

Data Driven Dashboards

with Kibana and Elasticsearch

Philipp Krenn

@xeraa



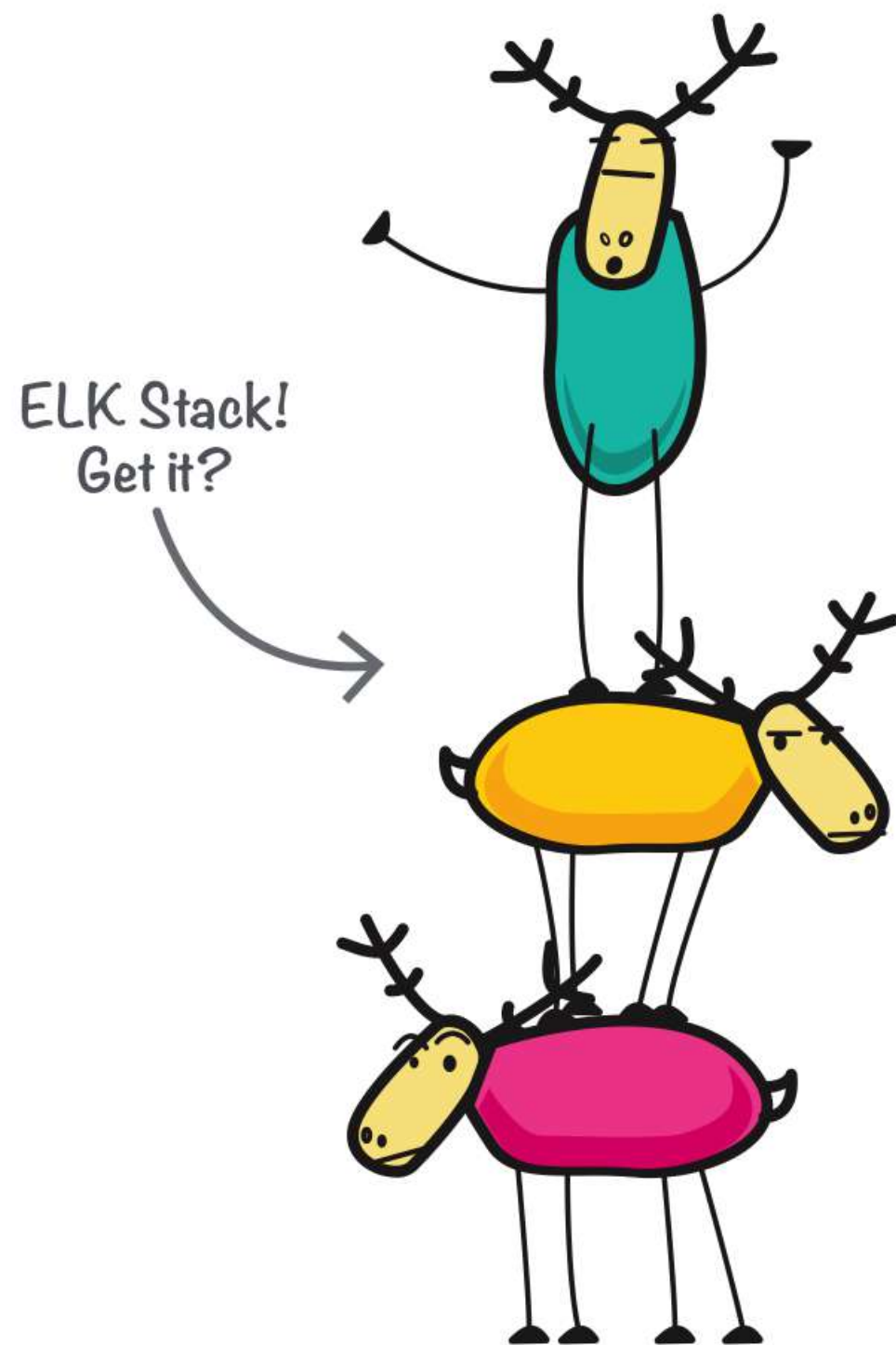
Developer 🥑



elasticsearch



kibana  logstash

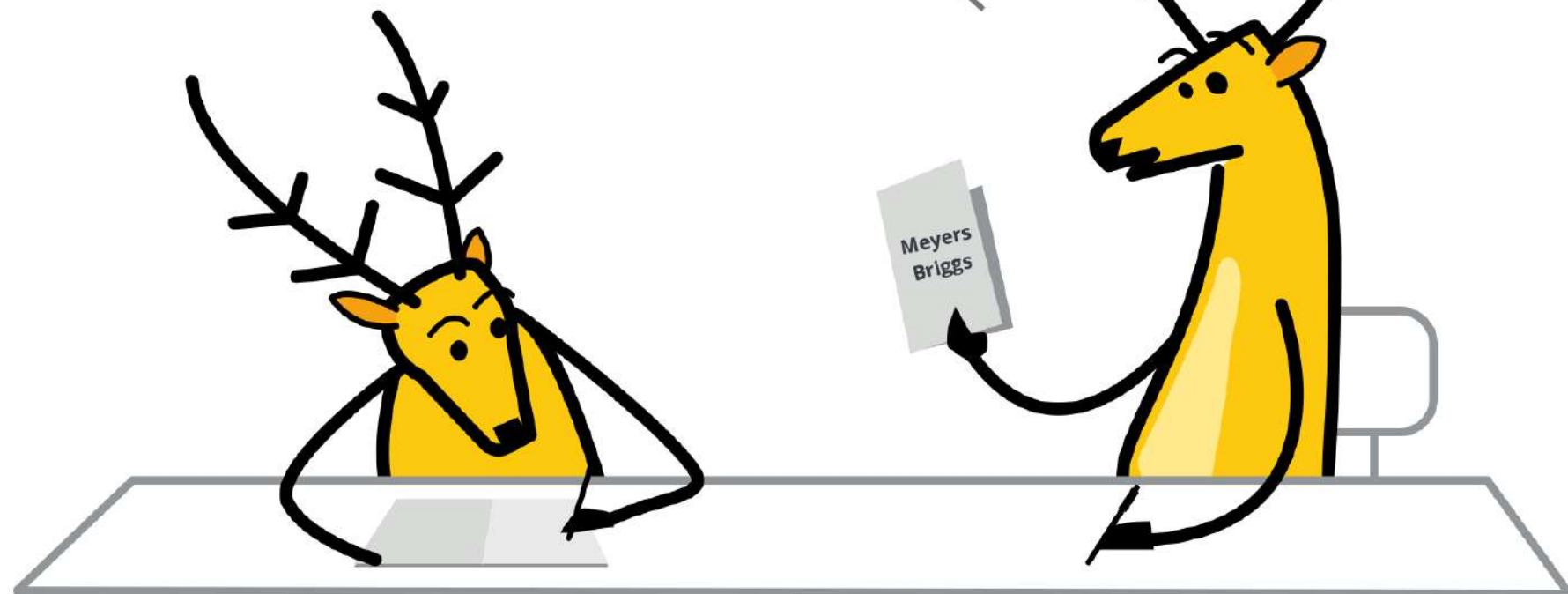


E Elasticsearch

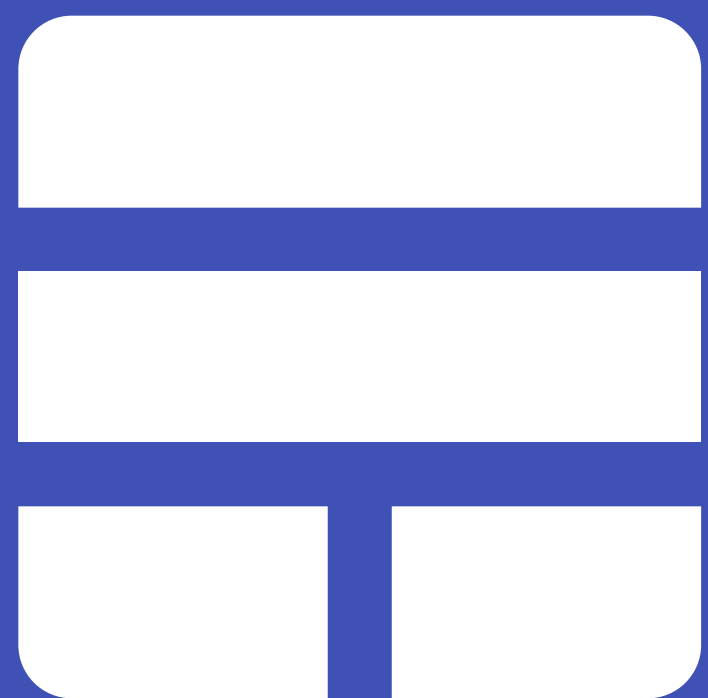
L Logstash

K Kibana

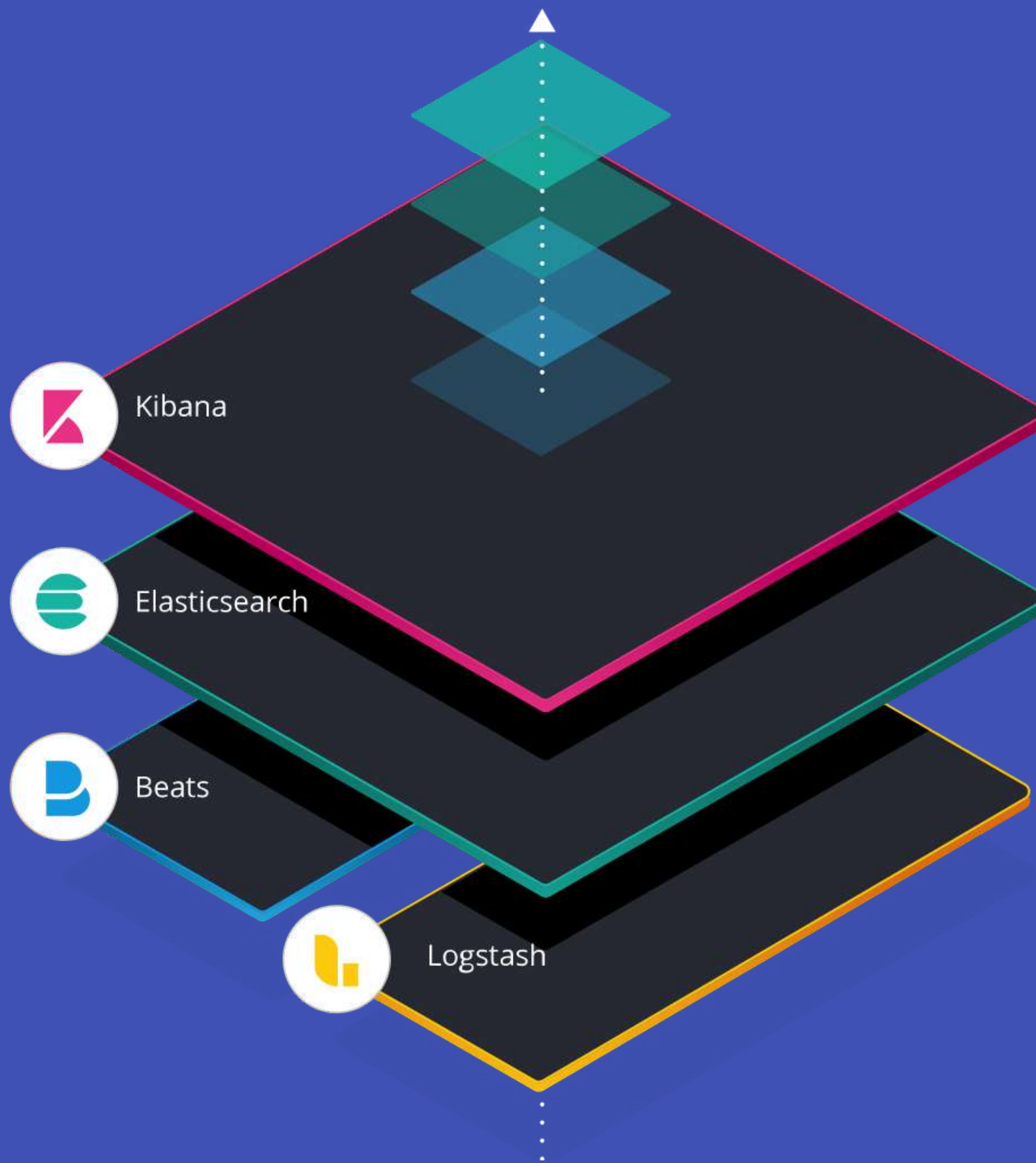
*Apparently, I'm an
ELKB personality.*







elastic stack



Run the Stack Cloud

Instances

All instances5

aws.master.r41

aws.data.highio.i32

aws.ml.m51

aws.kibana.r41

eu-west-1a



AWS.DATA.HIGHIO.I3

