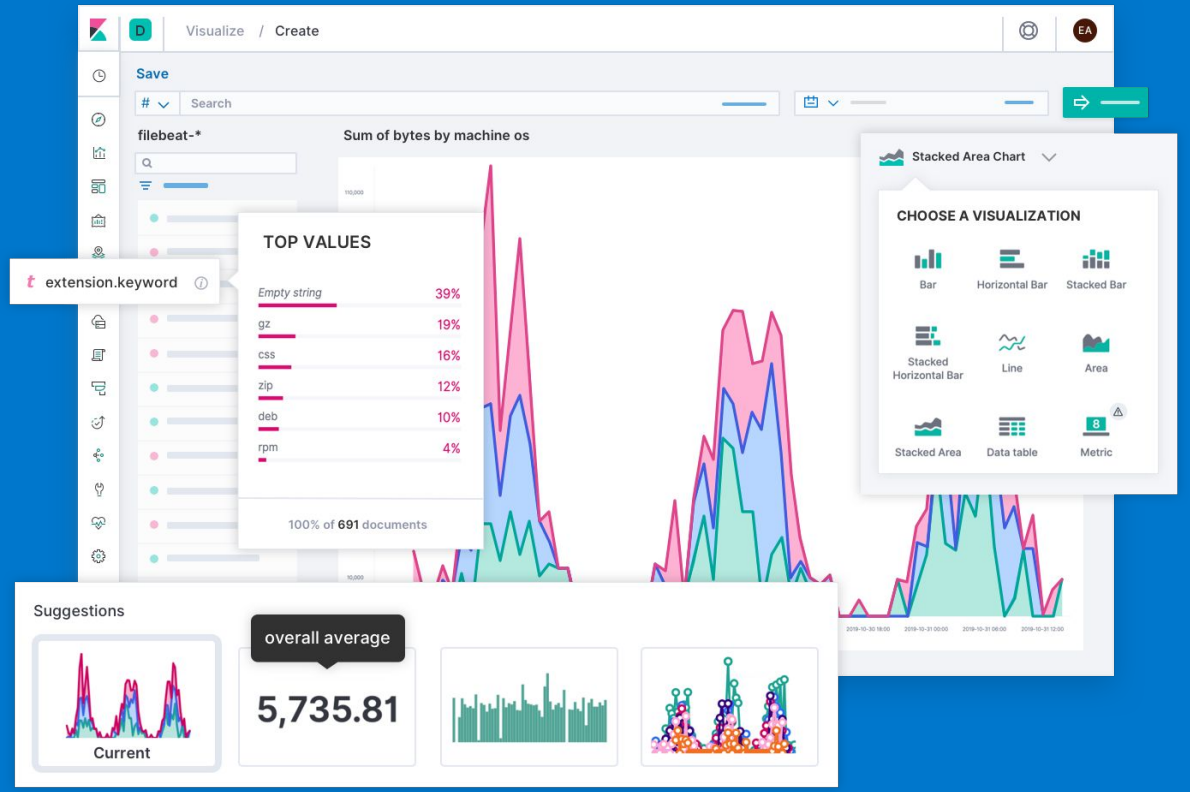


# Lens

## Your data in front of you
Explore your data fields in a click

## Drag and drop
Go from nothing to visual insights with a single mouse gesture

## Smart Suggestions
Let Lens help guide your analysis with useful chart suggestions






elastic

# Region map

## Join by ISO code

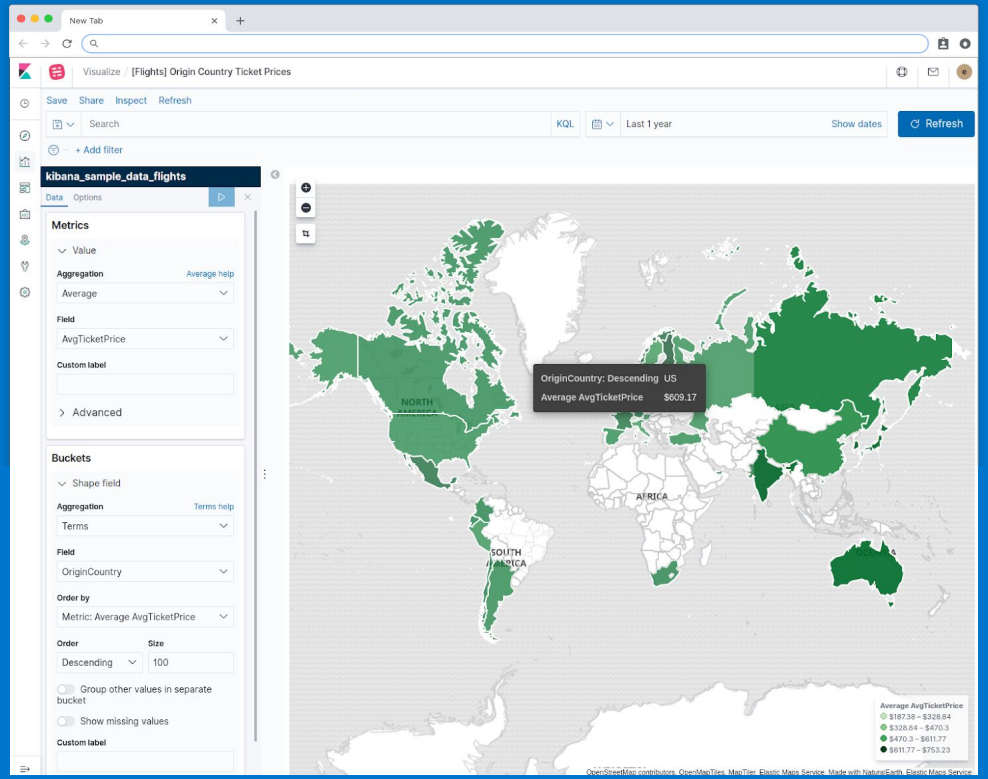
Join your data with ISO country/region codes to create choropleth maps

## Metrics

Get the count, average, and other metrics

## Basemap

Use the default map or a custom WMS server






elastic

# Coordinate map

## Aggregations

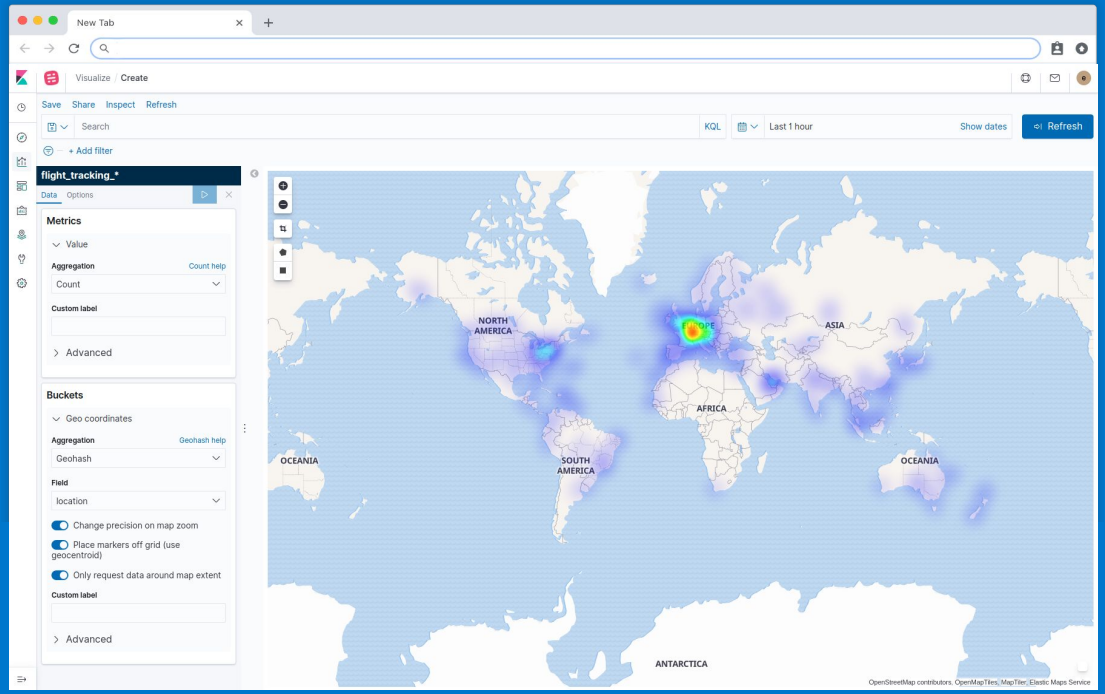
Show your data in clusters, geohash grid, or as a heatmap

