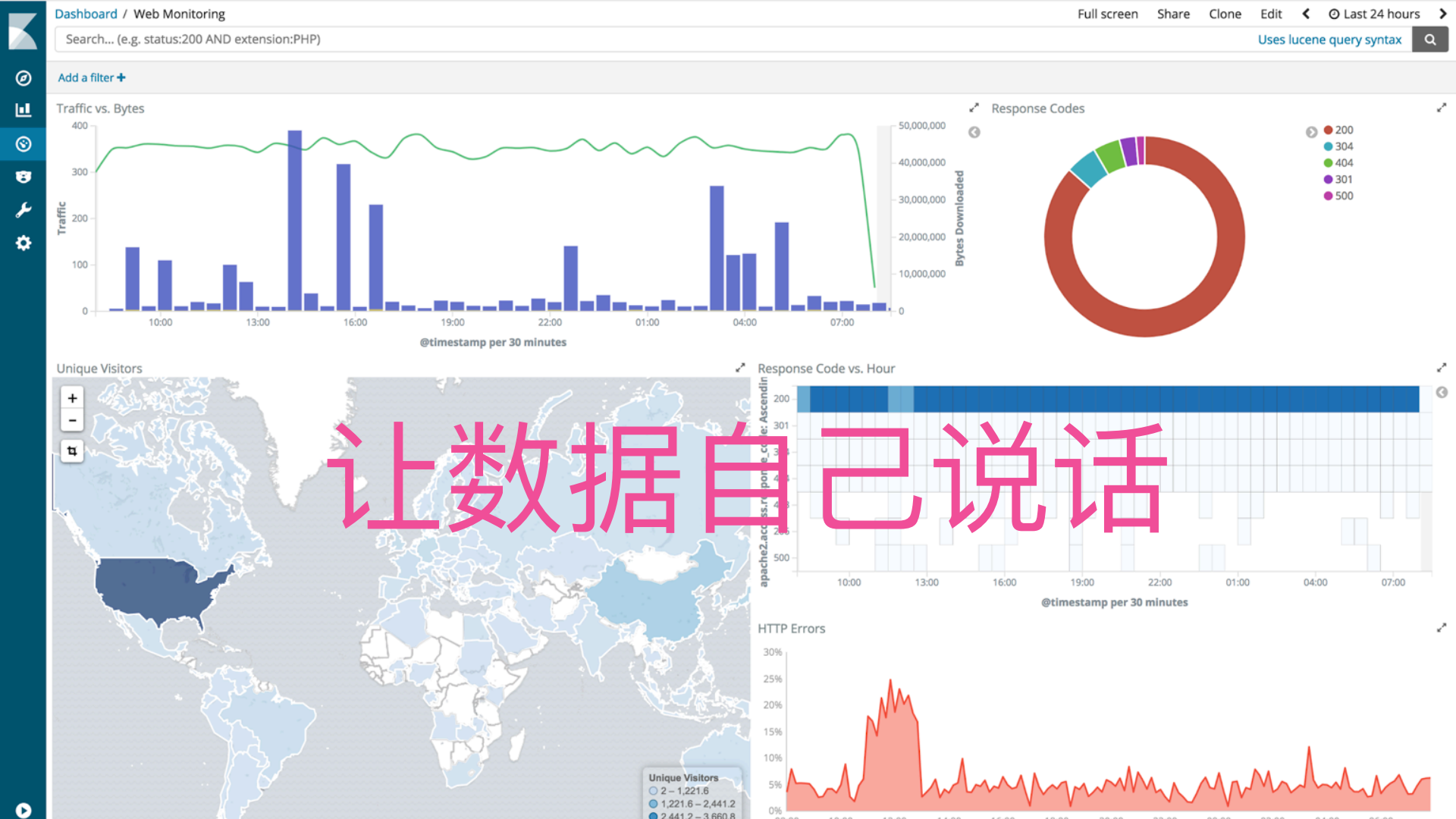

WARNING
Don’t go away!
Awesome Inside!


elastic



http://docmanagement.com.br/08/30/2016/sonda-investe-na-ativas-empresa-de-servicos-de-data-center/


