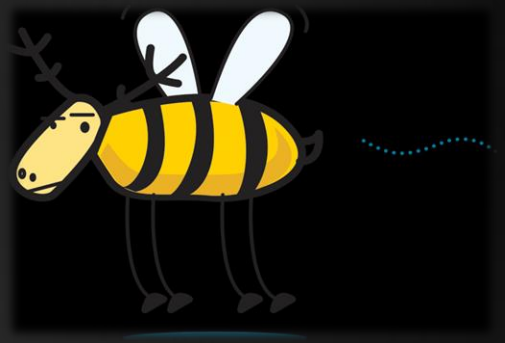
ELK – From zero to (coding class) hero

Josip Kovaček

ELK => ELASTIC STACK



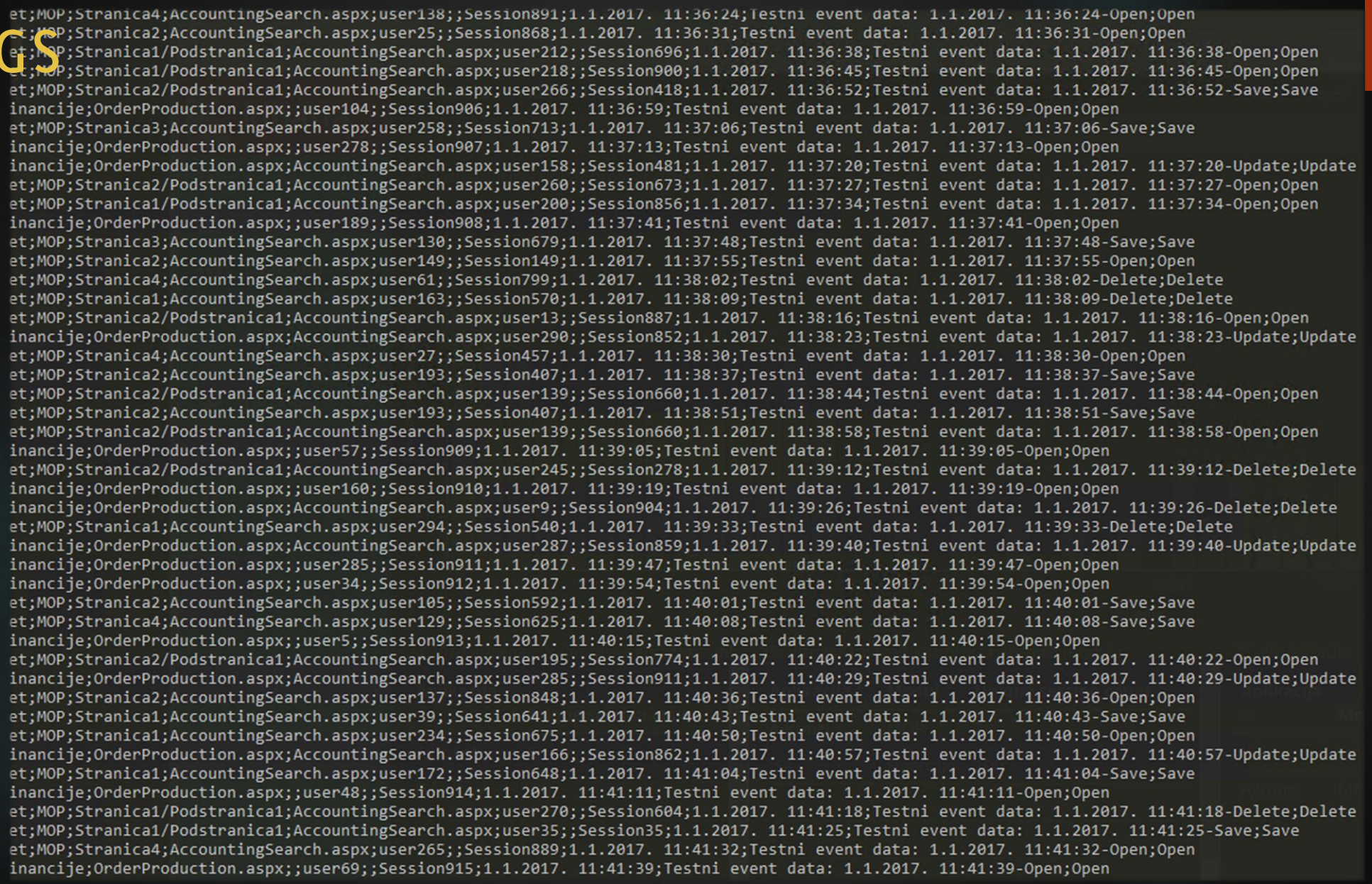
Agenda

- Logs
- Elastic Stack
- Setup
- Monitoring
- Alerting

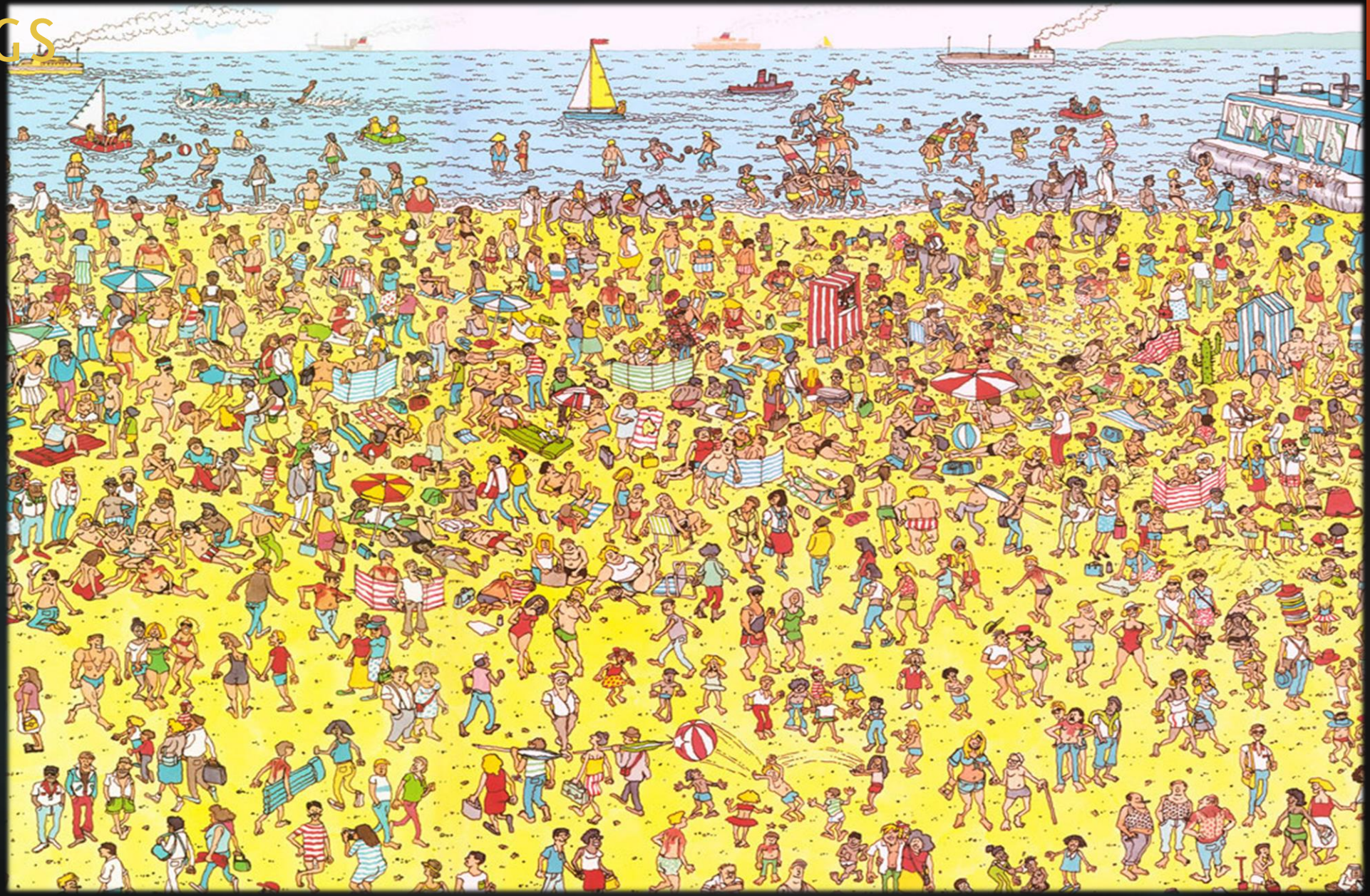
Logs

[2017-10-21 12:03:55.478, 8.8.8.8, Pero, /search, q=Changecon ticket]

