

Kibana Overview

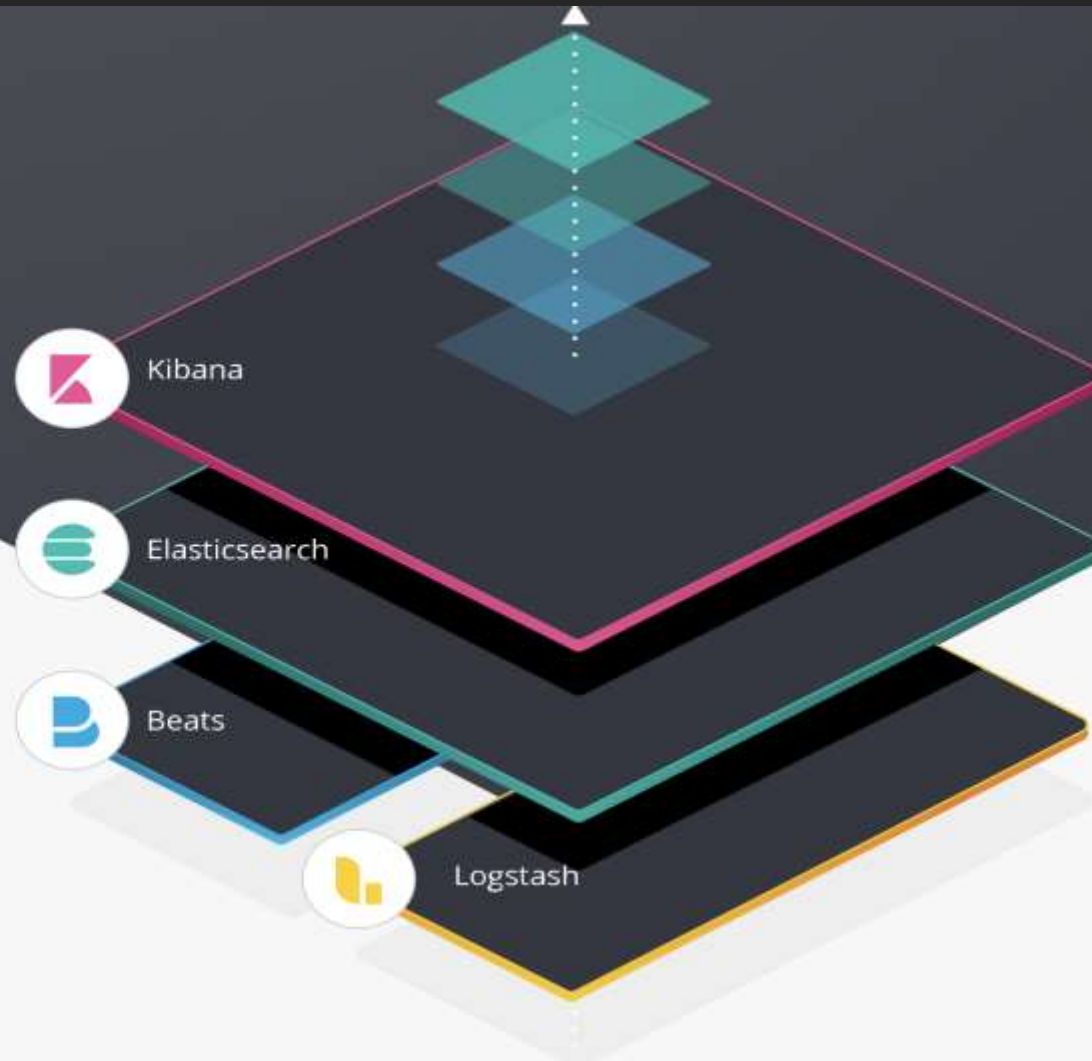
Outline

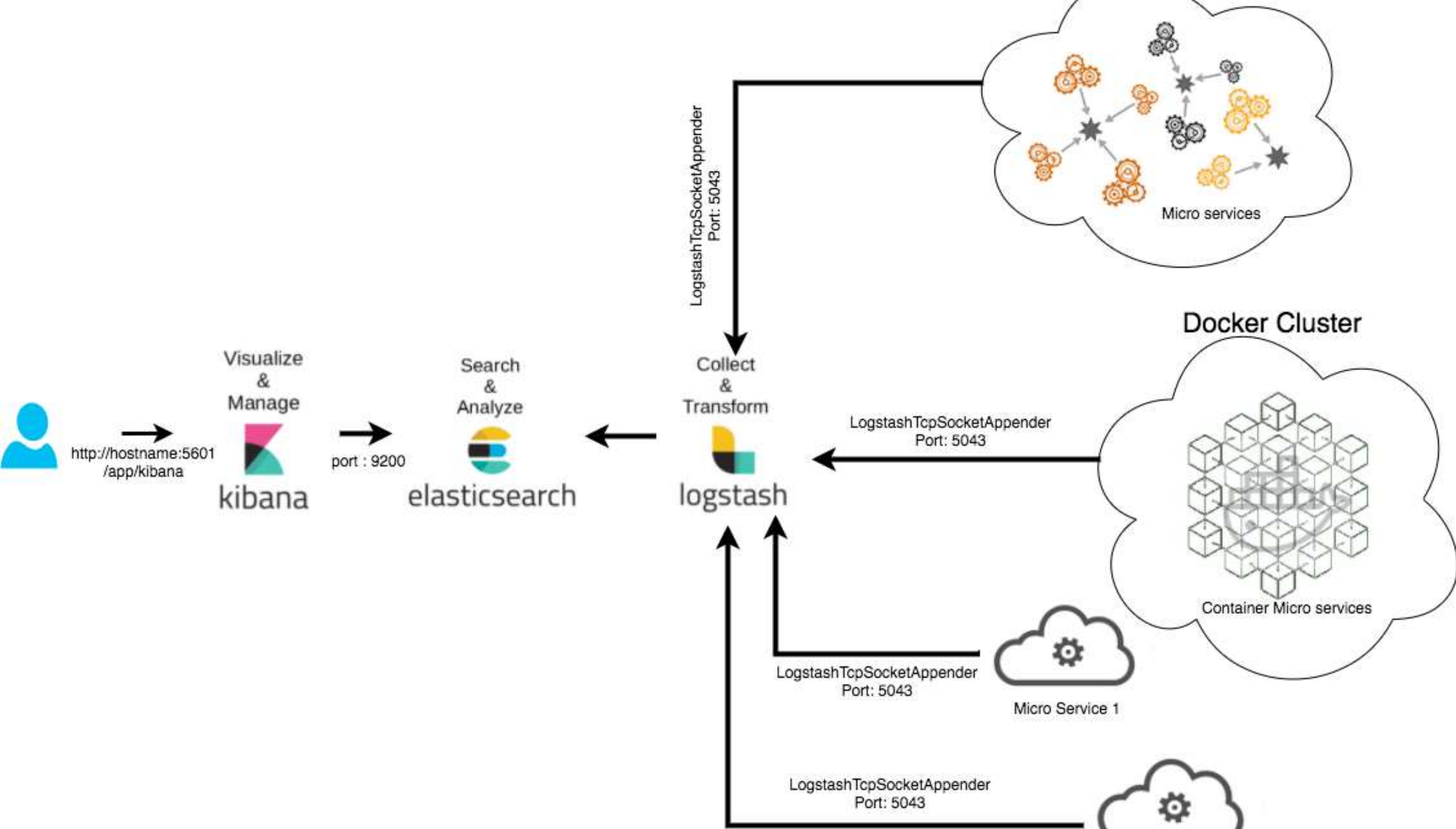
- Definition and History of ELK Stack
- Kibana Essentials Visualizer
 - Discover
 - Visualize
 - Dashboard
- Workshop
- Dev Tools & X-Pack
 - Machine Learning
 - Graph

Etymology

- 黄花 - yellow flower
- Rashid Khan, the creator of Kibana, in Swahili a hut.

What is behind Kibana?