数据、数据、数据


Dashboard / Web Monitoring
Full screen
Share
Clone
Edit
Last 24 hours
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
Traffic vs. Bytes
Traffic
Bytes Downloaded
@timestamp per 30 minutes
Response Codes
200
304
404
301
500
Unique Visitors
Unique Visitors
2 – 1,221.6
1,221.6 – 2,441.2
2,441.2 – 3,660.8
Response Code vs. Hour
@timestamp per 30 minutes
HTTP Errors
让数据自己说话

Kibana 从 0 到 100

Elastic 技术布道师 - 曾勇（Medcl）
medcl@elastic.co
github.com/medcl
@medcl

Elastic 是一家什么公司？

Elastic 提供一系列解决方案



基于开源的前沿技术



Elastic 拥有庞大的社区



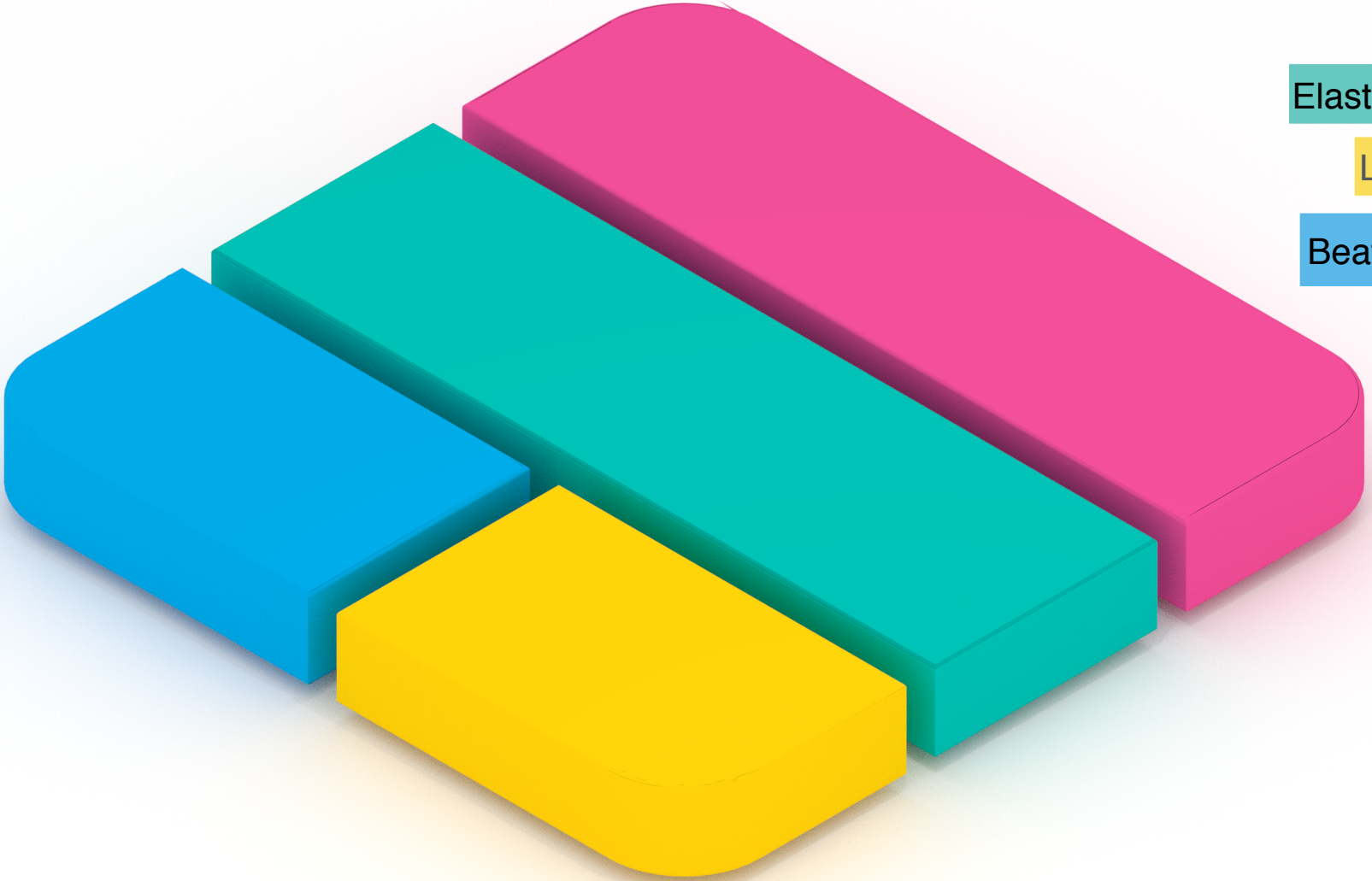
提供完整的企业级产品
security, analytics 及 AI



也提供技术支持和咨询



elastic


Kibana
Elasticsearch
Logstash
Beats / APM



Elastic Cloud Enterprise

Kibana

Elasticsearch

Logstash

Beats / APM

Elastic Cloud Enterprise 可以集中管理

Elasticsearch, Kibana, Logstash, Beats, APM,

Swiftype's (site + app + enterprise) search



有谁在用 Kibana？

这些公司也在用


salesforce
docker
PSA PEUGEOT CITROËN
ACTIVISION BLIZZARD
BNP PARIBAS
SwissLife
Crédit Mutuel ARKEA
Unilever
Goldman Sachs
SOCIETE GENERALE
NASA
BlaBlaCar
Audi
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
SeLoger.com
NETFLIX
Symantec
The New York Times
CISCO
ebay
