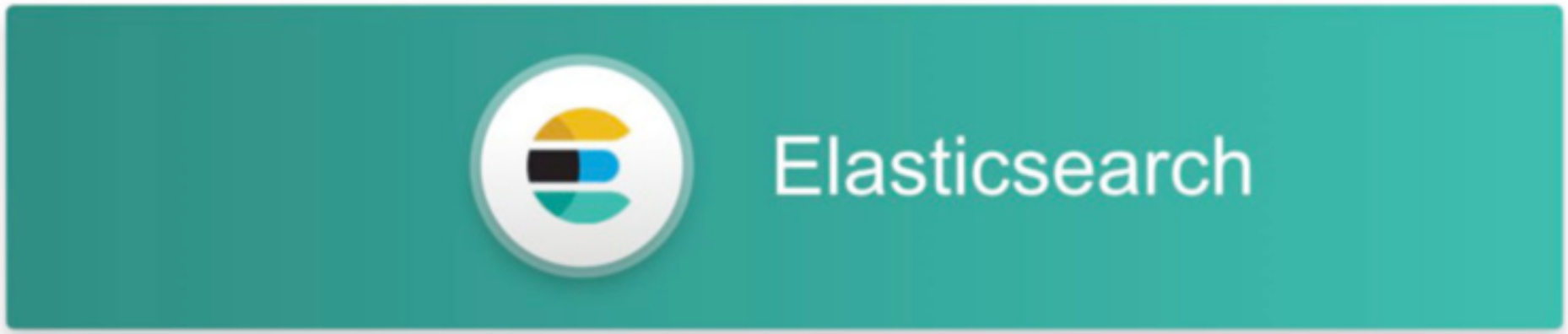
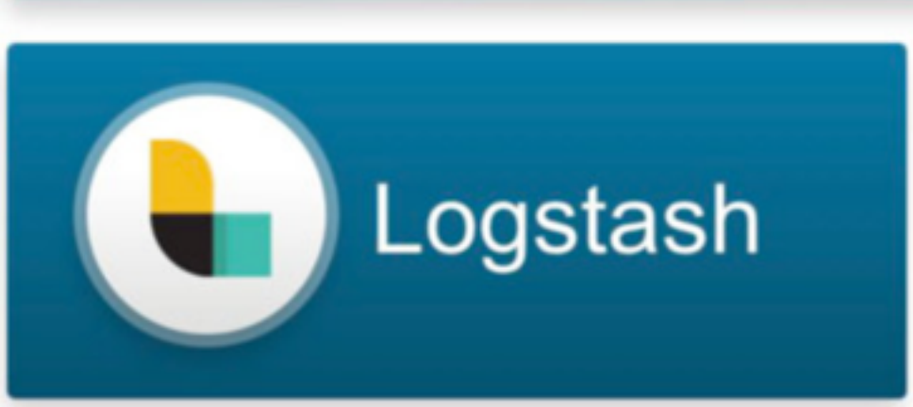