Instance #7

v7.3.2

2 GB RAM

data

master

ingest

JVM memory pressure15%

Disk usage1.56% of 60 GB

Stop routing



AWS.ML.M5

Instance #9

v7.3.2

2 GB RAM

ml

Disk usage0% of 4 GB

Stop routing

eu-west-1b



AWS.DATA.HIGHIO.I3

Instance #6

v7.3.2

2 GB RAM

data

master eligible

ingest

JVM memory pressure18%

Disk usage18.95% of 60 GB

Stop routing



AWS.KIBANA.R4

Instance #2

v7.3.2

1 GB RAM

Disk usage0% of 2 GB

Stop routing

eu-west-1c



AWS.MASTER.R4

Tiebreaker #8

v7.3.2

1 GB RAM

master eligible

JVM memory pressure16%

Disk usage0% of 2 GB

Stop routing

Run the Stack

Docker

```
---
version: '2'
services:

  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:$ELASTIC_VERSION
    environment:
      - "ES_JAVA_OPTS=-Xms512m -Xmx512m"
      - discovery.type=single-node
    mem_limit: 1g
    volumes:
      - esdata1:/usr/share/elasticsearch/data
    ports:
      - 9200:9200

  kibana:
    image: docker.elastic.co/kibana/kibana:$ELASTIC_VERSION
    links:
      - elasticsearch
    ports:
      - 5601:5601

volumes:
  esdata1:
    driver: local
```