## Metrics

Get the count, average, and other metrics

## Basemap

Use the default map or a custom WMS server






elastic

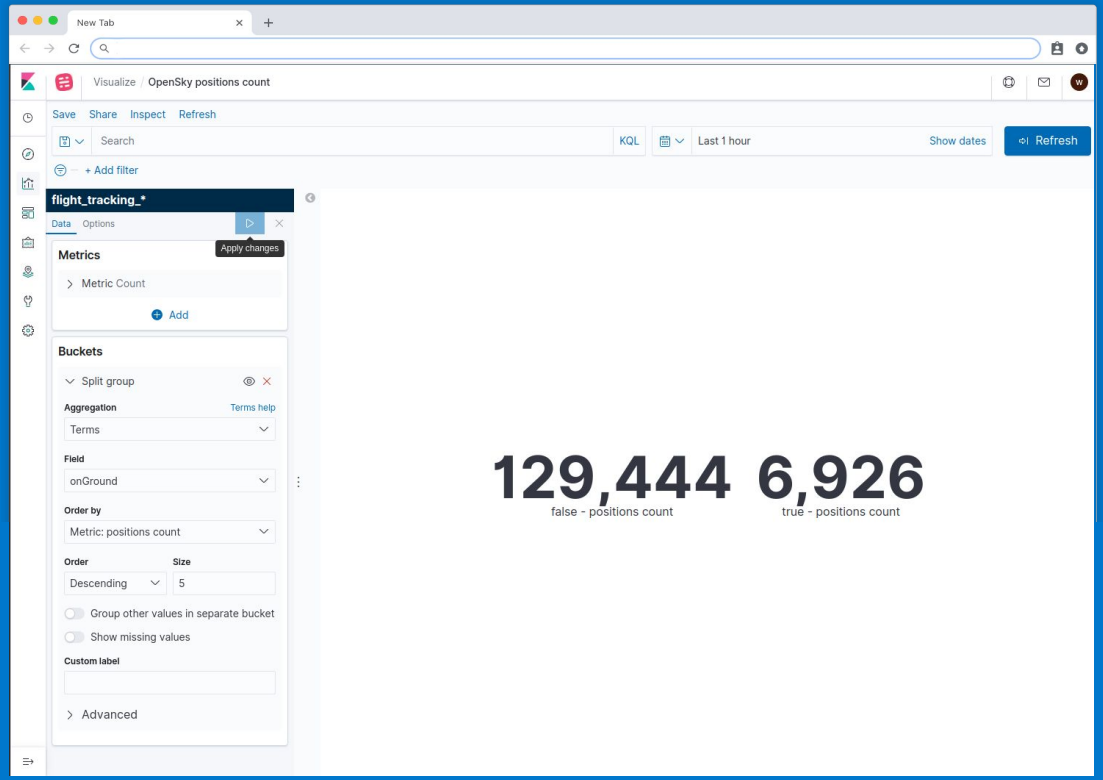
# Metric

## Metrics

Select the aggregation for your data: count, sum, avg, ...

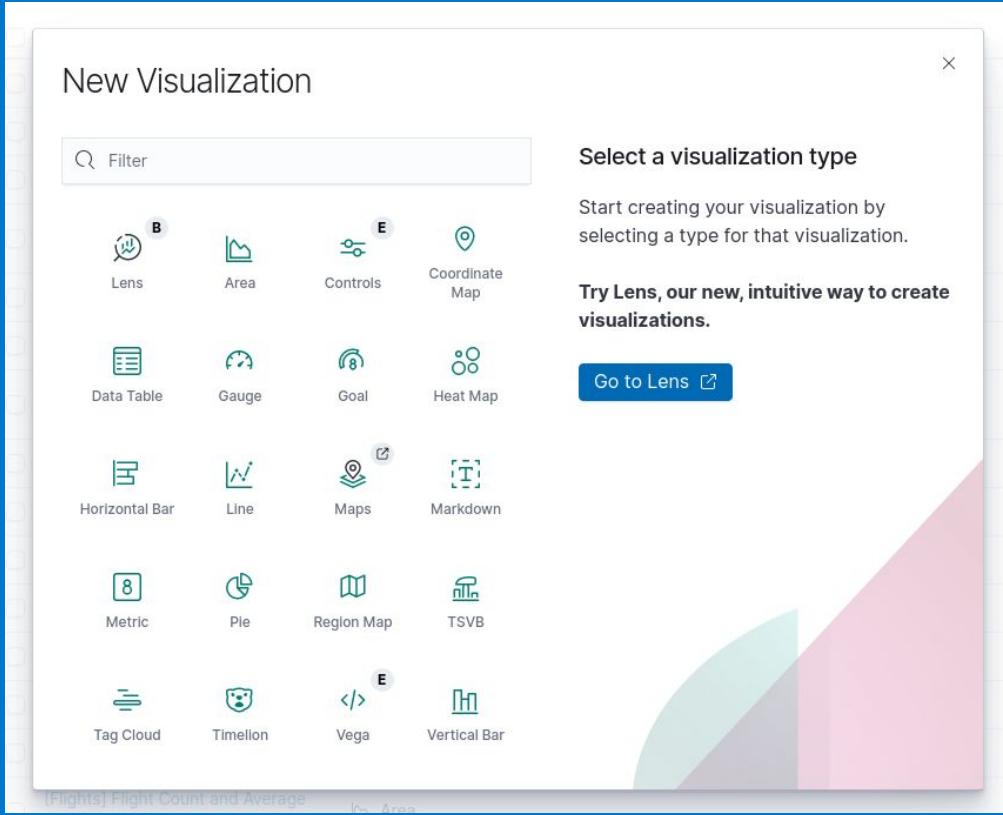
## Buckets

Get a single value or bucket your results by terms, range, ...



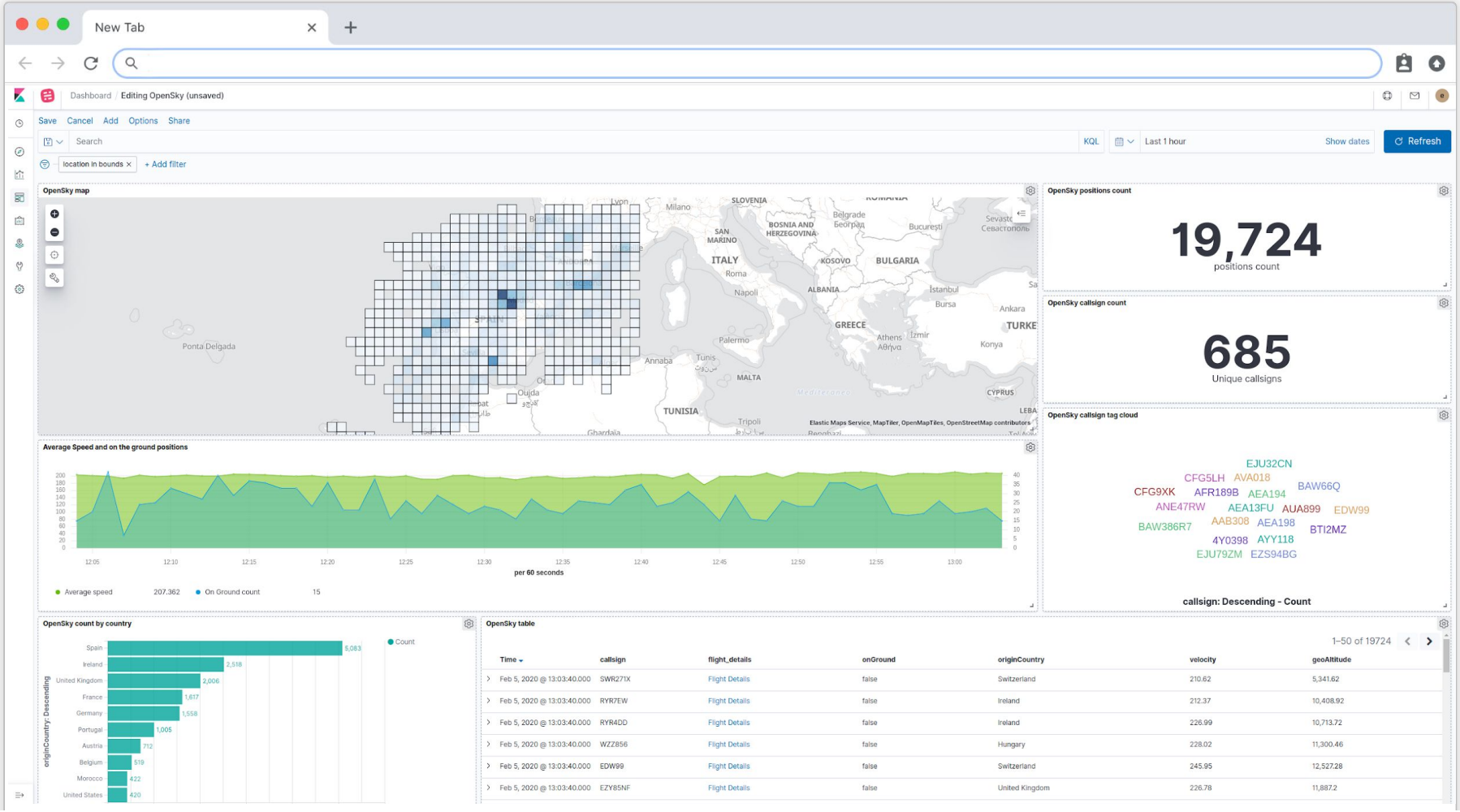



elastic




# … and many other options

elastic


New Tab
Dashboard / Editing OpenSky (unsaved)
Save Cancel Add Options Share
Search
KQL
Last 1 hour
Show dates
Refresh
location in bounds
+ Add filter
OpenSky map
Elastic Maps Service, MapTiler, OpenMapTiles, OpenStreetMap contributors
OpenSky positions count
19,724
positions count
OpenSky callsign count
685
Unique callsigns
OpenSky callsign tag cloud
EJU32CN
CFG5LH AVA018
BAW66Q
CFG9XK AFR189B AEA194
ANE47RW AEA13FU AUA899 EDW99
BAW386R7 AAB308 AEA198
BTI2MZ
4Y0398 AYY118
EJU79ZM EZS94BG
callsign: Descending - Count
Average Speed and on the ground positions
per 60 seconds
Average speed 207.362
On Ground count 15
OpenSky count by country
originCountry: Descending
Count
Spain 5,083
Ireland 2,518
United Kingdom 2,006
France 1,617
Germany 1,558
Portugal 1,005
Austria 712
Belgium 519
Morocco 422
United States 420
OpenSky table
1–50 of 19724
Time callsign flight_details onGround originCountry velocity geoAltitude
Feb 5, 2020 @ 13:03:40.000 SWR271X Flight Details false Switzerland 210.62 5,341.62
Feb 5, 2020 @ 13:03:40.000 RYR7EW Flight Details false Ireland 212.37 10,408.92
Feb 5, 2020 @ 13:03:40.000 RYR4DD Flight Details false Ireland 226.99 10,713.72
Feb 5, 2020 @ 13:03:40.000 WZZ856 Flight Details false Hungary 228.02 11,300.46
Feb 5, 2020 @ 13:03:40.000 EDW99 Flight Details false Switzerland 245.95 12,527.28
Feb 5, 2020 @ 13:03:40.000 EZY85NF Flight Details false United Kingdom 226.78 11,887.2