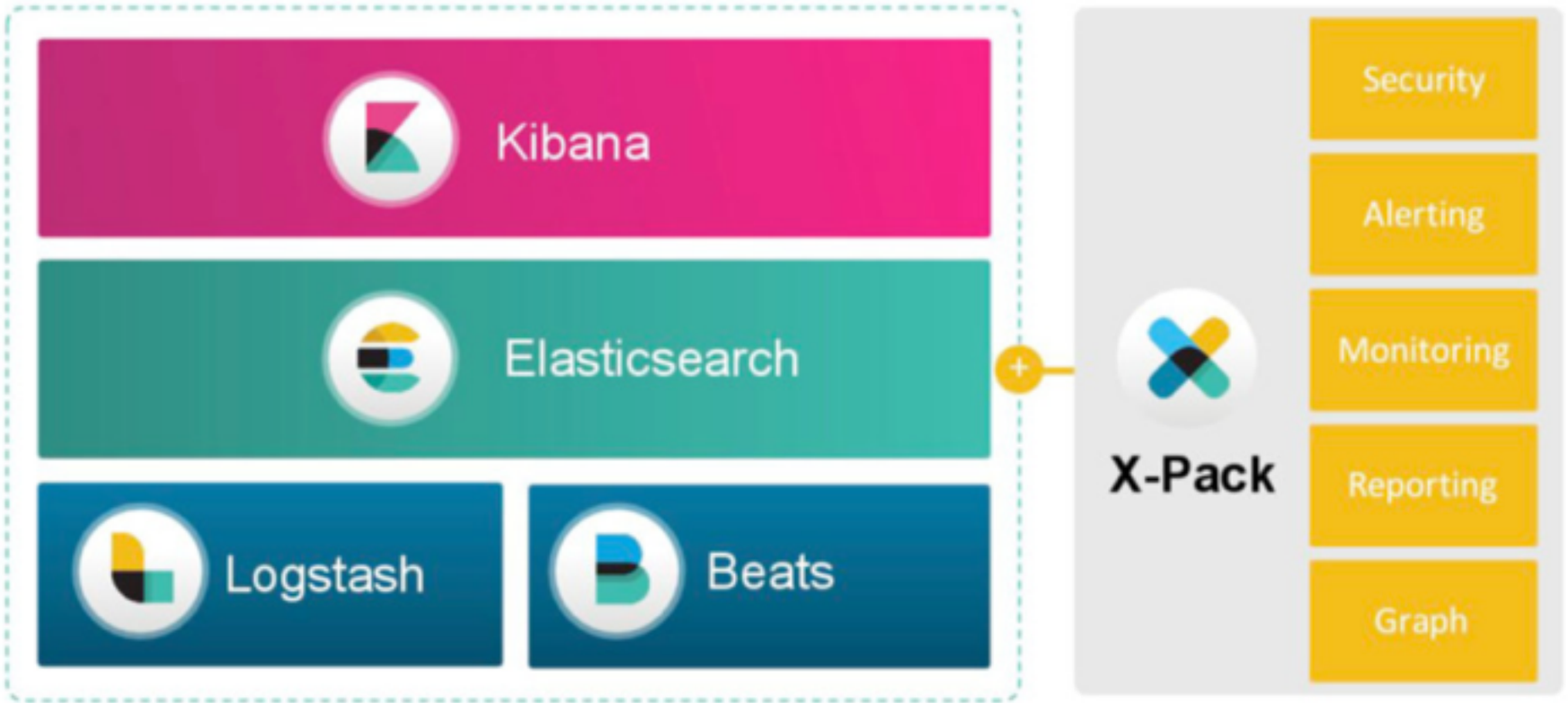
Elastic Stack

