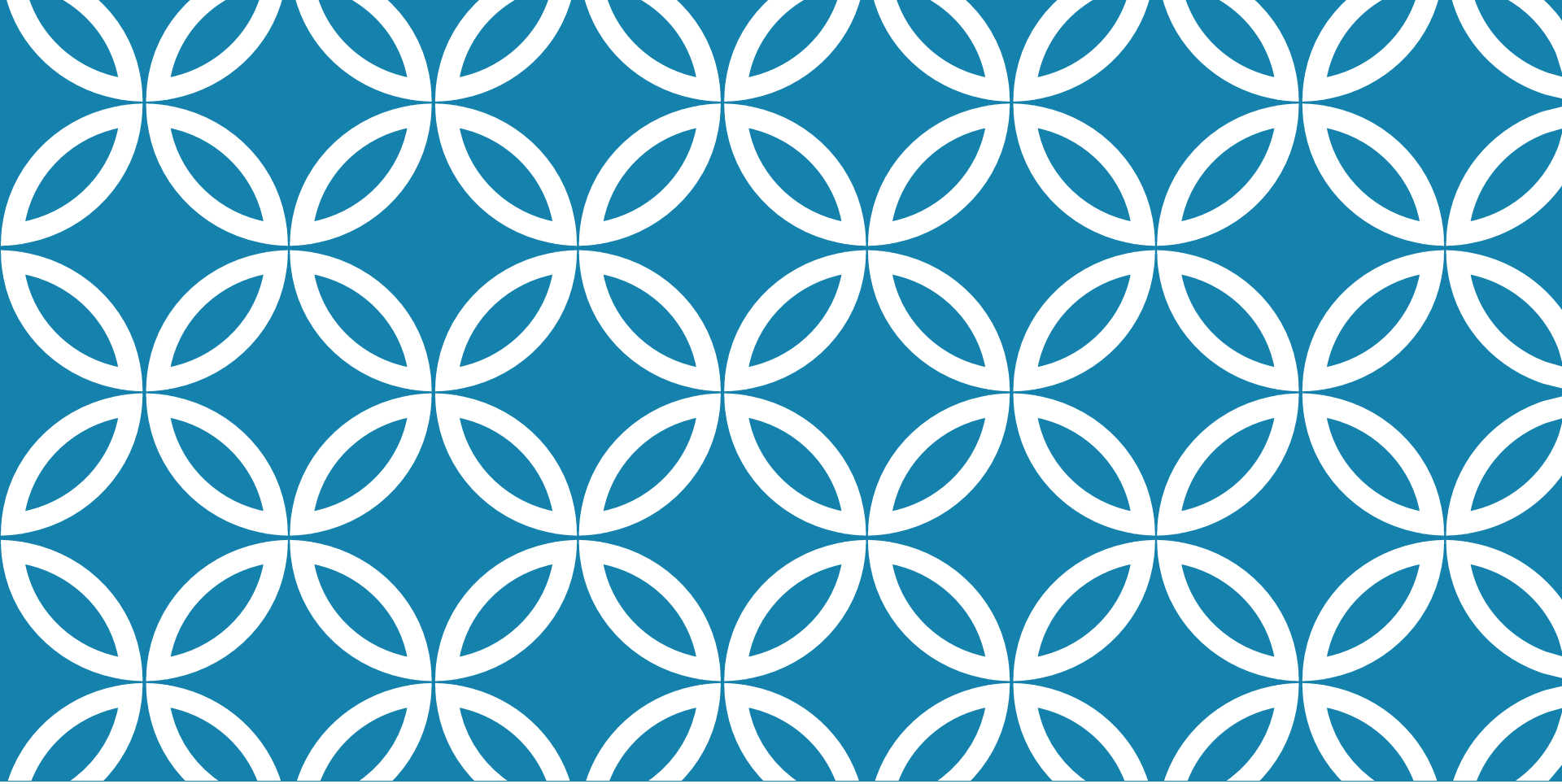
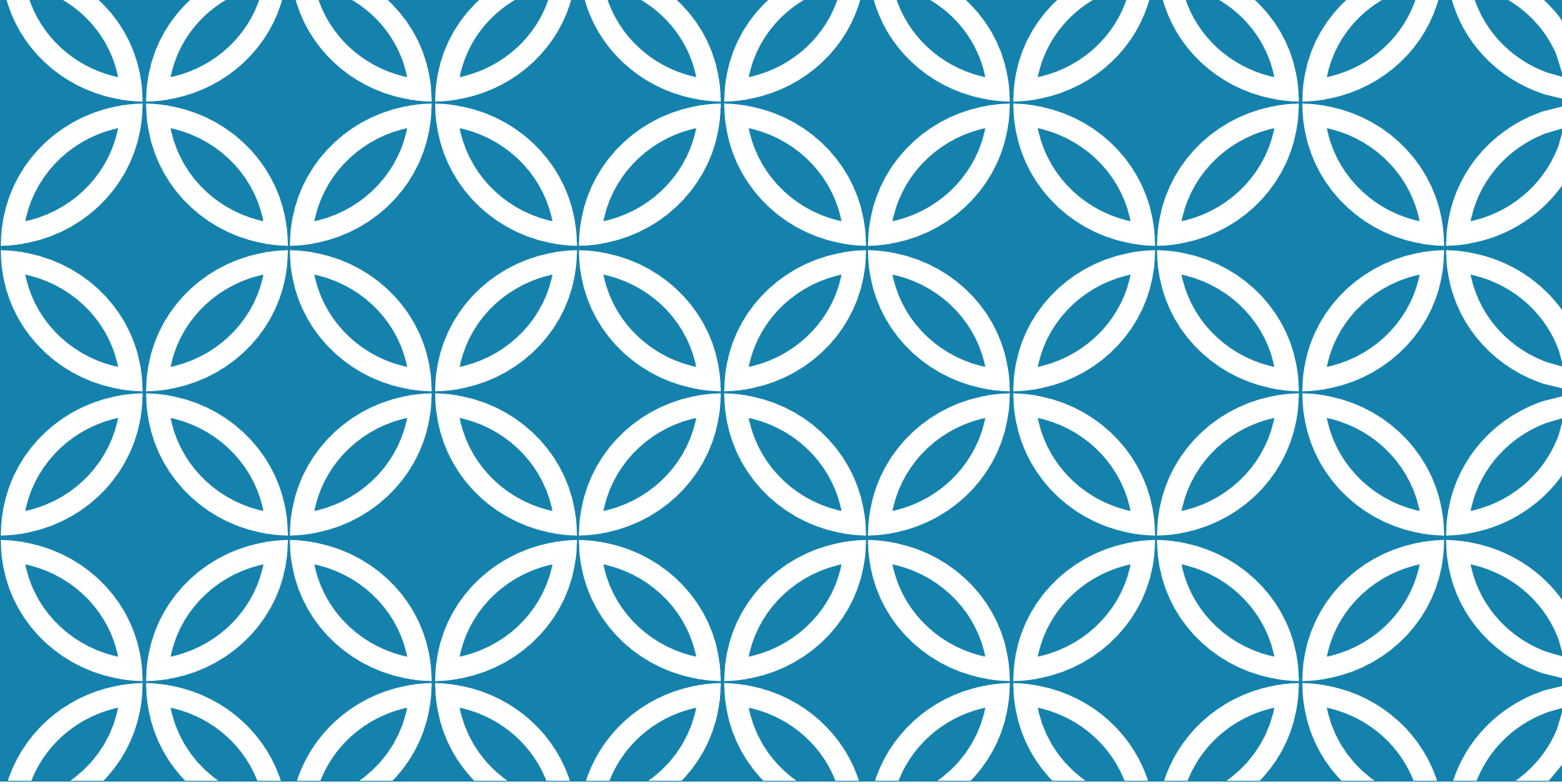


EUROPEN 2016: TUTORIAL

Vašek Lorenc



2ND PART

GrayLog2 + ELK

CONTENTS

Open source solutions

- GrayLog2
- Elastic Stack

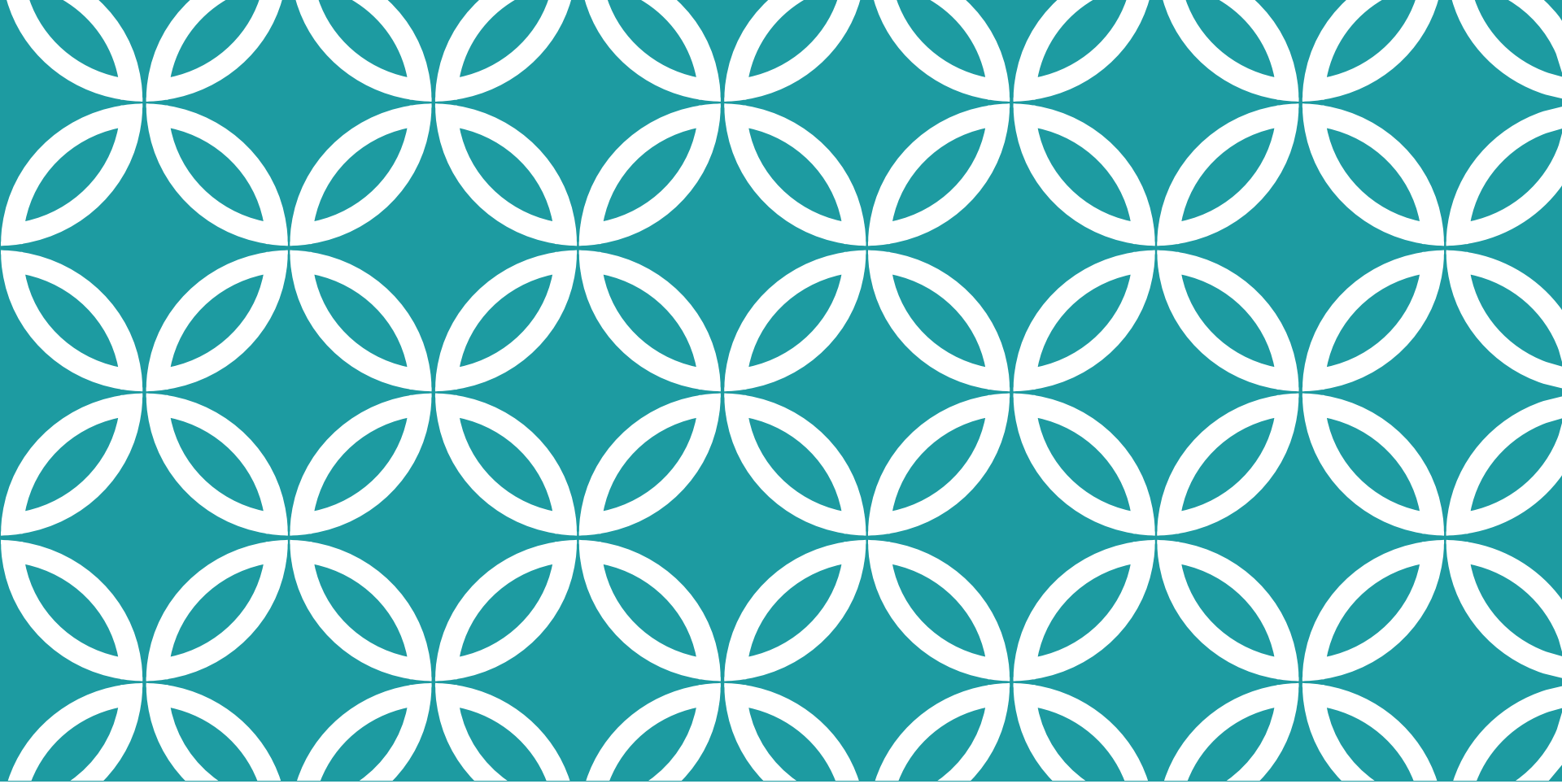
Hands-on Examples

- Cisco (ASA) logy
- Twitter API
- E-mails processing (IMAP)
- VirusShare/APTNotes

Further sources of (security) data

Related tools

Q&A



GRAYLOG2

Brief Introduction

GRAYLOG2

VM:

graylog-box.ova

Accesses:

admin/admin (web)

europen/europen (ssh)

Ports on your host:

8081/tcp (web)

12201/{udp,tcp}

5044/{udp,tcp}

2222/tcp (ssh)