Sample Data

eCommerce orders

Kibana: Discover

17 days ago to 16 day from now


```
> Oct 6, 2019 @ 01:45:36.000 category: Men's Shoes, Men's Clothing currency: EUR customer_first_name: Youssef
customer_full_name: Youssef Jensen customer_gender: MALE customer_id: 31 customer_last_name: Jensen
customer_phone: day_of_week: Saturday day_of_week_i: 5 email: youssef@jensen-family.zzz
manufacturer: Low Tide Media order_date: Oct 6, 2019 @ 01:45:36.000 order_id: 592109 products: {
"base_price": 49.99, "discount_percentage": 0, "quantity": 1, "manufacturer": "Low Tide Media",

> Oct 6, 2019 @ 01:31:12.000 category: Women's Clothing, Women's Accessories currency: EUR customer_first_name: Sonya
customer_full_name: Sonya Smith customer_gender: FEMALE customer_id: 28 customer_last_name: Smith
customer_phone: day_of_week: Saturday day_of_week_i: 5 email: sonya@smith-family.zzz
manufacturer: Oceanavigations, Pyramidindustries order_date: Oct 6, 2019 @ 01:31:12.000 order_id: 592097
```

Two Types of Data

Entity-centric vs timeseries

Entity-Centric

Transformations

Group by: `customer_full_name.keyword`

Aggregations: `products.price.sum` and
`oder_id.value_count`

D

Machine Learning / Data Frames / Create transform

PK

1

Define pivot

Index pattern

kibana_sample_data_ecommerce

Query

e.g. method:GET -is:active

Use a query string to filter the source data (optional).

Group by

customer_full_name.keyword

Add a group by field ...

Aggregations

products.price.sum

order_id.value_count

Add an aggregation ...

X

Advanced editor

Source index kibana_sample_data_ecommerce

showing 5 of 28 fields

	category ↑	currency	customer_first_na...	customer_full_na...	customer_gender
✓	Men's Accessories	EUR	Robert	Robert Hodges	MALE
✓	Men's Accessories	EUR	Ahmed Al	Ahmed Al Garza	MALE
✓	Men's Accessories	EUR	Robert	Robert Shaw	MALE
✓	Men's Accessories	EUR	Ahmed Al	Ahmed Al Morrison	MALE
✓	Men's Accessories, Men's Clothing	EUR	Kamal	Kamal James	MALE

Rows per page: 5

< 1 2 3 4 5 ... 200 >

Data frame pivot preview

customer_full_name.keyword	order_id.value_count	products.price.sum ↓
Abd Shaw	5	622.89453125
Abd Graham	5	601.8828125
Abd King	4	460.9140625
Abd Evans	4	435.90625
Abd Barnes	4	410.9453125