Haydar KÜLEKCİ





Elastic Stack



Elastic Stack & X-Pack

X-Pack

X-Pack

Security

(formerly Shield)

Protect your data across the Elastic Stack.

Learn More

Alerting

(via Watcher)

Get notifications about changes in your data.

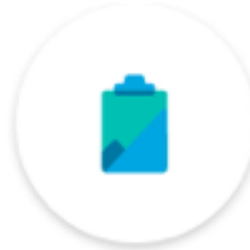
Learn More

Monitoring

(formerly Marvel)

Keep a pulse on the health of the Elastic Stack.

Learn More



Reporting

Generate, schedule, and email reports.

Learn More

Graph

Explore meaningful relationships in your data.

Learn More

Logstash & Beats

Logstash & Beats

- Ingest any data, from any source, in any format.
  - **Beats** is a platform for lightweight shipper.
  - **Logstash** is a dynamic data collection pipeline.

Beats

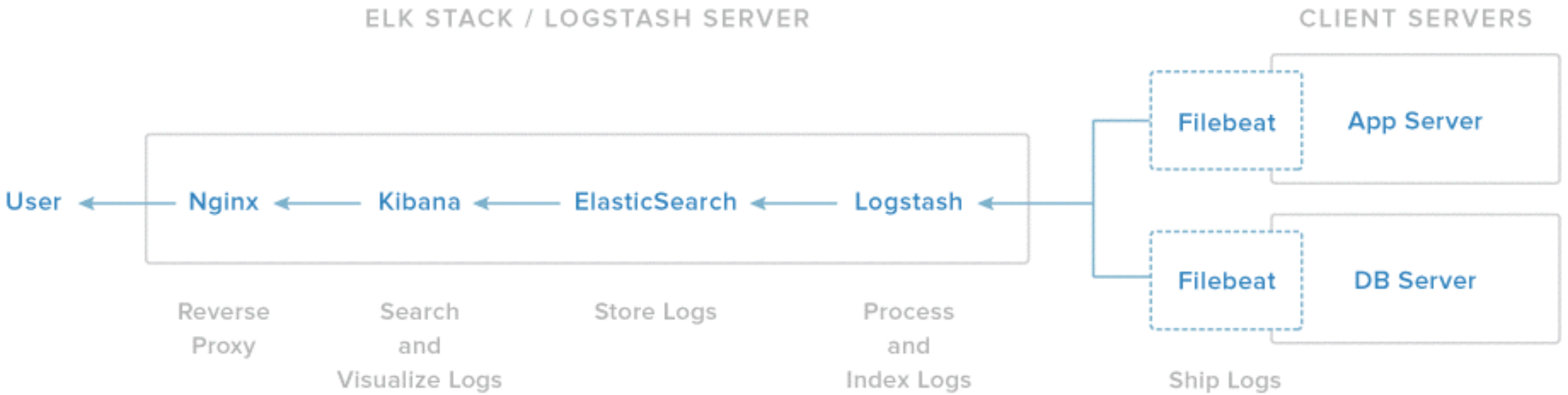
- **Filebeat** helps you keep the simple things simple by offering a lightweight way to forward and centralize logs and files.