Description

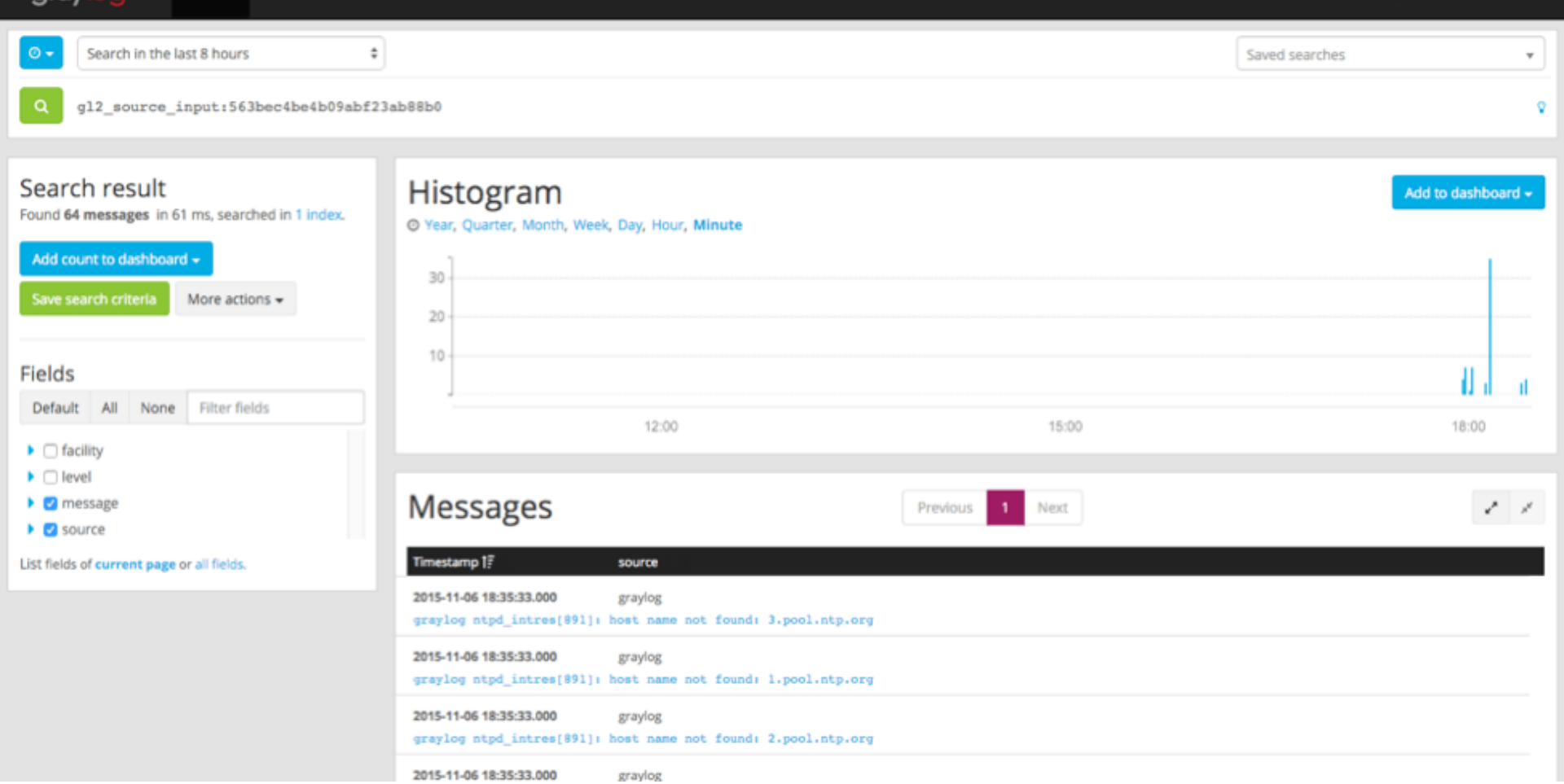
Inputs

Extractors

Dashboards

Streams

Alerts



BASIC USER INTERFACE

All-In-One

GRAYLOG2: BRIEF INTRODUCTION

Easy-to-use Solution (just like Splunk)

- Powerful search capabilities + syntax completion
- Dashboards
- Authentication, roles
- Alerting, notifications(Slack, JIRA, PagerDuty, …)
- Company-wide deployment scenarios, documented
- Scalable
- Plenty of various input modules, easy setup
- API

Drawbacks

- Aggregation functions missing

EXAMPLE: CISCO ASA

Input configuration

- Syslog TCP, port 5044

Extractors

Data processing configuration

- (See the next picture)

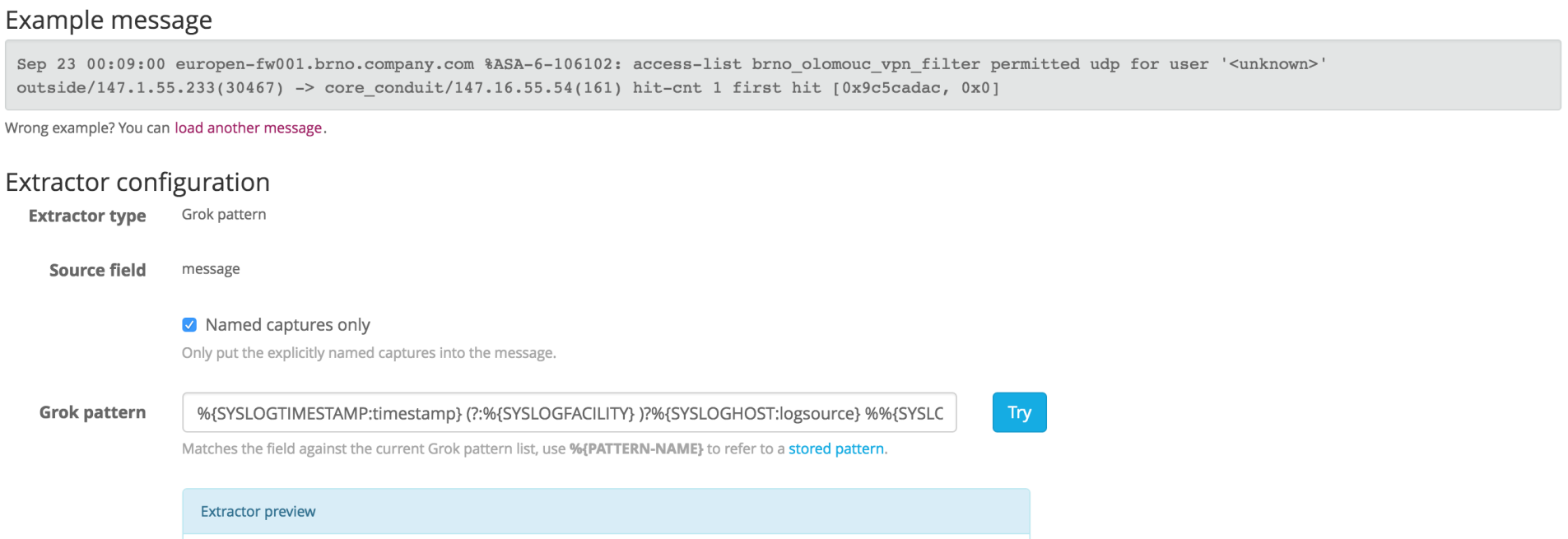
Searching

- Do your own searches!

Dashboard

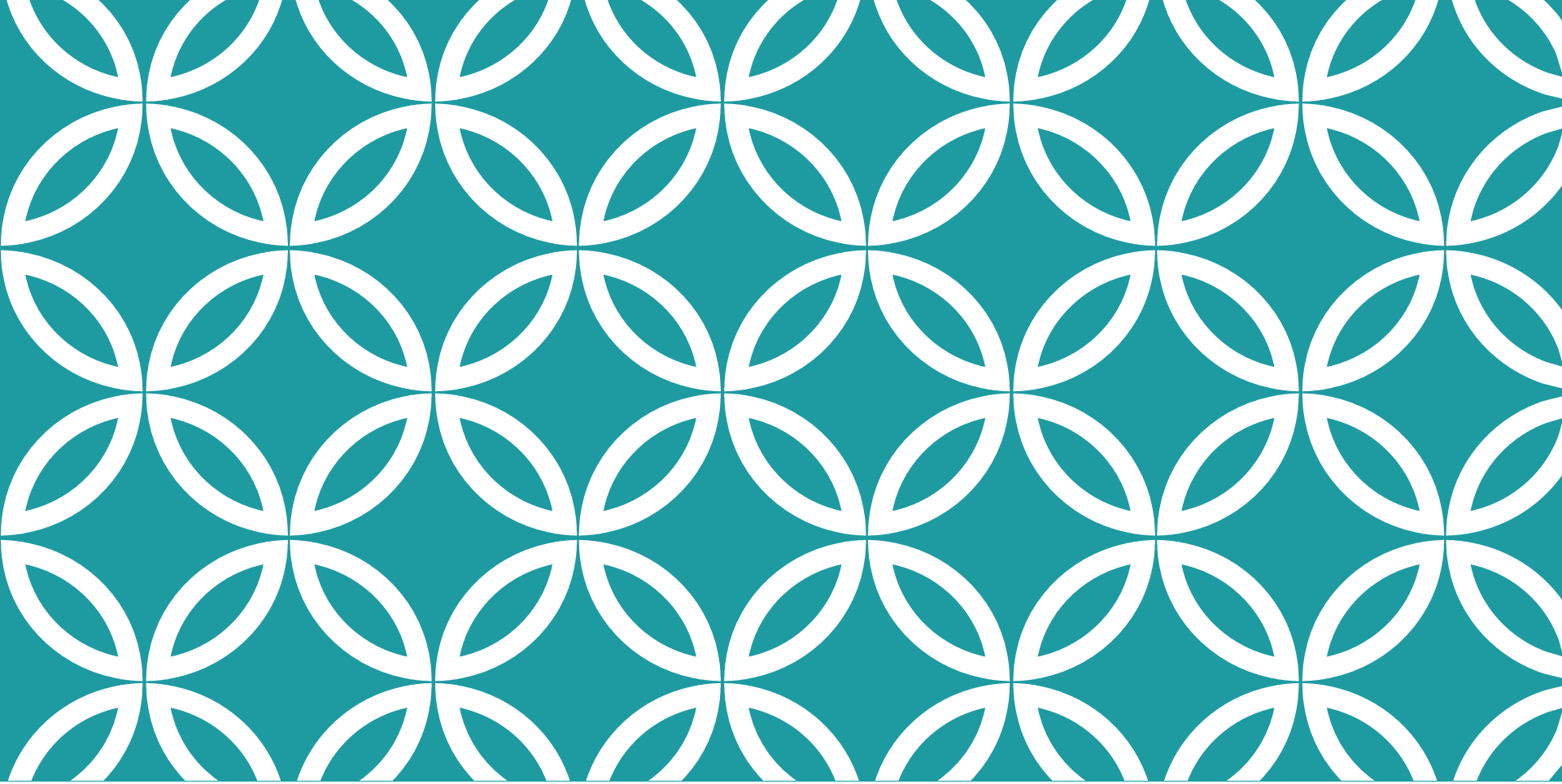
- First, create an empty dashboard, second add widgets from searches

Streams + Alerting



CREATING AN EXTRACTOR

... in Graylog



ELASTIC STACK

Not-so-brief Introduction

ELASTIC STACK

VM:

vagrant-elk-box.ova

Accesses:

europen/europen (ssh)

Ports on your host:

5601/tcp (kibana)
9200/tcp (elasticsearch)
2222/tcp (ssh)

Versions installed:

Elasticsearch 2.3.5
Kibana 4.5.0
Logstash 2.4

Elasticsearch

- Capabilities, options, indexes
- Data types
- Data mapping, templates

Logstash

- Samples of various inputs and configs

Kibana

- Visualizations (simple or powerful)
- Additional applications

elastic

{ELASTIC STACK, ELK, ELK STACK}

Elasticsearch + …

Elastisearch

- Data processing and indexing
- Apache Lucene
- Full-text
- Document database
- JSON

Beats

- Input plugins (Filebeat, …)

… Logstash + Kibana

Logstash

- Powerful tool for data transformations
- Filtering, input and output plugins

Kibana

- Visualization framework
- Plugins available
- Whole app platform (Kibana apps)

ELK VS. {GRAYLOG2, SPLUNK}

What may bother?

