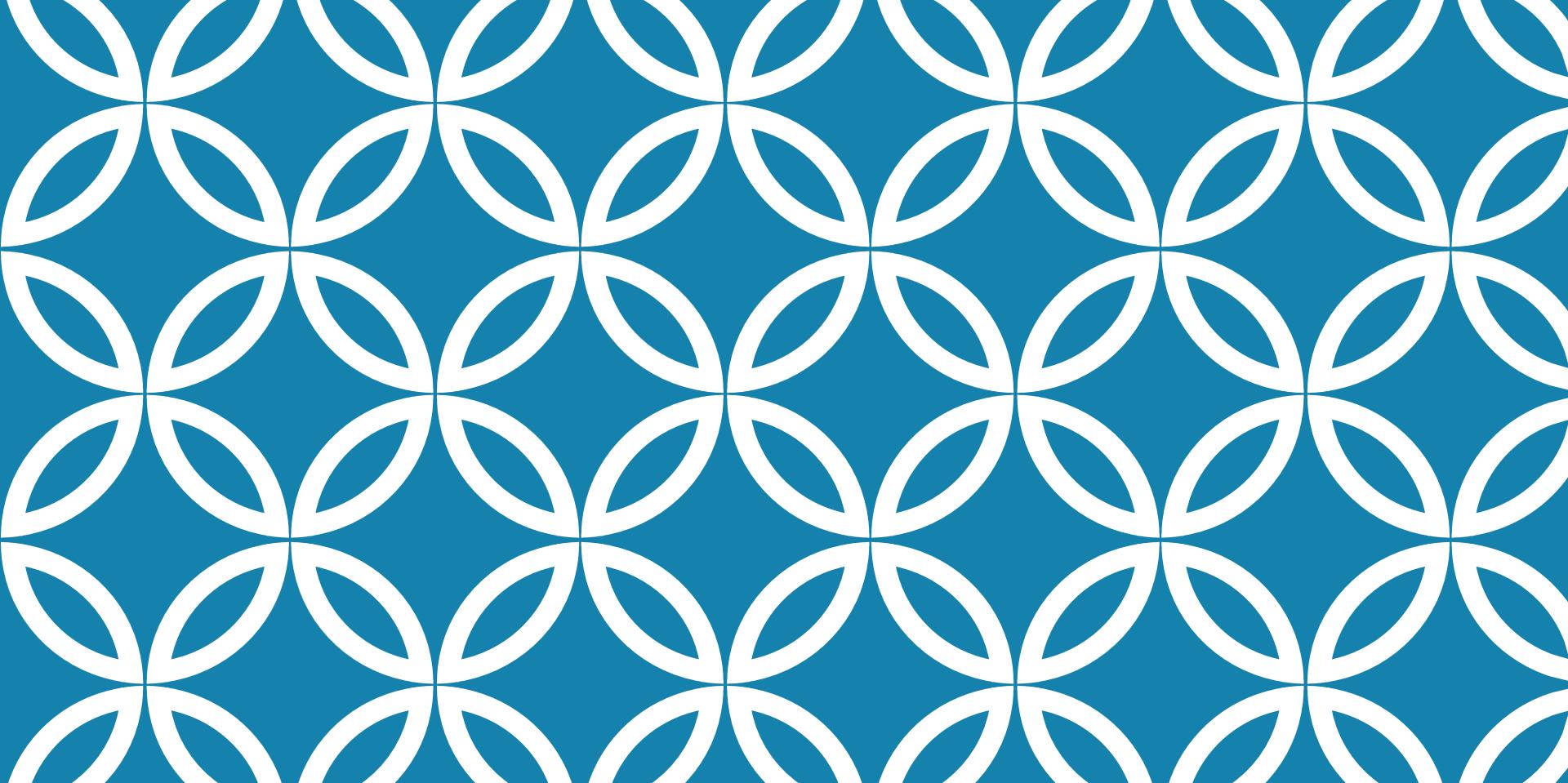


# EUROOPEN 2016: TUTORIÁL

Vít Bukač  
Vašek Lorenc



# 2. ČÁST TUTORIÁLU

GrayLog2 + ELK

# OSNOVA

## Open source řešení

- GrayLog2
- Elastic Stack

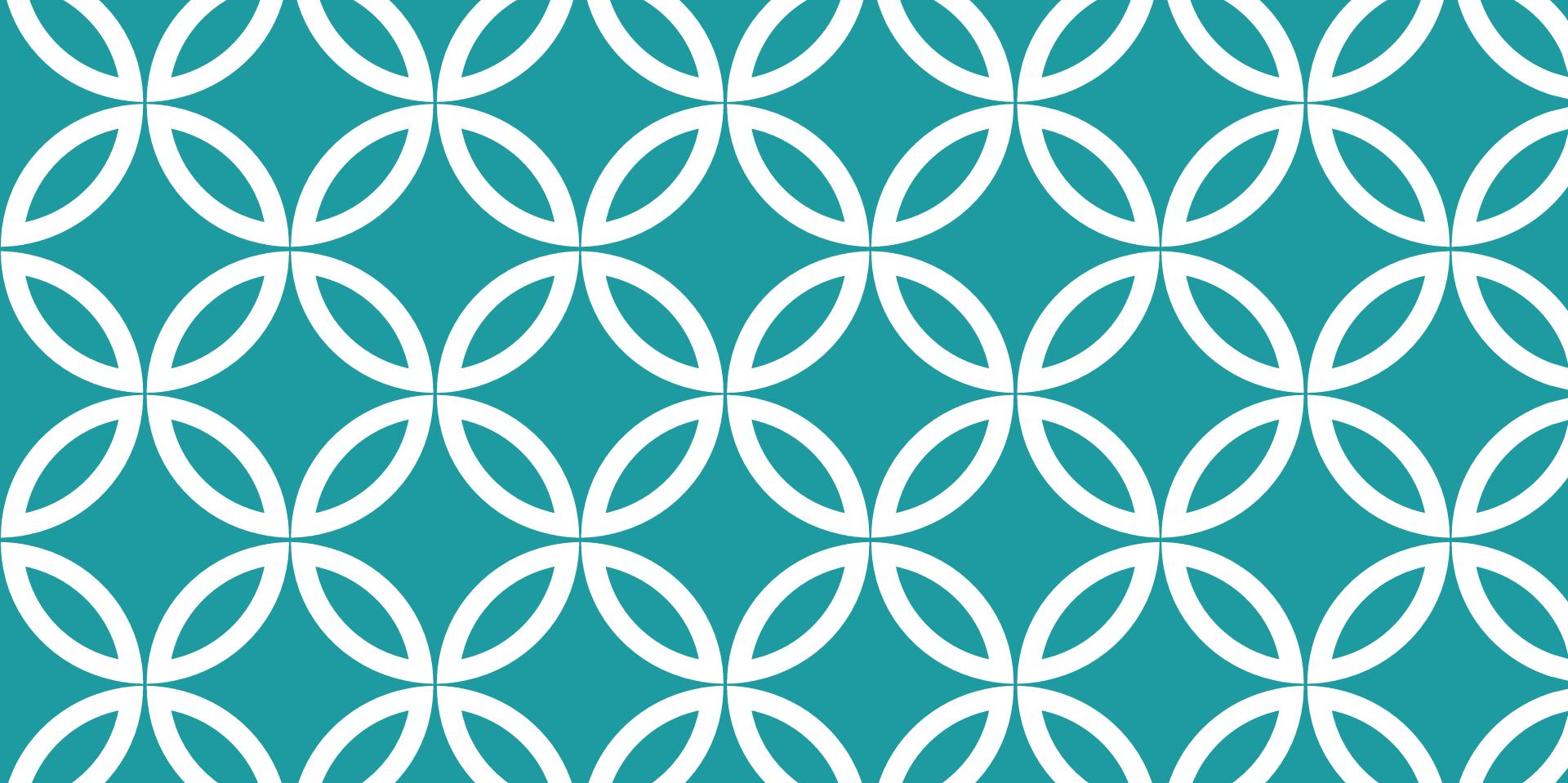
## Praktické příklady

- Cisco (ASA) logy
- Twitter API
- Zpracování e-mailů (IMAP)
- Transparentní účty volebních stran
- VirusShare/APTNotes

## Další zdroje bezpečnostních dat

## Související nástroje

## Diskuze



# GRAYLOG2

Stručný úvod

# GRAYLOG2

VM:

[graylog-box.ova](#)

Přístupy:

admin/admin (web)

europen/europen (ssh)

Porty:

**8081/tcp (web)**

12201/{udp,tcp}

5044/{udp,tcp}

**2222/tcp (ssh)**

Popis

Inputs

Extractors

Dashboards

Streams

Alerts





Search in the last 8 hours



Saved searches



gl2\_source\_input:563bec4be4b09abf23ab88b0



## Search result

Found 64 messages in 61 ms, searched in 1 index.