DELL
DHL
Expedia
GROUPON
HSBC
BANQUE DE FRANCE
Quora
Microsoft
Cadremploi.fr
UBER
stack overflow
PayPal
elastic


MR. ROBOT



kibana

开源的实时大数据可视化分析平台，与 *Elasticsearch* 深度集成。

小故事，名称来历：*Kibana = kiwi + banana*



https://share.america.gov/pt-br/boa-noticia-para-os-elefantes-em-2016-o-preco-do-marfim-despenca/



https://www.siemens-home.bsh-group.cn/products/refrigeration-and-freezing/refrigerator-freezers


100% 开源软件
https://github.com/elastic/kibana



https://www.fsi.com.my/literaturehistorylinguistic-%E6%96%87%E5%8F%B2%E4%B8%8E%E8%AF%AD%E8%A8%80%E7%B3%BB-%E5%8E%86%E5%8F%B2/

升学互动网 - fsi.com.my

logstash - Mozilla Firefox

File Edit View History Bookmarks Tools Help

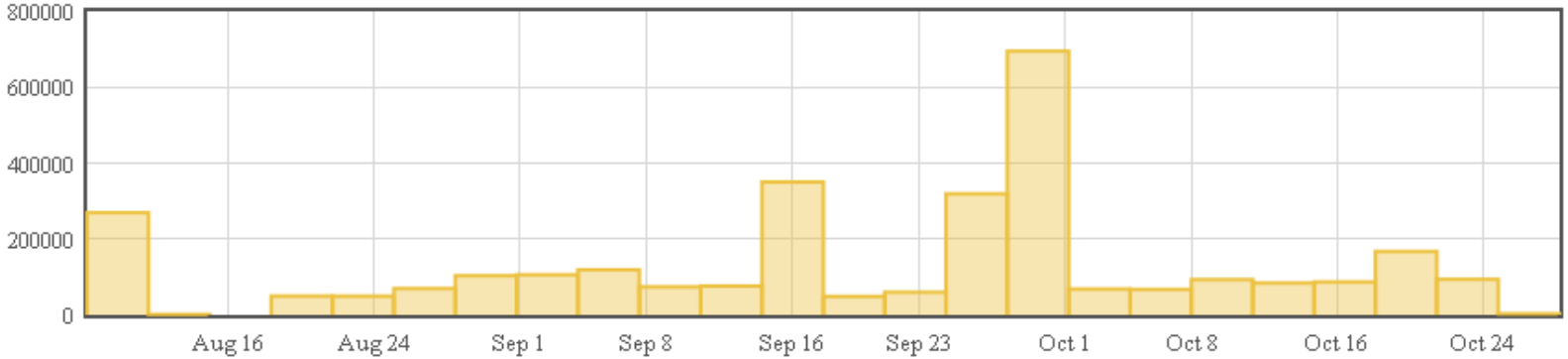
logstash

http://127.0.0.1:9292/search#{"offset"%3A0%2C"count"%3A50%2C"q"%3A"* @timestamp%3A[2011-08-01 TO 2011-

Most Visited Getting Started Latest Headlines Read It Later

Query: * @timestamp:[2011-08-01 TO 2011-10-26] Search Clear **logstash.**

You can click on any search result to see what kind of fields we know about for that event. You can also click on the graph to zoom to that time period. The query language is that of Lucene's string query (docs).