Heart of ELK stack: Elasticsearch

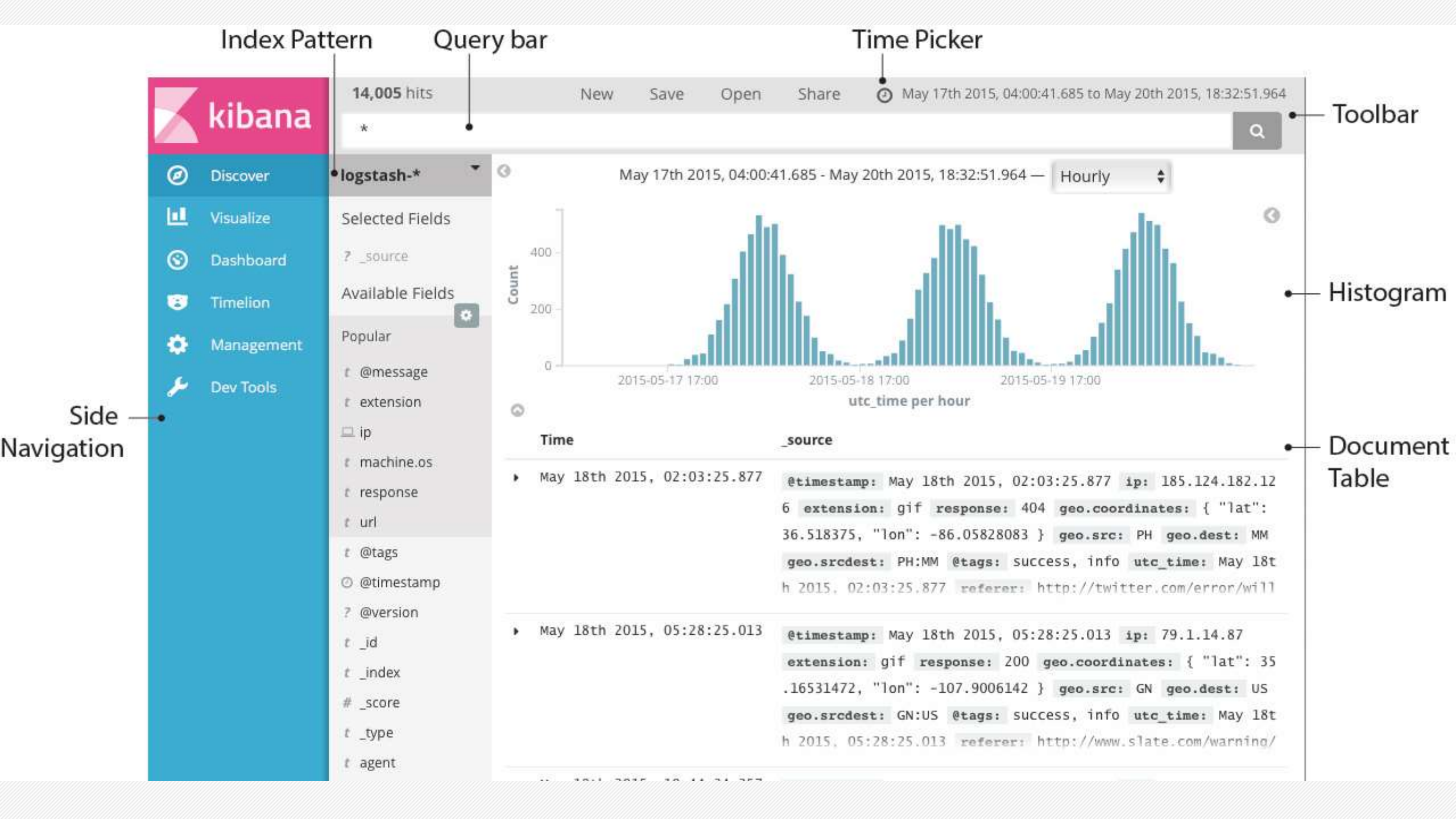


- Based on Apache Lucene
- Shay Banon, Compass to Elasticsearch, released in 2010
- In 2012 Elastic was founded in **Amsterdam**
- RESTful search and analytics engine



Kibana essentials

- Discover
- Visualizer
- Dashboard



Index Pattern

Query bar

Time Picker

Toolbar

Histogram

Document Table

Side Navigation

Discover

- Query bar - Lucene query syntax
- Filter - Elasticsearch Query DSL

Select visualization type

Q Search visualization types...

Basic Charts

A row of six icons representing different chart types: Area, Heat Map, Horizontal Bar, Line, Pie, and Vertical Bar.