[Add count to dashboard](#)[Save search criteria](#)[More actions](#)

## Fields

[Default](#) [All](#) [None](#) [Filter fields](#)

- ▶  facility
- ▶  level
- ▶  message
- ▶  source

[List fields of current page or all fields.](#)

## Histogram

[Year, Quarter, Month, Week, Day, Hour, Minute](#)[Add to dashboard](#)

## Messages

[Previous](#) [1](#) [Next](#)

Timestamp	source
2015-11-06 18:35:33.000	graylog graylog ntpd_intres[891]: host name not found: 3.pool.ntp.org
2015-11-06 18:35:33.000	graylog graylog ntpd_intres[891]: host name not found: 1.pool.ntp.org
2015-11-06 18:35:33.000	graylog graylog ntpd_intres[891]: host name not found: 2.pool.ntp.org
2015-11-06 18:35:33.000	graylog

# ZÁKLADNÍ ROZHRANÍ

All-In-One

# GRAYLOG2: STRUČNÝ POPIS

Jednoduché řešení (podobně jako Splunk)

- Přehledné vyhledávání + doplňování syntaxe
- Dashboardy
- Autentizace, role
- Alerting, notifikace (Slack, JIRA, PagerDuty, ...)
- Dokumentace pro firemní nasazení
- Škálovatelnost
- Velká řada vstupních modulů, snadné nastavení
- API

Nevýhody

- Chybějící agregační funkce

# UKÁZKA: CISCO ASA

## Konfigurace vstupu

- Syslog TCP, port 5044

## Extractory

## Konfigurace zpracování vlastních dat

- Viz další obrázek

## Vyhledávání

- Směle do vlastního zkoumání!

## Dashboard

- Nejdřív vytvořit dashboard a poté do něj přidávat prvky

## Stream + Alerting

## Example message

```
Sep 23 00:09:00 europen-fw001.brno.company.com %ASA-6-106102: access-list brno_olomouc_vpn_filter permitted udp for user '<unknown>' outside/147.1.55.233(30467) -> core_conduit/147.16.55.54(161) hit-cnt 1 first hit [0x9c5cadac, 0x0]
```

Wrong example? You can [load another message](#).

## Extractor configuration

**Extractor type** Grok pattern

**Source field** message

Named captures only

Only put the explicitly named captures into the message.

**Grok pattern**

```
%{SYSLOGTIMESTAMP:timestamp} (%:{SYSLOGFACILITY} )%{SYSLOGHOST:logsource} %%{SYSLC
```

Try

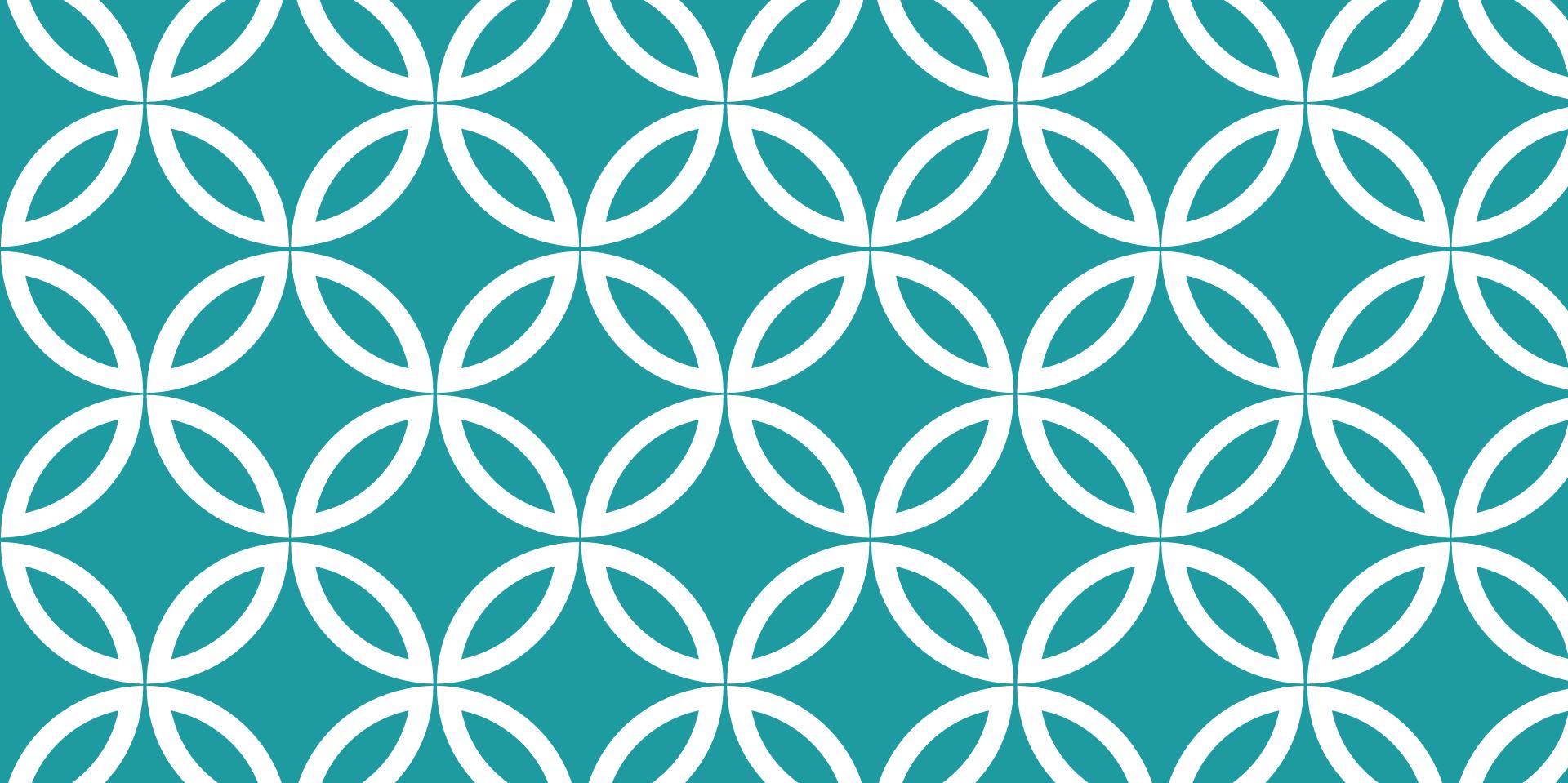
Matches the field against the current Grok pattern list, use **%{PATTERN-NAME}** to refer to a [stored pattern](#).

### Extractor preview

```
aclname  
brno_olomouc_vpn_filter  
ciscotag  
ASA-6-106102  
logsource  
europen-fw001.brno.company.com  
program  
ASA-6-106102  
timestamp  
Sep 23 00:09:00
```

# TVOŘÍME EXTRAKTOR

Pomocí Graylogu



# ELASTIC STACK

Ne-až-tak-stručný úvod

# ELASTIC STACK

VM:

[vagrant-elk-box.ova](#)

Přístupy:

european/european (ssh)

Porty:

**5601/tcp (kibana)**

9200/tcp (elasticsearch)

2222/tcp (ssh)

Verze:

Elasticsearch 2.3.5

Kibana 4.5.0

Logstash 2.4

## Elasticsearch

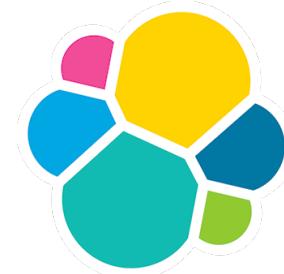
- Schopnosti, možnosti, indexy
- Datové typy
- Mapování, šablony

## Logstash

- Ukázky různých vstupů a konfigurací

## Kibana

- Jednoduché vizualizace
- Dodatečné aplikace



elastic

# {ELASTIC STACK, ELK, ELK STACK}

Elasticsearch + ...

Elastisearch

- Zpracování a indexování dat
- Apache Lucene
- Full-text
- Dokumentová databáze
- JSON

Beats

- Vstupní pluginy (Filebeat, ...)

... Logstash + Kibana

Logstash

- Mocný nástroj na transformaci dat
- Filtrování, vstupní a výstupní pluginy

Kibana

- Vizualizace
- Pluginy
- Celá další platforma (Kibana apps)