No auth and roles by default

No alerting

No cross-joins and lookups

Complicated to set up

Rapid development

What's nice?

Price

Flexibility

Logstash included

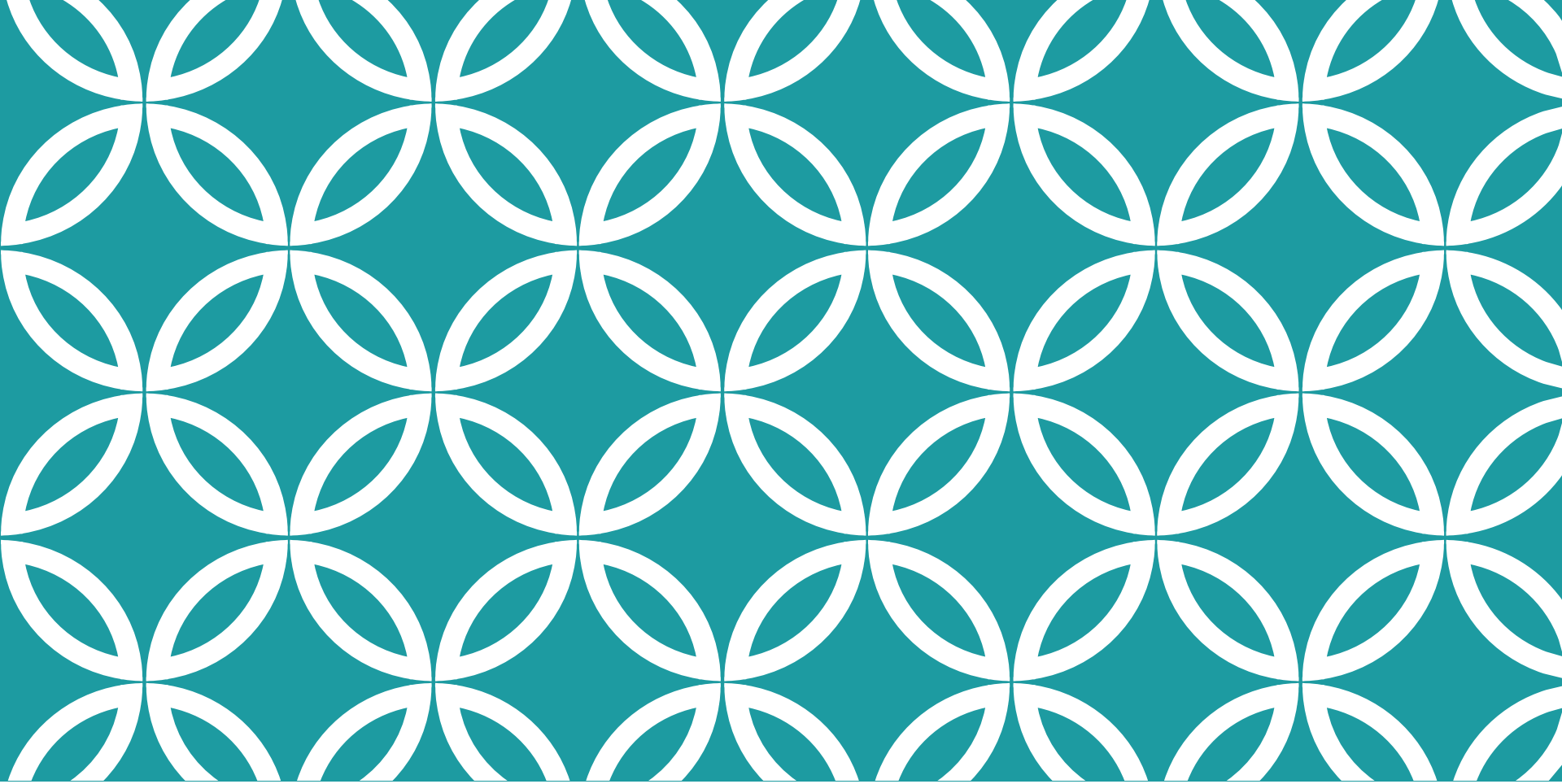
Detailed data management

Rapid development

Community

Similarity search(!)

REST API



LOGSTASH

Transforming Data

LOGSTASH: BASIC WORKFLOW

1. INPUT

   Variety of input plugins and codecs

2. FILTER

   Programming language, in fact (Ruby)

   With all the benefits and drawbacks

   "*grok is the new grep*"

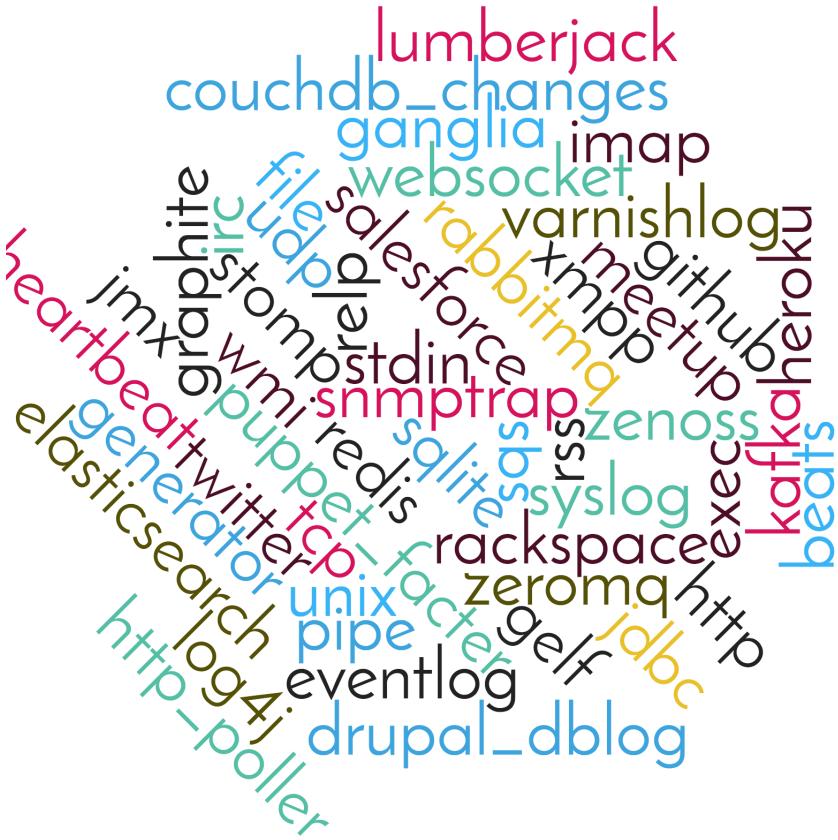
3. OUTPUT

   Variety of output plugins again

   We need just one for Elastic output though…

LOGSTASH: INPUT

imap
file
stdin
tcp
twitter
…



LOGSTASH: FILTER

grok

mutate

cidr

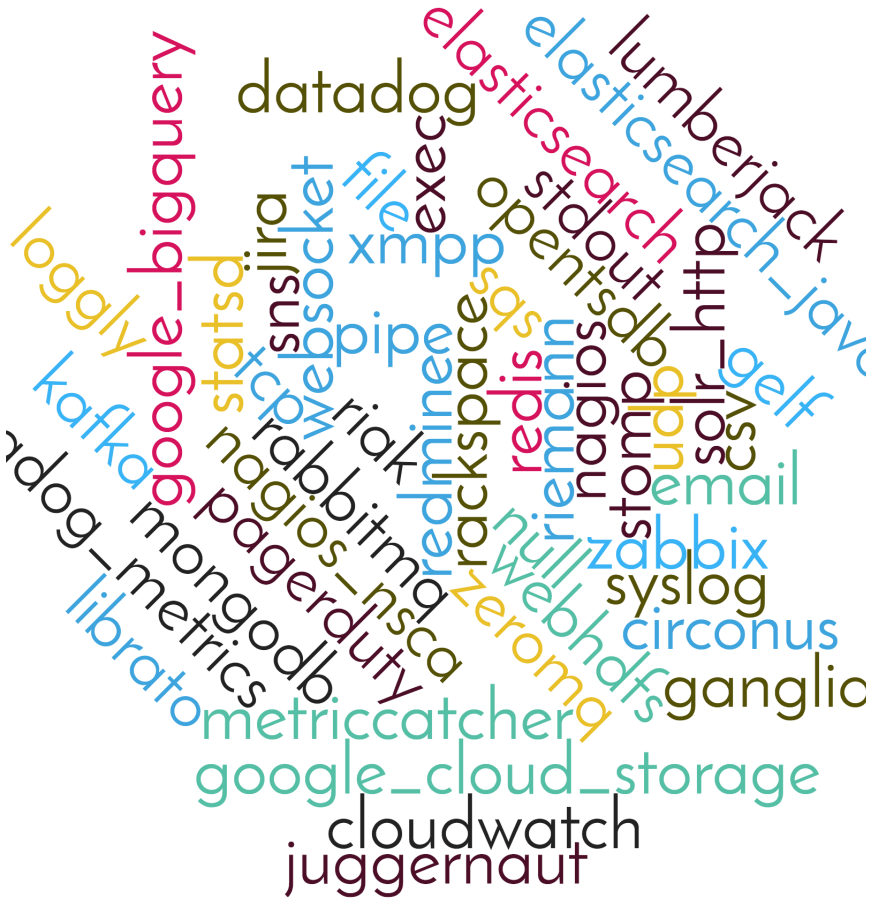
geoip

csv

…

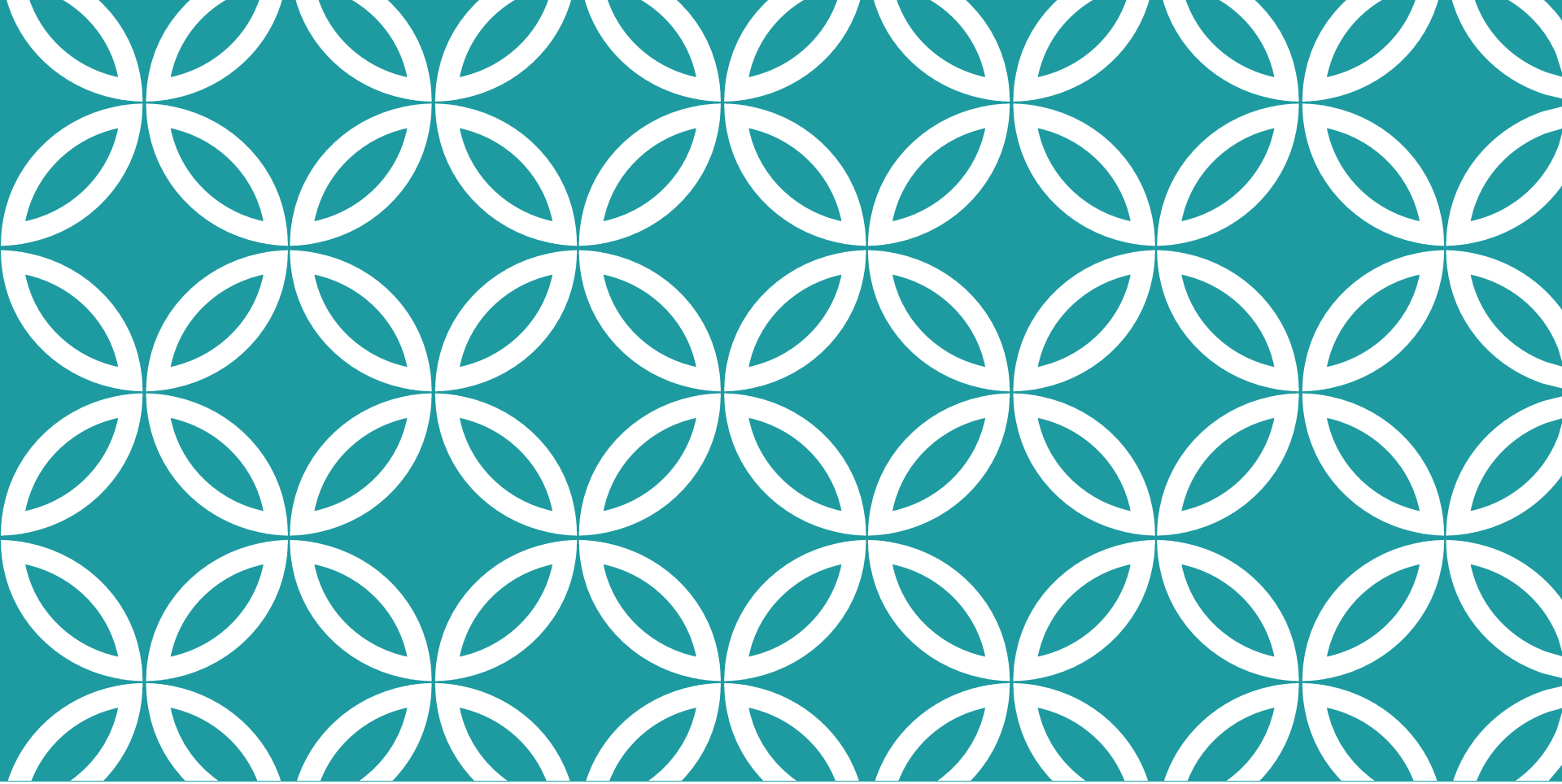
LOGSTASH: OUTPUT

stdout
file
elasticsearch
gelf
…



JSON EVERYWHERE

"Deal with it"