Data

The diagram illustrates four types of data visualizations arranged horizontally in a row. Each visualization is contained within a light gray square box. From left to right: 1. 'Data Table' features a 3x3 grid icon. 2. 'Gauge' features a semi-circular gauge icon with a needle. 3. 'Goal' features a semi-circular icon with the number '8' inside. 4. 'Metric' features the large number '42'.

Maps

Time Series

The image shows two logos side-by-side. On the left is the Timelion logo, which consists of a stylized black bear head icon above the text 'Timelion'. On the right is the Visual Builder logo, which consists of a stylized black icon of a person sitting at a desk with a monitor, above the text 'Visual Builder'. A small bell icon is visible in the top right corner of the Visual Builder logo's container.

kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Dashboard / Example Dashboard

Share Edit < ⌚ Last 15 minutes >

Filter...

Q

Markdown Example


Pie Chart Example

Area Chart Example

This is a tutorial dashboard

The markdown widget uses **markdown** syntax

Blockquotes in Markdown use the > character



Search Example

Time

_source

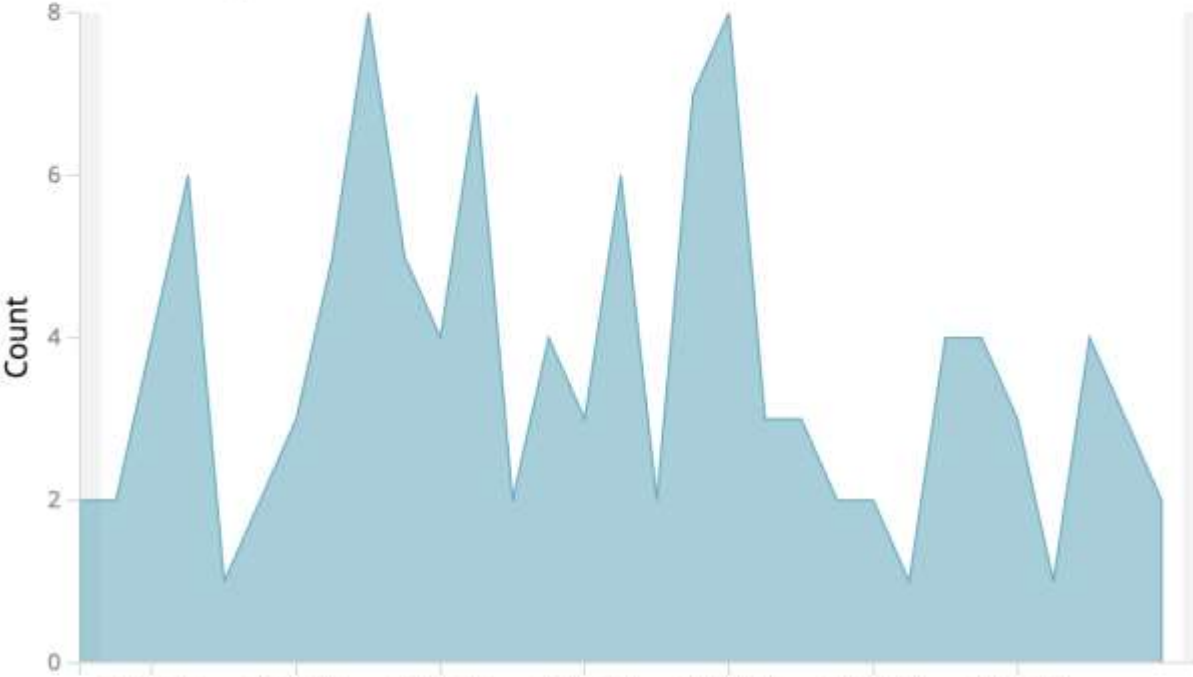
March 30th 2017, 10:55:03.582

index: logstash-0 @timestamp: March 30th 2017, 10:55:03.582 ip: 27.72.124.209 extension: jpg response: 200

geo.coordinates: { "lat": 33.89177944, "lon": -89.02367194 } geo.src: US geo.dest: MX geo.srcdest: US:MX @tags: success, security utc_time: March 30th 2017, 10:55:03.582 referer: http://facebook.com/success/george-nelson agent: Mozilla/5.0 (X11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24 clientip: 27.72.124.209 bytes: 2,895

host: media-for-the-masses.theacademyofperformingartsandscience.org request: /uploads/zhai-zhigang.jpg url: https://media-f

Count



@timestamp per 30 seconds

1

2

3

»



Let's try it out!