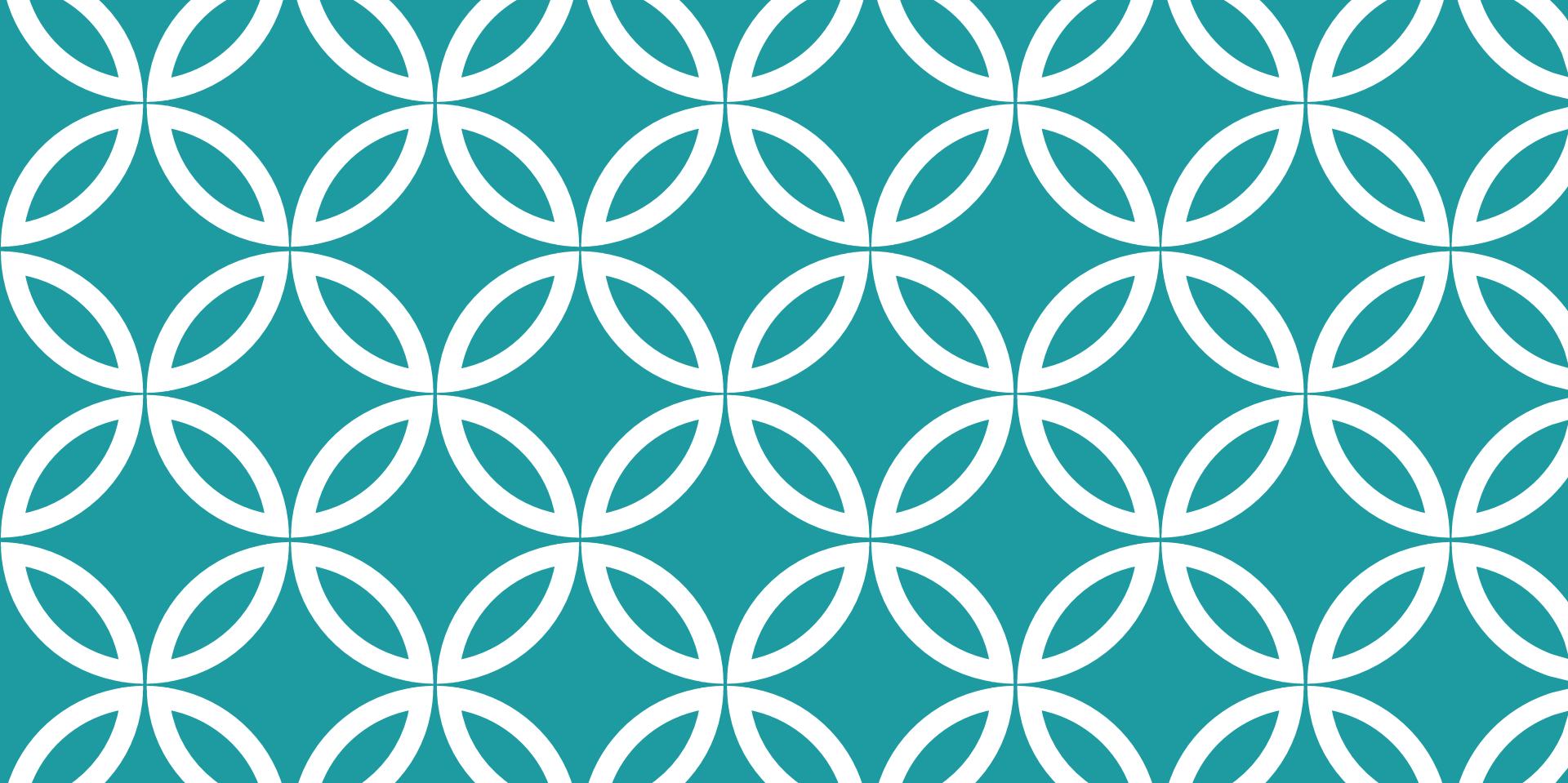
# ELK VS. {GRAYLOG2, SPLUNK}

## Co může vadit?

- Žádná autentizace a role
- Chybějící alerting
- Cross-join, lookup funkce
- Komplikovanější
- Rychlý vývoj

## Co je fajn?

- Cena
- Flexibilita
- Logstash jako součást řešení
- Přesnější správa dat
- Rychlý vývoj
- Komunita
- Přibližné vyhledávání
- REST API



**LOGSTASH**

Převádíme data

# LOGSTASH: ZÁKLADNÍ WORKFLOW

## 1. INPUT

Celá řada vstupních pluginů a kodeků

## 2. FILTER

V podstatě programovací jazyk (Ruby)

Se všemi výhodami a nevýhodami

“*grok is the new grep*“

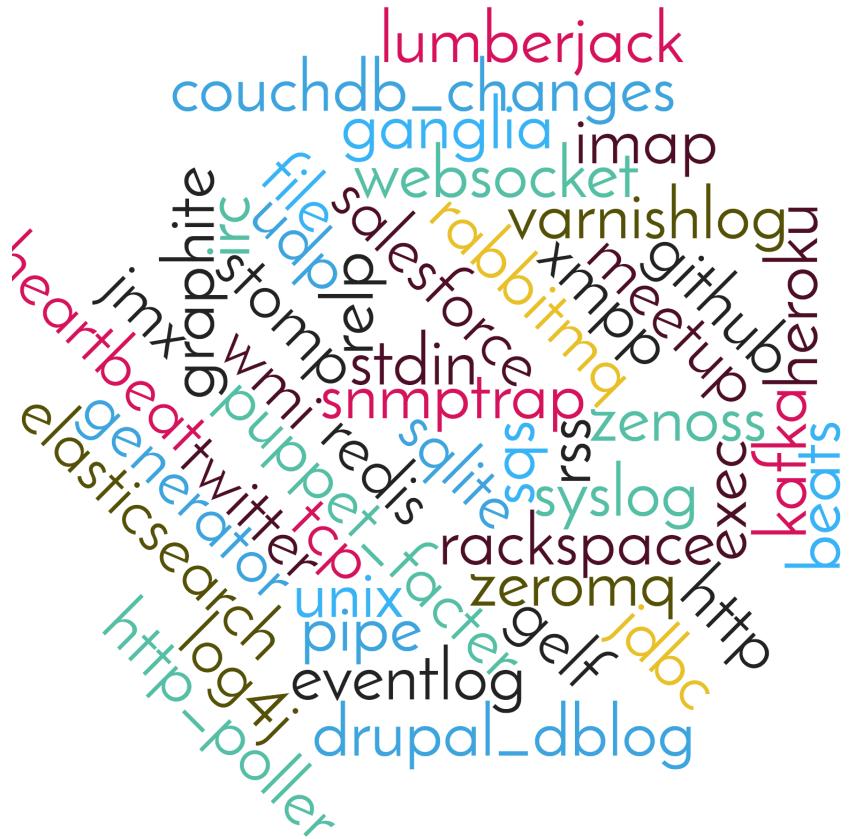
## 3. OUTPUT

Opět celá řada možných výstupů

Pro potřeby Elasticu nás však zajímá jen jeden...

# LOGSTASH: INPUT

imap  
file  
stdin  
tcp  
twitter  
...



A word cloud visualization showing various Logstash input plugin names. The words are arranged in a cluster, with larger and more prominent words indicating higher frequency or importance. The colors of the words vary randomly.

lumberjack  
couchdb\_changes  
ganglia  
imap  
websocket  
varnishlog  
github  
xmpp  
meetup  
salesforce  
rabbitmq  
kafka  
heroku  
beats  
graphite  
file  
udp  
stomp  
stdin  
jmx  
wmi  
redis  
snmptrap  
salite  
bs  
rss  
zenoss  
syslog  
exec  
stomp\_src  
tcp  
puppet  
tcp  
fact  
rackspace  
zeromq  
http  
jdbc  
generator  
heartbeat  
twitter  
unix  
pipe  
gelf  
eventlog  
elasticsearch  
log4j  
drupal\_dblog  
http\_poller

# LOGSTASH: FILTER

**grok**

**mutate**

**cidr**

**geoip**

**csv**

...

A word cloud diagram centered around the word "environment". The words are colored in various shades of blue, green, yellow, red, and purple. The size of each word represents its frequency or importance within the Logstash filter ecosystem. The words include: grok, mutate, cidr, geoip, csv, ..., environment, extractnumbers, elapsed, anonymize, urldecode, cipher, geoip, environment, aggregate, checksum, throttle, json\_encode, json\_decode, split, de\_dot, dns, ilog, log, sleep, prune, multiline, range, event, timestamp, useragent, cidr, grok, alter, metrics, drop, clone, date, xml, translate, fingerprint, collate, elasticsearch.