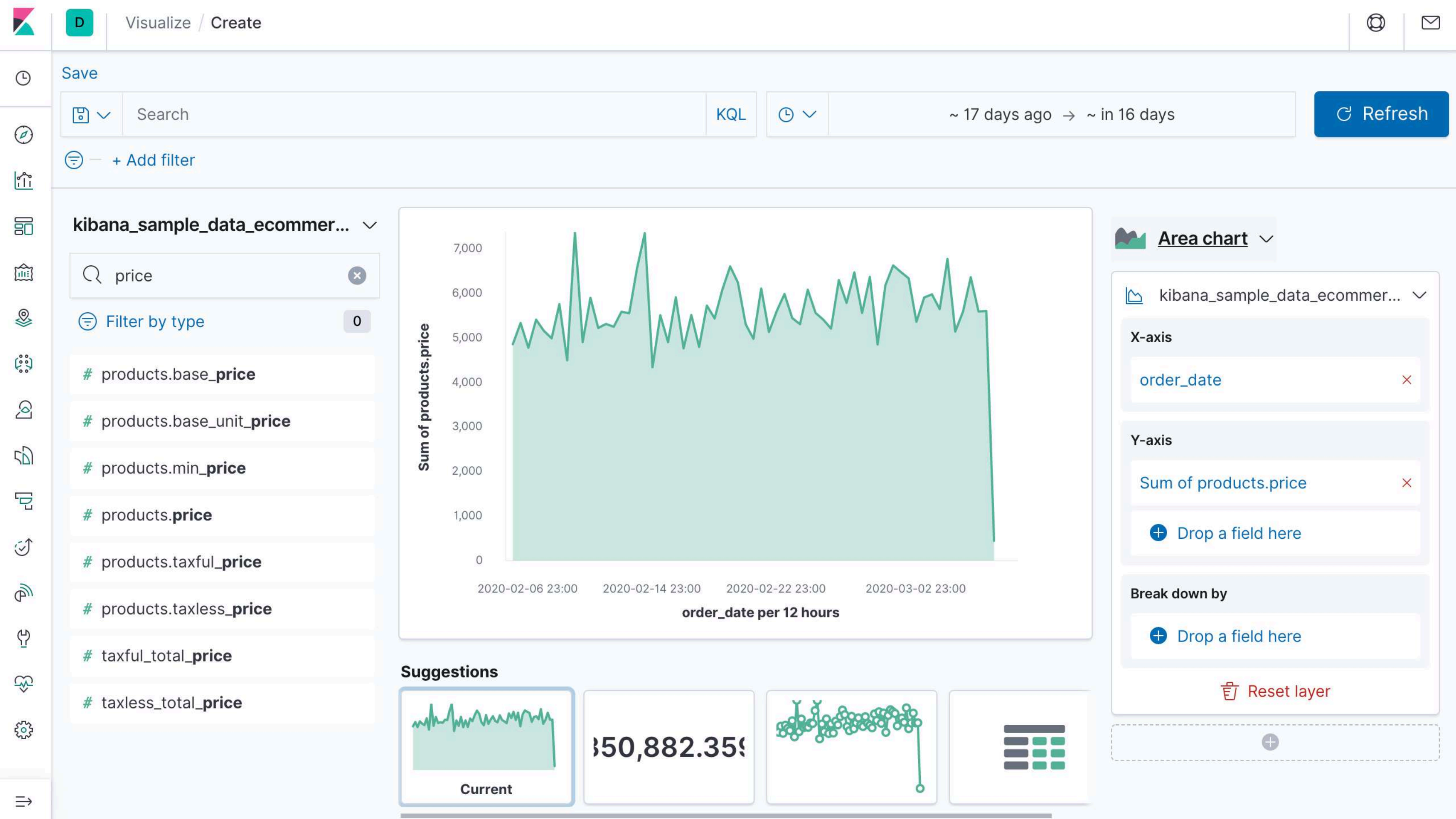
Rows per page: 5

< 1 2 3 4 5 ... 20 >

Timeseries

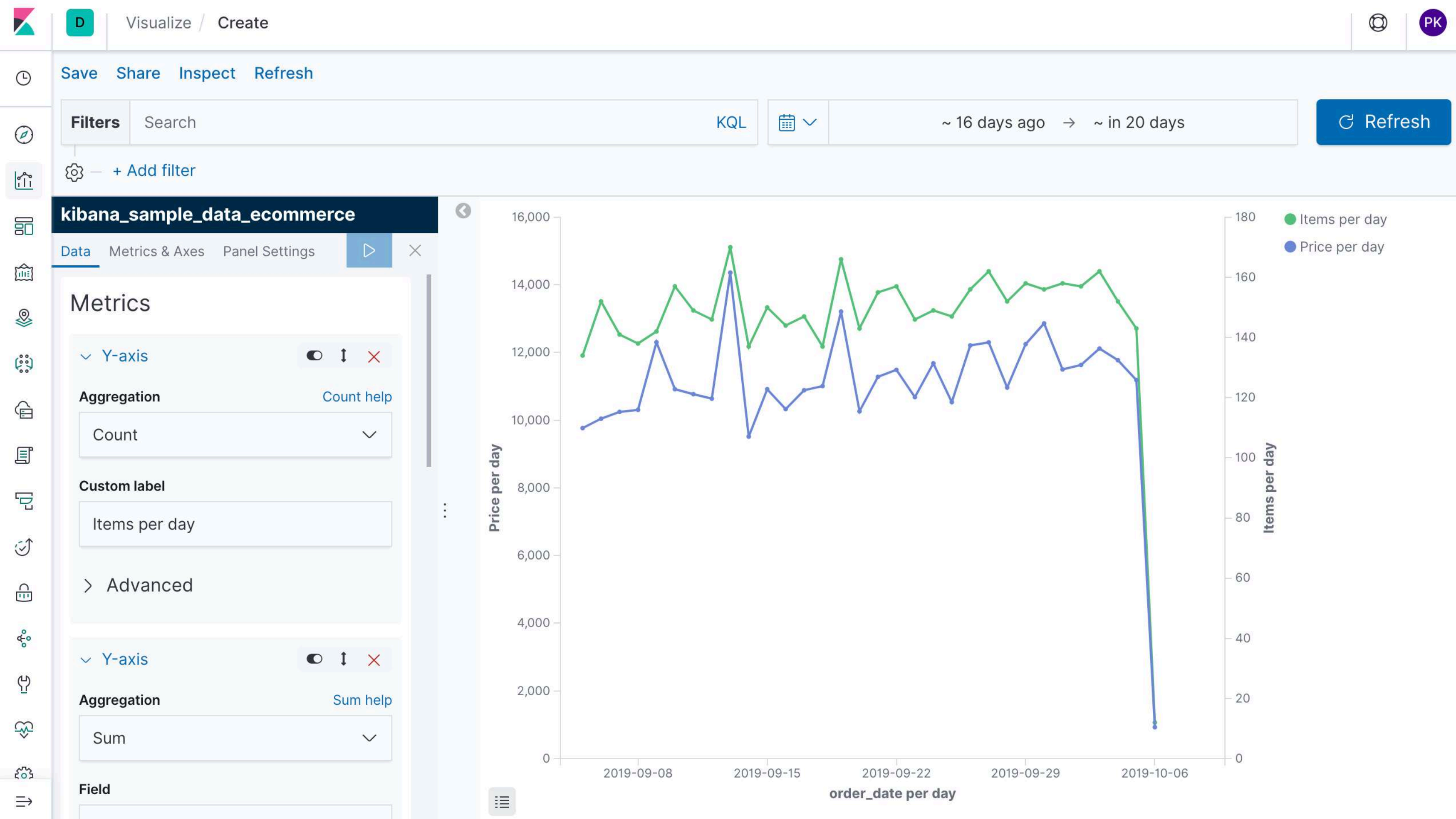