# Dashboards

- Combine visualizations: **panels**
- Time Range + Search Bar + Filters
- Panels generate filters to **drill down**
- Panels can have **custom time range** filter
- **Sharing**
- **Exporting** as PDF and PNG

# Canvas

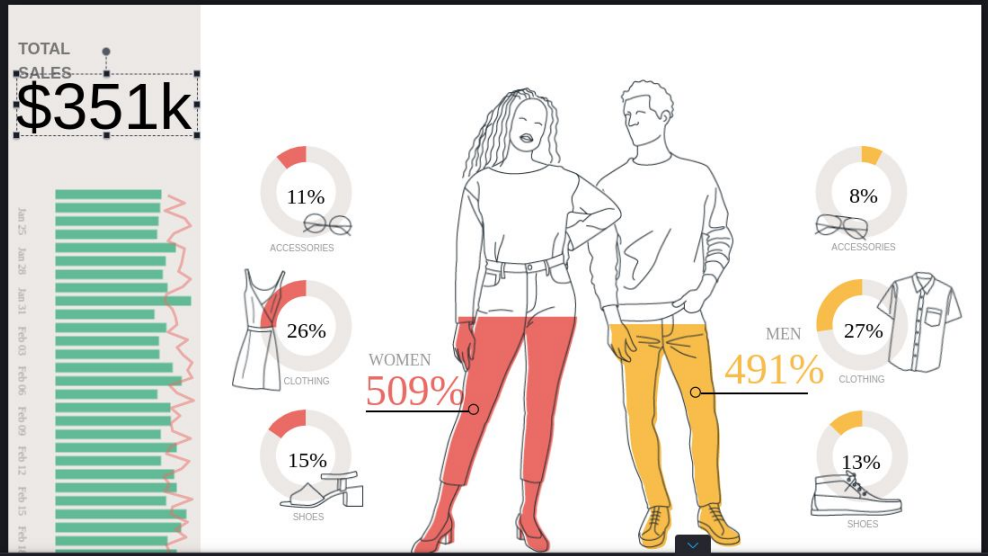
- **Slides** driven by your data: **live** and **pixel perfect** infographies
- Who is Canvas for?
  - **kiosks** and **show rooms**
  - **frequent** presenters
- Charts, tables, markdown text, all backed by **Elasticsearch SQL**
- Powerful **expression editor**
- Checkout: stand out with canvas

[eCommerce] Revenue Tracking

5dbfbf991cb04e9597f6709c52e5a219.eu-central-1.aws.cloud.es.io:9243/app/canvas#/workpad/workpad-e08b9bdb-ec14-4339-94c4-063bddfd610e/page/1

Canvas [eCommerce] Revenue Tracking

Manage assets | Add element




Selected element

Display | Data

Change your data source →

Elasticsearch SQL query

```
SELECT
sum(taxless_total_price) AS
sum_total_price FROM
"kibana_sample_data_ecommerc
e"
```

Preview | Save

```
essql
  query="SELECT sum(taxless_total_price) AS sum_total_price FROM \"kibana_sample_data_ecommerce\""
| math "sum_total_price"
| formatNumber "$0a"
| metric
  metricFont={font family="'Avenir', Helvetica, Arial, sans-serif" size=72 align="left" color="#000000" weight="normal" underline=false italic=false}
| render
```

Run | Close

Learn expression syntax | Maximize editor

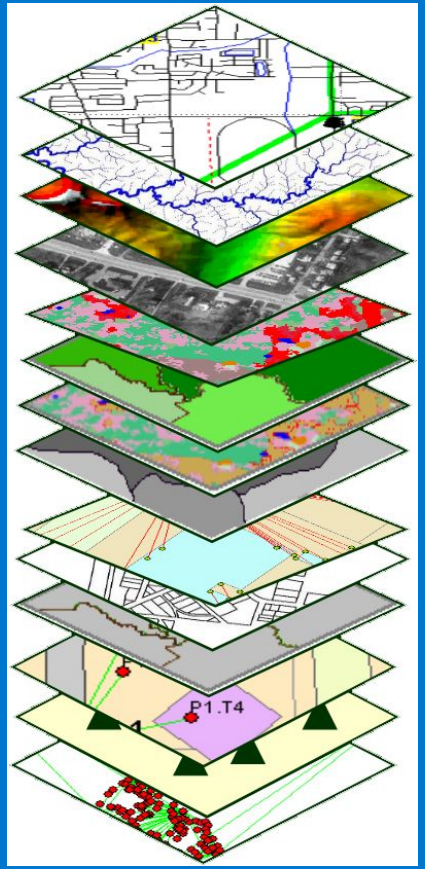
[eCommerce] Revenue Tracking Page 1 of 2

Expression editor

# Intermission: Intro to Geographical Information Systems

Jorge Sanz
Ramiro Aznar

elastic




*“A geographic information system or geographical information system (GIS) is a system designed to capture, store, manipulate, analyze, manage, and present all types of spatial or geographical data.”*

elastic

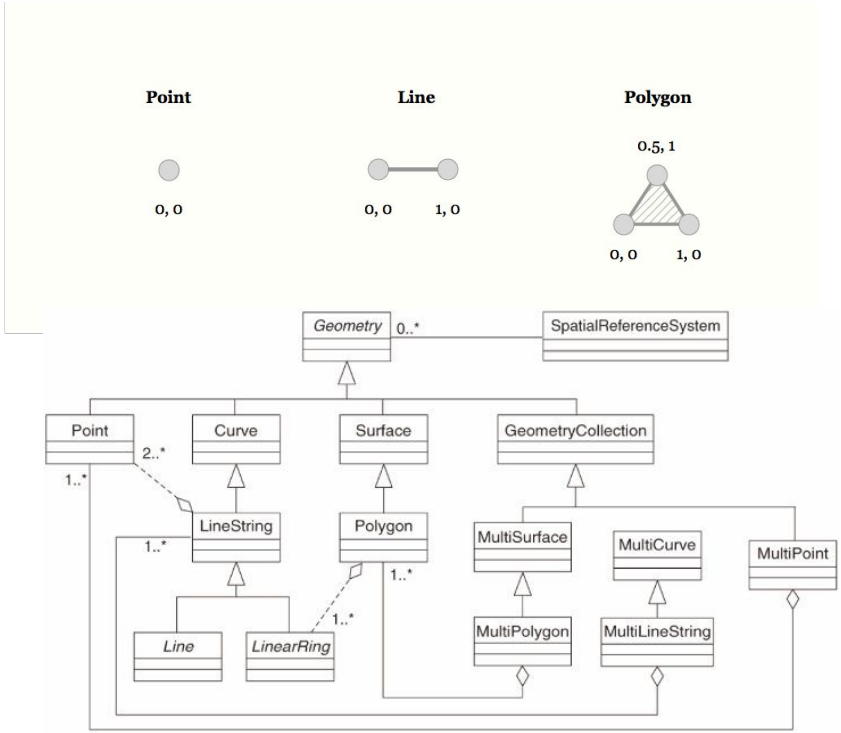
# Spatial Data

## Rasters and **vectors**

**Types**: points, lines and polygons.

Some vector data keeps track of **topology**, the relationships between different shapes.

Vector **formats**: .shp, .GeoJSON, .KML, .gpkg....






elastic

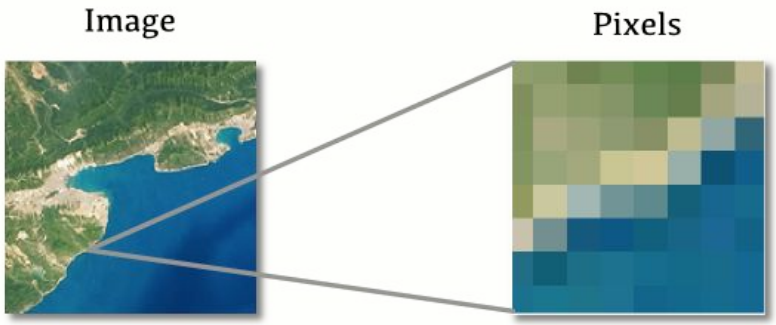
# Spatial Data

## **Rasters** and vectors

“A raster data type is, in essence, any type of **digital image** represented by reducible and enlargeable **grids**.”

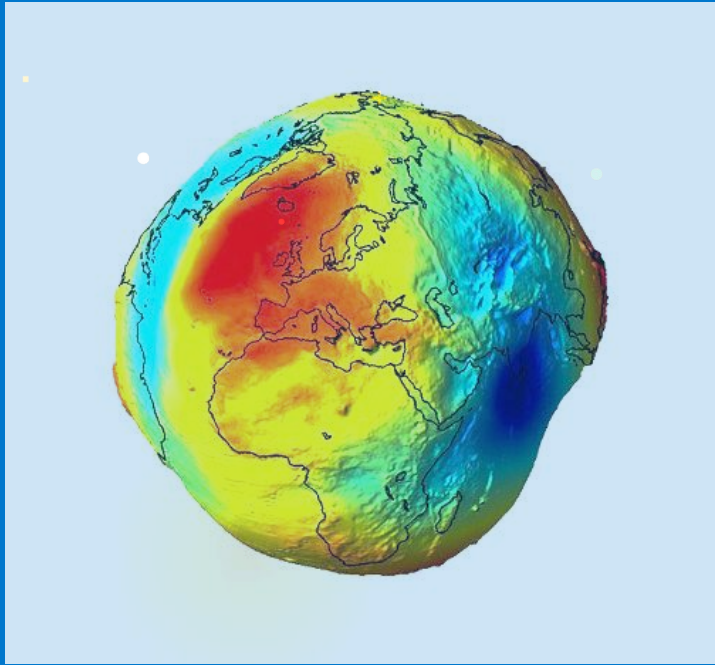
“Raster data type consists of rows and columns of cells, with each cell storing a **single value**. (...) While a raster cell stores a single value, it can be extended by using **raster bands**.”

Raster **formats**: .jpg, .tiff, .GeoTiff...