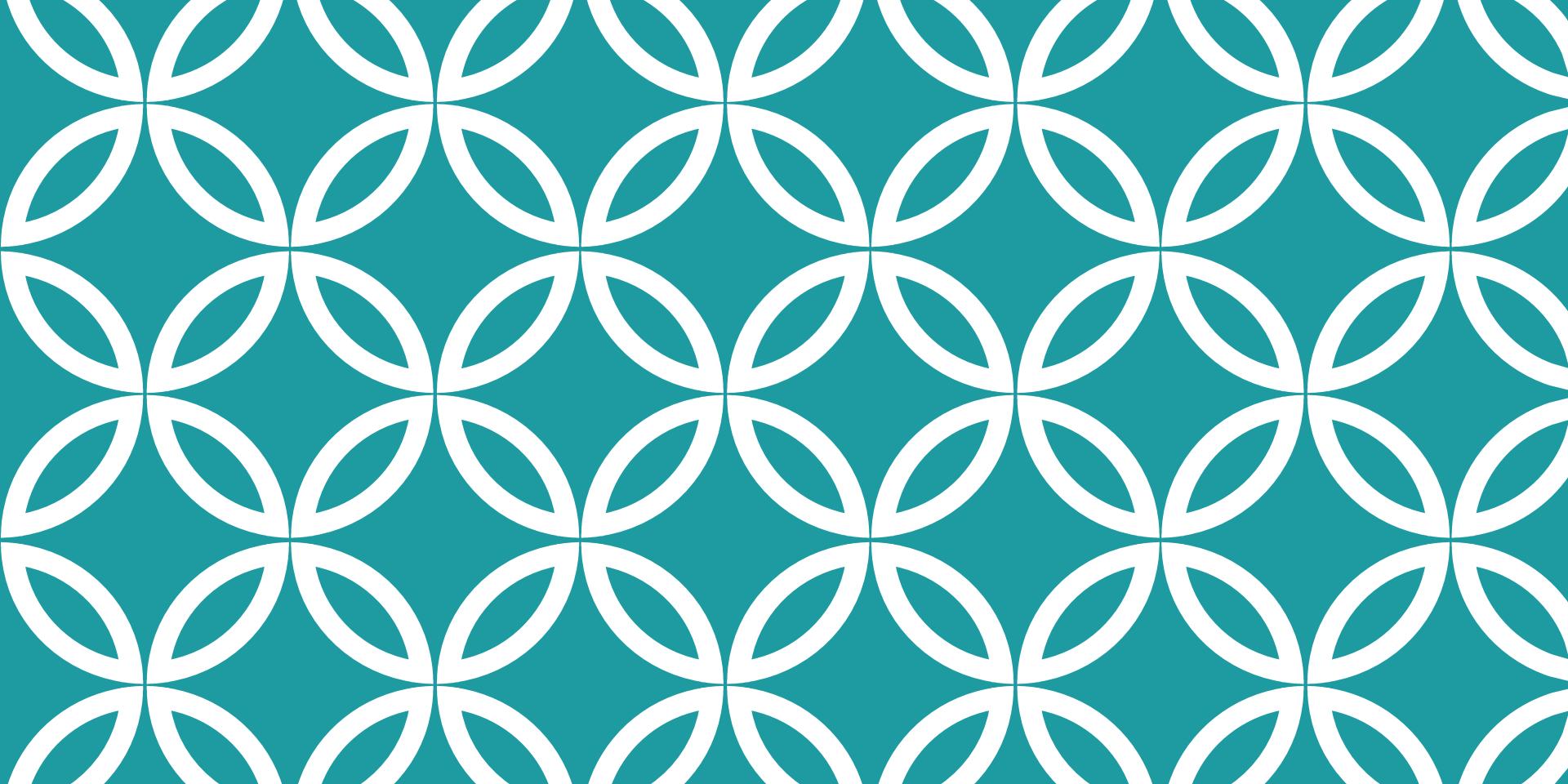
# LOGSTASH: OUTPUT

stdout  
file  
**elasticsearch**  
**gelf**  
...



JSON EVERYWHERE

“Se stim smiř”



**KIBANA**

Zobrazujeme data  
Verze 3, v4, v5, ...

# KIBANA: VIZUALIZAČNÍ FRAMEWORK

Dotazování nad daty

Vizualizace

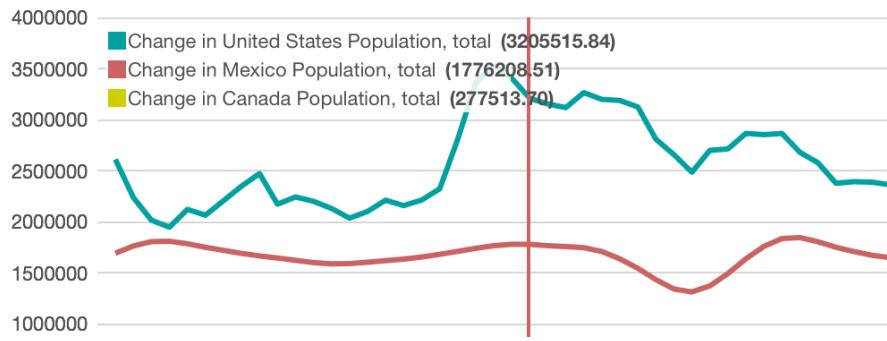
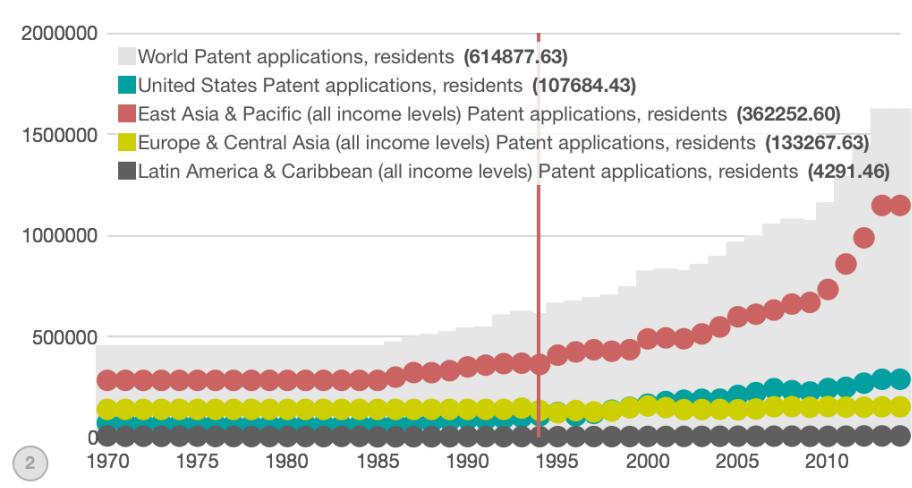
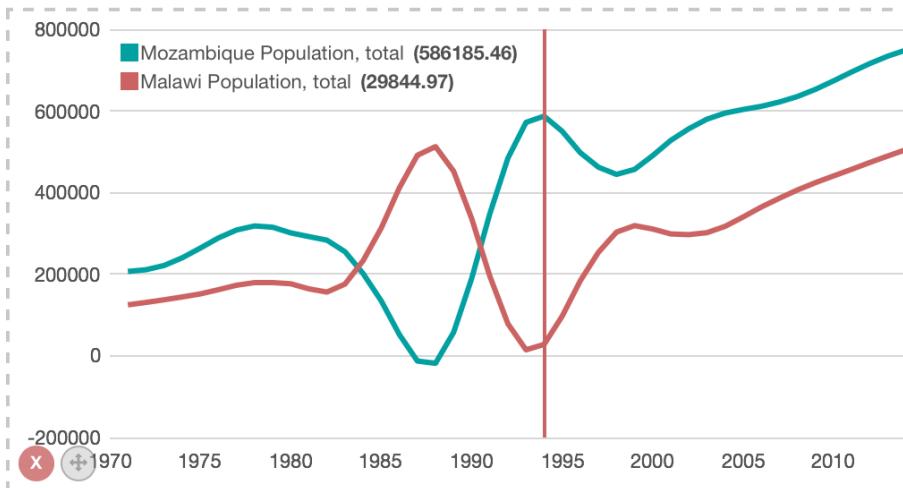
- Celá řada vizualizačních pluginů
- Do vaší instalace jsem některé přidal