- **Metricbeat** is a lightweight way to send system and service statistics.
- **Packetbeat** is a lightweight network packet analyzer that sends data to Logstash or Elasticsearch.
- **Winlogbeat** live streams Windows event logs to Elasticsearch and Logstash in a lightweight way.
- **Heartbeat** (beta) asks the simple question: “Are you alive?” and ships this information and response time to the rest of the Elastic Stack for further analysis.

Logstash

- **Input** plugin enables a specific source of events to be read by Logstash. (Beats, Elasticsearch, Eventlog, File, Irc, RabbitMQ, ZeroMQ, Redis, Kafka, etc.)

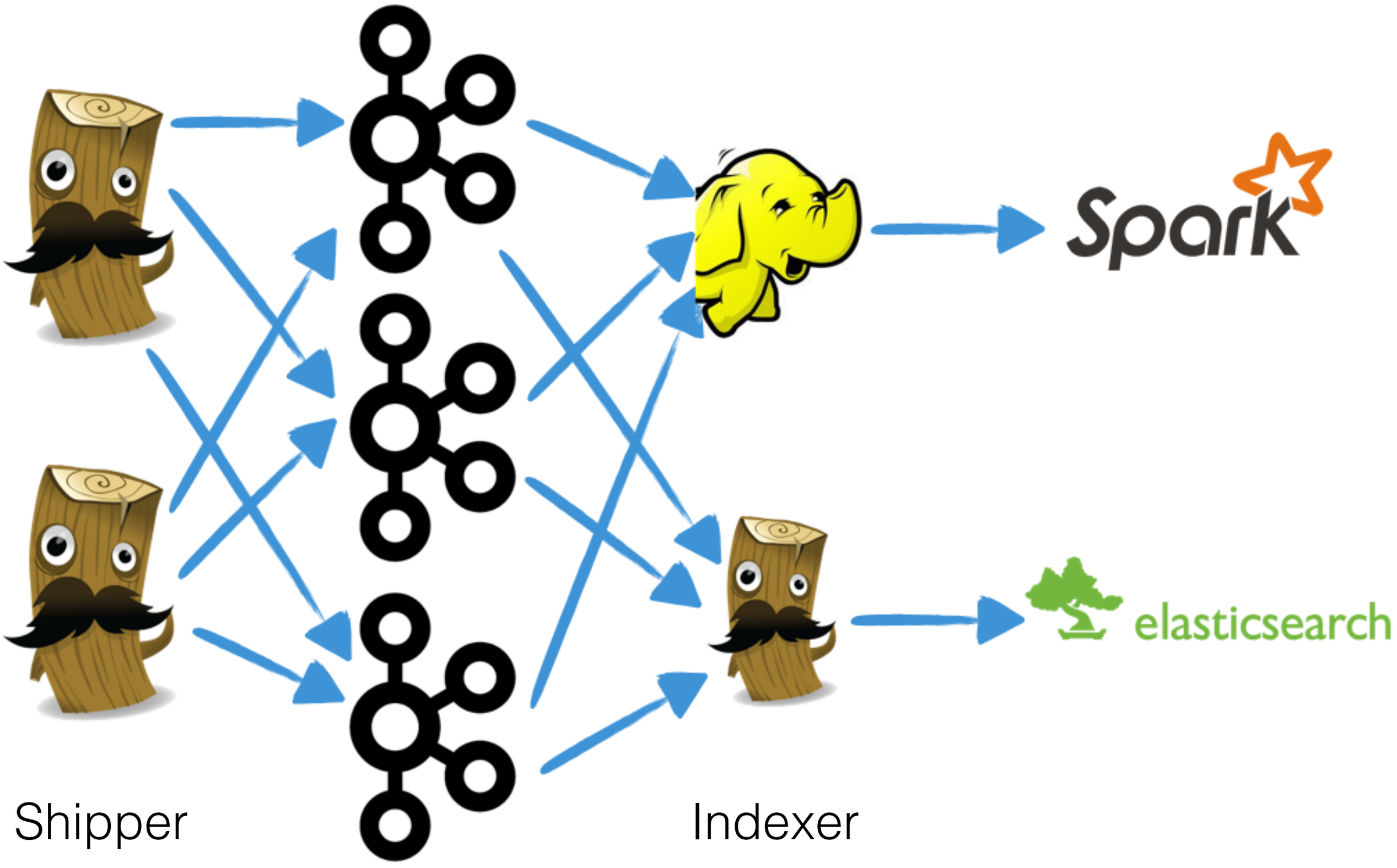
- **Filter** plugin performs intermediary processing on an event. (Aggregate, Clone, Csv, Date, Geoip, Grok, Json, Split, Urldecode, Xml, etc.)