KIBANA

Showing Data

Versions 3, v4, v5, …

KIBANA: VISUALIZATION FRAMEWORK

UI for queries over the data

Visualization

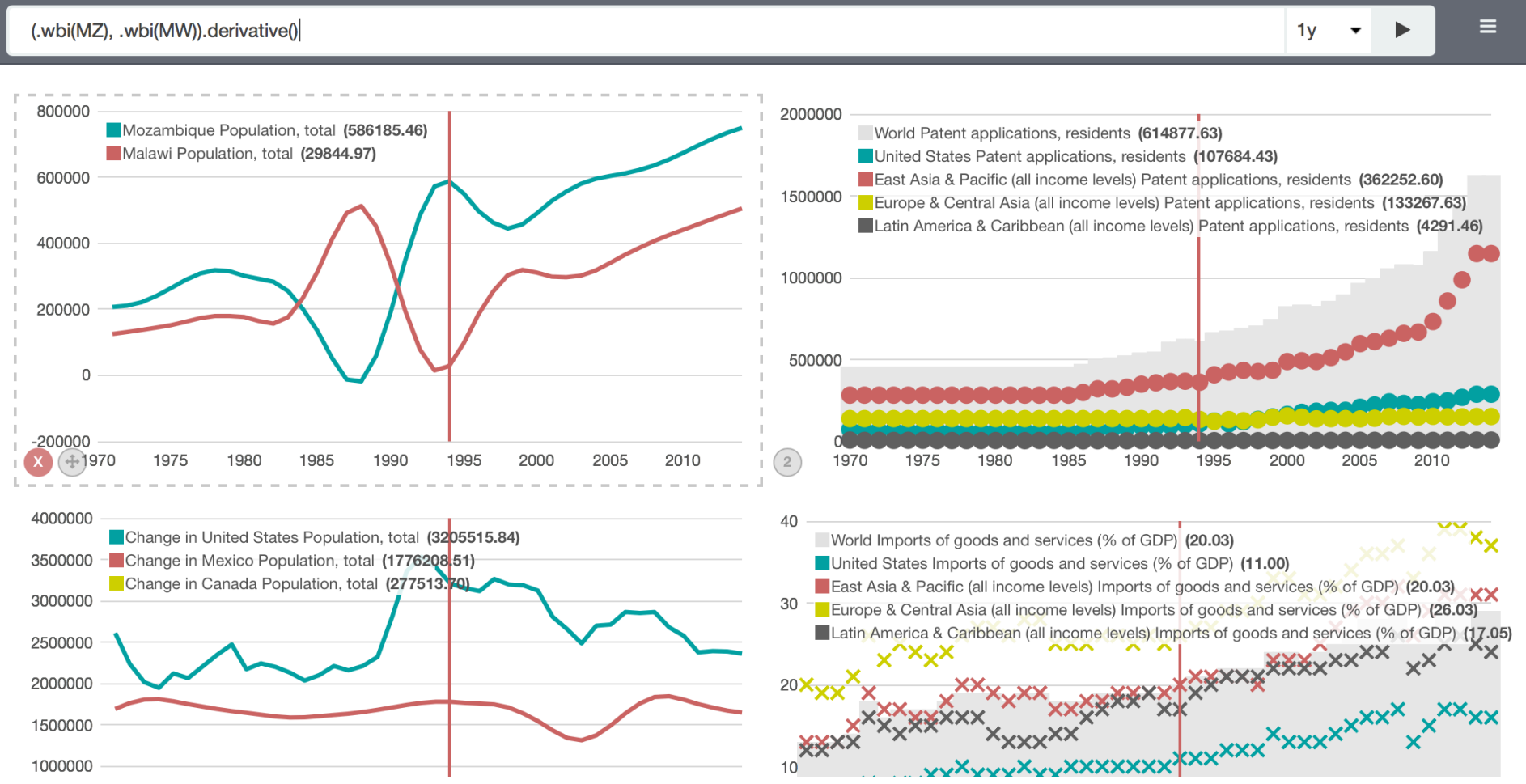
- Variety of visualization plugins
- Some of the non-standard were added to the VM prepared for this tutorial

Application Platform

- Running on node.js, you can write your own plugins and apps

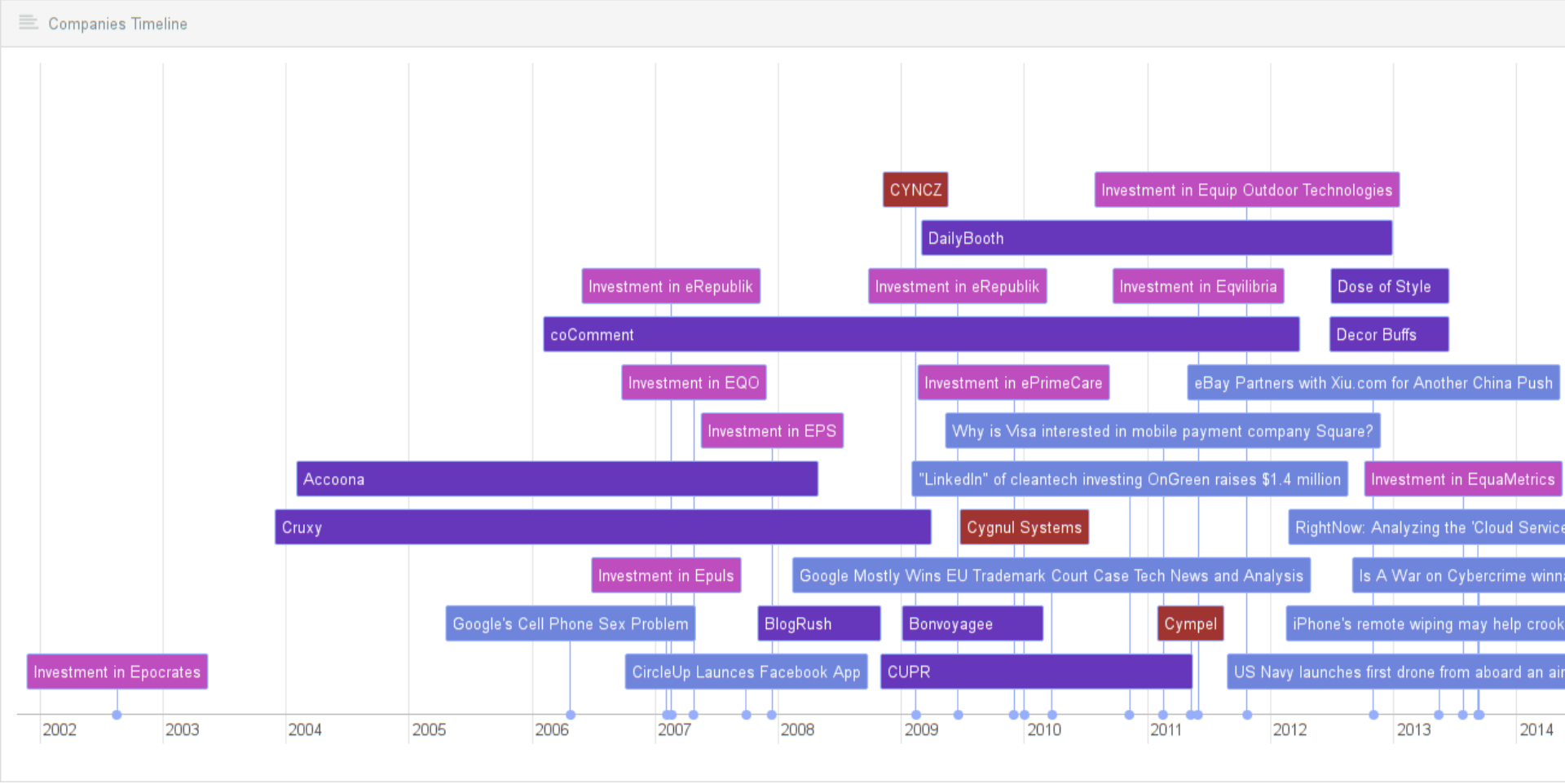
Pre-installed Apps

- Kibana
- Timelion
- Sense
- KAAE (Kibana Alert & Report App for Elastic)



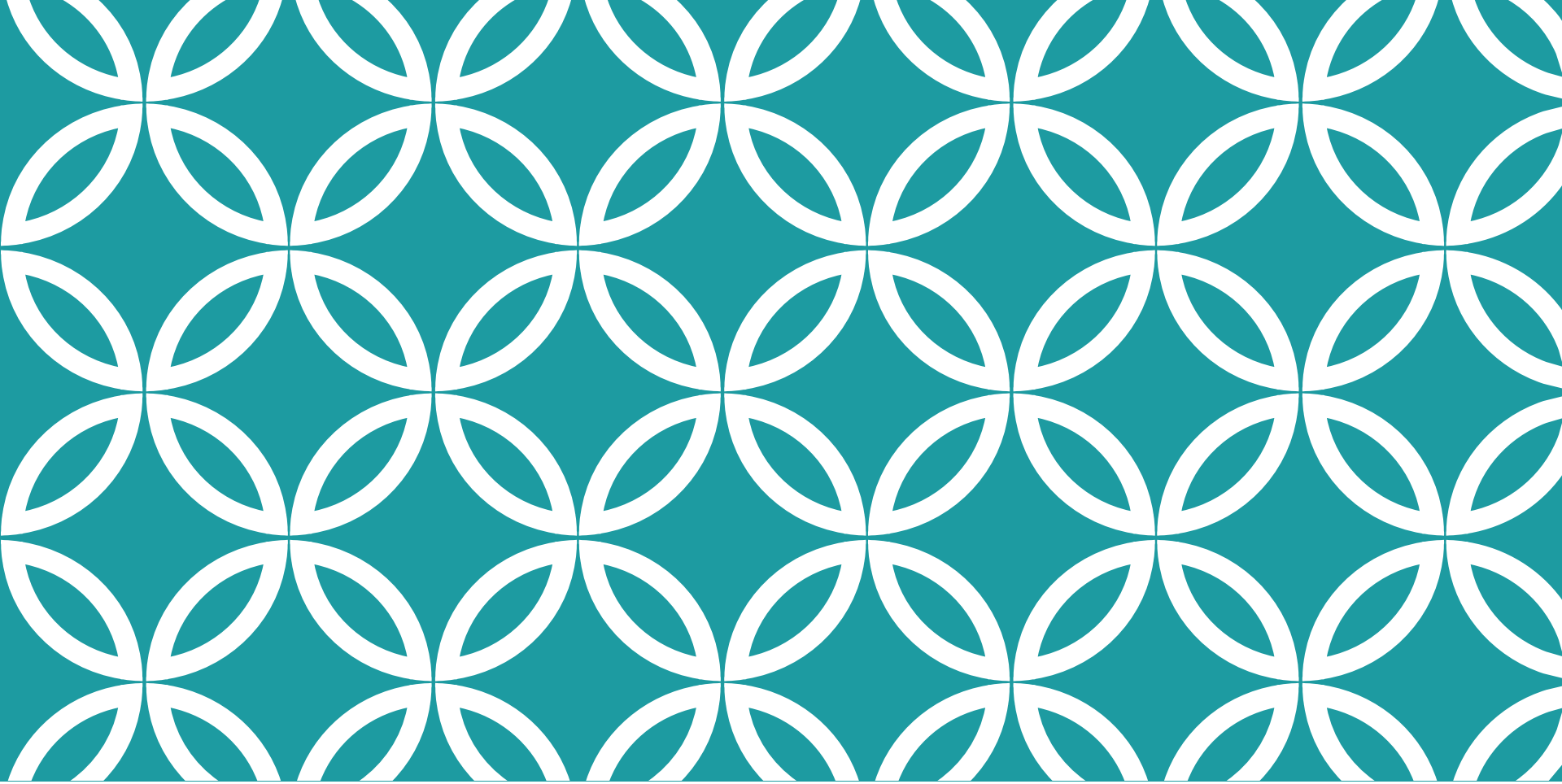
TIMELION

Complex Visualization Example



KIBI TIMELINE

Complex Visualization Example



HANDS-ON EXAMPLES!