Aplikační platforma

- Běží nad node.js, můžete si psát vlastní pluginy a aplikace

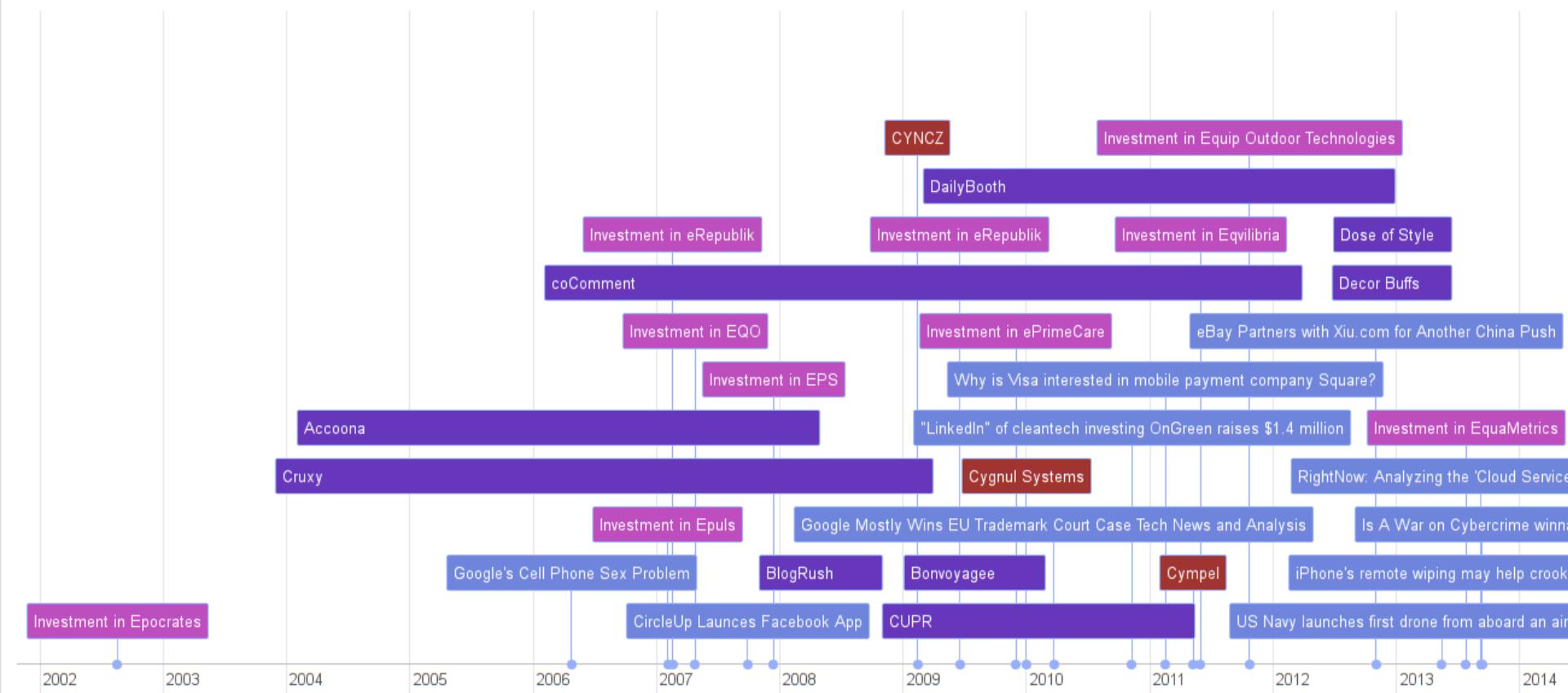
Předinstalované aplikace

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



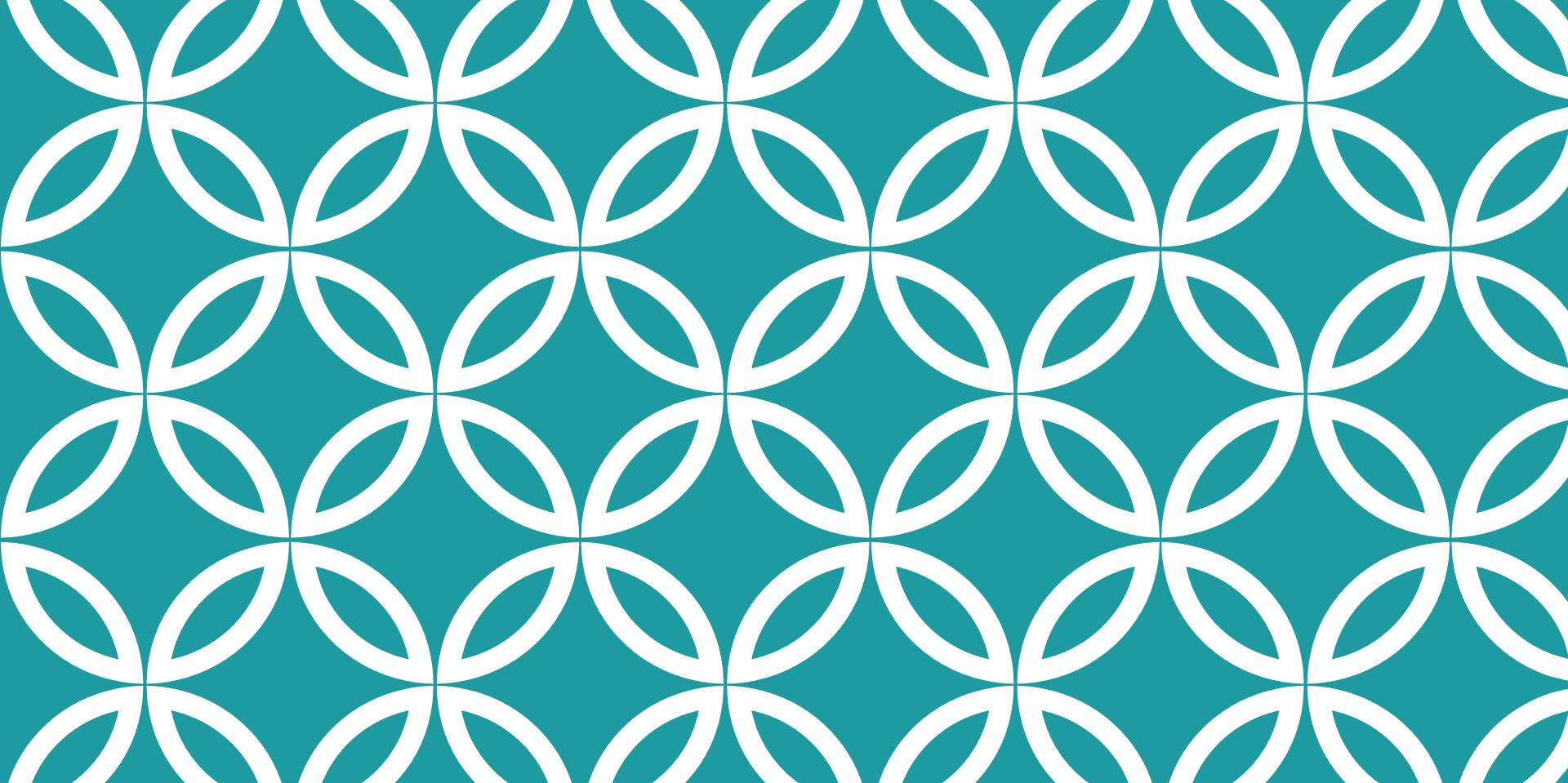
# TIMELION

Ukázka komplexní  
vizualizace



# KIBI TIMELINE

Ukázka komplexní  
vizualizace



# PRAKTICKÉ PŘÍKLADY!

Elastic Stack

# POSTUP PŘI KAŽDÉM PŘÍKLADU

1. Prohlédneme si vstupní data
2. Vymyslíme název indexu
3. Zkusíme nakonfigurovat Logstash
4. Vytvoříme konfiguraci Kibany pro daný index
5. Prohledávání, vizualizace
6. (*Hledání chyb*)
7. Oprava chyb, znovu na krok 2
8. Přejdeme na další příklad!

# SYSLOG: CISCO LOGY V ELASTIC STACKU

Ukázka zpracování předchozích dat v ELKu

## Využití Logstashe

- Konfigurace vstupu, filtru a výstupu
- Grok filter & debugger

## Vizualizace

## Úprava konfiguračního souboru pro Logstash

- Pro využití v Graylogu

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

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

filter {

}

output {
    elasticsearch { }
}
```

```
Oct 07 00:00:23 %ASA-6-106102: access-list brno.olomouc.vpn.filter permitted tcp for user '<unknown>' outside/12.130.60.5(35335) -> inside/10.174.96.92(5666) hit-cnt 1 first hit [0x9c5cadac, 0x0]
```

```
%{CISCOTIMESTAMP} %{CISCOTAG}: access-list %{WORD:policy_id} %{CISCO_ACTION:action} %{WORD:protocol} for user \%
{DATA:src_fwuser}\' %{DATA:src_interface}/%{IP:src_ip}\(%{INT:src_port}\)(\(%{DATA:src_fwuser}\'))? -> %{DATA:dst_interface}/%
{IP:dst_ip}\(%{INT:dst_port}\) hit-cnt %{INT:hit_count} %{CISCO_INTERVAL:interval} \[%{DATA:hashcode1}, %{DATA:hashcode2}\]
```

Add custom patterns  Keep Empty Captures  Named Captures Only  Singles

Autocomplete

Go

One per line, the syntax for a grok pattern is [%{SYNTAX:SEMANTIC}](#)

Custom patterns

# GROK DEBUGGER

Jak snáz vytvářet grok  
výrazy

# GROK KONFIGURACE

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

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

# API: ZPRACOVÁNÍ DAT Z TWITTERU

Ukázka živých dat

Využití vstupního modulu Logstash

- Máte-li vlastní Twitter, můžete použít ten
- Pište tweety s hesly euopen, euopen2016 :)

Hledání, vizualizace

Aplikace Sense

Detailní vhled do fungování ELKu

- Datové typy Elasticsearche
- Mapování, šablony