- **Output** sends event data to a particular destination. Outputs are the final stage in the event pipeline. (Csv, Email, Elasticsearch, File, Http, Irc, Kafka, Redis, Sqlite, Syslog, Websocket, RabbitMQ, ZeroMQ, etc.)



https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04

Example Topology With Kafka

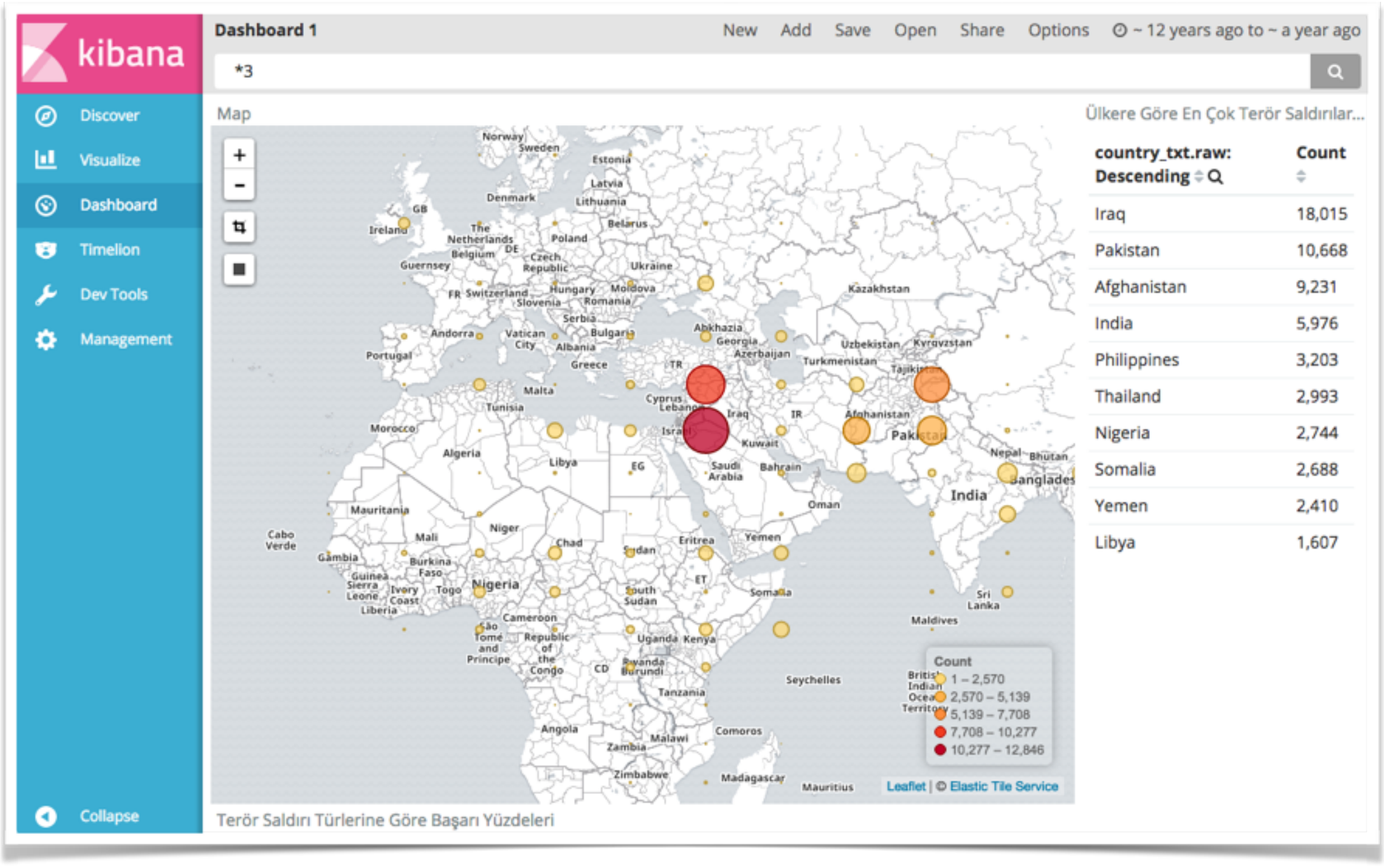


Kibana

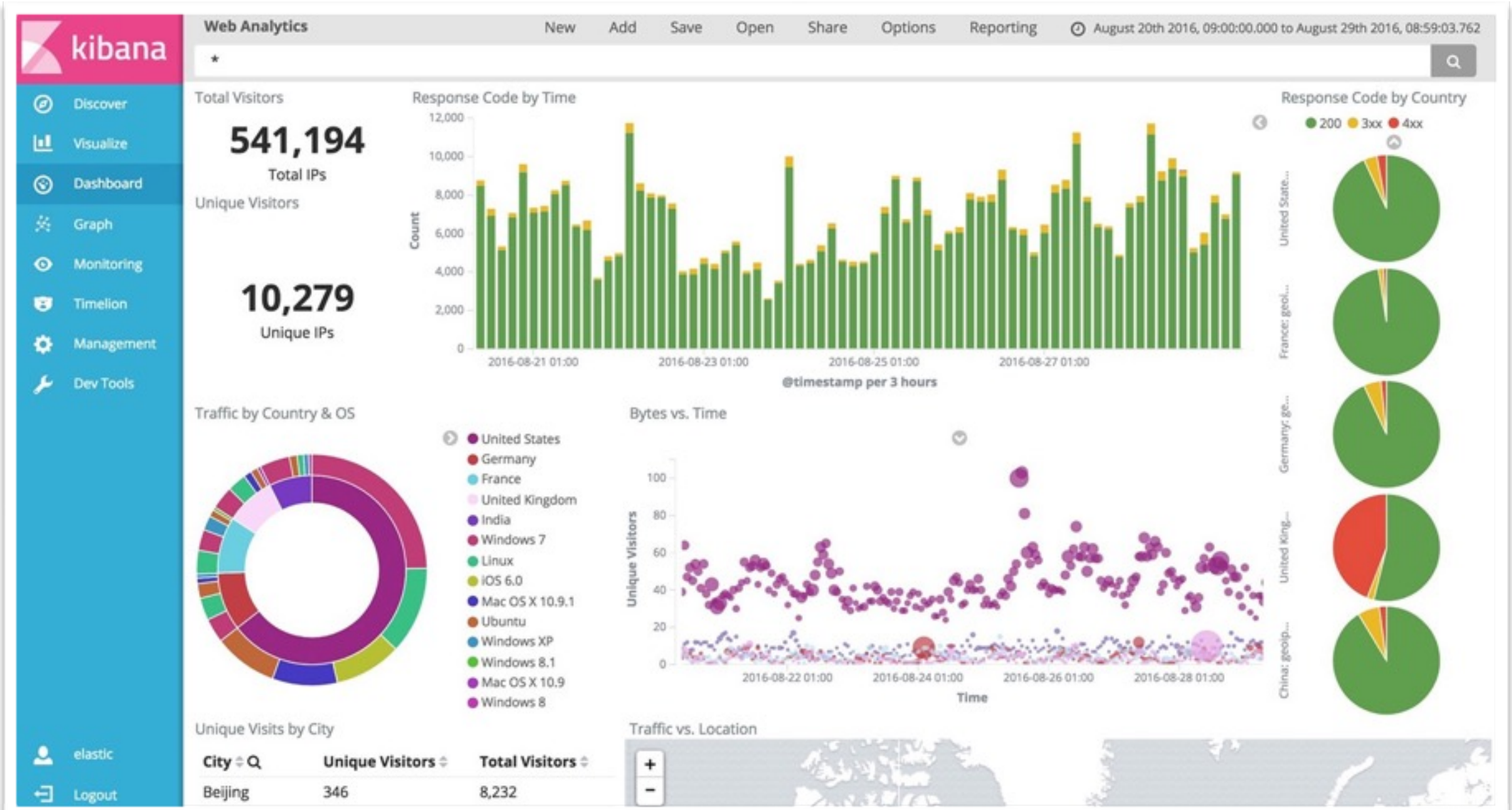
Kibana


kibana
Dev Tools
Console
History
Settings
Help
Discover
Visualize
Dashboard
Graph
Monitoring
Timelion
Management
Dev Tools
elastic
Logout
Collapse
GET /social-*/_search
{
"query": {
"match": {
"request": "myProduct"
}
},
"aggregations": {
"top_10_states": {
"terms": {
"field": "state",
"size": 10
}
}
}
}
{
"took": 66,
"timed_out": false,
"_shards": {
"total": 150,
"successful": 150,
"failed": 0
},
"hits": {},
"aggregations": {
"top_10_states": {
"doc_count_error_upper_bound": 0,
"sum_other_doc_count": 0,
"buckets": [
{
"key": "Indonesia",
"doc_count": 8878
},
{
"key": "China",
"doc_count": 8786
},
{
"key": "Kazakhstan",
"doc_count": 8763
},
{

Kibana


kibana
Dashboard 1
New
Add
Save
Open
Share
Options