Elastic Stack

WORKFLOW FOR EACH EXAMPLE

1. Let's check the raw input data
2. Find a name for the Elasticsearch index
3. Try to configure Logstash
4. Configure Kibana for our index
5. Searching, visualization
6. *(Troubleshooting)*
7. Fixing all issues found, goto 2
8. Another example is waiting!

SYSLOG: CISCO LOGS IN ELASTIC STACK

The data processed in Graylog, now on ELK

Leveraging Logstash

- Configuration of input, filter a output sections
- Grok filter & debugger

Visualization

Tweaking of Logstash configuration files

- Same config can be used for output to Graylog and ELK!

LOGSTASH-CISCO-ELK.CONF (-GELF.CONF)

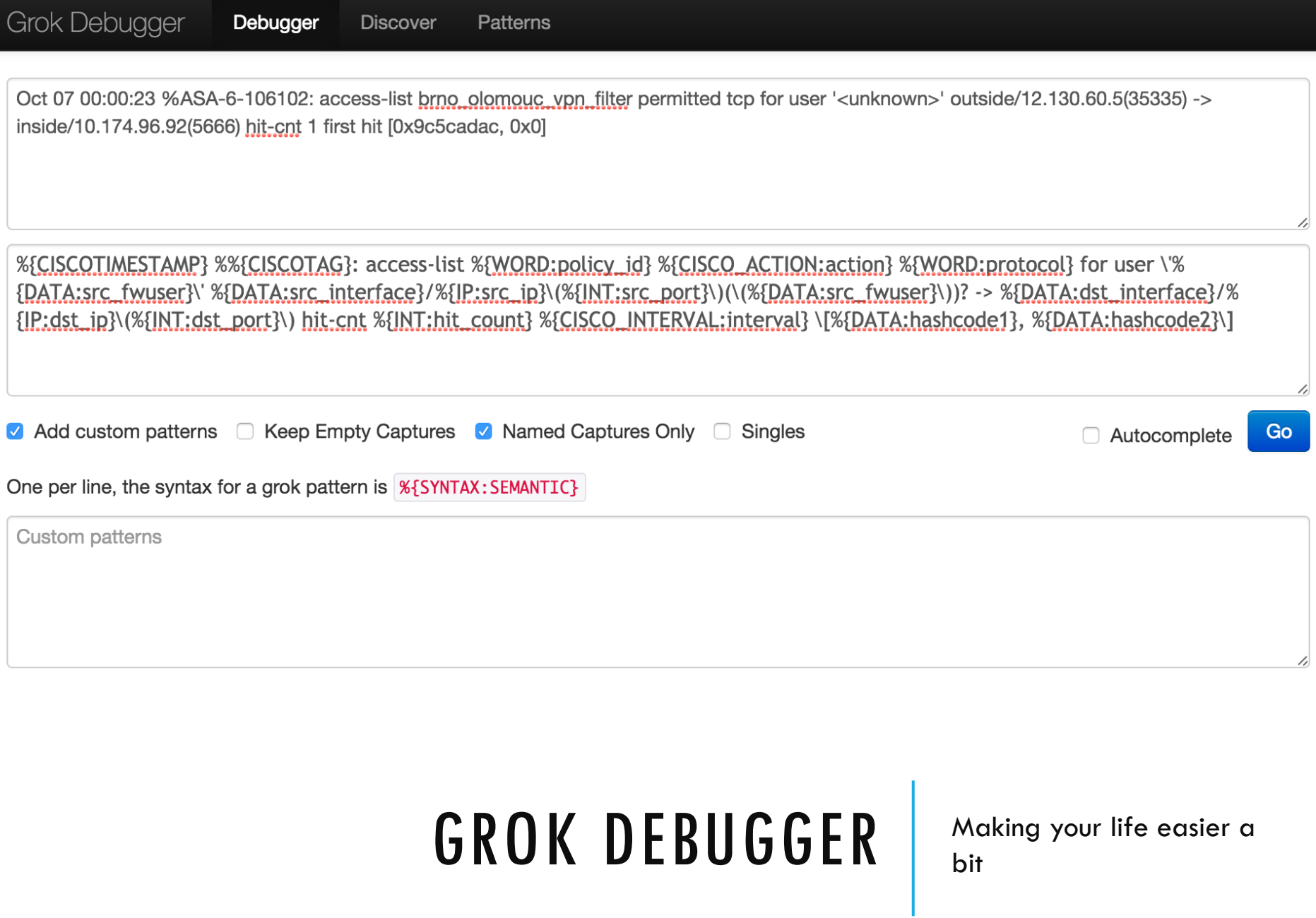
```
input {
    tcp {
        port => 5602
        type => europeninput
    }
}



filter {
}



output {
    elasticsearch { }
}
```



GROK DEBUGGER

Making your life easier a bit

GROK CONFIGURATION

```
filter {
    grok {
      match => ["message", "%{CISCOTIMESTAMP:timestamp}
%{SYSLOGHOST:sysloghost} %%{CISCOTAG:ciscotag}:
%{GREEDYDATA: cisco_message}"]
    }

    grok {
      match => [
        "cisco_message", "%{CISCOFW106100_2_3}",
        "cisco_message", "%{CISCOFW106001}",]
    }

}
```

API: TWITTER FEEDS PROCESSING

Working with live data

Logstash input module for Twitter

- If you have your own Twitter, you can use it
- Processing tweets with europen, europen2016 hashtags

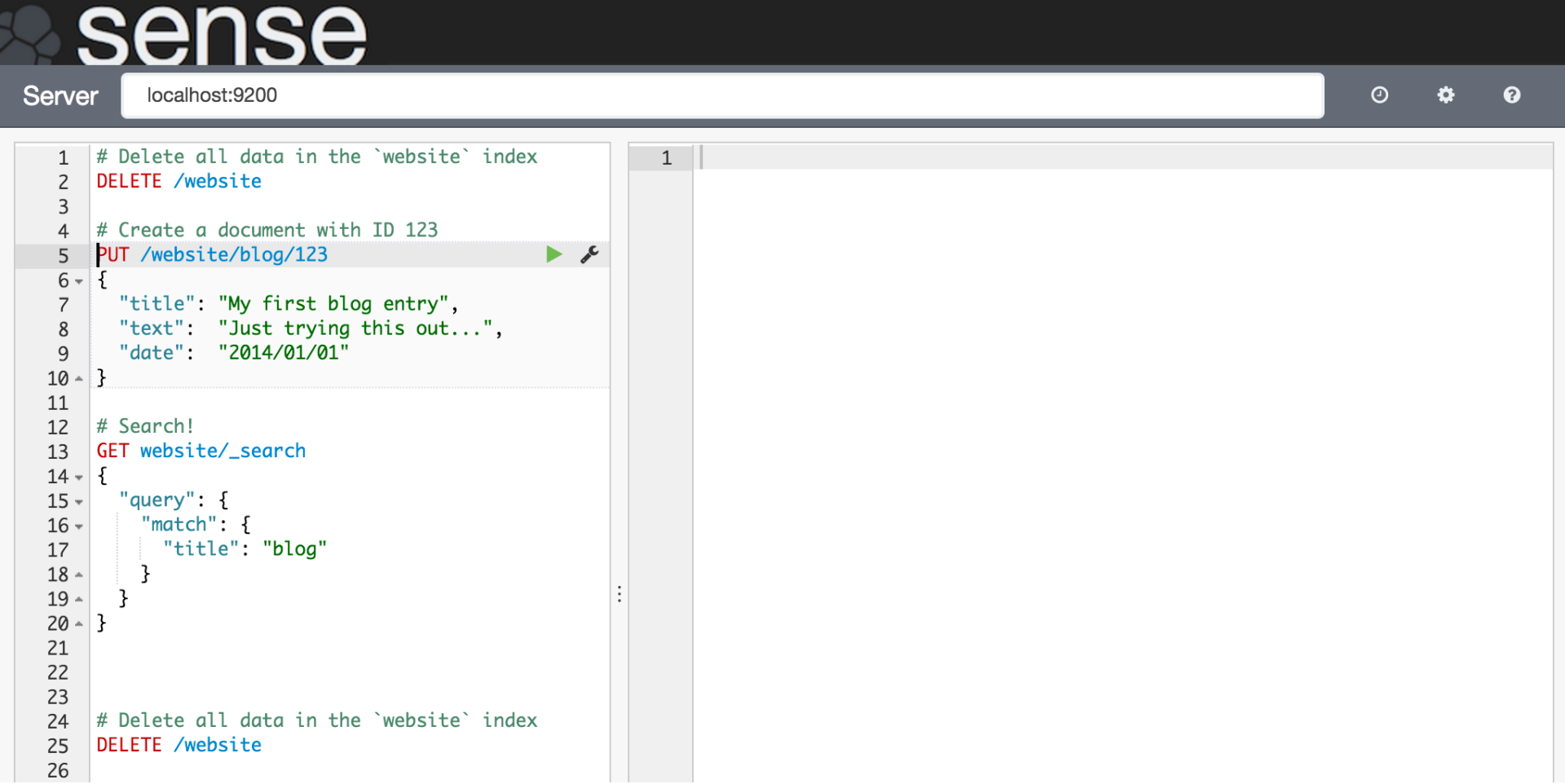
Searching, Visualization

Sense Application

- Direct access to Elasticsearch REST API

Detailed insight into ELK

- Data types of Elaticsearch
- Mapping, templates



SENSE APPLICATION UI

REST API exposed

ELASTICSEARCH: {DATA TYPES, MAPPING}

1. Basic data types
   1. string
   2. long, integer, short, byte, double, float
   3. {date, boolean, binary}
2. Complex types
   1. object, nested
   2. *No arrays? – each field can contain 0, 1 or more items by default.*
3. And there's more!
   1. {geo_point, geo_shape, ip}
   2. Support for IPv4 now, IPv6 as strings only (will be implemented in 5.x)
   3. multifields (analyzed, not_analyzed indexes)

ELASTICSEARCH: {DATA TYPES, MAPPING}

1. Dynamic mapping
   1. Automatic data types guessed by Elasticsearch
2. Static mapping
   1. That's what we are up to now!
   2. Fixing Elasticsearch's wrong guesses
   3. Or if we need more complex data types ("nested")
3. Both can be combined
   1. .. So that you can just tweak indexes for selected fields
   2. You can adjust for languages (English, Czech, …)

It's always better to start with the default mapping via Sense app.