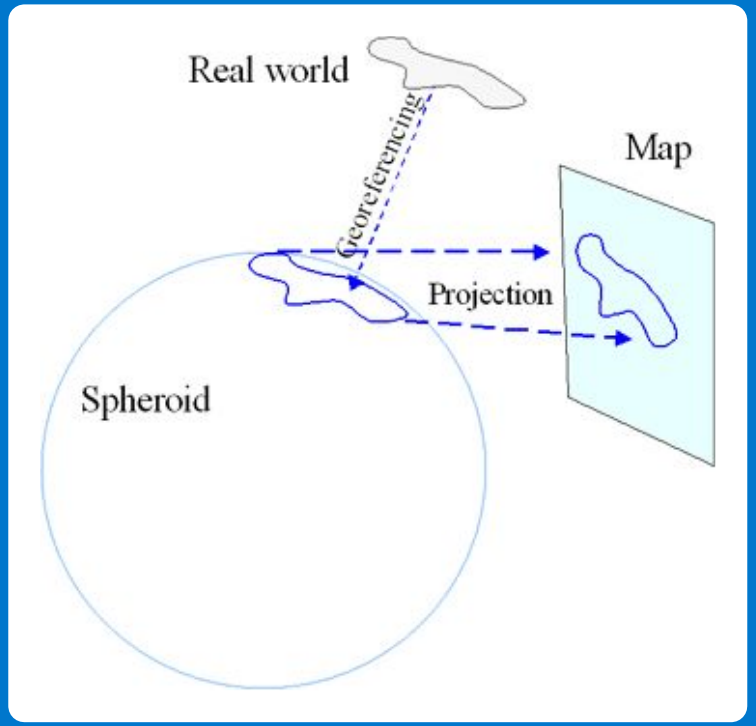



elastic



# Earth shape... is complicated

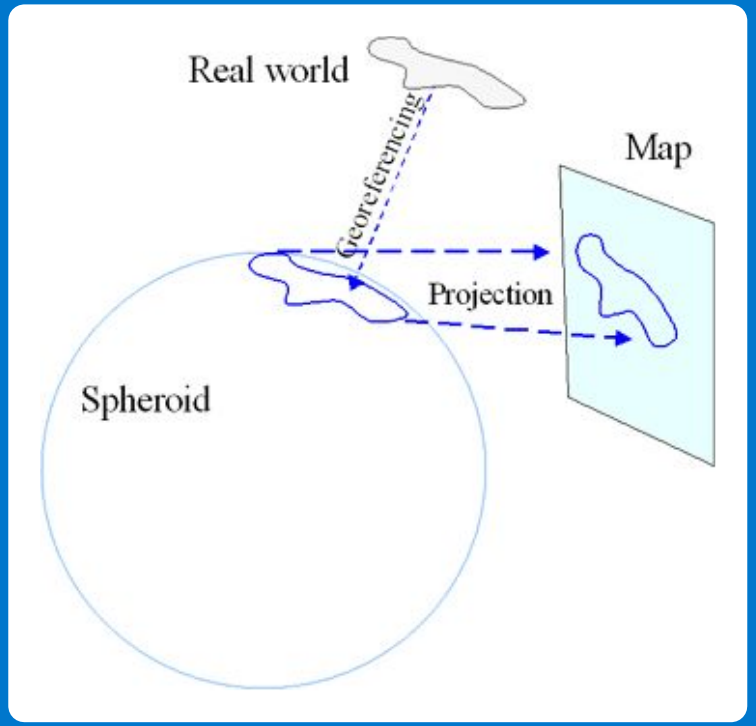
elastic




*"**Projections** are what we call the mathematical equations that do the trick of turning the world into some flat shape that fits on a printout or a computer screen."*

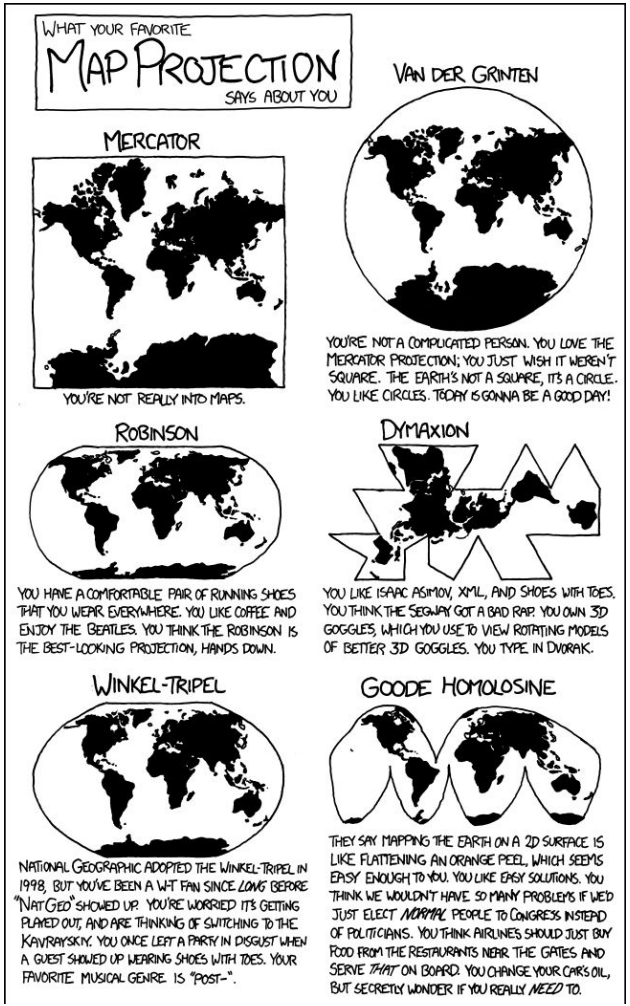
*Projections are a compromise between **shape**, **angles**, and **distances***

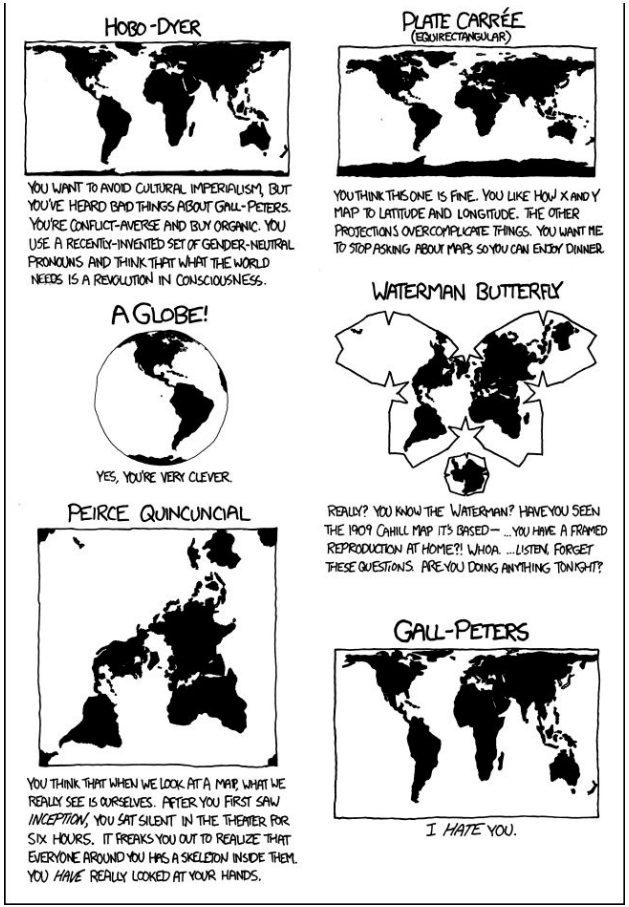
elastic




*"A **Spatial Reference System Identifier** (SRID) is a unique value used to unambiguously identify projected, unprojected, and local spatial coordinate system definitions."*