~ 12 years ago to ~ a year ago
*3
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Map
Ülkere Göre En Çok Terör Saldırılar...
country_txt.raw: Descending
Count
Iraq 18,015
Pakistan 10,668
Afghanistan 9,231
India 5,976
Philippines 3,203
Thailand 2,993
Nigeria 2,744
Somalia 2,688
Yemen 2,410
Libya 1,607
Count
1 – 2,570
2,570 – 5,139
5,139 – 7,708
7,708 – 10,277
10,277 – 12,846
Leaflet | © Elastic Tile Service
Terör Saldırı Türlerine Göre Başarı Yüzdeleri

Kibana


kibana
Web Analytics
New
Add
Save
Open
Share
Options
Reporting
August 20th 2016, 09:00:00.000 to August 29th 2016, 08:59:03.762
Discover
Visualize
Dashboard
Graph
Monitoring
Timelion
Management
Dev Tools
elastic
Logout
Total Visitors
541,194
Total IPs
Unique Visitors
10,279
Unique IPs
Response Code by Time
Count
@timestamp per 3 hours
Response Code by Country
200
3xx
4xx
Traffic by Country & OS
United States
Germany
France
United Kingdom
India
Windows 7
Linux
iOS 6.0
Mac OS X 10.9.1
Ubuntu
Windows XP
Windows 8.1
Mac OS X 10.9
Windows 8
Bytes vs. Time
Unique Visitors
Time
Unique Visits by City
City
Unique Visitors
Total Visitors
Beijing
346
8,232
Traffic vs. Location