API: IMAP MAILS PROCESSING

Working with live data

Leveraging Logstash input module for IMAP

- You can send e-mails to europen2016.elk@seznam.cz

Searching, Visualizations

Further improvements

- Detailed and more reliable mail parsing (py-cgmail project, e.g.)
- E-mails sandbox logs processing
- …

JSON: APTNOTES DATA PROCESSED

Working with JSON data

- PDF parsed by "jager" project
- https://github.com/sroberts/jager

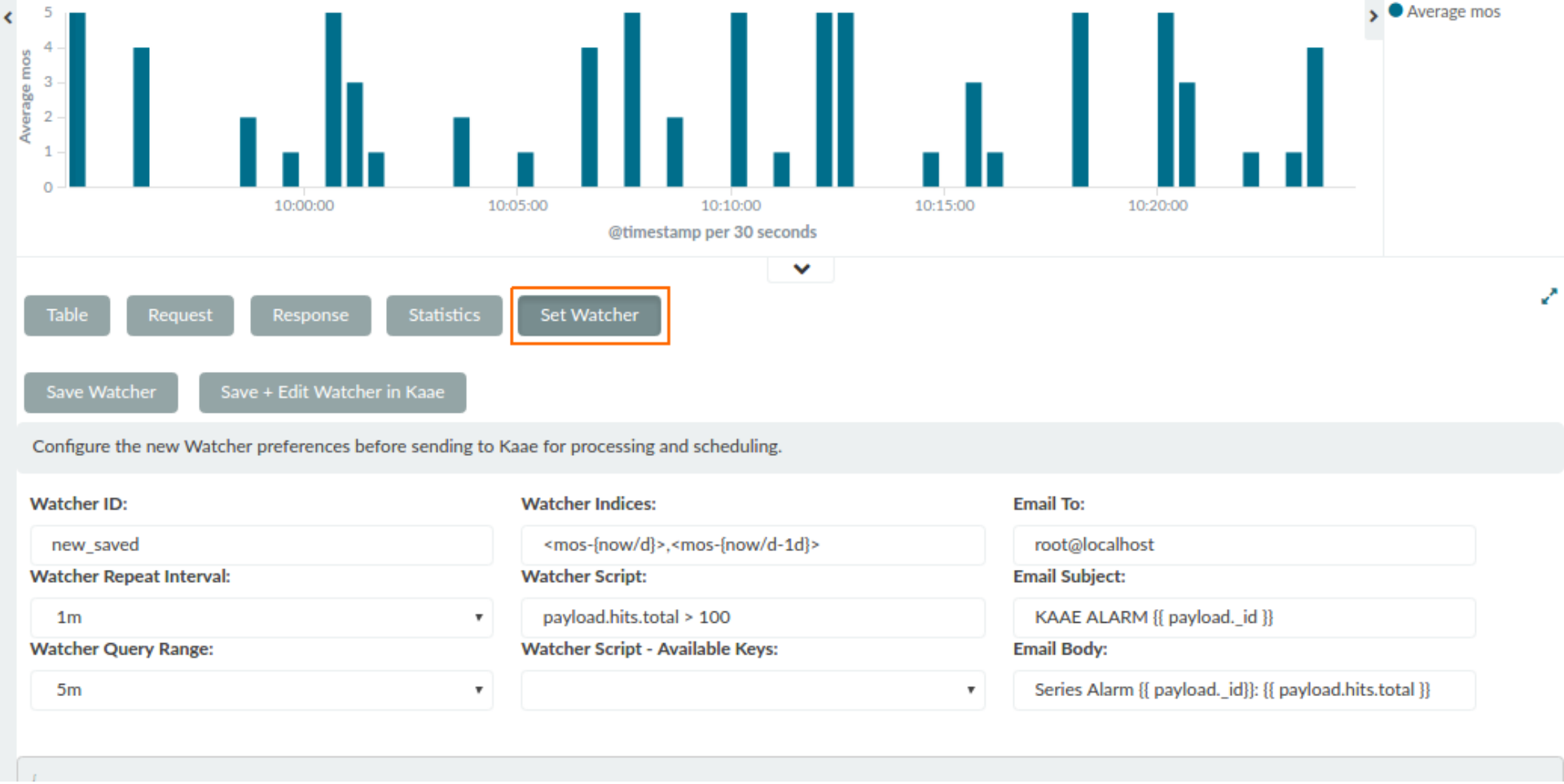
Logstash input module for JSON