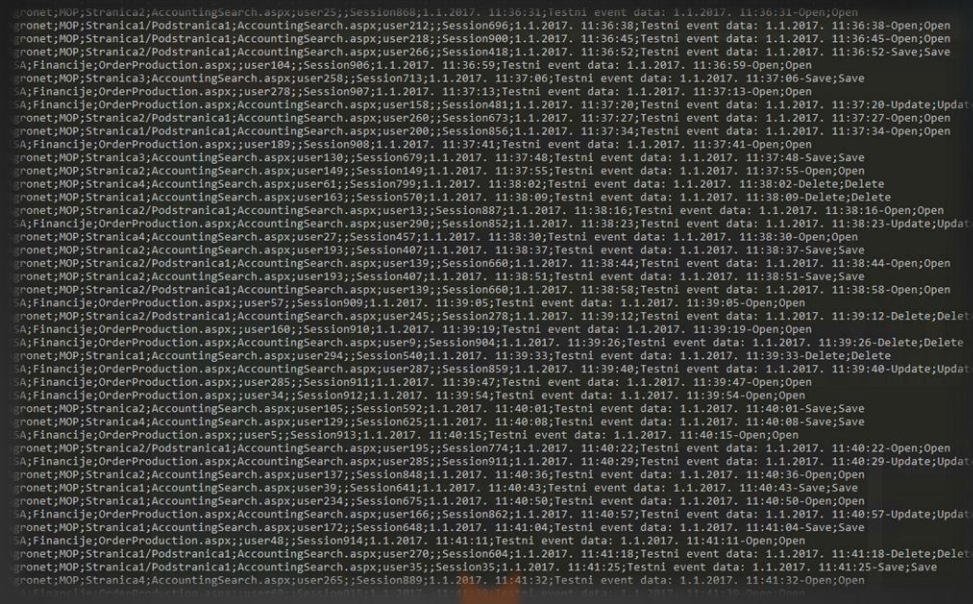
Logs

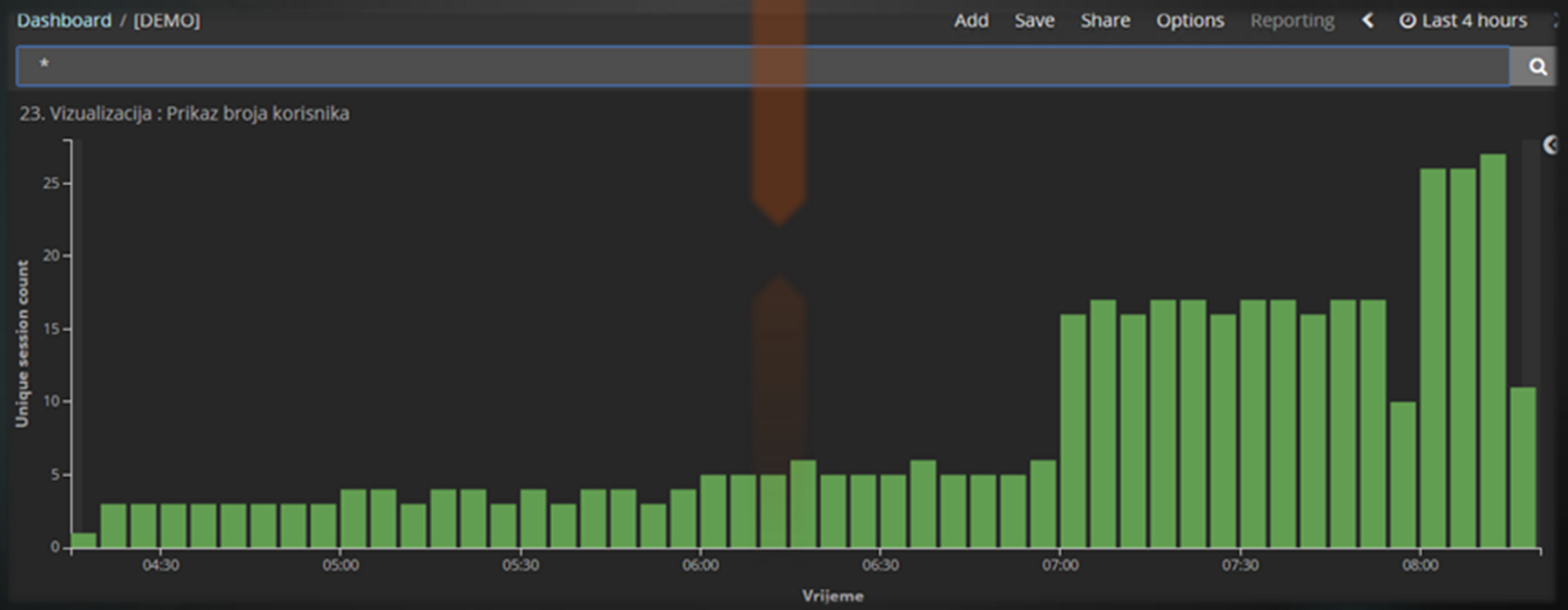

et;MOP;Stranica4;AccountingSearch.aspx;user138;;Session891;1.1.2017. 11:36:24;Testni event data: 1.1.2017. 11:36:24-Open;Open
et;MOP;Stranica2;AccountingSearch.aspx;user25;;Session868;1.1.2017. 11:36:31;Testni event data: 1.1.2017. 11:36:31-Open;Open
et;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user212;;Session696;1.1.2017. 11:36:38;Testni event data: 1.1.2017. 11:36:38-Open;Open
et;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user218;;Session900;1.1.2017. 11:36:45;Testni event data: 1.1.2017. 11:36:45-Open;Open
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user266;;Session418;1.1.2017. 11:36:52;Testni event data: 1.1.2017. 11:36:52-Save;Save
inancije;OrderProduction.aspx;;user104;;Session906;1.1.2017. 11:36:59;Testni event data: 1.1.2017. 11:36:59-Open;Open
et;MOP;Stranica3;AccountingSearch.aspx;user258;;Session713;1.1.2017. 11:37:06;Testni event data: 1.1.2017. 11:37:06-Save;Save
inancije;OrderProduction.aspx;;user278;;Session907;1.1.2017. 11:37:13;Testni event data: 1.1.2017. 11:37:13-Open;Open
inancije;OrderProduction.aspx;AccountingSearch.aspx;user158;;Session481;1.1.2017. 11:37:20;Testni event data: 1.1.2017. 11:37:20-Update;Update
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user260;;Session673;1.1.2017. 11:37:27;Testni event data: 1.1.2017. 11:37:27-Open;Open
et;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user200;;Session856;1.1.2017. 11:37:34;Testni event data: 1.1.2017. 11:37:34-Open;Open
inancije;OrderProduction.aspx;;user189;;Session908;1.1.2017. 11:37:41;Testni event data: 1.1.2017. 11:37:41-Open;Open
et;MOP;Stranica3;AccountingSearch.aspx;user130;;Session679;1.1.2017. 11:37:48;Testni event data: 1.1.2017. 11:37:48-Save;Save
et;MOP;Stranica2;AccountingSearch.aspx;user149;;Session149;1.1.2017. 11:37:55;Testni event data: 1.1.2017. 11:37:55-Open;Open
et;MOP;Stranica4;AccountingSearch.aspx;user61;;Session799;1.1.2017. 11:38:02;Testni event data: 1.1.2017. 11:38:02-Delete;Delete
et;MOP;Stranica1;AccountingSearch.aspx;user163;;Session570;1.1.2017. 11:38:09;Testni event data: 1.1.2017. 11:38:09-Delete;Delete
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user13;;Session887;1.1.2017. 11:38:16;Testni event data: 1.1.2017. 11:38:16-Open;Open
inancije;OrderProduction.aspx;AccountingSearch.aspx;user290;;Session852;1.1.2017. 11:38:23;Testni event data: 1.1.2017. 11:38:23-Update;Update
et;MOP;Stranica4;AccountingSearch.aspx;user27;;Session457;1.1.2017. 11:38:30;Testni event data: 1.1.2017. 11:38:30-Open;Open
et;MOP;Stranica2;AccountingSearch.aspx;user193;;Session407;1.1.2017. 11:38:37;Testni event data: 1.1.2017. 11:38:37-Save;Save
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user139;;Session660;1.1.2017. 11:38:44;Testni event data: 1.1.2017. 11:38:44-Open;Open
et;MOP;Stranica2;AccountingSearch.aspx;user193;;Session407;1.1.2017. 11:38:51;Testni event data: 1.1.2017. 11:38:51-Save;Save