```
1 # Delete all data in the `website` index
2 DELETE /website
3
4 # Create a document with ID 123
5 PUT /website/blog/123
6 {
7   "title": "My first blog entry",
8   "text": "Just trying this out...",
9   "date": "2014/01/01"
10 }
11
12 # Search!
13 GET website/_search
14 {
15   "query": {
16     "match": {
17       "title": "blog"
18     }
19   }
20 }
21
22
23
24 # Delete all data in the `website` index
25 DELETE /website
26
```

1

# UKÁZKA APLIKACE SENSE

REST API jako na dlani

# ELASTICSEARCH: {TYPY DAT, MAPOVÁNÍ}

## 1. Základní typy dat

1. string
2. long, integer, short, byte, double, float
3. {date, boolean, binary}

## 2. Complexní typy

1. object, nested
2. Kde jsou pole?

## 3. Další

1. {geo\_point, geo\_shape, ip}
2. Podpora pouze pro IPv4, IPv6 je třeba ukládat jako string
3. multifields (analyzed, not\_analyzed)

# ELASTICSEARCH: {TYPY DAT, MAPOVÁNÍ}

## 1. Dynamické mapování

1. Automaticky, prováděné elasticsearchem

## 2. Statické mapování

1. To si právě teď vyzkoušíme
2. Když se elastic netrefí
3. Nebo v případě komplexnějších dat ("nested")

## 3. Je možné různě kombinovat

1. A například vhodně nastavovat indexy určitých objektů
2. Nebo také jazyky (angličtina, čeština, ...)

Pro ruční vytváření je dobré začít přes Sense.

# API: ZPRACOVÁNÍ DAT Z IMAPU

Ukázka živých dat

Využití vstupního modulu Logstash

- Posílejte e-maily na [european2016.elk@seznam.cz](mailto:european2016.elk@seznam.cz)

Hledání, vizualizace

Možnosti vylepšení

- Detailnější a spolehlivější parser mailů
- Napojení na sandbox
- ...

# JSON: ZPRACOVÁNÍ DAT Z APTNOTES

Ukázka zpracování JSON dat

- Vyrobeno za pomoci projektu “jager”
- <https://github.com/sroberts/jager>