elastic




https://xkcd.com/977/



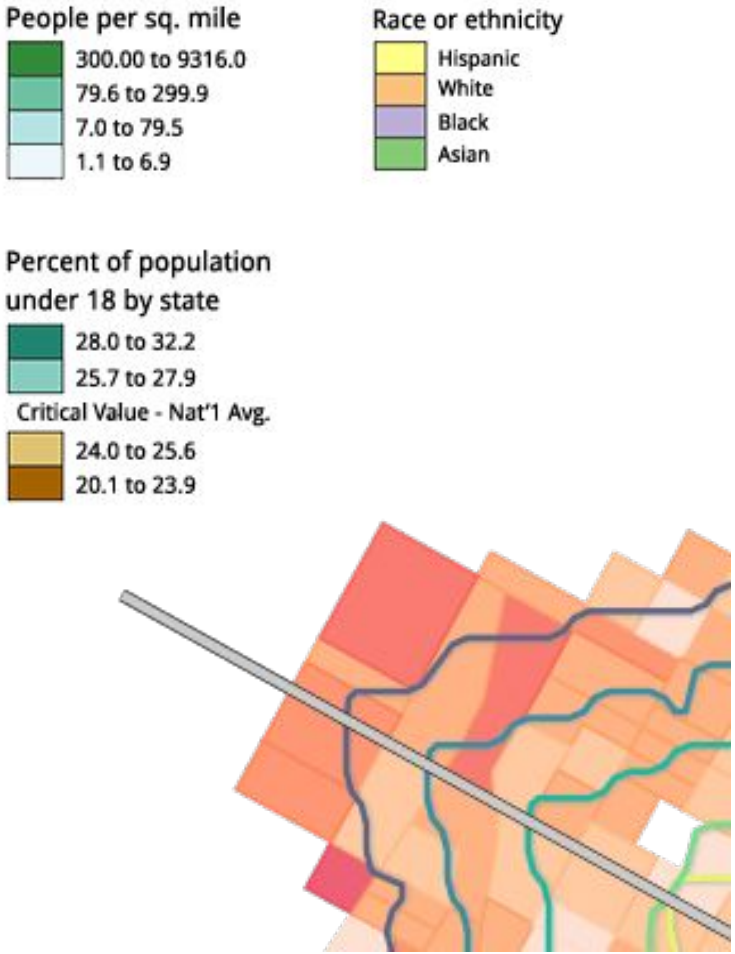
elastic


Tartu
New York
San Francisco

# Symbolization

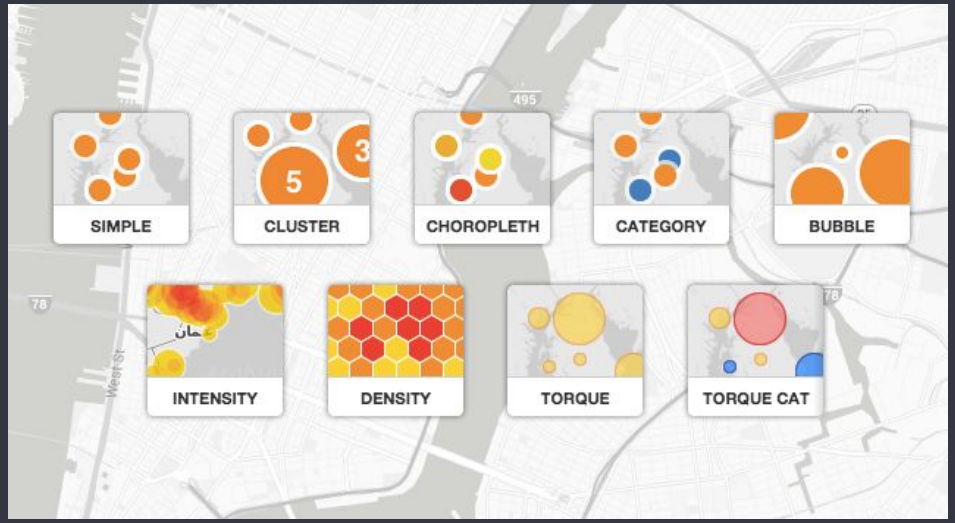
## Qualitative and quantitative

- Sequential ramps
- Diverging ramps
- Qualitative palettes



# Map Types

- Points:
  - Heatmap
  - Density
  - Clusters & Bubbles
- Thematic:
  - Choropleth (sequential)
  - Category (categorical)






elastic

# Elastic Maps

## Bringing GIS concepts to Kibana

elastic

# Elastic Maps

## Multiple Sources, One Map

Build maps with multiple layers and from multiple data sources

## Individual Documents

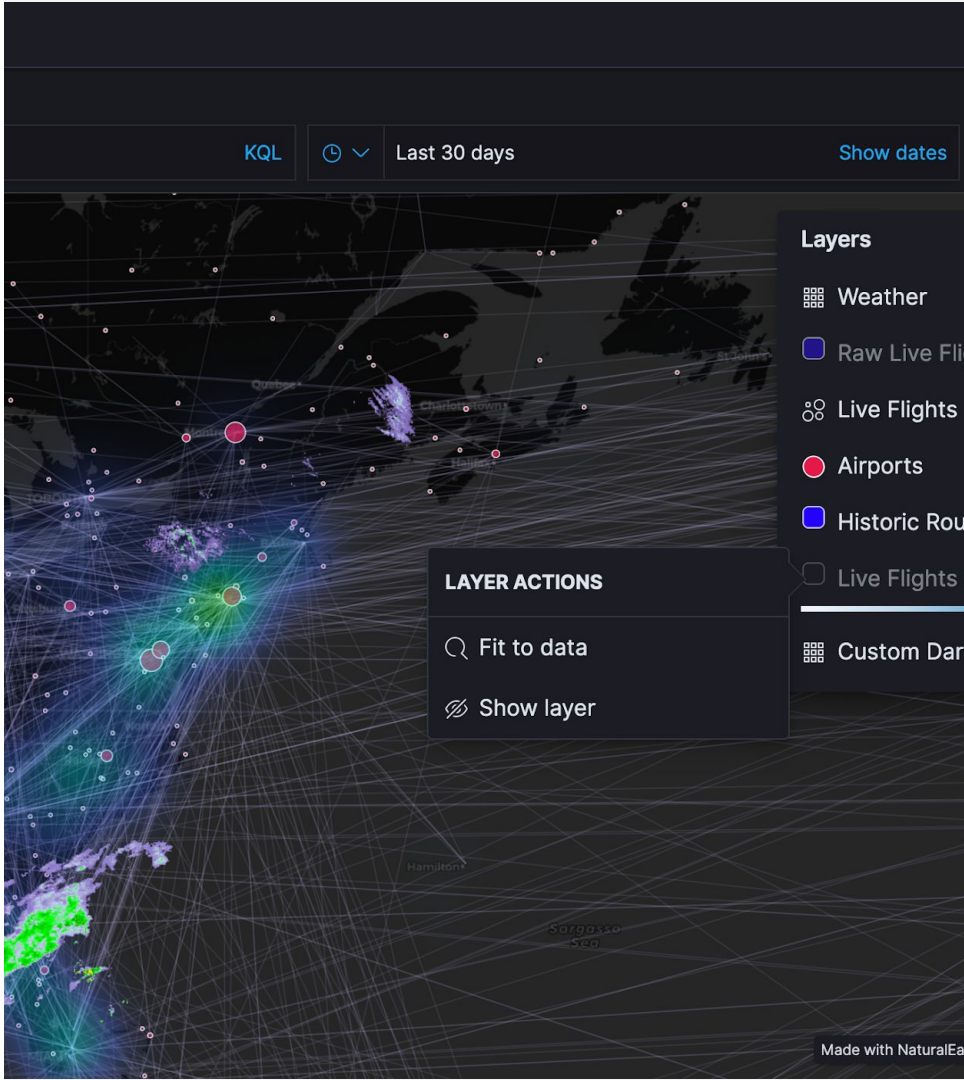
Map individual `geo_points` and `geo_shapes` on a map, and control exactly when you want to see them

## Client Side Styling

Choose colors for borders & fills and dynamically size them

## Out-of-the-Box Maps

Take full advantage of the free Elastic Maps Service to join your data with our shapes



# Elastic Maps Service

maps.elastic.co

## 18 zoom levels

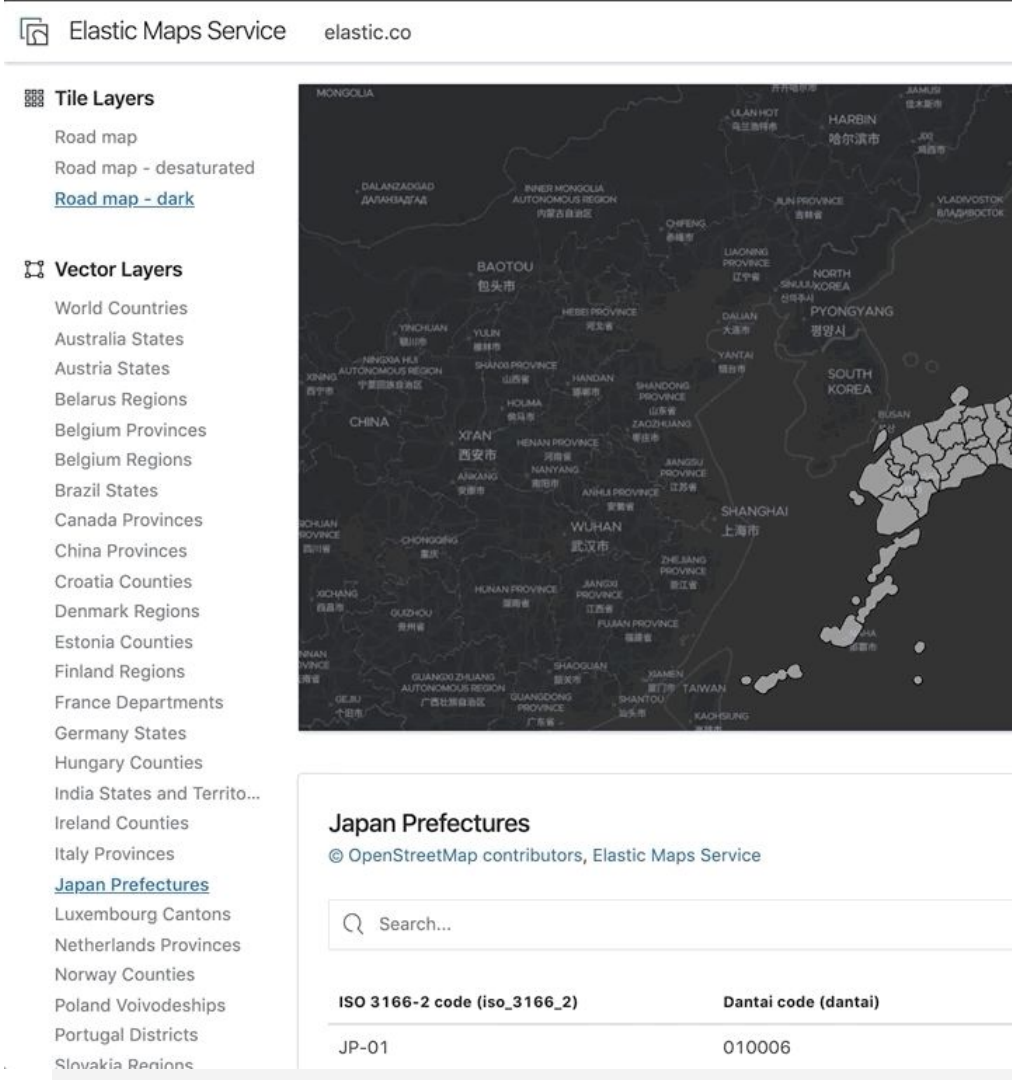
Render from **world** to **city** level data

## Three basemap styles

See your data on top of beautifully designed **dark**, **light**, or **colorful** basemaps

## Administrative Boundaries

More than **60 layers** for country region boundaries



*Learning is pleasurable (?) but doing is the height of enjoyment*

**Novalis**

# Practice time

- Create a new map*
- Add the airports GeoJSON layer*
- Add the OpenSky positions as a grid aggregation (z0 to z6)
- Add the OpenSky positions as single documents (z6 to z24)
- Add tooltip elements, play with the legend, etc
- ...