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user139;;Session660;1.1.2017. 11:38:58;Testni event data: 1.1.2017. 11:38:58-Open;Open
inancije;OrderProduction.aspx;;user57;;Session909;1.1.2017. 11:39:05;Testni event data: 1.1.2017. 11:39:05-Open;Open
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user245;;Session278;1.1.2017. 11:39:12;Testni event data: 1.1.2017. 11:39:12-Delete;Delete
inancije;OrderProduction.aspx;;user160;;Session910;1.1.2017. 11:39:19;Testni event data: 1.1.2017. 11:39:19-Open;Open
inancije;OrderProduction.aspx;AccountingSearch.aspx;user9;;Session904;1.1.2017. 11:39:26;Testni event data: 1.1.2017. 11:39:26-Delete;Delete
et;MOP;Stranica1;AccountingSearch.aspx;user294;;Session540;1.1.2017. 11:39:33;Testni event data: 1.1.2017. 11:39:33-Delete;Delete
inancije;OrderProduction.aspx;AccountingSearch.aspx;user287;;Session859;1.1.2017. 11:39:40;Testni event data: 1.1.2017. 11:39:40-Update;Update
inancije;OrderProduction.aspx;;user285;;Session911;1.1.2017. 11:39:47;Testni event data: 1.1.2017. 11:39:47-Open;Open
inancije;OrderProduction.aspx;;user34;;Session912;1.1.2017. 11:39:54;Testni event data: 1.1.2017. 11:39:54-Open;Open
et;MOP;Stranica2;AccountingSearch.aspx;user105;;Session592;1.1.2017. 11:40:01;Testni event data: 1.1.2017. 11:40:01-Save;Save
et;MOP;Stranica4;AccountingSearch.aspx;user129;;Session625;1.1.2017. 11:40:08;Testni event data: 1.1.2017. 11:40:08-Save;Save
inancije;OrderProduction.aspx;;user5;;Session913;1.1.2017. 11:40:15;Testni event data: 1.1.2017. 11:40:15-Open;Open
et;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user195;;Session774;1.1.2017. 11:40:22;Testni event data: 1.1.2017. 11:40:22-Open;Open
inancije;OrderProduction.aspx;AccountingSearch.aspx;user285;;Session911;1.1.2017. 11:40:29;Testni event data: 1.1.2017. 11:40:29-Update;Update
et;MOP;Stranica2;AccountingSearch.aspx;user137;;Session848;1.1.2017. 11:40:36;Testni event data: 1.1.2017. 11:40:36-Open;Open
et;MOP;Stranica1;AccountingSearch.aspx;user39;;Session641;1.1.2017. 11:40:43;Testni event data: 1.1.2017. 11:40:43-Save;Save
et;MOP;Stranica1;AccountingSearch.aspx;user234;;Session675;1.1.2017. 11:40:50;Testni event data: 1.1.2017. 11:40:50-Open;Open
inancije;OrderProduction.aspx;AccountingSearch.aspx;user166;;Session862;1.1.2017. 11:40:57;Testni event data: 1.1.2017. 11:40:57-Update;Update
et;MOP;Stranica1;AccountingSearch.aspx;user172;;Session648;1.1.2017. 11:41:04;Testni event data: 1.1.2017. 11:41:04-Save;Save
inancije;OrderProduction.aspx;;user48;;Session914;1.1.2017. 11:41:11;Testni event data: 1.1.2017. 11:41:11-Open;Open
et;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user270;;Session604;1.1.2017. 11:41:18;Testni event data: 1.1.2017. 11:41:18-Delete;Delete
et;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user35;;Session35;1.1.2017. 11:41:25;Testni event data: 1.1.2017. 11:41:25-Save;Save
et;MOP;Stranica4;AccountingSearch.aspx;user265;;Session889;1.1.2017. 11:41:32;Testni event data: 1.1.2017. 11:41:32-Open;Open
inancije;OrderProduction.aspx;;user69;;Session915;1.1.2017. 11:41:39;Testni event data: 1.1.2017. 11:41:39-Open;Open