- Example of Visualize & Dashboard
- Little exercise.

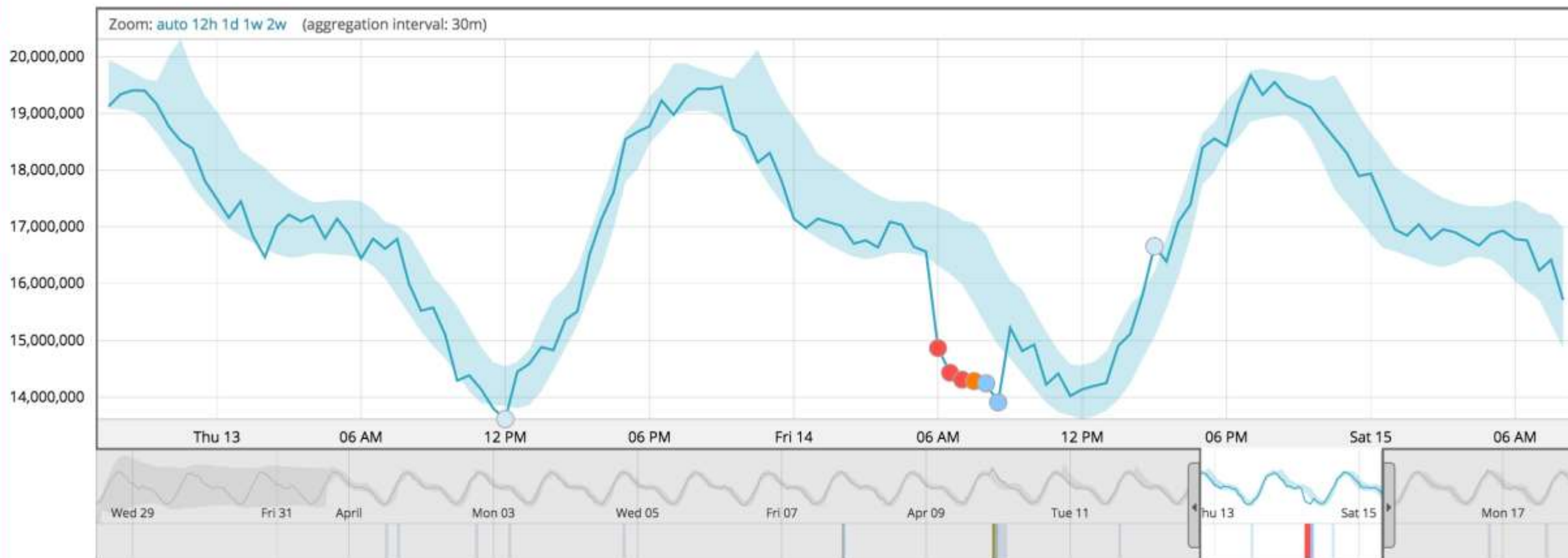
Dev Tools

- Console
- Search Profiler

X-Pack beyond Essentials

- Security
- Monitoring
- Alerting and Notification
- Reporting
- Graph
- Machine Learning

Time series analysis



Anomalies

Severity threshold: ▲ warning ▼

Interval: Auto ▼

time ↕	max severity ↕	detector ↕	actual ↕	typical ↕	description ↕	job ID ↕
▶ April 14th 2017, 06:00	▲ 95	sum(total) (total-request)	14432600	16609200	↓ 1.2x lower	total-request
▶ April 14th 2017, 07:00	▲ 83	sum(total) (total-request)	14310100	16421500	↓ 1.1x lower	total-request
▶ April 14th 2017, 08:00	▲ 24	sum(total) (total-request)	13909700	15499400	↓ 1.1x lower	total-request
▶ April 13th 2017, 12:00	▲ 1	sum(total) (total-request)	13615600	14113400	↓ Unusually low	total-request
▶ April 14th 2017, 15:00	▲ < 1	sum(total) (total-request)	16659900	15863700	↑ 1.1x higher	total-request