Visualize Sum of Prices

Lens (7.5+)



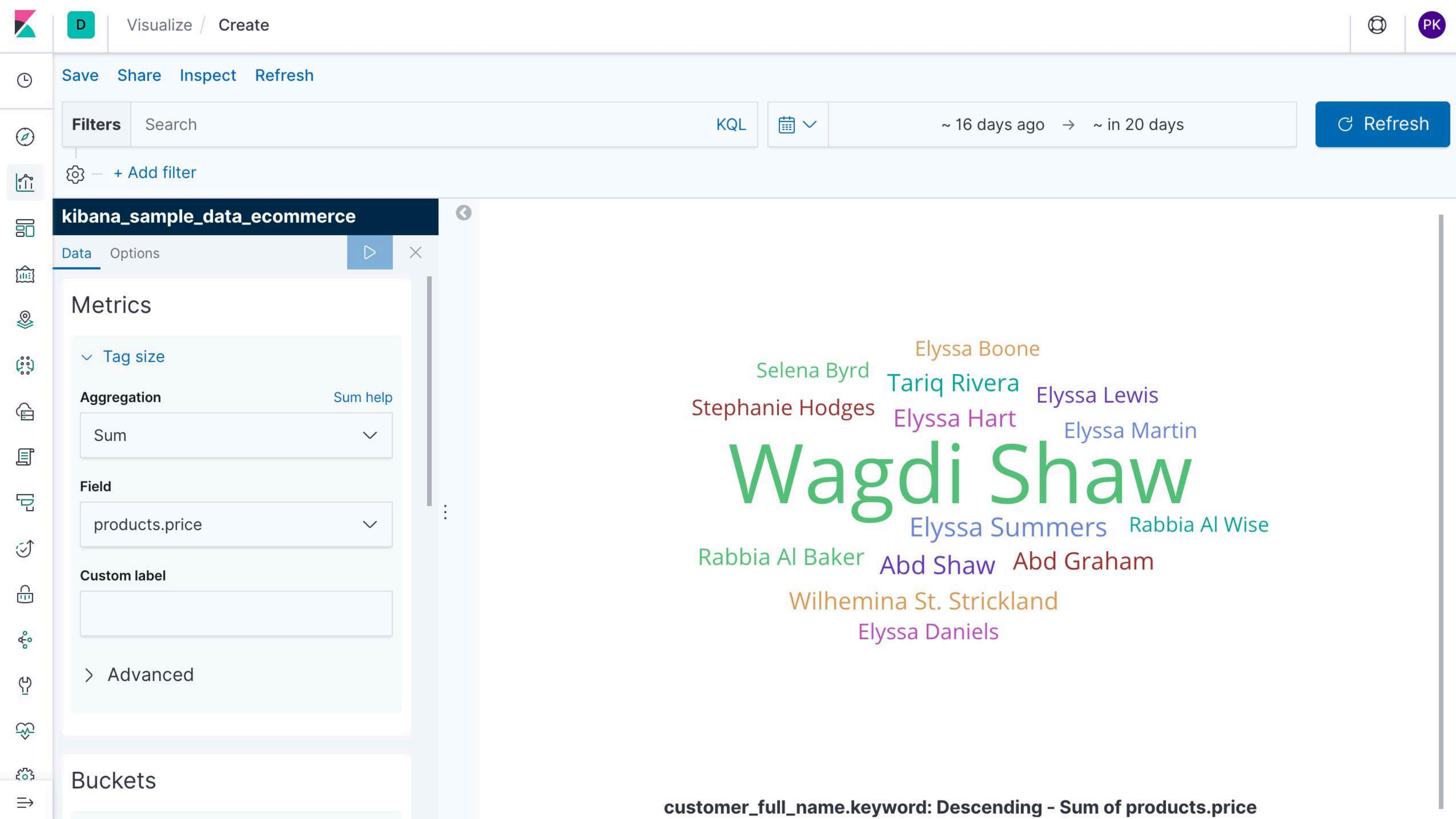
Visualize Sales — Items and Sum

Line chart (for example)