Využití modulu Logstash

Hledání, vizualizace

Detailní vhled do fungování ELKu

- Ruční výroba mapování a šablony

Nový pokus s daty z APTNotes

# CSV: ZPRACOVÁNÍ BANKOVNÍCH ÚČTŮ

Ukázka zpracování CSV dat

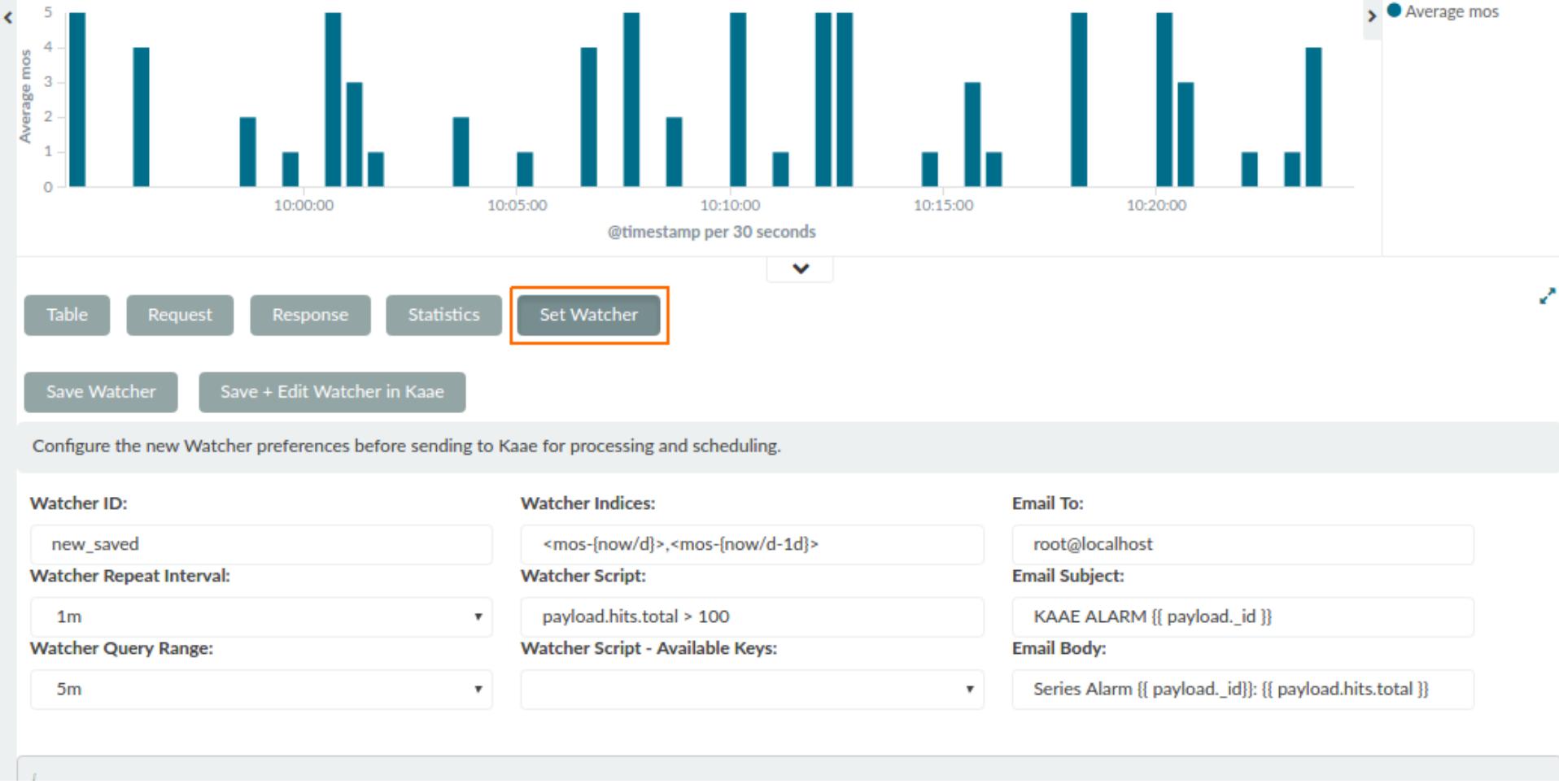
- Posbíraná data z transparentních účtů volebních stran

Využití modulu Logstash

Hledání, vizualizace

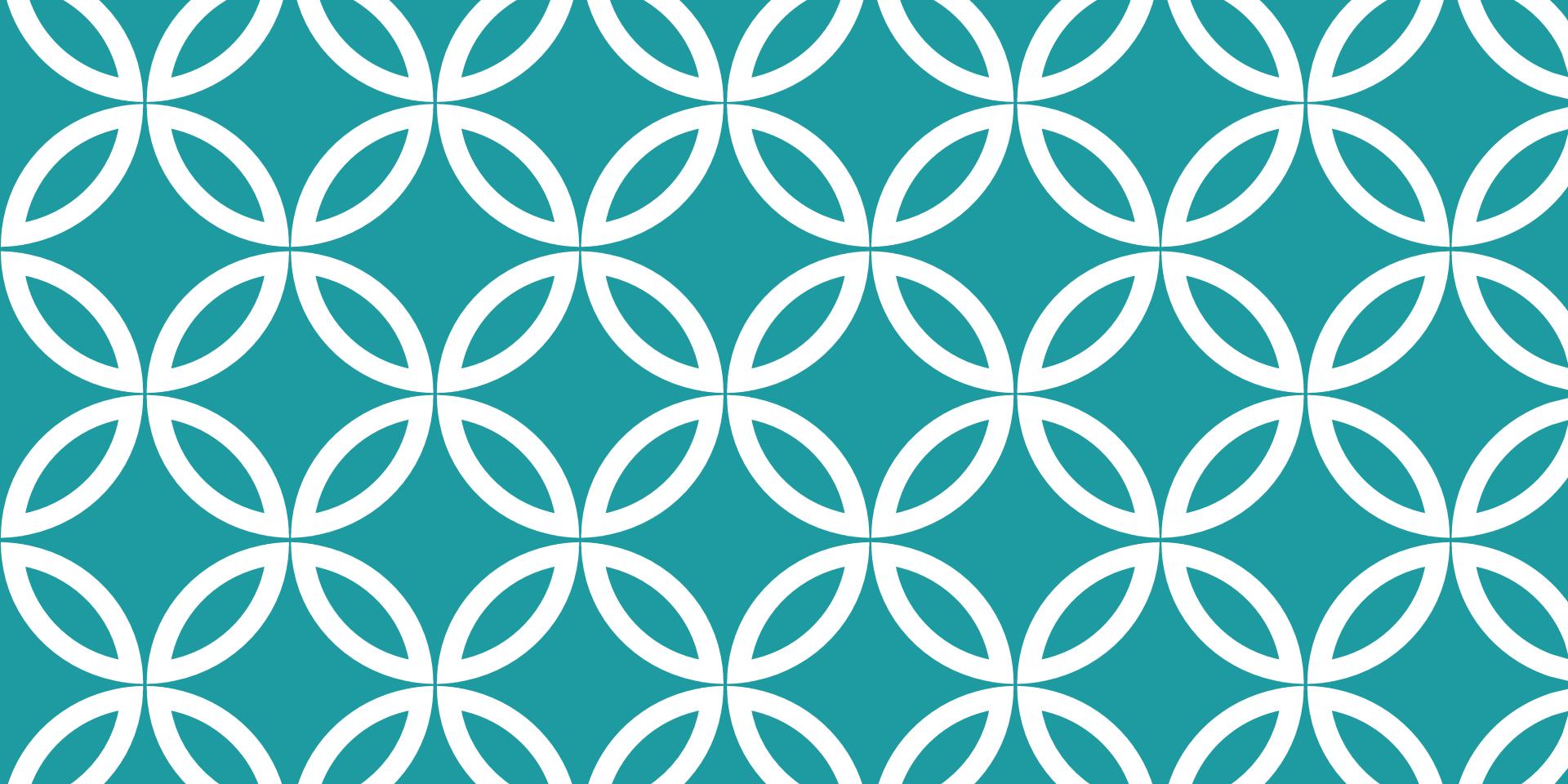
Ruční výroba mapování a šablony

Nový pokus s daty z APTNotes



# KAAE: KIBANA ALERT APP

Relativně nová aplikace  
pro alerting



KIBANA 5

Náhled nové verze

\*



Discover



Visualize



Dashboard



Timelion



Graph

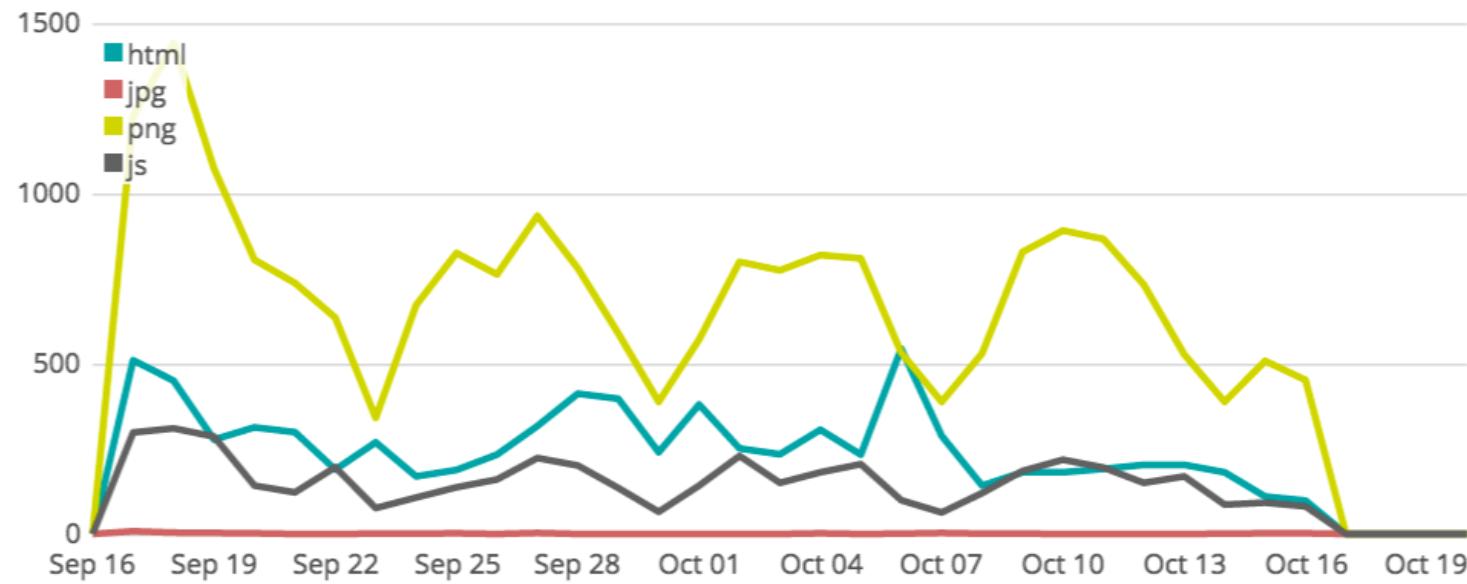


Monitoring



Settings

### Content Types



### Country by OS



# NOVÉ ROZHRANÍ

Integrovaný Sense  
Timelion



1. Select

2. Review

3. Upload

Pick a CSV file to get started. Please follow the instructions below.

Drop your file here

or

Select File

Maximum upload file size: 1 GB

Reset

Next

# PODPORA VKLÁDÁNÍ CSV

Konečně snadná data!



**Review the index pattern.** Here we'll define how and where to store your parsed events. We've made some intelligent guesses for you, but most fields can be changed if we got it wrong!

#### Index name

The name of the Elasticsearch index you want to create for your data.

Name	Type	Example
Transaction_date	string	1/2/09 6:17
Product	string	Product1
Price	number	1200
Payment_Type	string	Mastercard
Name	string	carolina
City	string	Basildon
State	string	England
Country	string	United Kingdom
Account_Created	string	1/2/09 6:00
Last_Login	string	1/2/09 6:08

1 2 »

Page Size 10

# EDITACE TYPŮ

Další zjednodušení

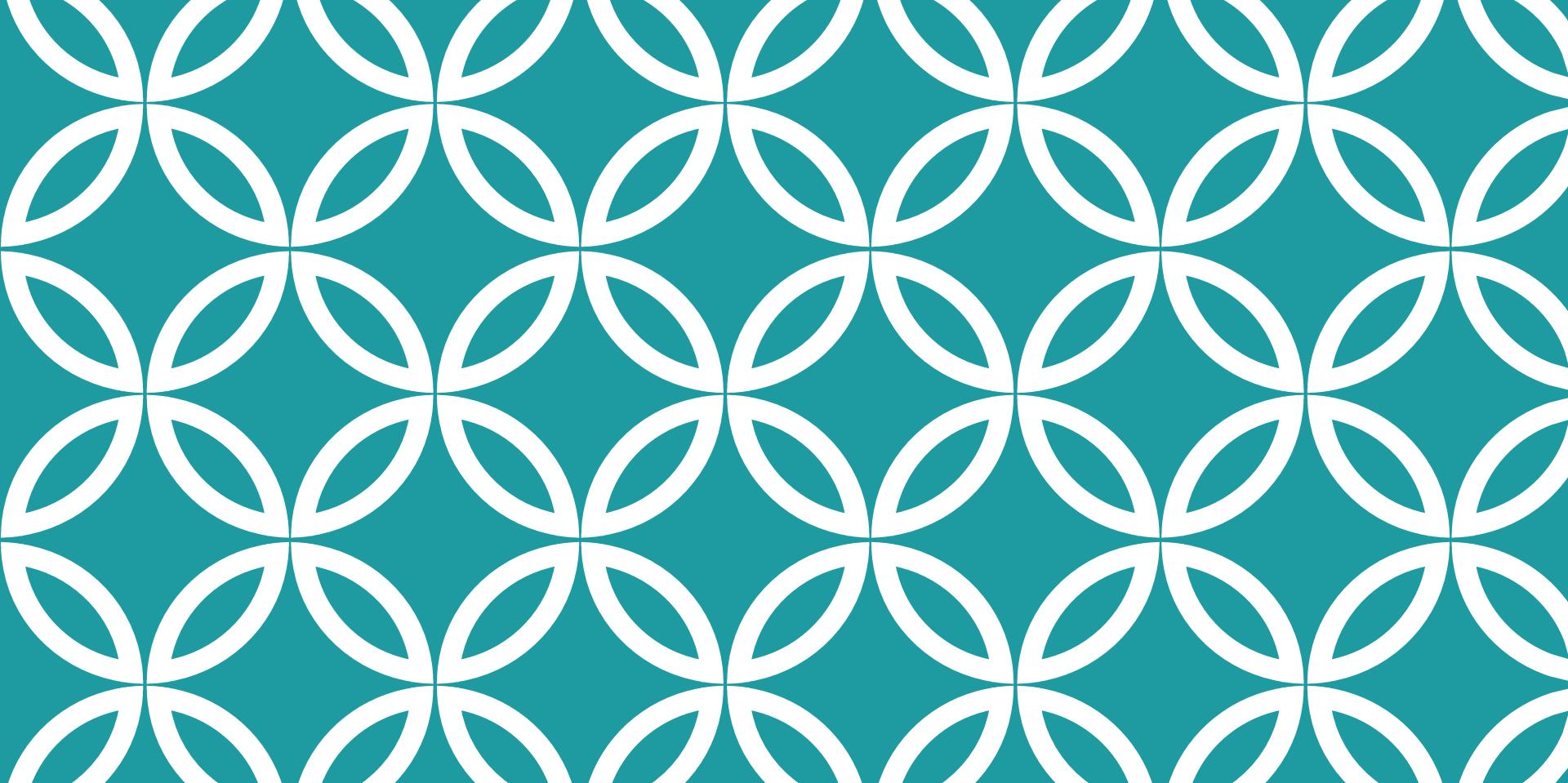