Logs



Logs


gronet;MOP;Stranica2;AccountingSearch.aspx;user25;;Session868;1.1.2017. 11:36:31;Testni event data: 1.1.2017. 11:36:31-Open;Open
gronet;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user212;;Session696;1.1.2017. 11:36:38;Testni event data: 1.1.2017. 11:36:38-Open;Open
gronet;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user218;;Session900;1.1.2017. 11:36:45;Testni event data: 1.1.2017. 11:36:45-Open;Open
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user266;;Session418;1.1.2017. 11:36:52;Testni event data: 1.1.2017. 11:36:52-Save;Save
SA;Financije;OrderProduction.aspx;;user104;;Session906;1.1.2017. 11:36:59;Testni event data: 1.1.2017. 11:36:59-Open;Open
gronet;MOP;Stranica3;AccountingSearch.aspx;user258;;Session713;1.1.2017. 11:37:06;Testni event data: 1.1.2017. 11:37:06-Save;Save
SA;Financije;OrderProduction.aspx;;user278;;Session907;1.1.2017. 11:37:13;Testni event data: 1.1.2017. 11:37:13-Open;Open
SA;Financije;OrderProduction.aspx;AccountingSearch.aspx;user158;;Session481;1.1.2017. 11:37:20;Testni event data: 1.1.2017. 11:37:20-Update;Updat
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user260;;Session673;1.1.2017. 11:37:27;Testni event data: 1.1.2017. 11:37:27-Open;Open
gronet;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user200;;Session856;1.1.2017. 11:37:34;Testni event data: 1.1.2017. 11:37:34-Open;Open
SA;Financije;OrderProduction.aspx;;user189;;Session908;1.1.2017. 11:37:41;Testni event data: 1.1.2017. 11:37:41-Open;Open
gronet;MOP;Stranica3;AccountingSearch.aspx;user130;;Session679;1.1.2017. 11:37:48;Testni event data: 1.1.2017. 11:37:48-Save;Save
gronet;MOP;Stranica2;AccountingSearch.aspx;user149;;Session149;1.1.2017. 11:37:55;Testni event data: 1.1.2017. 11:37:55-Open;Open
gronet;MOP;Stranica4;AccountingSearch.aspx;user61;;Session799;1.1.2017. 11:38:02;Testni event data: 1.1.2017. 11:38:02-Delete;Delete
gronet;MOP;Stranica1;AccountingSearch.aspx;user163;;Session570;1.1.2017. 11:38:09;Testni event data: 1.1.2017. 11:38:09-Delete;Delete
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user13;;Session887;1.1.2017. 11:38:16;Testni event data: 1.1.2017. 11:38:16-Open;Open
SA;Financije;OrderProduction.aspx;AccountingSearch.aspx;user290;;Session852;1.1.2017. 11:38:23;Testni event data: 1.1.2017. 11:38:23-Update;Updat
gronet;MOP;Stranica4;AccountingSearch.aspx;user27;;Session457;1.1.2017. 11:38:30;Testni event data: 1.1.2017. 11:38:30-Open;Open
gronet;MOP;Stranica2;AccountingSearch.aspx;user193;;Session407;1.1.2017. 11:38:37;Testni event data: 1.1.2017. 11:38:37-Save;Save
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user139;;Session660;1.1.2017. 11:38:44;Testni event data: 1.1.2017. 11:38:44-Open;Open
gronet;MOP;Stranica2;AccountingSearch.aspx;user193;;Session407;1.1.2017. 11:38:51;Testni event data: 1.1.2017. 11:38:51-Save;Save
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user139;;Session660;1.1.2017. 11:38:58;Testni event data: 1.1.2017. 11:38:58-Open;Open
SA;Financije;OrderProduction.aspx;;user57;;Session909;1.1.2017. 11:39:05;Testni event data: 1.1.2017. 11:39:05-Open;Open
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user245;;Session278;1.1.2017. 11:39:12;Testni event data: 1.1.2017. 11:39:12-Delete;Delet
SA;Financije;OrderProduction.aspx;;user160;;Session910;1.1.2017. 11:39:19;Testni event data: 1.1.2017. 11:39:19-Open;Open
SA;Financije;OrderProduction.aspx;AccountingSearch.aspx;user9;;Session904;1.1.2017. 11:39:26;Testni event data: 1.1.2017. 11:39:26-Delete;Delete
gronet;MOP;Stranica1;AccountingSearch.aspx;user294;;Session540;1.1.2017. 11:39:33;Testni event data: 1.1.2017. 11:39:33-Delete;Delete
SA;Financije;OrderProduction.aspx;AccountingSearch.aspx;user287;;Session859;1.1.2017. 11:39:40;Testni event data: 1.1.2017. 11:39:40-Update;Updat
SA;Financije;OrderProduction.aspx;;user285;;Session911;1.1.2017. 11:39:47;Testni event data: 1.1.2017. 11:39:47-Open;Open
SA;Financije;OrderProduction.aspx;;user34;;Session912;1.1.2017. 11:39:54;Testni event data: 1.1.2017. 11:39:54-Open;Open
gronet;MOP;Stranica2;AccountingSearch.aspx;user105;;Session592;1.1.2017. 11:40:01;Testni event data: 1.1.2017. 11:40:01-Save;Save
gronet;MOP;Stranica4;AccountingSearch.aspx;user129;;Session625;1.1.2017. 11:40:08;Testni event data: 1.1.2017. 11:40:08-Save;Save
SA;Financije;OrderProduction.aspx;;user5;;Session913;1.1.2017. 11:40:15;Testni event data: 1.1.2017. 11:40:15-Open;Open
gronet;MOP;Stranica2/Podstranica1;AccountingSearch.aspx;user195;;Session774;1.1.2017. 11:40:22;Testni event data: 1.1.2017. 11:40:22-Open;Open
SA;Financije;OrderProduction.aspx;AccountingSearch.aspx;user285;;Session911;1.1.2017. 11:40:29;Testni event data: 1.1.2017. 11:40:29-Update;Updat
gronet;MOP;Stranica2;AccountingSearch.aspx;user137;;Session848;1.1.2017. 11:40:36;Testni event data: 1.1.2017. 11:40:36-Open;Open
gronet;MOP;Stranica1;AccountingSearch.aspx;user39;;Session641;1.1.2017. 11:40:43;Testni event data: 1.1.2017. 11:40:43-Save;Save
gronet;MOP;Stranica1;AccountingSearch.aspx;user234;;Session675;1.1.2017. 11:40:50;Testni event data: 1.1.2017. 11:40:50-Open;Open
SA;Financije;OrderProduction.aspx;AccountingSearch.aspx;user166;;Session862;1.1.2017. 11:40:57;Testni event data: 1.1.2017. 11:40:57-Update;Updat
gronet;MOP;Stranica1;AccountingSearch.aspx;user172;;Session648;1.1.2017. 11:41:04;Testni event data: 1.1.2017. 11:41:04-Save;Save
SA;Financije;OrderProduction.aspx;;user48;;Session914;1.1.2017. 11:41:11;Testni event data: 1.1.2017. 11:41:11-Open;Open
gronet;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user270;;Session604;1.1.2017. 11:41:18;Testni event data: 1.1.2017. 11:41:18-Delete;Delet
gronet;MOP;Stranica1/Podstranica1;AccountingSearch.aspx;user35;;Session35;1.1.2017. 11:41:25;Testni event data: 1.1.2017. 11:41:25-Save;Save
gronet;MOP;Stranica4;AccountingSearch.aspx;user265;;Session889;1.1.2017. 11:41:32;Testni event data: 1.1.2017. 11:41:32-Open;Open