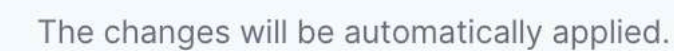


Visualize the Biggest Spenders

Tag Cloud



Price per Item Visual Builder (TSVB)



000

 $= \oplus$

▼

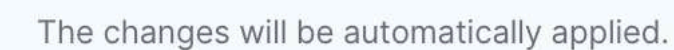
Annotation

```
PUT events/_doc/1
```

```
{  
  "@timestamp": "2020-02-09T14:00:00.000",  
  "description": "Spring sale"  
}
```


 Refresh

Table



Data sources

@timestamp

Ignore panel filters?

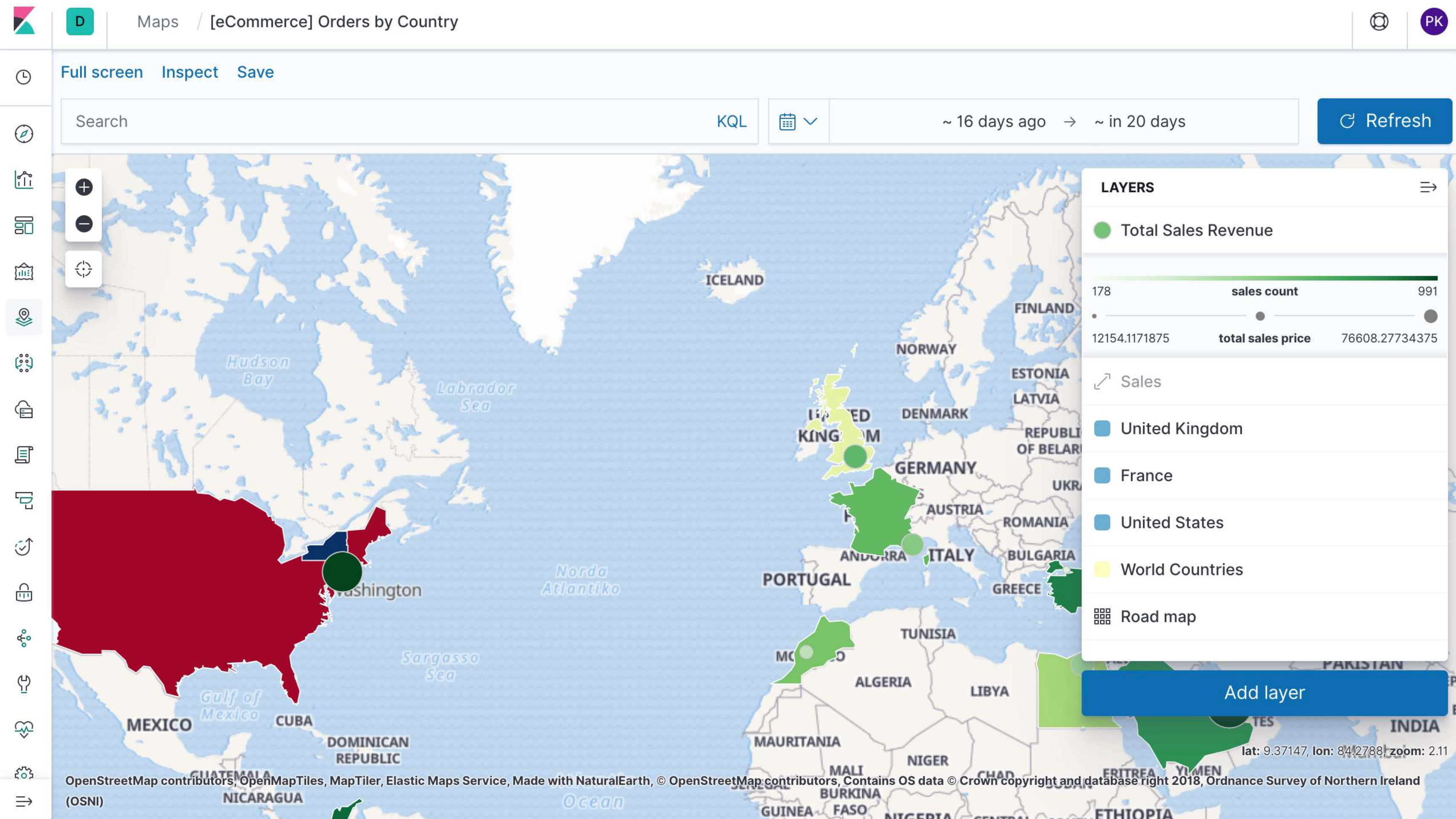
☐ No

Dashboards

Reports

PDF, PNG, CSV (context dependant)