Elasticsearch

Elasticsearch

- Near Real-time Search
- Analysis
- Clustering
- High Availability
- Full-Text Search
- Document Base
- Developer Friendly Rest API
- Based on Lucene

Elasticsearch

- Provide a Rest API
- Full-text search and filtering with Search API
- Storing Logs with Elasticsearch and Filtering with Kibana
- Near Real-time Analysis with Aggregations

Basic Concepts

- **Cluster** : One or more your nodes (servers).
- **Node** : A single server that is part of your cluster.
- **Index** : A collection of documents that have similar characteristics.
- **Type** : An option to categorize your data of your index.
- **Document** : A basic unit of information that can be indexed. (JSON)
- **Shards & Replica** : A concept to solve scaling and storing large amount of data.

ElasticSearch http://localhost:9200/ Connect **Bench, Morris** cluster health: green (4, 26)

Overview | Browser | Structured Query | Any Request | Info | Status | Nodes Stats | Cluster Nodes | Cluster State | Cluster Health

Cluster Overview New Index Refresh

	_river	sites	models	agents	devices	data_products
	size: 7.8kb (16.3kb) docs: 10 (10) Info Actions	size: 430b (760b) docs: 0 (0) Info Actions	size: 430b (760b) docs: 0 (0) Info Actions	size: 430b (760b) docs: 0 (0) Info Actions	size: 430b (760b) docs: 0 (0) Info Actions	size: 430b (760b) docs: 0 (0) Info Actions
Shaw, Shinobi ZTaGxKnhSBekG7JwLjO3zg inet[/192.168.1.52:9203] Info Actions		0 1 3	1 3	0 3	0 1 2	0 1 3
Bench, Morris G2xjUudmT_K3HeE2AV7H4A inet[/192.168.1.52:9200] Info Actions		0 1 4	0 2	2 3	0 3 4	0 2 4
Solitaire eieKB2jaS4uCcpthSzv1Jw inet[/192.168.1.52:9201] Info Actions		0 2 3	1 2 4	1 2 4	1 3	1 3
Pete Wisdom 5CLeFNIuRC2nZcvQo-x4QQ inet[/192.168.1.52:9202] Info Actions		0 2 4	0 3 4	0 1 4	2 4	2 4

Mapping

- Mapping is the process of defining how a document, and the fields it contains, are stored and indexed.

- **Dynamic Mapping:** new mapping types and new field names will be added automatically, just by indexing a document.

- **Explicit Mapping:** Elasticsearch has already know your data sctructure (fields and types). And you can not index the data which is different structured from mapping.

Analysis

- Analysis is the process of converting text, like the body of any email, into tokens or terms which are added to the inverted index for searching.

- An analyzer -whether built-in or custom- is just a package which contains three lower-level building blocks: character filters, tokenizers, and token filters.

- Standard Analyzer

  "The QUICK brown foxes jumped over the lazy dog!"
  [the, quick, brown, foxes, jumped, over, the, lazy, dog]

- Whitespace Analyzer

  "The QUICK brown foxes jumped over the lazy dog!"
  [The, QUICK, brown, foxes, jumped, over, the, lazy, dog!]

Demo

Haydar KÜLEKCİ

elasticsearch.kulekci.net

https://tr.linkedin.com/in/hkulekci

https://github.com/hkulekci/es5-devnot

Creating Index

```
PUT twitter
{
    "settings" : {
        "index" : {
            "number_of_shards" : 3,
            "number_of_replicas" : 2
        }
    }
}
```

Creating Type & Mapping

```
POST twitter_with_mapping/tweet/_mapping
{
    "properties": {
        "timestamp_ms": {
            "type":"date"
        },
        "user": {
            "properties": {
                "name": {
                    "type": "string",
                    "index":"not_analyzed"
                }
            }
        },
        "place": {
            "properties": {
                "country": {
                    "type": "string",
                    "index": "not_analyzed"
                }
            }
        }
    }
}
```