```
1 GET _search
2 {
3   "query": {
4     "match_all": {}
5   }
6 }
```

```
1 {
2   "took": 15,
3   "timed_out": false,
4   "_shards": {
5     "total": 21,
6     "successful": 21,
7     "failed": 0
8   },
9   "hits": {
10    "total": 38638,
11    "max_score": 1,
12    "hits": [
13      {
14        "_index": ".kibana",
15        "_type": "visualization",
16        "_id": "test1",
17        "_score": 1,
18        "_source": {
19          "title": "test1",
20          "visState": "{\"title\":\"test1\",\"type\":\"histogram\",\"params\":{\"shareYAxis\":true,\"addTooltip\":true,\"addLegend\":true,\"scale\":\"linear\",\"mode\":\"stacked\",\"times\":[],\"addTimeMarker\":false,\"defaultYExtents\":false,\"setYExtents\":false,\"yAxis\":{}},\"aggs\":[{\"id\":\"1\",\"enabled\":true,\"type\":\"count\",\"schema\":\"metric\",\"params\":{}},{\"id\":\"2\",\"enabled\":true,\"type\":\"terms\",\"schema\":\"segment\",\"params\":{\"field\":\"policyID\",\"size\":5,\"order\":[\"desc\"],\"orderBy\":[\"1\"]},{\"id\":\"3\",\"enabled\":true,\"type\":\"cardinality\",\"schema\":\"metric\",\"params\":[\"field\":\"fr_site_limit\"]}],\"listeners\":{}}",
21          "uiStateJSON": "{\"vis\":{\"legendOpen\":true}}",
22          "description": "",
23          "version": 1,
24        },
25        "kibanaSavedObjectMeta": {
26          "searchSourceJSON": "{\"index\":\"insurance\",\"query\":{\"query_string\":{\"query\":\"*\"},\"analyze_wildcard\":true}},\"filter\":[]"
27        }
28      },
29    ],
30  }
```

# UKÁZKA CONSOLE

Bez zbytečných starostí



# DALŠÍ DATOVÉ ZDROJE?

Sky is the limit

# JAKÉ DALŠÍ ZDROJE ZPRACOVÁVAT?

Antivirus | často i HIDS/HIPS logy

Endpoint Security Protection | podpora pro {Splunk, ElasticSearch}

DNS logy | PassiveDNS v nějaké podobě

Proxy logy | + související (např. WAF, Apache, IIS, haproxy)

Firewally | Cisco ASA a podobné

IDS | Suricata už umí přímo JSON

Honeypoty | alespoň část metadat

Windows logy | události, RDP, AD, ...

# JAKÉ DALŠÍ ZDROJE ZPRACOVÁVAT?/2

VPN | Přihlášení a klidně i další detailly

Forenzní nálezy, IOCs | Zejména z analyzovaných incidentů

Sandbox data | Cuckoo, Lastline, ...

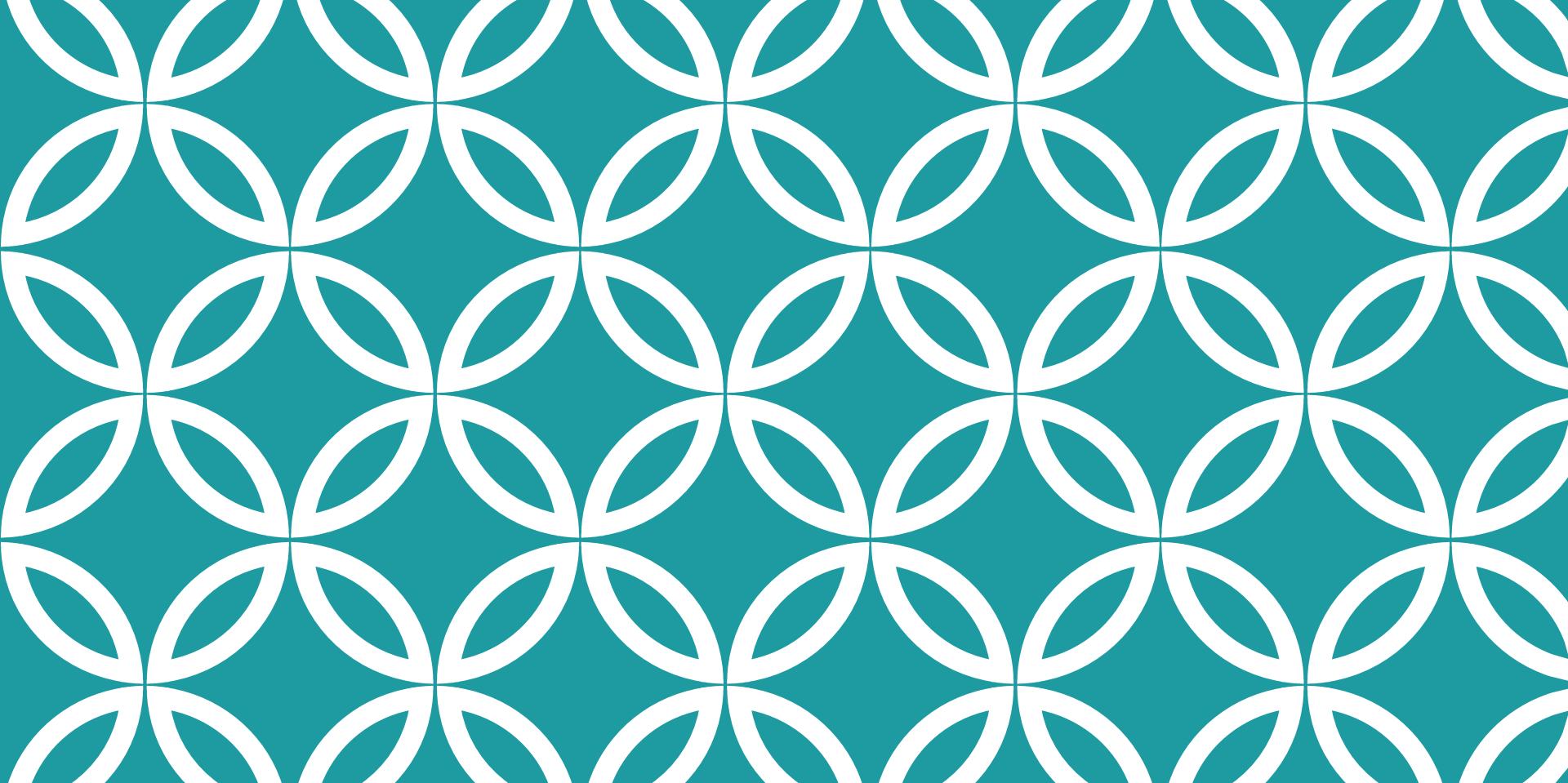
Ticketovací systémy | Metriky, dashboardy

Průběhy backupů | Vhodné při prevenci ransomware

Threat Intel | Korelace, měření kvality zdrojů

CIRT maily | vhodné pro hlášené phishingy

**Cokoliv, co budete potřebovat!**



## DALŠÍ PROJEKTY

Silná komunita -- základ  
úspěchu

# ELASTICSEARCH & DALŠÍ ŘEŠENÍ

Grafická rozhraní nad daty

[ElasticUI](#)

[SearchKit](#)

Metriky

[Grafana](#)

Alerting

[ElastAlert](#)

[411](#)

PCAP collector

[Moloch](#)

Incident Response

[nightHawkResponse](#)

Kibana pluginy

[Kibana: Known Plugins](#)

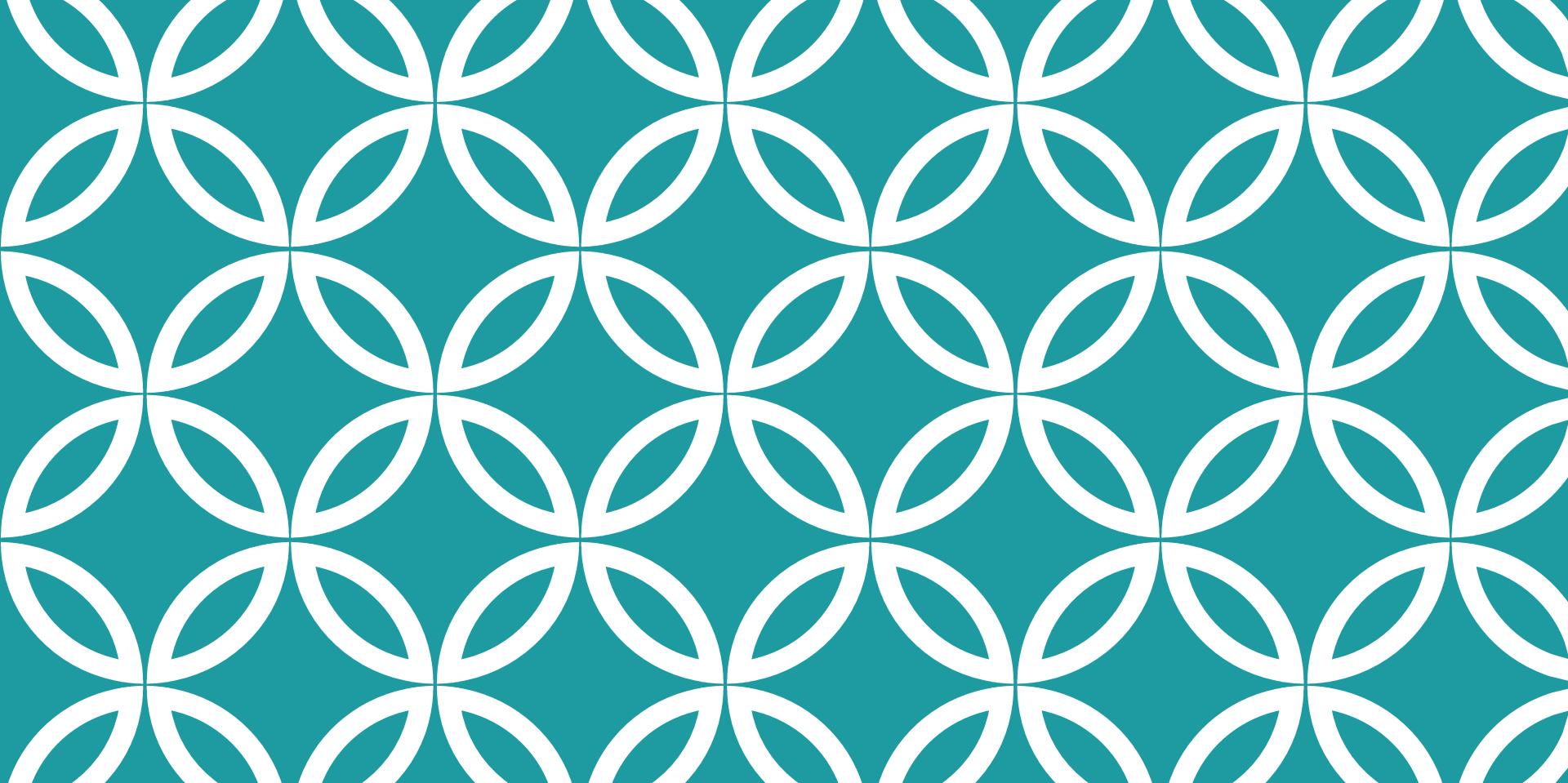
# ELASTIC AS A SERVICE

## logz.io

- <http://site2.logz.io/pricing/>
- Zdarma: 1 GB/den | 3denní retence | alerty

## LogSene

- <http://sematext.com/logsene/>
- Zdarma: 512 MB/den | 7denní retence | role-based access



# DISKUZE

Otázky  
Odpovědi  
Postřehy