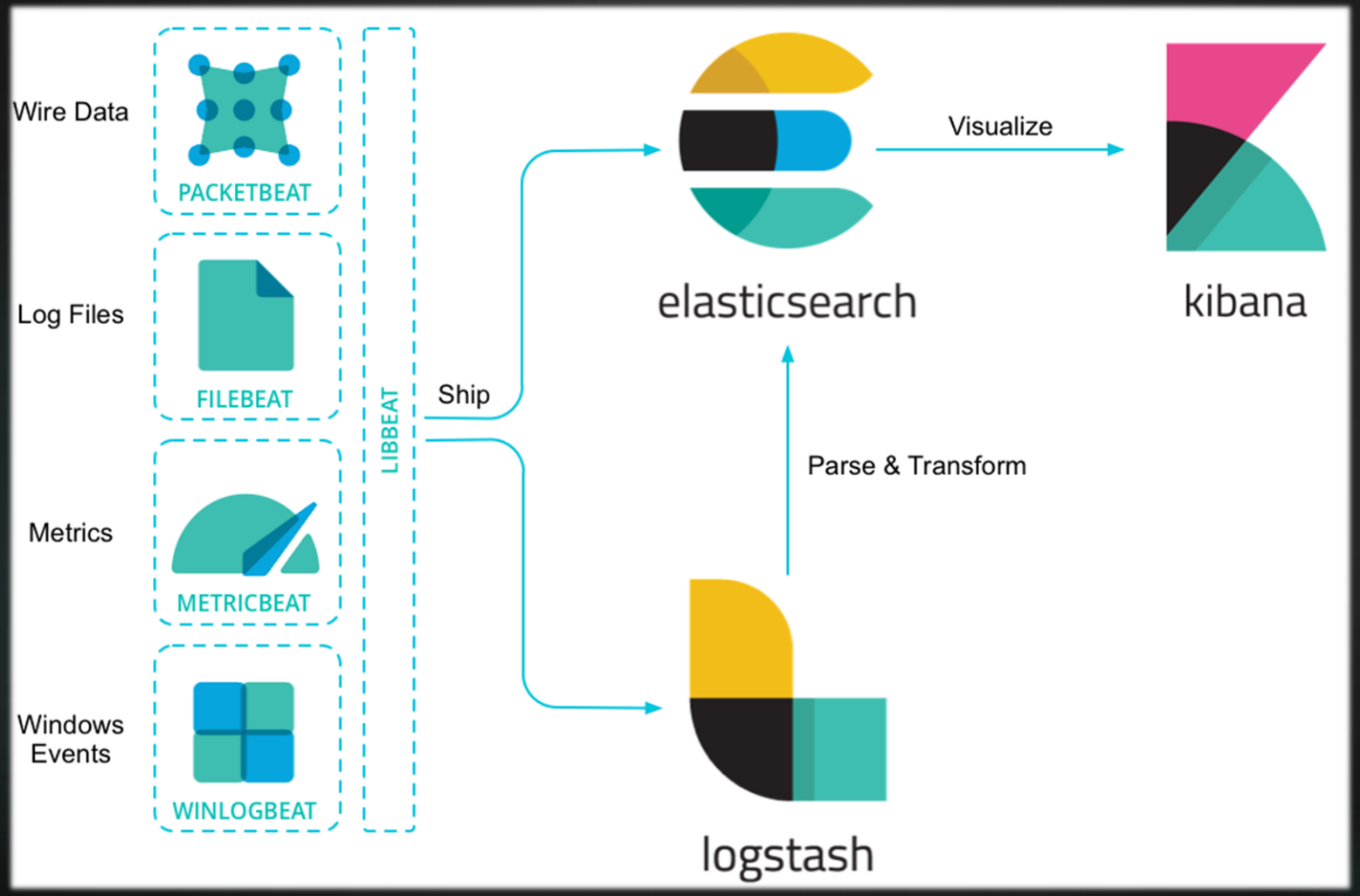

Dashboard / [DEMO]
Add
Save
Share
Options
Reporting
Last 4 hours
*
23. Vizualizacija : Prikaz broja korisnika
Unique session count
0
5
10
15
20
25
04:30
05:00
05:30
06:00
06:30
07:00
07:30
08:00
Vrijeme

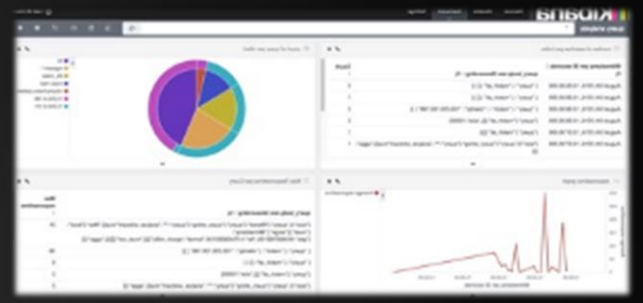
Elastic Stack

Elastic Stack