*If using my Elastic Cloud account, remember to save all new indexes and objects with the wecode00 prefix

# Agenda

1. Intro to the Elastic stack
2. Lab set up and data import
3. Kibana overview: Dashboards, Lens, Maps, canvas
4. Elasticsearch (geo) queries
5. Web mapping 101

# Elasticsearch queries

Small intro to ES query DSL

## Use Kibana DevTools Console

Or curl, postman, ...

## Creating new indexes

How to define field types, including geo

## Inserting

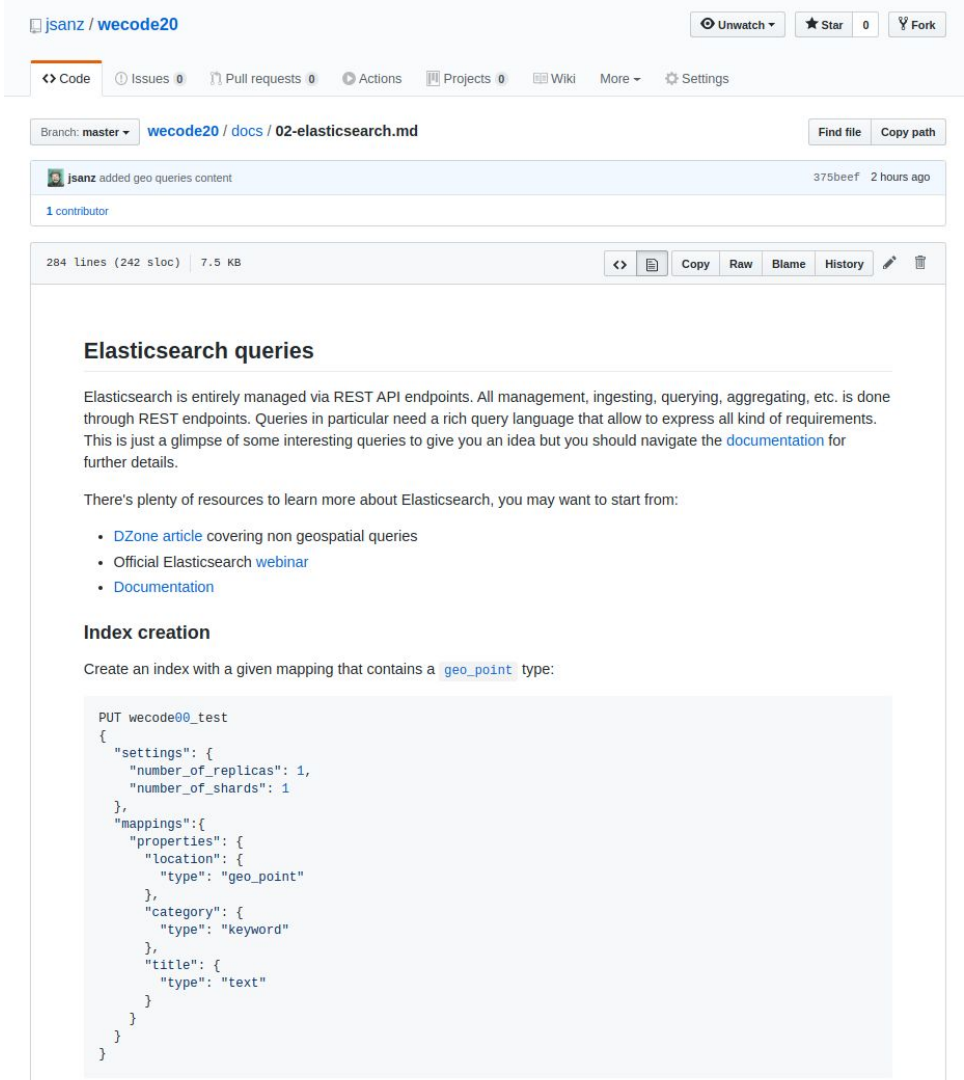
Adding data to your index

## Querying

Retrieving individual documents

## Aggregations

Put your data into buckets



# Elasticsearch geo queries

ES querying geospatial features

## Searching

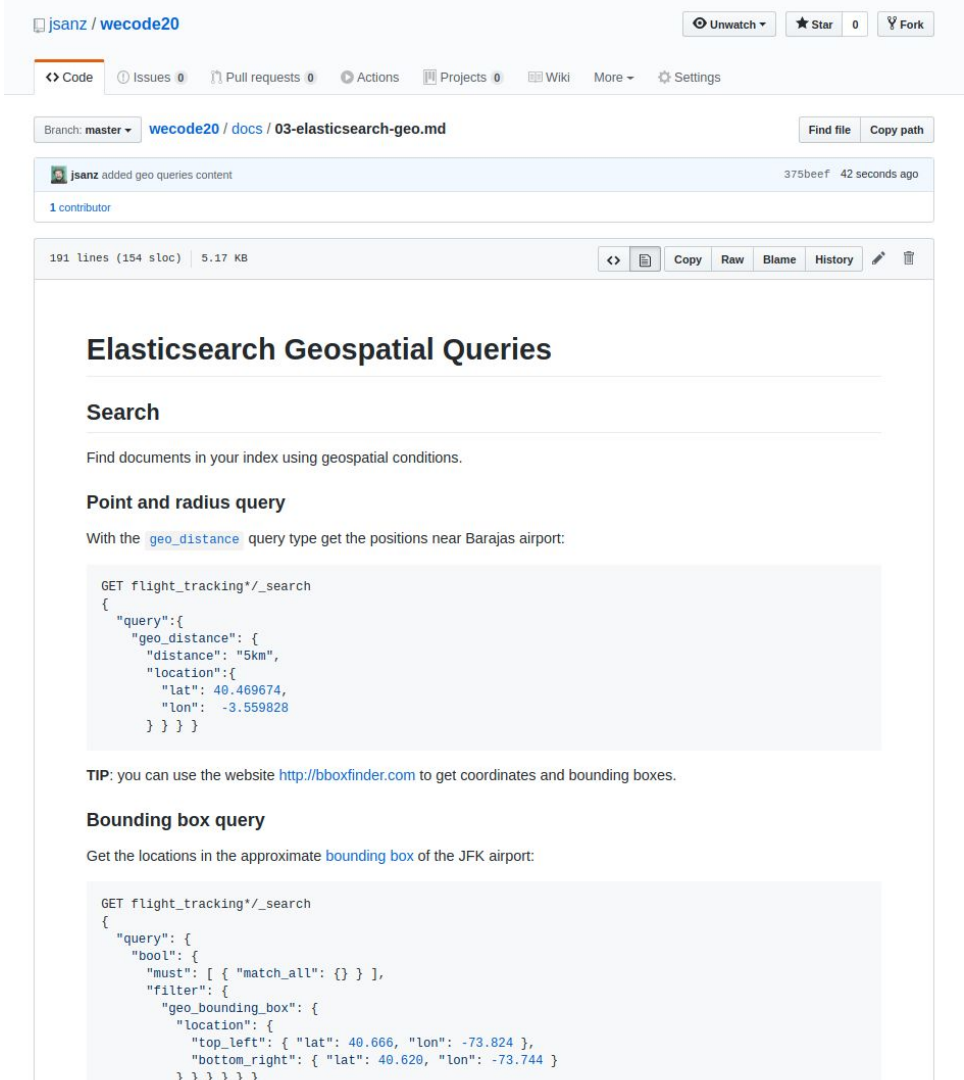
Finding documents with point & radius, bounding box, and polygon queries

## Metric aggs

Find the centroid or the bounding box of your query results

## Bucket aggs

Aggregate your results using geospatial features like rings or grids



jsanz / wecode20

Unwatch | Star 0 | Fork

Code | Issues 0 | Pull requests 0 | Actions | Projects 0 | Wiki | More | Settings

Branch: master | wecode20 / docs / 03-elasticsearch-geo.md | Find file | Copy path

jsanz added geo queries content — 375beef — 42 seconds ago

1 contributor

191 lines (154 sloc) | 5.17 KB | Copy | Raw | Blame | History

### Elasticsearch Geospatial Queries

#### Search

Find documents in your index using geospatial conditions.

#### Point and radius query

With the `geo_distance` query type get the positions near Barajas airport:

```
GET flight_tracking*/_search
{
  "query":{
    "geo_distance": {
      "distance": "5km",
      "location":{
        "lat": 40.469674,
        "lon":  -3.559828
      } } } }
```

**TIP**: you can use the website http://bboxfinder.com to get coordinates and bounding boxes.

#### Bounding box query

Get the locations in the approximate bounding box of the JFK airport:

```
GET flight_tracking*/_search
{
  "query": {
    "bool": {
      "must": [ { "match_all": {} } ],
      "filter": {
        "geo_bounding_box": {
          "location": {
            "top_left": { "lat": 40.666, "lon": -73.824 },
            "bottom_right": { "lat": 40.620, "lon": -73.744 }
          } } } } }
```

# Agenda

1. Intro to the Elastic stack
2. Lab set up and data import
3. Kibana overview: Dashboards, Lens, Canvas, and Maps
4. Elasticsearch (geo) queries
5. Web mapping 101