Searching, Visualizations

Better insight into ELK functionality

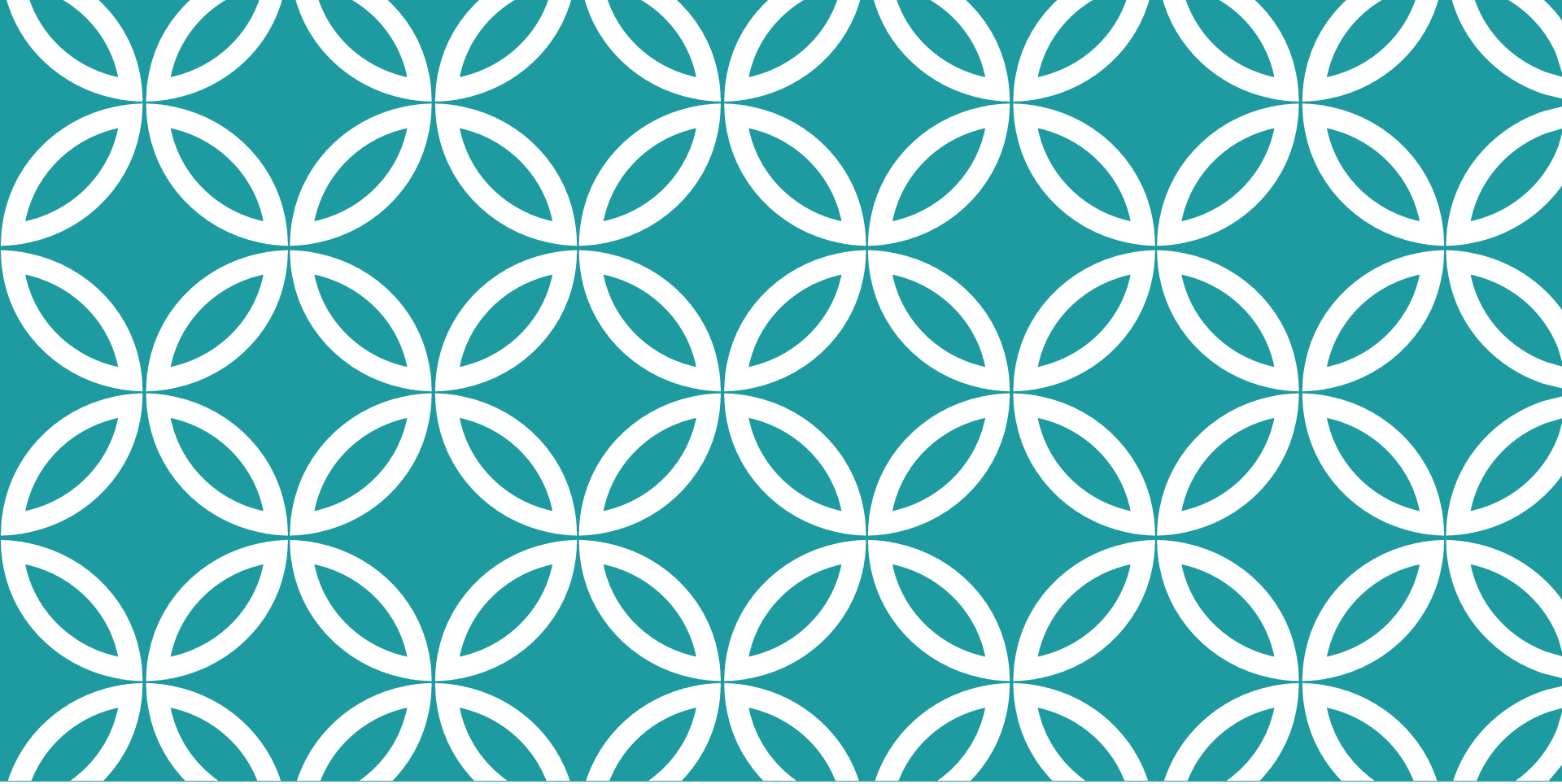
- Manual data mapping and templates

Another round with data from APTNotes



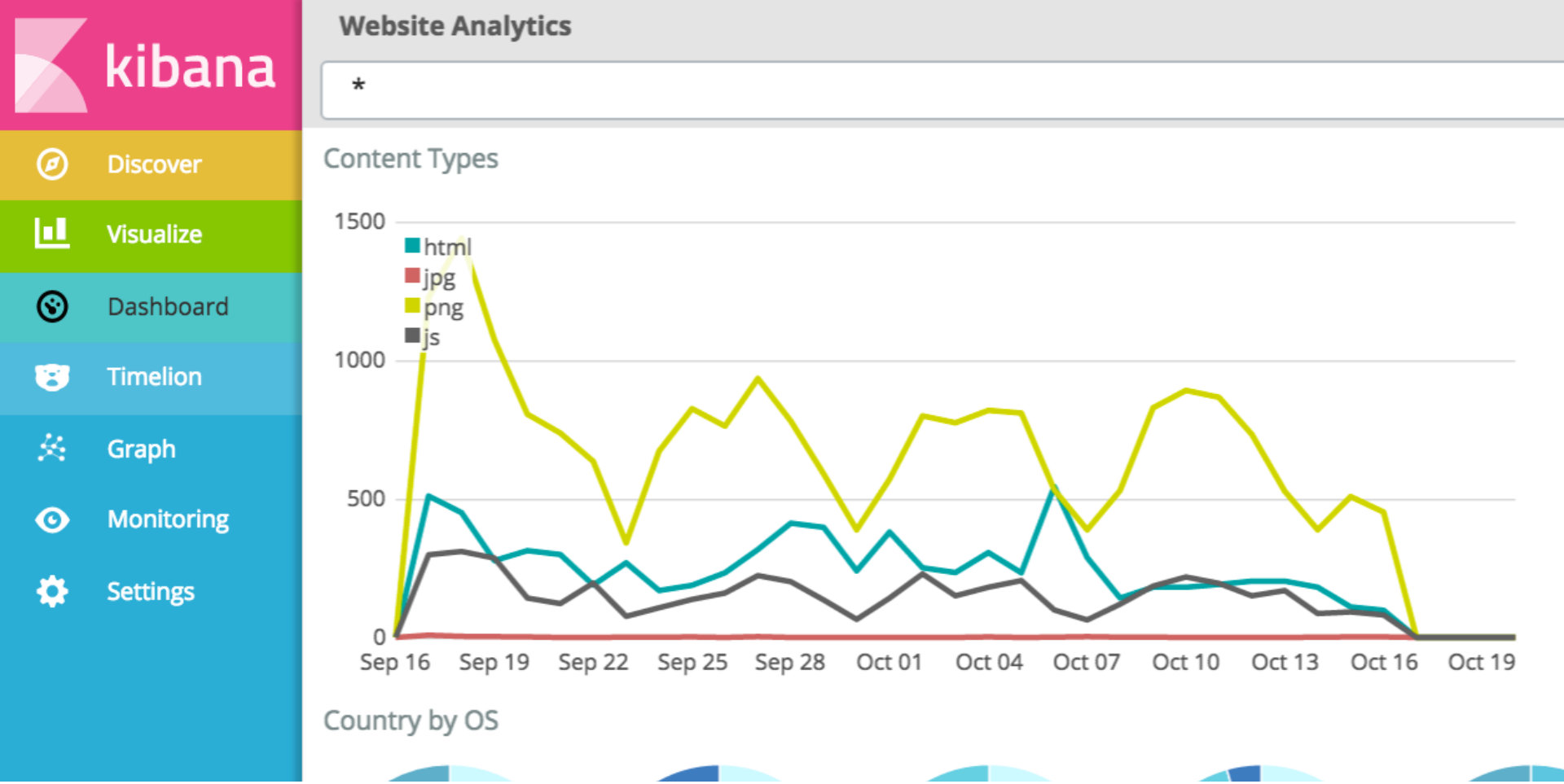
KAAE: KIBANA ALERT APP

A new alerting app for Kibana



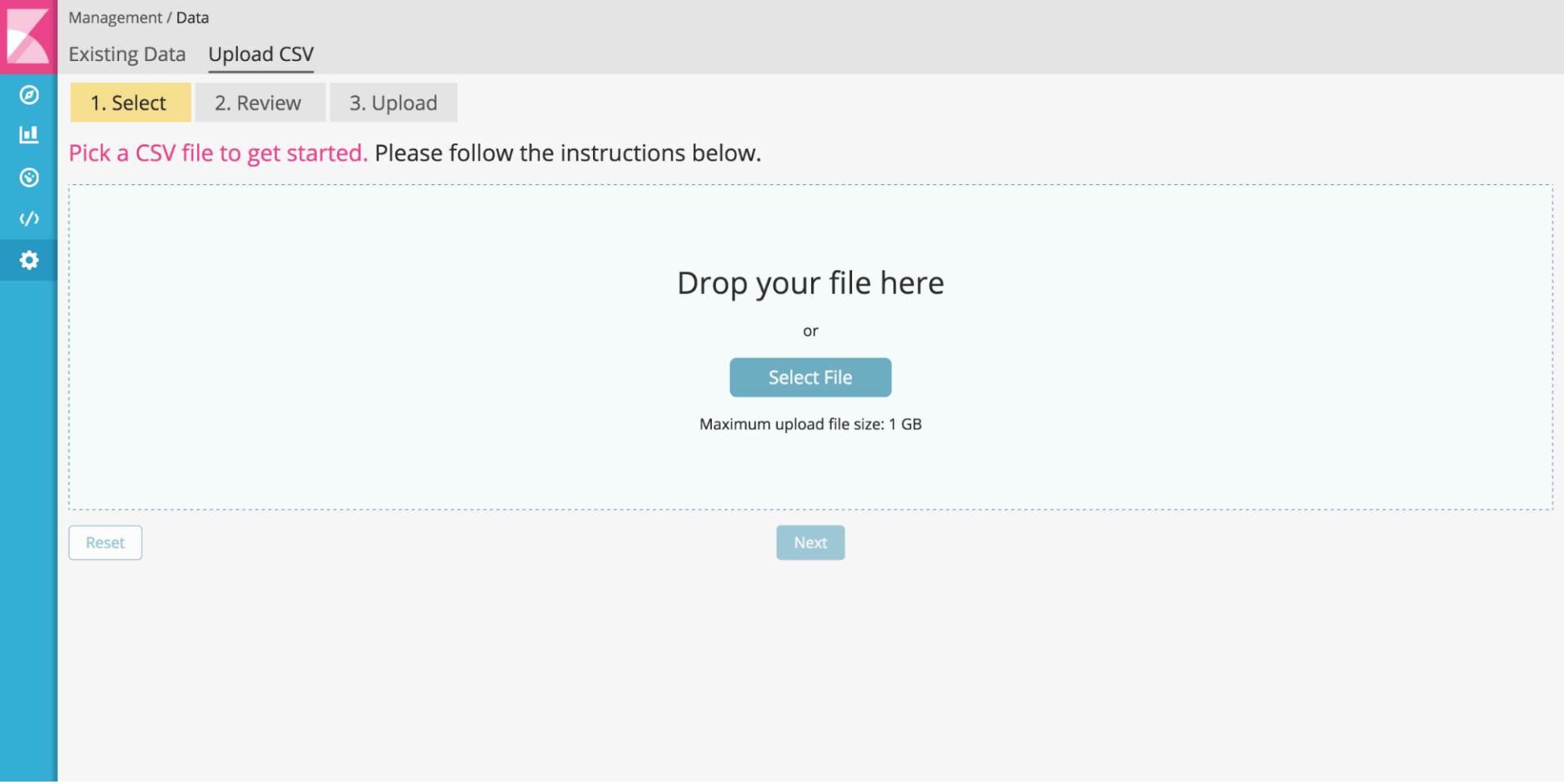
KIBANA 5

Sneak Peek



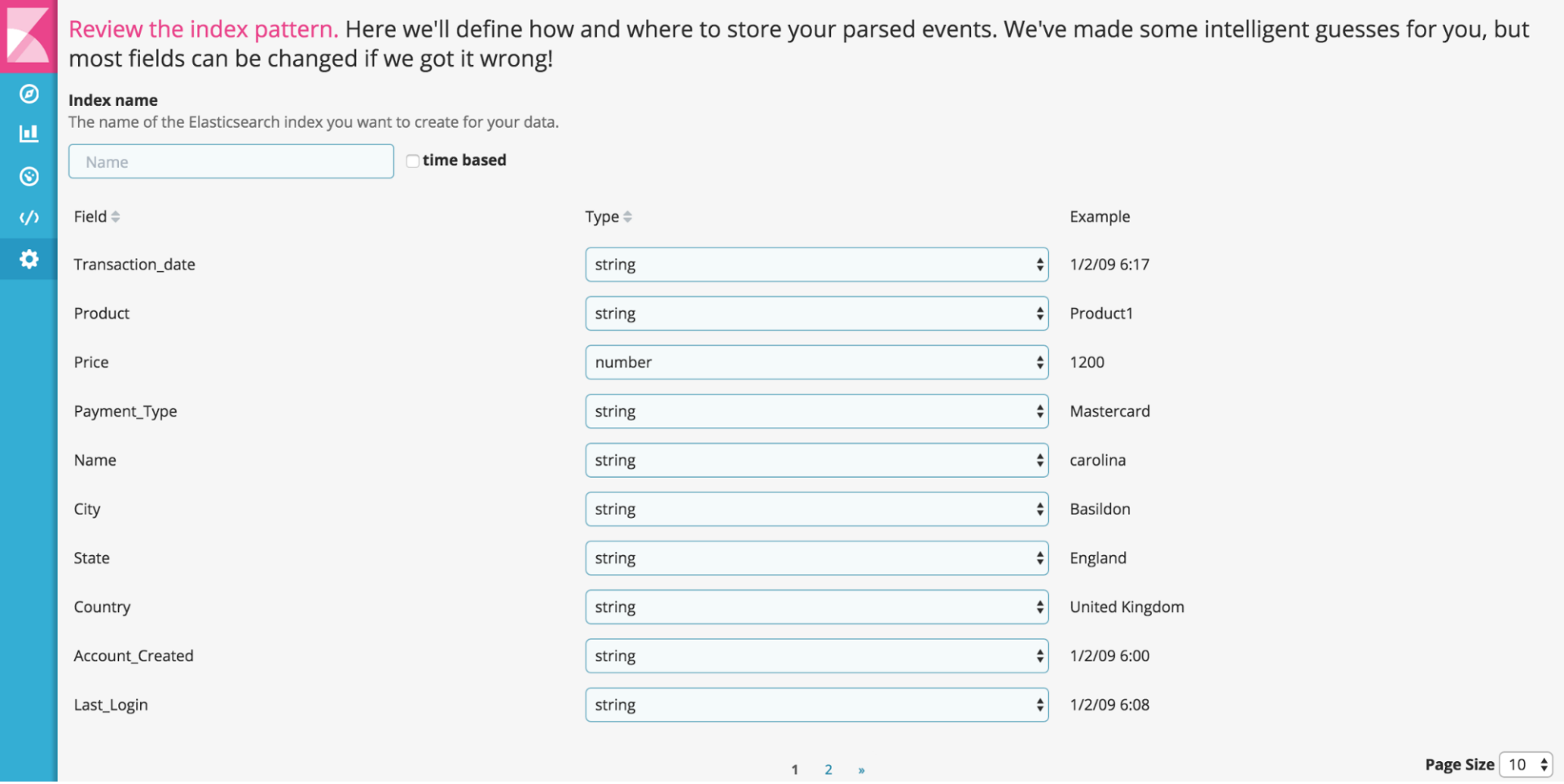
BRAND NEW UI

Sense & Timelion
Integrated



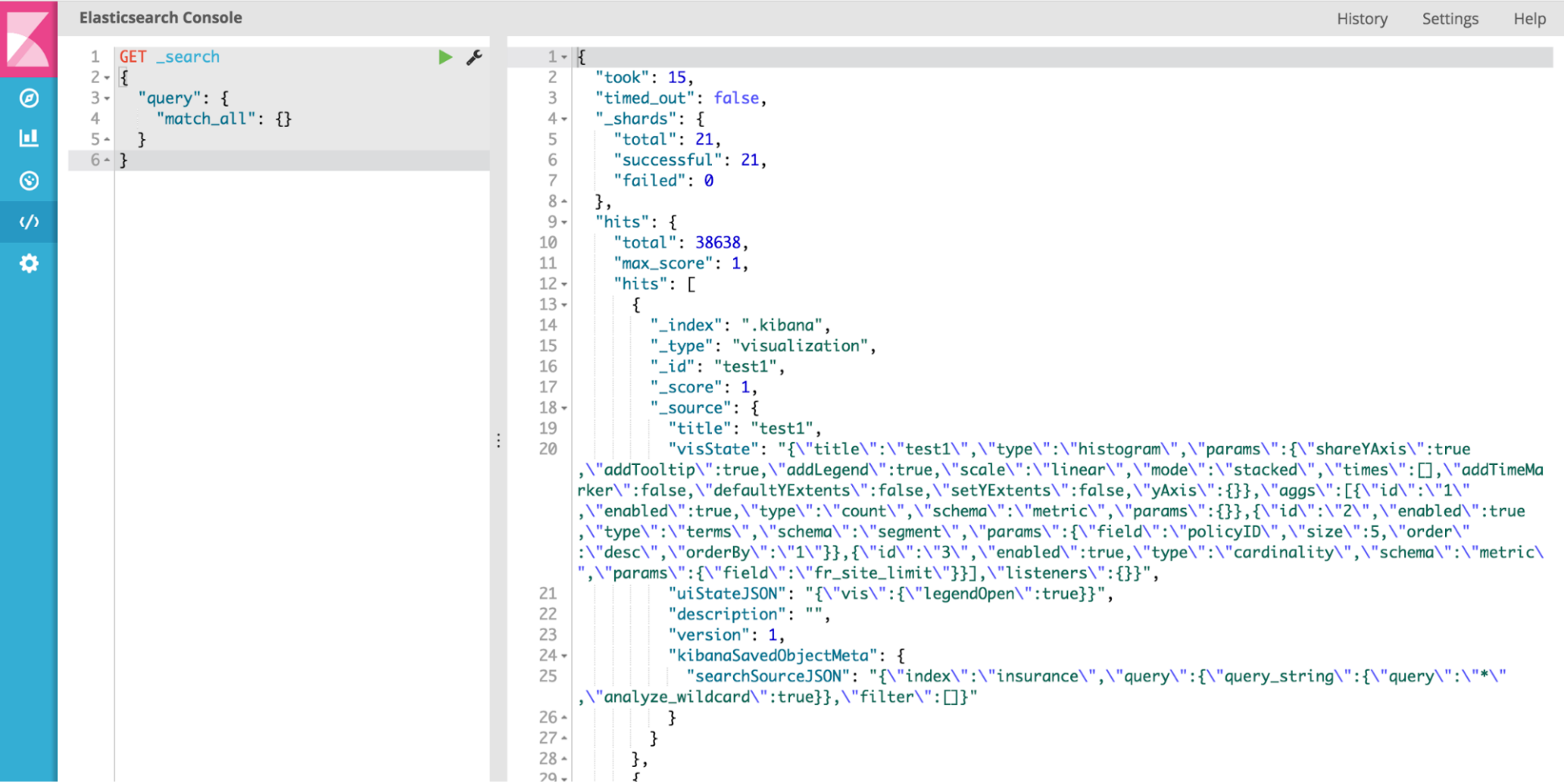
EASY CSV PROCESSING

Finally!