Plugins…Lots of plugins

Elastic Stack





Beats

- Lightweight data shippers
- Filebeat, Metricbeat, Packetbeat, Winlogbeat, Heartbeat
- 60+ community beats

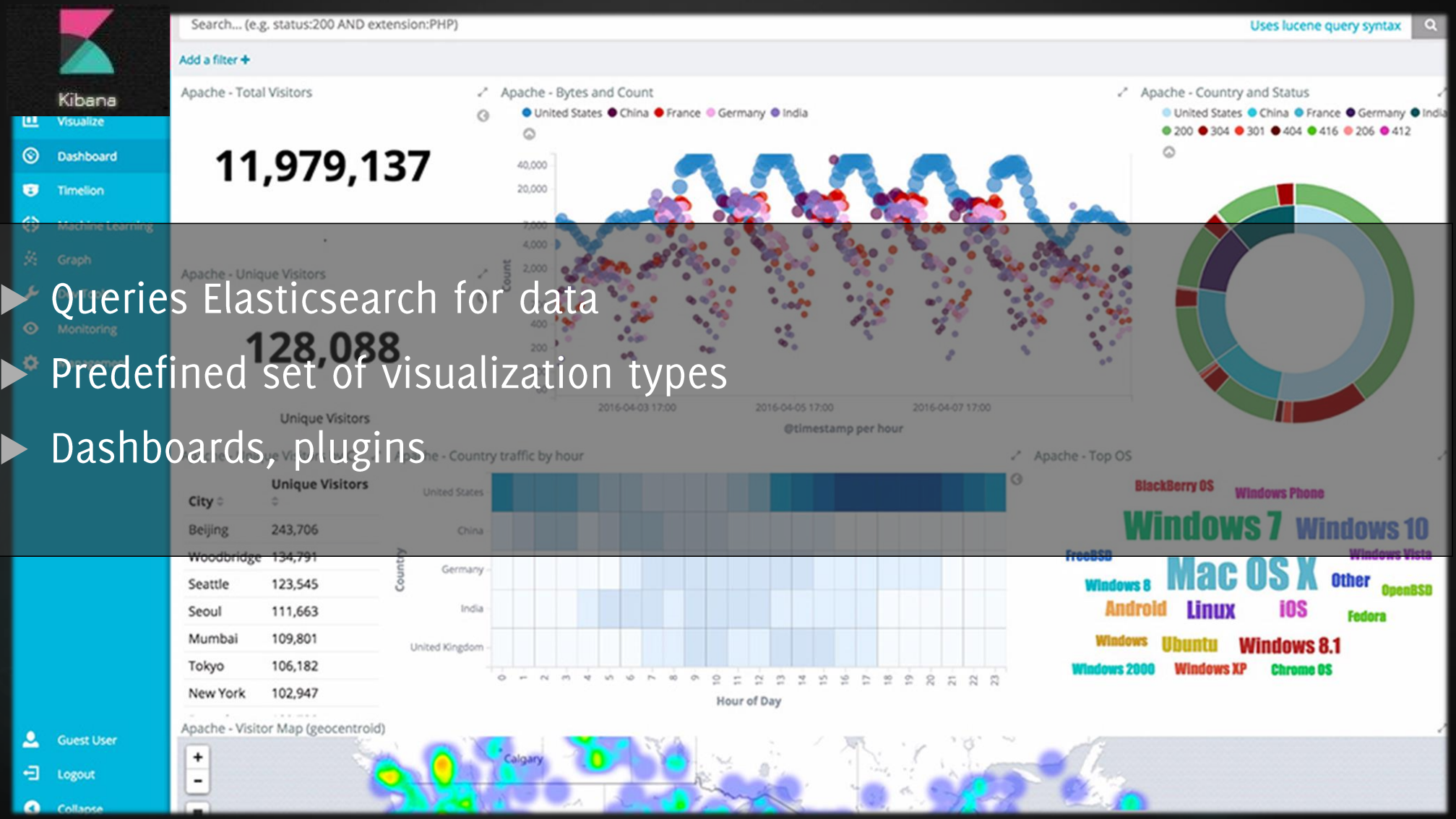
Logstash

- Input/output from 50+ destinations
- Extracts and transforms data
- 30+ plugins for data manipulation