Maps



Canvas

Name

[eCommerce] Revenue Tracking

Width

1080

Height

720

1080p

720p

A4

US Letter

- Global CSS overrides

Page

Background color



Accepts HEX, RGB or HTML Color names

Elements

Total

90

Loaded

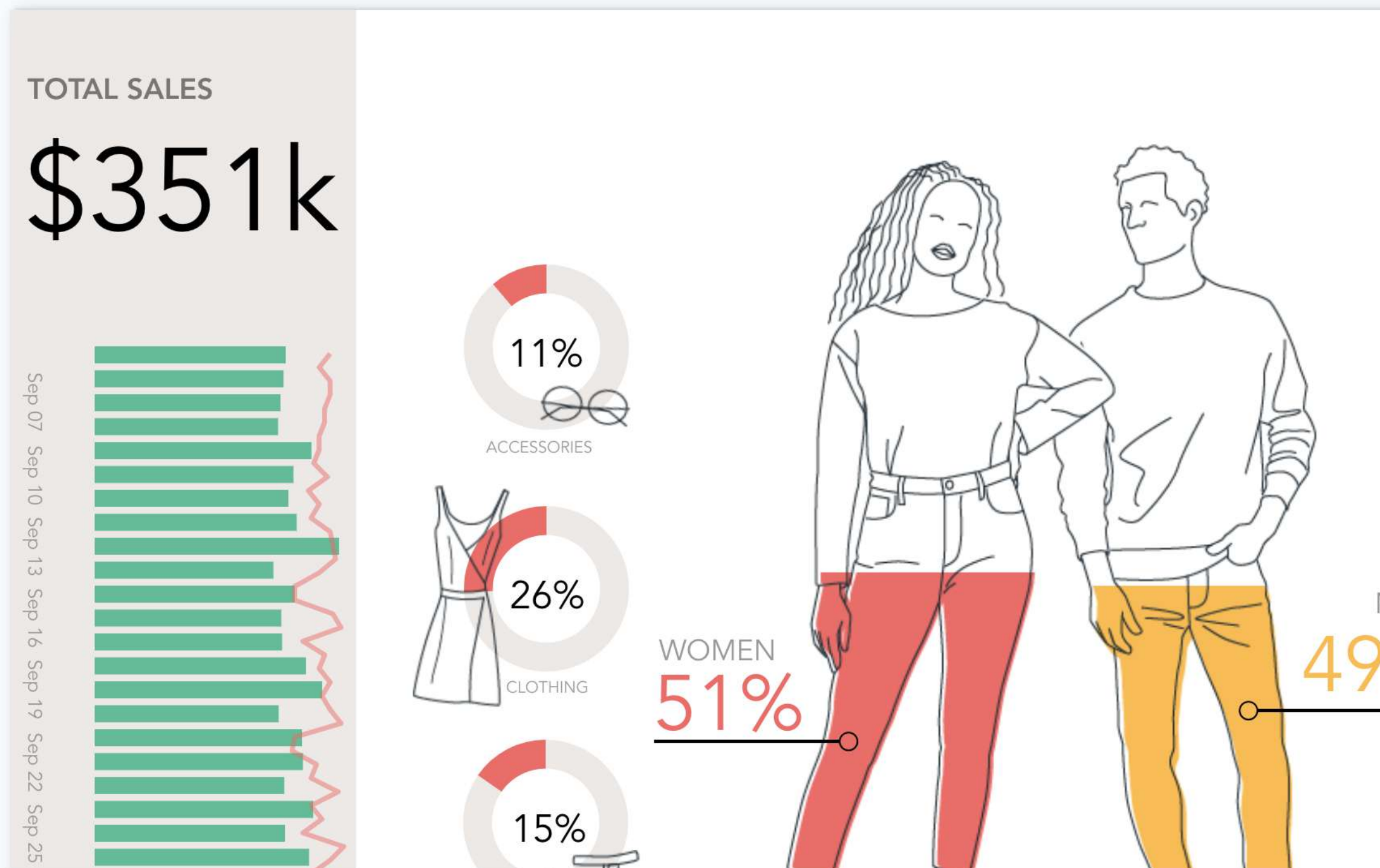
90

Failed

0

Progress

100%



Machine Learning*

* Commercial feature



@xeraa



Conclusion

Analytics

More than full-text search and logs

Data

Entity-centric vs timeseries

Various Visualizations

Data Driven Dashboards

with Kibana &
Elasticsearch

Philipp Krenn

@xeraa