# Quick intro to web mapping

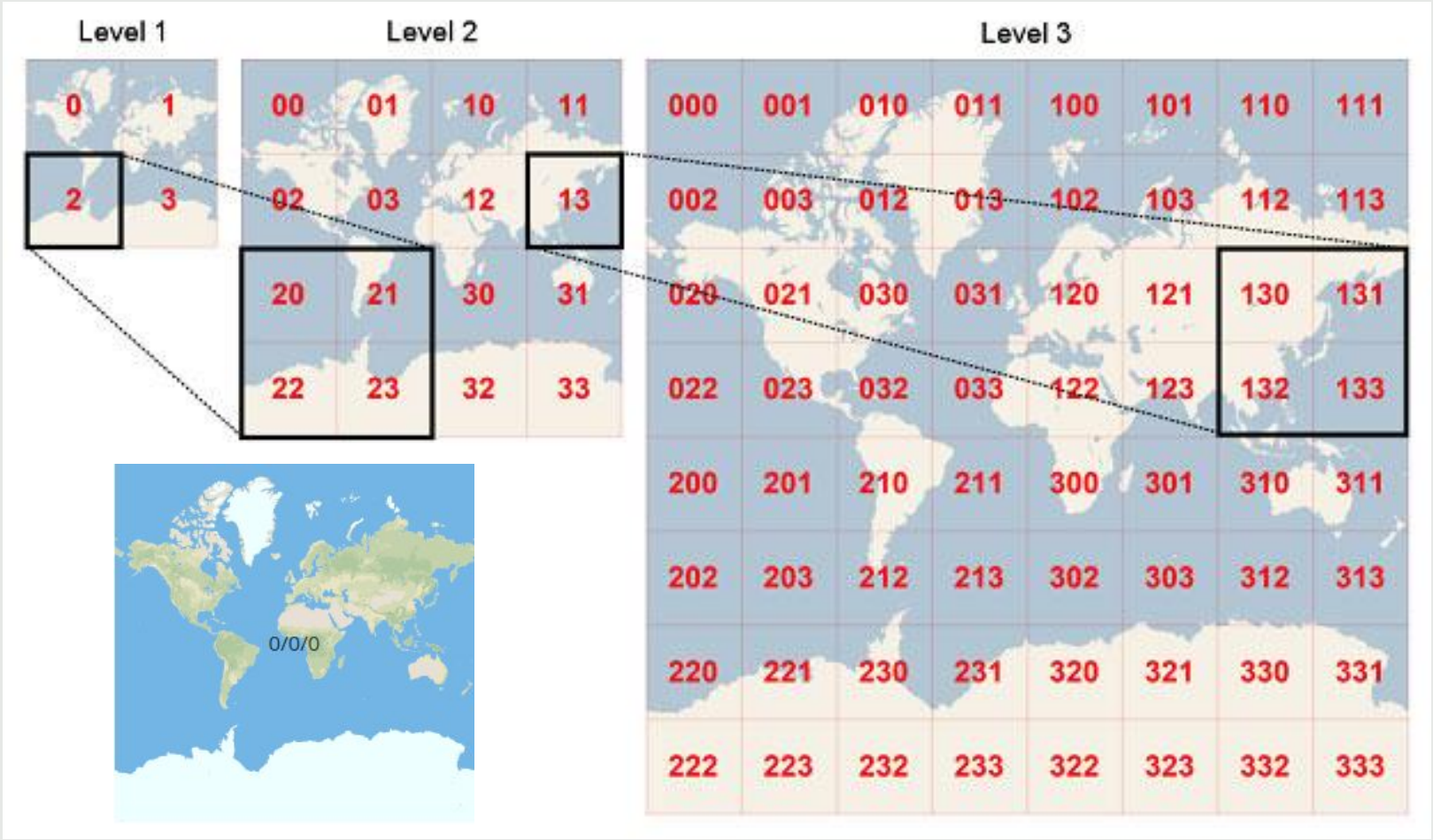
elastic


"A **tiled** web map, or **slippy** map is displayed in a browser by seamlessly joining dozens of individually image files (**vector** or **raster**) over the internet."

A web map can be **static** or **dynamic**.

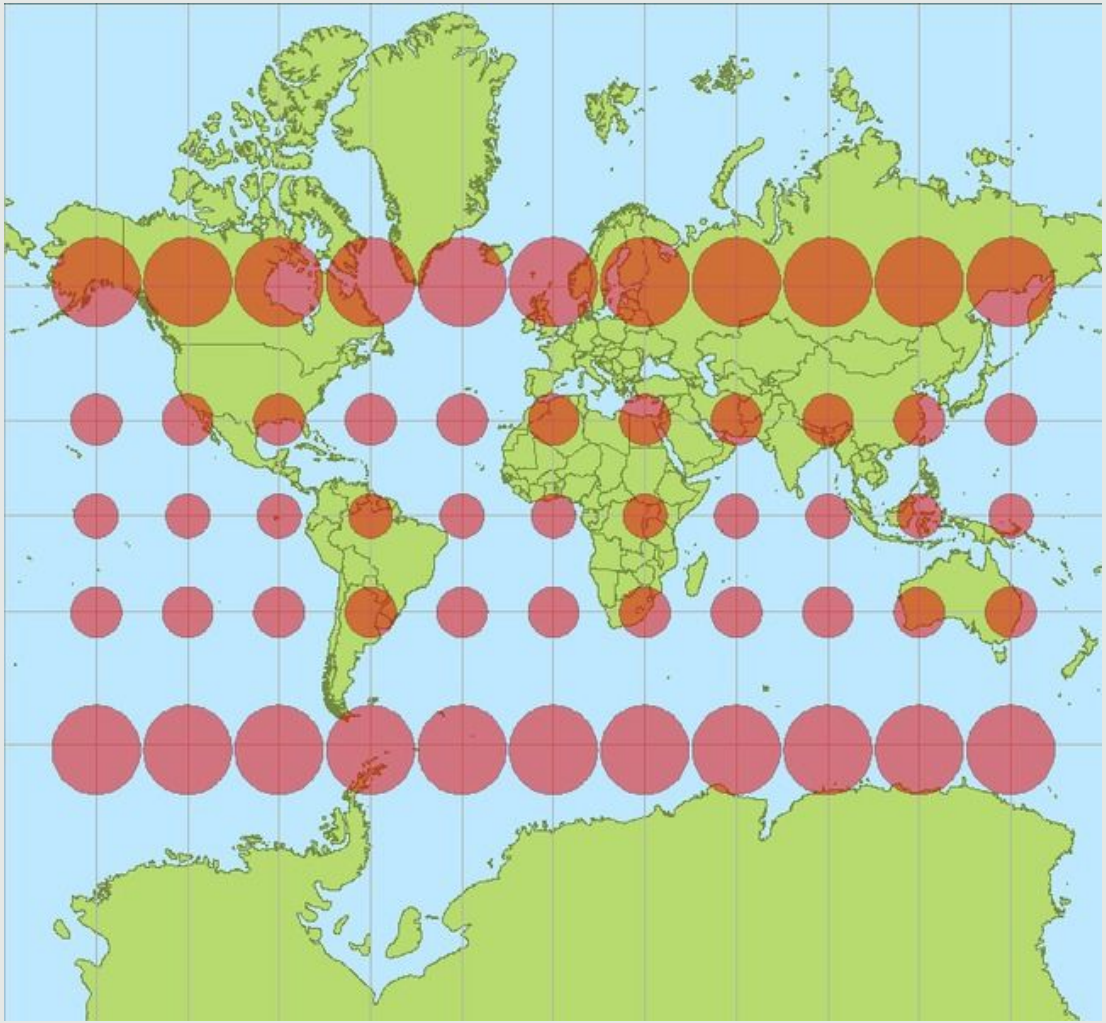


elastic


Level 1
Level 2
Level 3
0
1
2
3
00
01
10
11
02
03
12
13
20
21
30
31
22
23
32
33
000
001
010
011
100
101
110
111
002
003
012
013
102
103
112
113
020
021
030
031
120
121
130
131
022
023
032
033
122
123
132
133
200
201
210
211
300
301
310
311
202
203
212
213
302
303
312
313
220
221
230
231
320
321
330
331
222
223
232
233
322
323
332
333
0/0/0