Elasticsearch

- Real time search and analytics engine
- Restful JSON API
- Scalable, reliable
- Index and archives

Kibana



- Queries Elasticsearch for data
- Predefined set of visualization types
- Dashboards, plugins

Setup

- Running each component manually
- Installing as a service
- Docker, Vagrant image

- Configure input/output and component specific parameters
- Configure “index pattern”

Setup

```
input {
  # 55+ plugins (file, beats, twitter, http, jms, jdbc, elastic...)
}

# optional filter
filter {
  # 30+ plugins (csv, grok, i18n, useragent, mutate, json...)
}

output {
  # 55+ plugins (file, beats, twitter, http, jms, jdbc, elastic...)
}

```

logstash.yml configuration

Setup

*beatname.template.json

curl -XPUT "http://localhost:9200/_template/filebeat?pretty" -d@filebeat.template.json

```
λ curl 'localhost:9200/_cat/indices?v'
health status index                 uuid                   pri rep docs.count
yellow open   metricbeat-2017.10.15 Kqaa2Jf4TLuQVAvNr9XzYA   5   1      37814
yellow open   .kibana               aoYP9vCPTb-1Vlzs7SkFhg   1   1         22
yellow open   filebeat-2017.10.11   S-kHravKRraLRyIN-9V3Ng   5   1        556
yellow open   elastalert_status     ITGgI0IxQ9Wr2i6Za_wJJg   5   1         19
yellow open   httpbeat-2017.10.17   I6GeSMaGQCW2fuCbC3-1Mw   5   1      12322
yellow open   logstash-2017.10.17   XCmUuwfRRKCQ9BqI2YfCfQ   5   1       2860
yellow open   logstash-2017.10.16   vzih9sRuQSyRMi2ZQOki1Q   5   1        838
yellow open   httpbeat-2017.10.18   TkxwWP4YSr2q4MIXAHRZ6g   5   1       2676
```

Monitoring

- Application/integration endpoints heartbeat › HeartBeat
- System performance counters › MetricBeat
- Logs › FileBeat
- DB/performance counters › logstash-input-jdbc
- Spring Boot (Actuator) › HttpBeat

Alerting

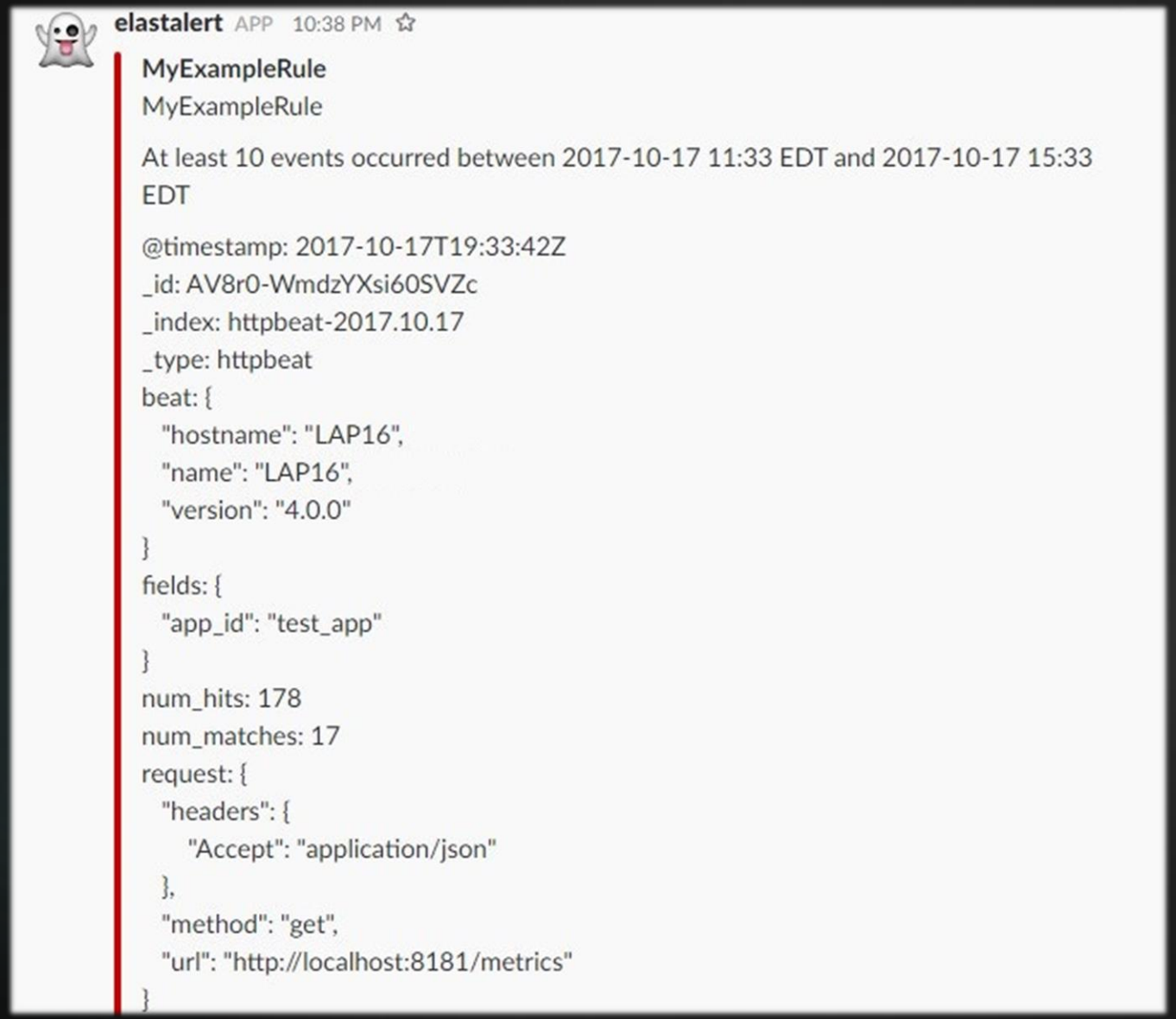
- X-Pack 

- ElastAlert – free alternative
- Alert via email, JIRA, Slack, Telegram, execute command...
- Rules:

- "Match where there are X events in Y time" (`frequency` type)
- "Match when the rate of events increases or decreases" (`spike` type)
- "Match when there are less than X events in Y time" (`flatline` type)
- "Match when a certain field matches a blacklist/whitelist" (`blacklist` and `whitelist` type)
- "Match on any event matching a given filter" (`any` type)
- "Match when a field has two different values within some time" (`change` type)

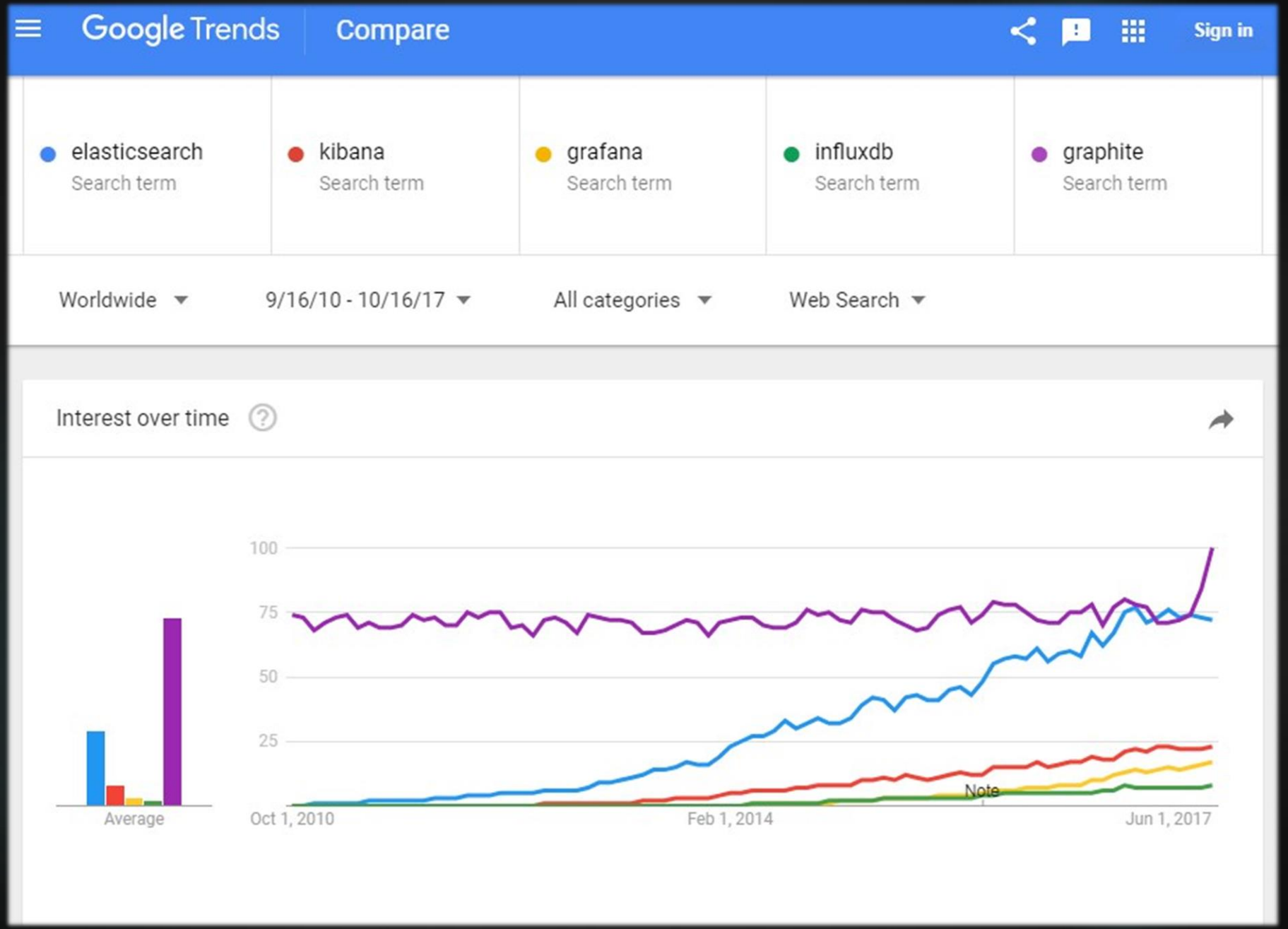
```yaml
# Alert when the rate of events exceeds a threshold

# Rule name, must be unique
name: MyExampleRule
# the frequency rule type alerts when num_events events occur with timeframe time
type: frequency
# Index to search, wildcard supported
index: httpbeat-*
# Alert when this many documents matching the query occur within a timeframe
num_events: 10
# num_events must occur within this amount of time to trigger an alert
timeframe:
  hours: 4
# A list of Elasticsearch filters used for find events
filter:
- term:
    response.statusCode  : "500"
# The alert is use when a match is found
alert:
- "slack"
slack:
slack_webhook_url: "https://hooks.slack.com/services/xxx/yyy"
```

Alerting


elastalert APP 10:38 PM
MyExampleRule
MyExampleRule
At least 10 events occurred between 2017-10-17 11:33 EDT and 2017-10-17 15:33 EDT
@timestamp: 2017-10-17T19:33:42Z
_id: AV8r0-WmdzYXsi60SVZc
_index: httpbeat-2017.10.17
_type: httpbeat
beat: {
"hostname": "LAP16",
"name": "LAP16",
"version": "4.0.0"
}
fields: {
"app_id": "test_app"
}
num_hits: 178
num_matches: 17
request: {
"headers": {
"Accept": "application/json"
},
"method": "get",
"url": "http://localhost:8181/metrics"
}

Conclusion

- Benefits/drawbacks
- Learn from logs
- Getting bigger picture, detecting hard to find patterns
- Predicting upcoming service disruption
- Automated alerts, buying time when service fails


Google Trends
Compare
Sign in
elasticsearch
Search term
kibana
Search term
grafana
Search term
influxdb
Search term
graphite
Search term
Worldwide
9/16/10 - 10/16/17
All categories
Web Search
Interest over time
100
75
50
25
Note
Average
Oct 1, 2010
Feb 1, 2014
Jun 1, 2017

Q/A

- https://demo.elastic.co
- https://hub.docker.com/r/sebp/elk/
- https://github.com/Yelp/elastalert
- https://github.com/dzharii/awesome-elasticsearch

Conference and Media Partners

KING ICT
SAP
ORACLE
VOXXEDDAYS BELGRADE
NETOKRACIJA
InfoQ
MREŽA
ICT Business