Search results for '* @timestamp:[2011-08-01 TO 2011-10-26]'

Results 0 - 50 of 3051955 | first | prev | next | last | refresh | (22.142 seconds)

timestamp	event
2011-10-25T00:07:42.435000Z	2011-10-24T20:07:27-04:00 corrin sendmail[883]: p9P07RcU000883: from=<ossecm@corrin.example.com>, size=1987, class=0, nrcpts=1, msgid=<201110250007.p9P07RcU000883@corrin.example.com>, proto=SMTP, daemon=MTA, relay=corrin.example.com [127.0.0.1]
2011-10-25T00:07:42.436000Z	2011-10-24T20:07:31-04:00 corrin nrpe[887]: Handling the connection...

Logstash Search

2 days ago to 3 minutes ago

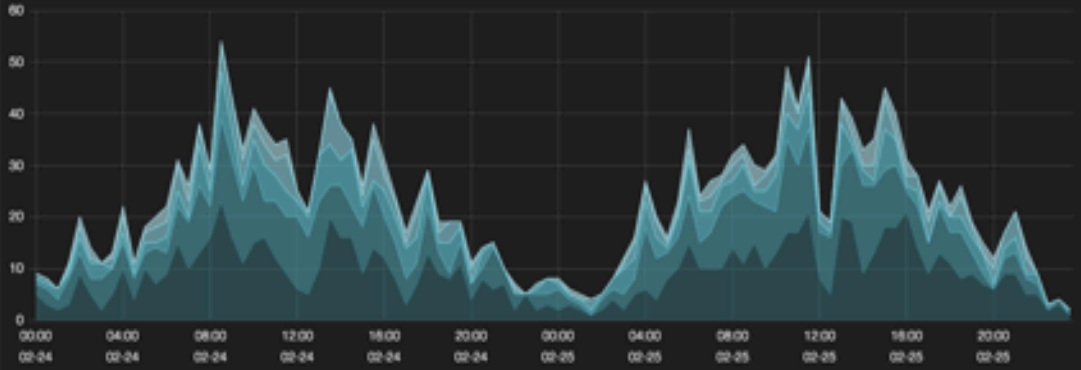
QUERY +

bytes:[0 TO 4000000] AND @tags:success

FILTERING +

EVENTS OVER TIME

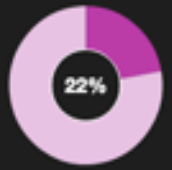
View + | Zoom Out | html (ext) (668) php (ext) (659) png (ext) (317) gif (ext) (229) css (ext) (121) count per **30m** | (**2214** hits)



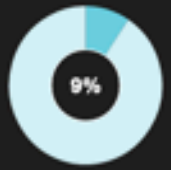
MAP



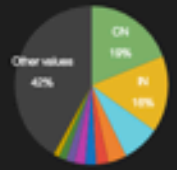
REVENUE



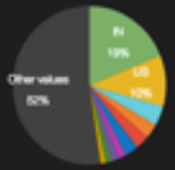
VOLUME



TOP DESTINATIONS



TOP SOURCES



GEO PAIRS



ALL EVENTS

0 to **100** of 500 available for paging

Fields

All (51) / Current (28)

Type to filter...

- @message
- @tags

@tags	geo.srcdet	extension	clientip	bytes	id	phpmemory	response
success,security	MYVN	html	187.12.22.189	8640	1066		200
success,info	IT:MM	png	164.87.170.73	2045	1903		200
success,info	ARES	html	222.23.102.238	1801	1133		200
success,info	INDZ	html	138.226.66.81	7029	1801		200