Selections

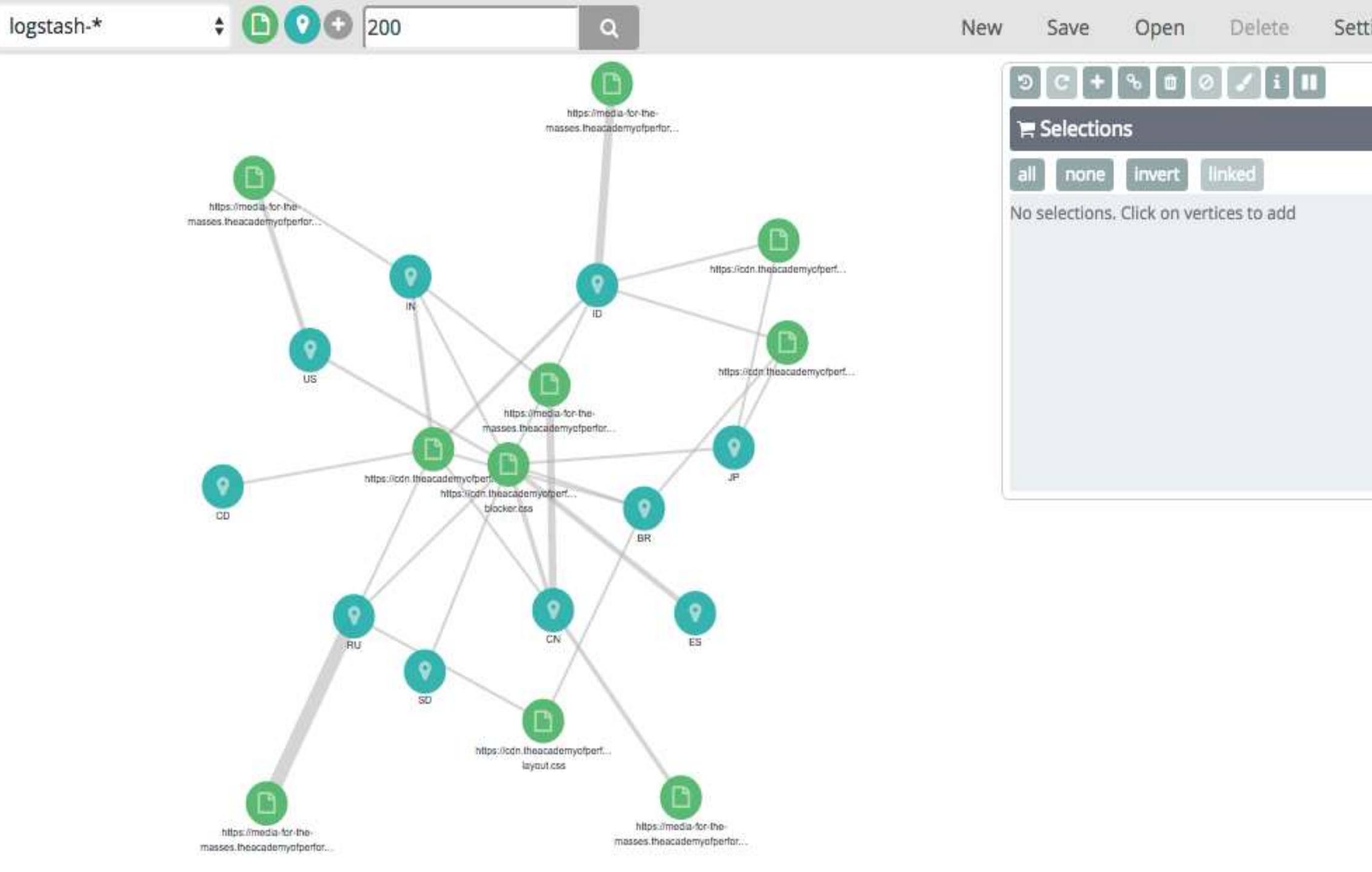
all none invert linked

all none invert linked

all none invert linked

all none invert linked

No selections. Click on vertices to add



Thank you!

- Don't spend time reading books about Kibana
- Use official documentation in [elastic.co](https://www.elastic.co/guide)
- Be careful with data!