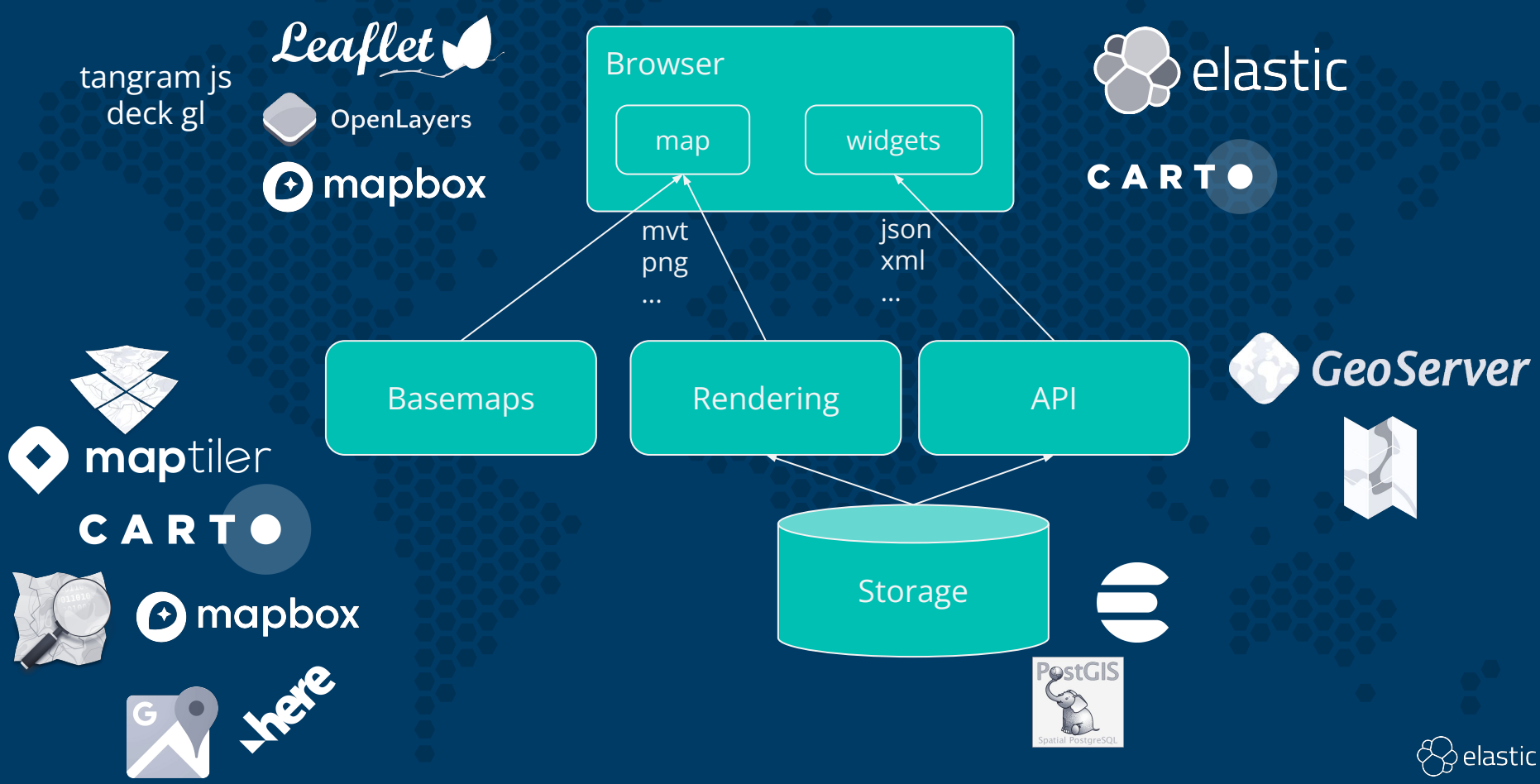


elastic





elastic


tangram js
deck gl
Leaflet
OpenLayers
mapbox
Browser
map
widgets
elastic
CARTO
mvt
png
...
json
xml
...
Basemaps
Rendering
API
GeoServer
maptiler
CARTO
mapbox
Storage
PostGIS
Spatial PostgreSQL
here
elastic

jsanz / **opensky-viewer**

Code | Issues 0 | Pull requests 0 | Actions | Projects 0

A demonstration on consuming Elasticsearch geospatial data using Mapb

Manage topics

**18** commits | **1** branch | **0** releas

**TypeScript** 89.9% | **HTML** 6.5%

Branch: **master**

**jsanz** fix

| | |
|---|---|
| backend | popup and style improvemnets |
| frontend | fix |
| .gitignore | docs |
| Procfile | uploading compiled files |
| README.md | typo |
| package-lock.json | refactor into two folders for back and |
| package.json | popup and style improvemnets |

# OpenSky viewer example

Example application that provides a simple API to query a Elastics map. The application is split into front and back-end subprojects:

- `backend` : NestJS project with controllers and service logic se located at `config.ts` . Using environment variables or an `.e` or any host. Adapting this to other configurations would need t

  The API exposes:

  - `/airports/geojson` : a GeoJSON representation of the e
  - `/positions/last/geojson` : filtering the last 15 minutes,

# Open Sky

**Last position:**

**Callsign**
SWR105V

**Origin Country**
Switzerland

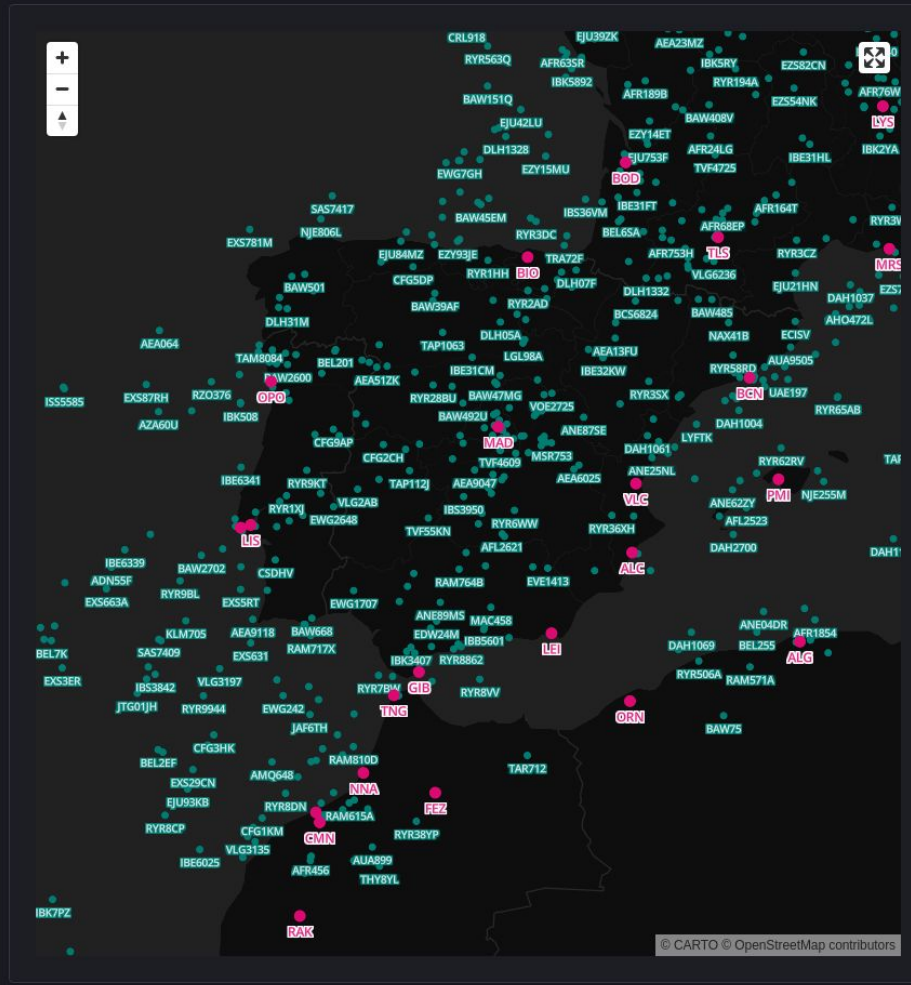
**Altitude m**
8648.7 m

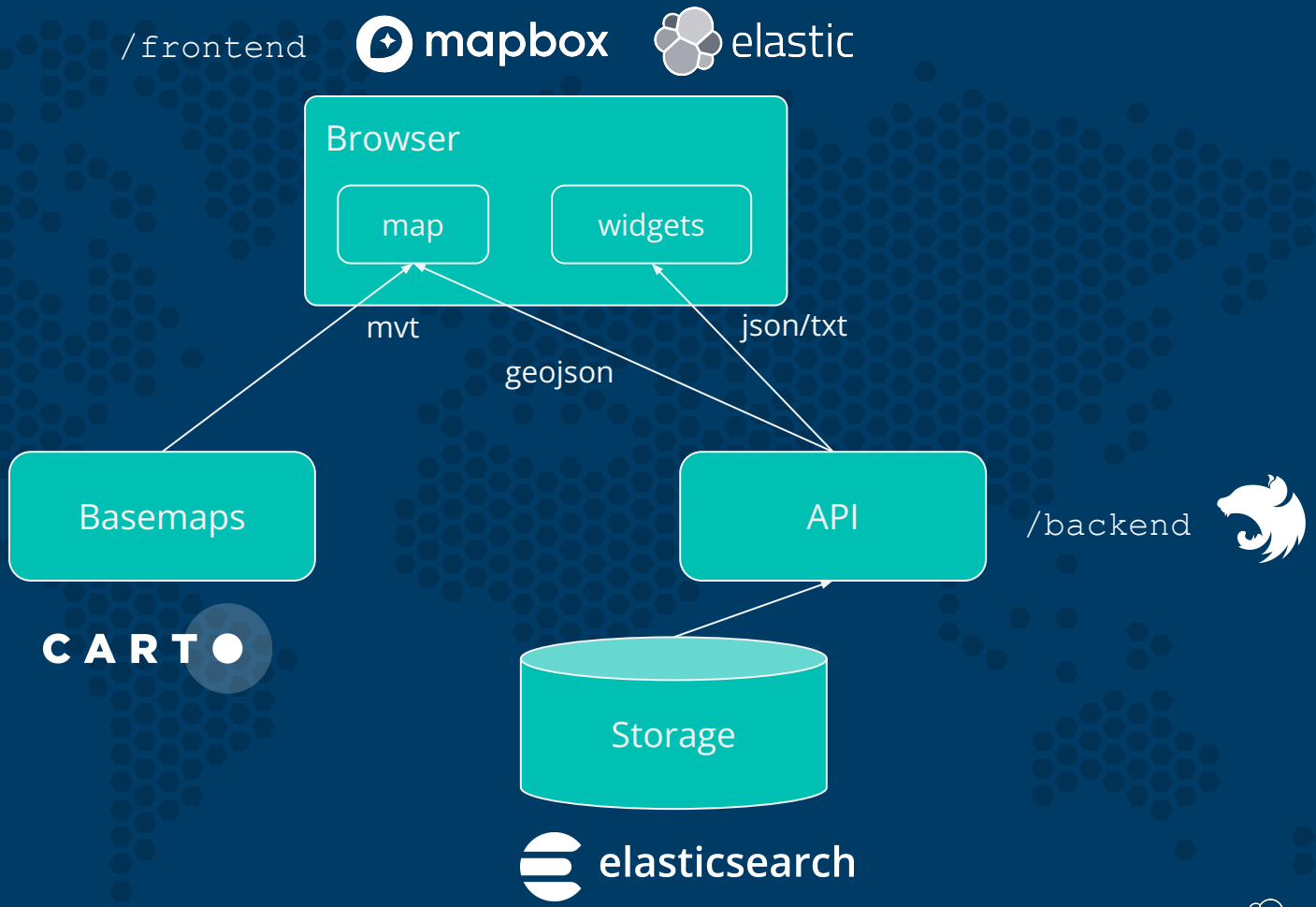
**Speed m/s**
252.55

**Position time**
12:28:00 PM UTC

**Positions count:**
9,163,427

Refresh




/frontend
mapbox
elastic
Browser
map
widgets
mvt
geojson
json/txt
Basemaps
API
/backend
CARTO
Storage
elasticsearch


# Thanks!!

Jorge Sanz
2020-02-08, Kibana, Elastic
xurxosanz jsanz

https://ela.st/wecode-2020
https://ela.st/wecode-2020-slides