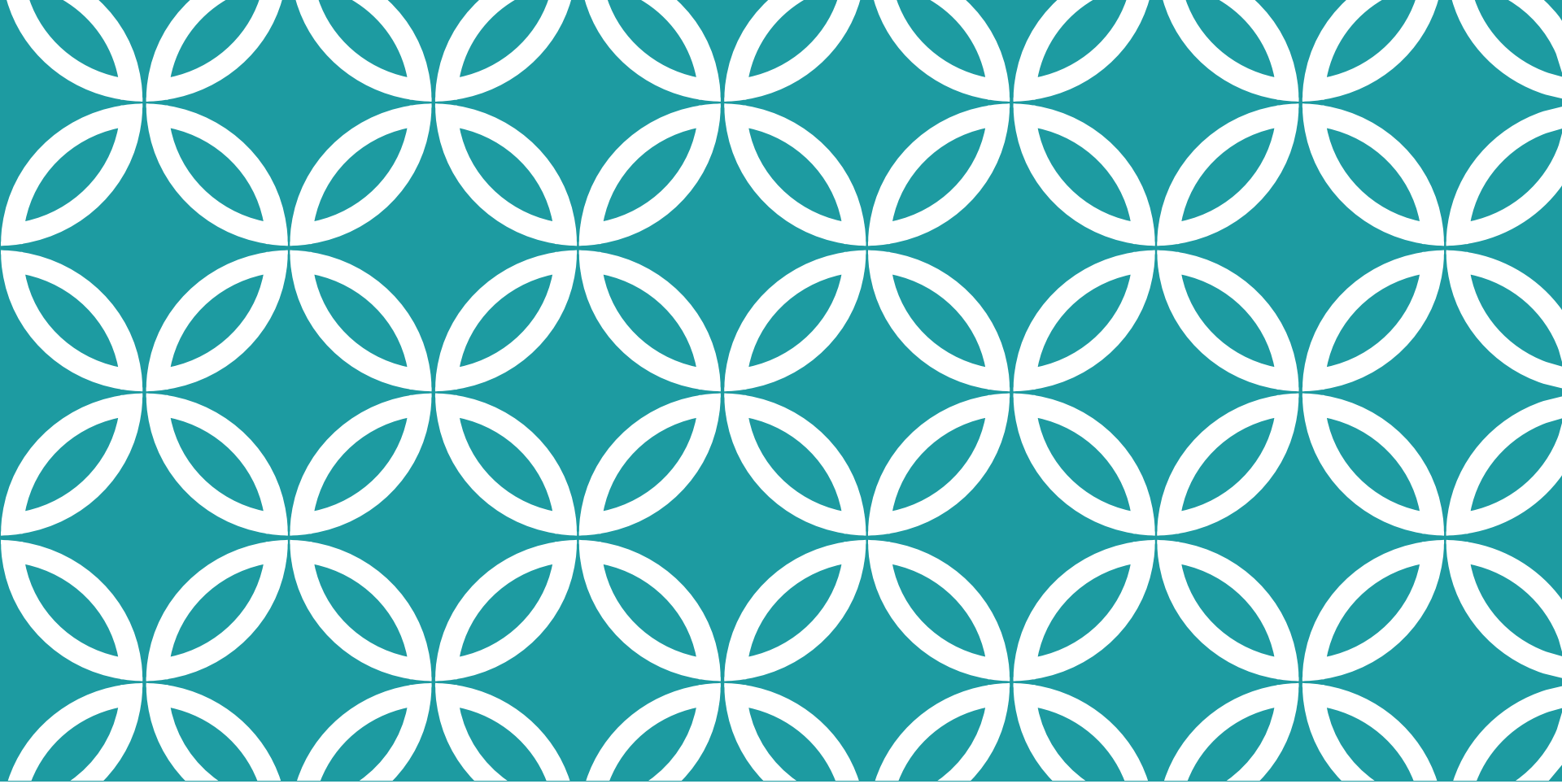
TYPE MAPPING IN UI

Data types made easy



CONSOLE INTEGRATED

Batteries included!



FURTHER DATA SOURCES?

Sky is the limit

WHAT COULD YOU POSSIBLY PROCESS?

Antivirus | HIDS/HIPS logs

Endpoint Security Protection | common support for {Splunk, ElasticSearch}

DNS logs | PassiveDNS in some form

Proxy logs | + pertinent stuff (WAF, Apache, IIS, haproxy)

Firewalls| Cisco ASA and similar

IDS | Suricata has direct JSON support

Honeypots | log at least the metadata

Windows logy | events, RDP, AD, …

WHAT COULD YOU POSSIBLY PROCESS?

VPN | Logons, certificate details, IPs, …

Forensic artifacts, IOCs | From the previous incidents

Sandbox data | Cuckoo, Lastline, …

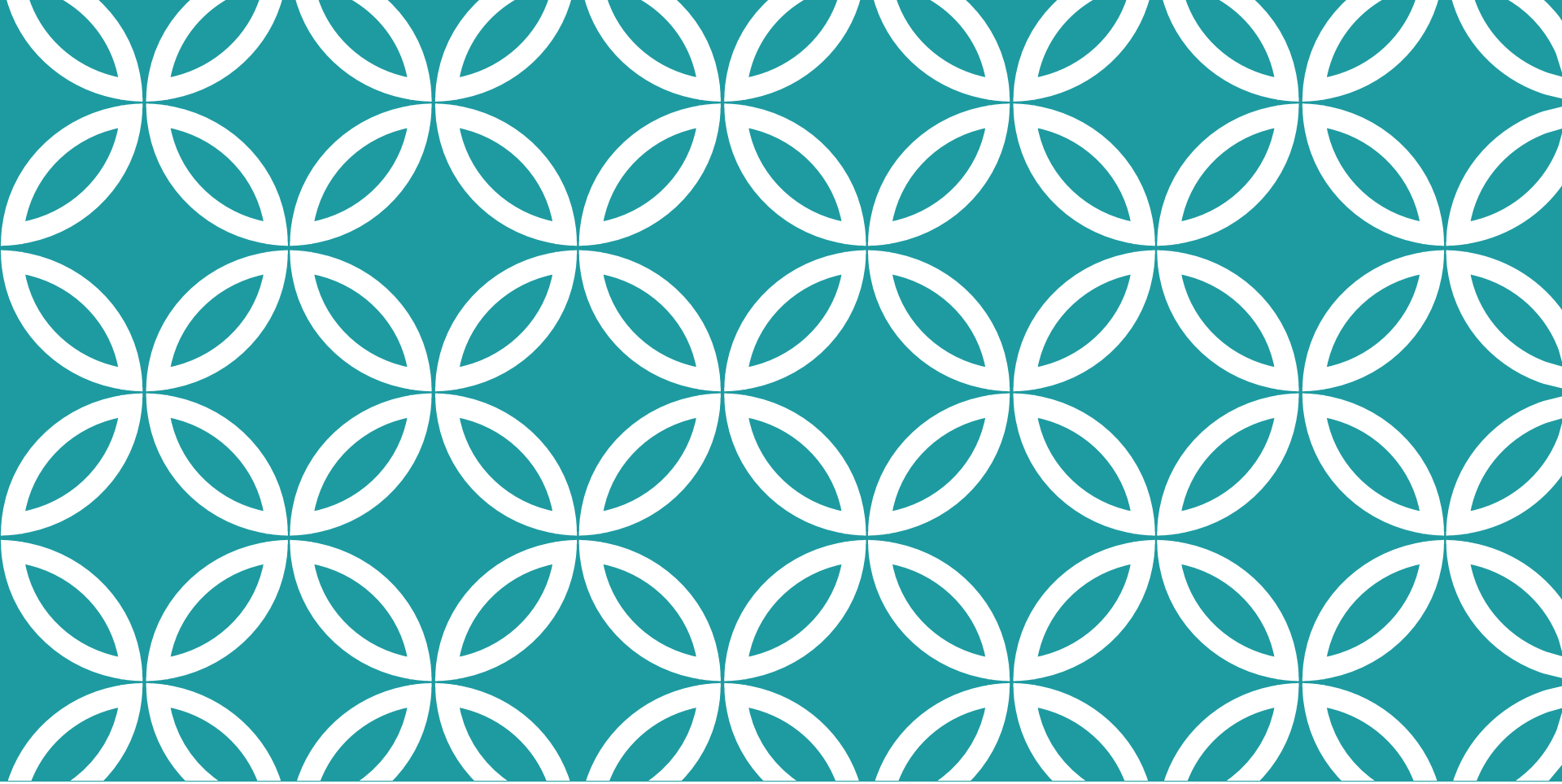
Ticketing Tools | Metrics, Dashboards, correlations with other tools

Backup info | Ransomware infections can be defeated by good backups

Threat Intel | Correlation source; you can measure their quality too!

CIRT emails | great for phishing campaigns analysis

Anything you could use in your company!



FURTHER PROJECTS

Strong Community Support

ELASTICSEARCH BASED

UI over the data stored

- ElasticUI
- SearchKit

Metrics

- Grafana

Alerting

- ElastAlert
- 411

PCAP collector

- Moloch

Incident Response

- nightHawkResponse

Kibana plugins

- Kibana: Known Plugins

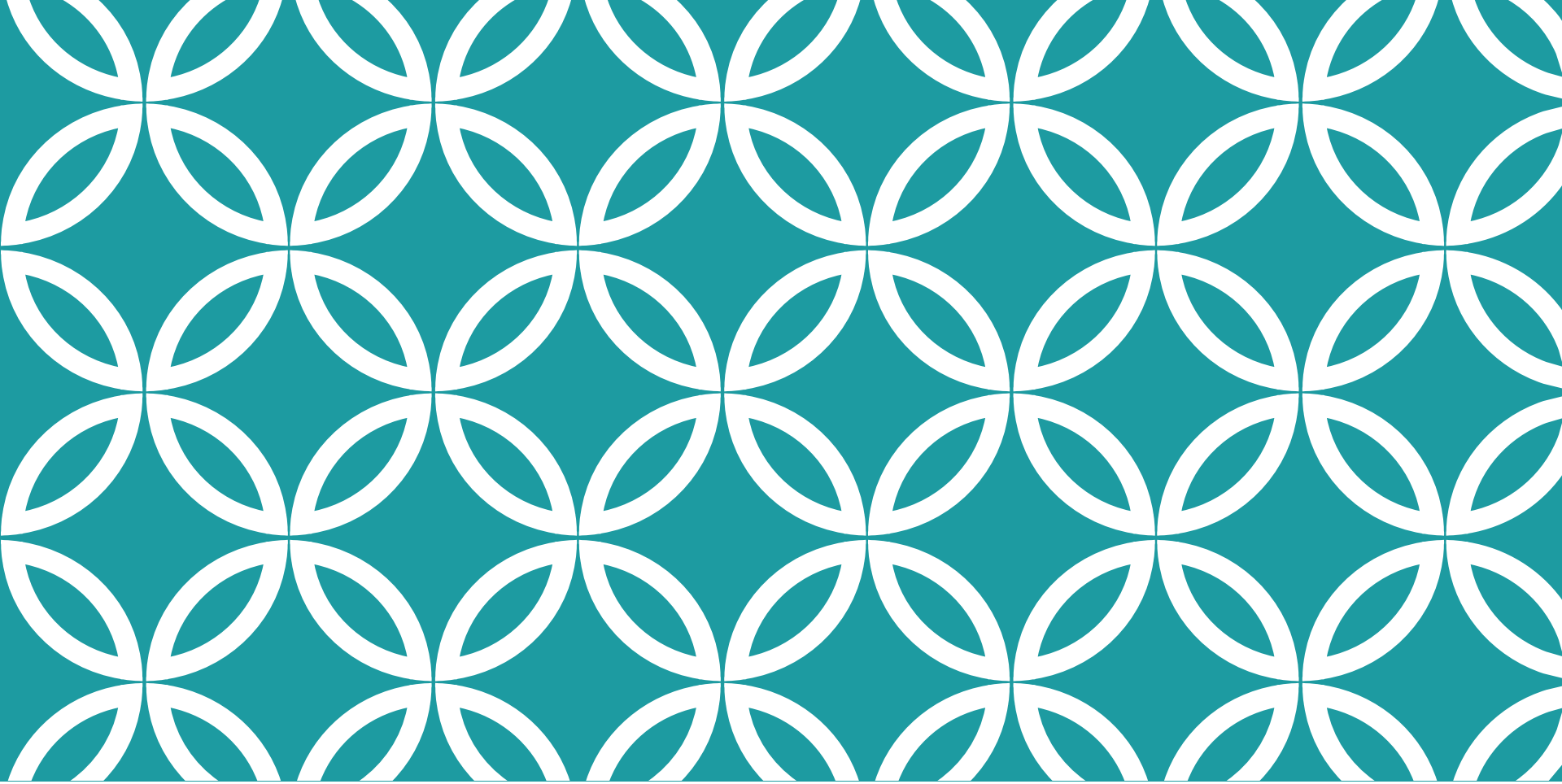
ELASTIC AS A SERVICE

logz.io

- http://site2.logz.io/pricing/
- Free: 1 GB/day| 3 days retention | alerting

LogSene

- http://sematext.com/logsene/
- Free: 512 MB/day | 7 days data retention | role-based access



QUESTIONS & ANSWERS

Questions
Answers
Comments