kibana

Discover | Visualize | Dashboard | Settings

June 1st 2011, 00:16:26.010 to May 7th 2013, 14:29:14.931

+article

+article

700,316 hits

Selected Fields

t _source

Fields

Popular fields

t agent

bytes

t geo.city

geo.coordinates

t geo.country_code

@timestamp

t _id

t _index

t _type

creation_time

t destination

t geo.region

t referrer

t request

t timezone

t user

June 1st 2011, 00:16:26.010 - May 7th 2013, 14:29:14.931

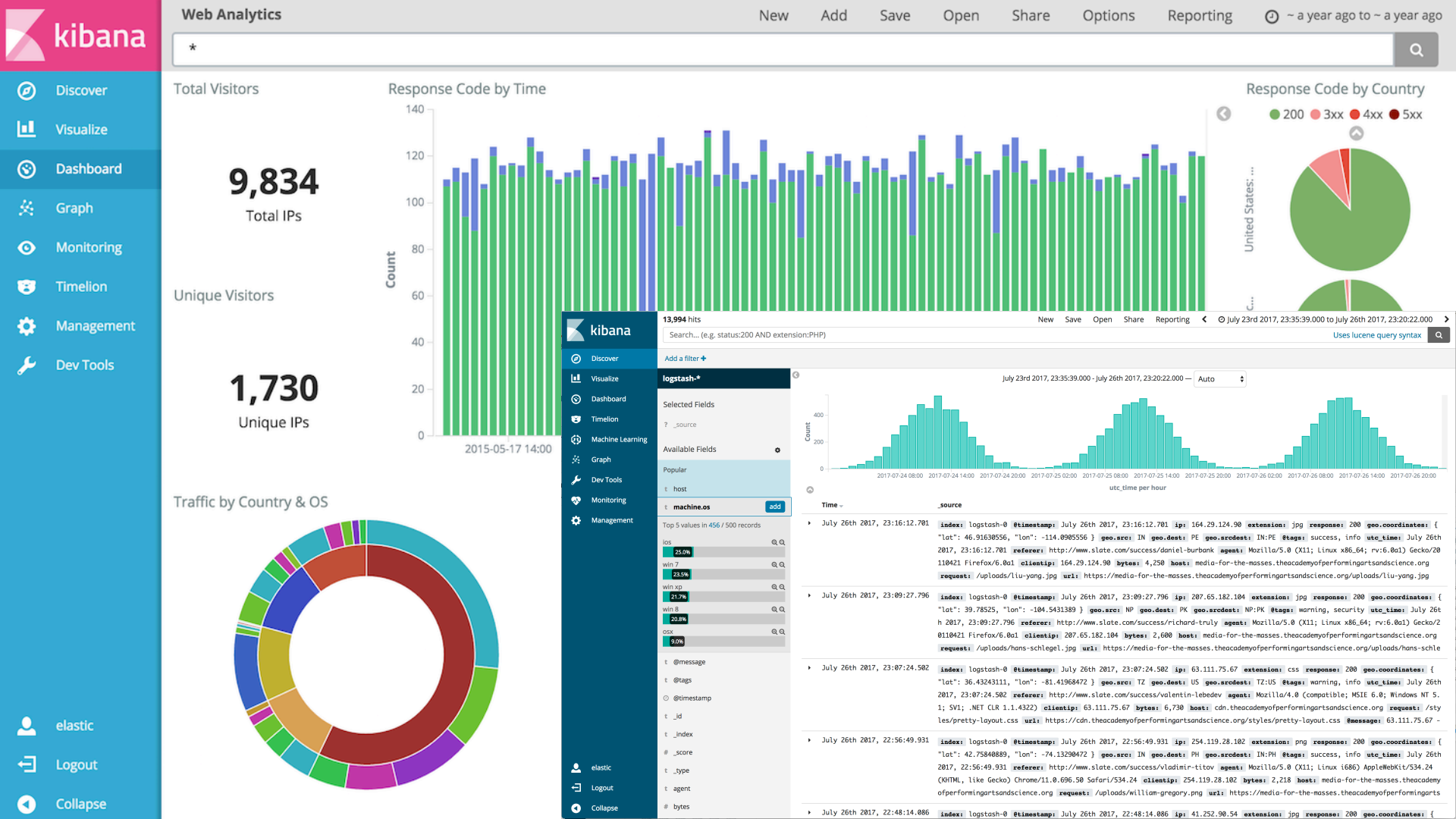


Time	_source
May 7th 2013, 14:29:02.000	referrer: http://www.spk.usace.army.mil/Media/NewsReleases/tabid/1034/Article/13480/corps-releases-inspection-rating-sacramento-river-west-bank-levees.aspx @timestamp: May 7th 2013, 14:29:02.000 creation_time: May 7th 2012, 14:15:25.000 agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0 bytes: 379990 geo.country_code: US geo.city: Fort Huachuca geo.region: AZ geo.coordinates: {"lat":31.5273,"lon":-110.360703} timezone: America/Phoenix request: http://bit.ly/JMGcUW destination: http://www.spk.usace.army.mil/M
May 7th 2013, 14:28:50.000	destination: http://www.spk.usace.army.mil/Media/NewsReleases/tabid/1034/Article/13480/corps-releases-inspection-rating-sacramento-river-west-bank-levees.aspx @timestamp: May 7th 2013, 14:28:50.000 creation_time: May 3rd 2013, 12:01:44.000 agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0 bytes: geo.country_code: US geo.city: Fort Huachuca geo.region: AZ geo.coordinates: {"lat":31.5273,"lon":-110.360703} timezone: America/Phoenix request: http://1.usa.gov/18ikFnb user: usacesacramento referrer: direct

Table JSON

Link to /usagov/log/AUuEF4d3npiyxElinDkv

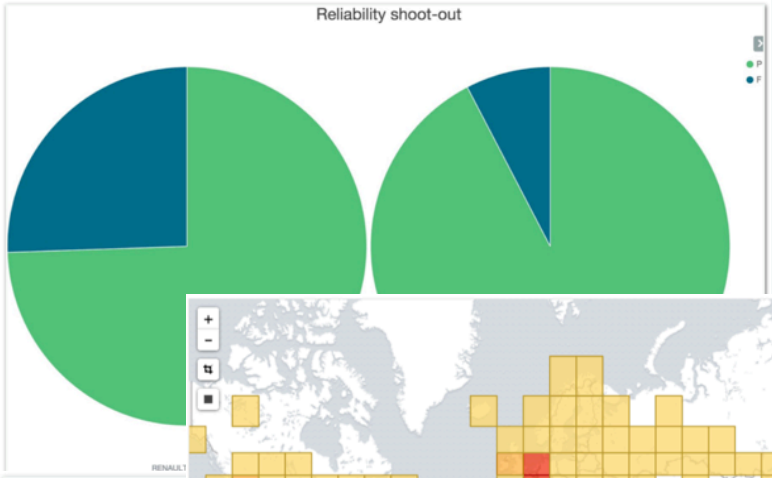
@timestamp May 7th 2013, 14:28:50.000

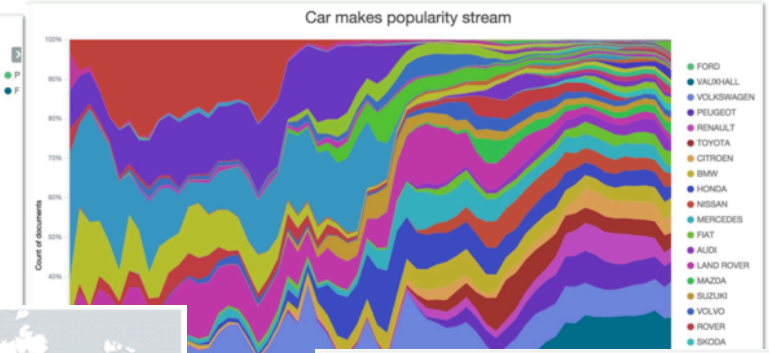

kibana
Web Analytics
New
Add
Save
Open
Share
Options
Reporting
~ a year ago to ~ a year ago
*
Discover
Visualize
Dashboard
Graph
Monitoring
Timelion
Management
Dev Tools
elastic
Logout
Collapse
Total Visitors
9,834
Total IPs
Unique Visitors
1,730
Unique IPs
Response Code by Time
Count
2015-05-17 14:00
Response Code by Country
200
3xx
4xx
5xx
United States: ...
Traffic by Country & OS
13,994 hits
New
Save
Open
Share
Reporting
July 23rd 2017, 23:35:39.000 to July 26th 2017, 23:20:22.000
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter
logstash-*
Selected Fields
_source
Available Fields
Popular
host
machine.os
add
Top 5 values in 456 / 500 records
ios
25.0%
win 7
23.5%
win xp
21.7%
win 8
20.8%
osx
9.0%
@message
@tags
@timestamp
_id
_index
_score
_type
agent
bytes
utc_time per hour
Time
_source

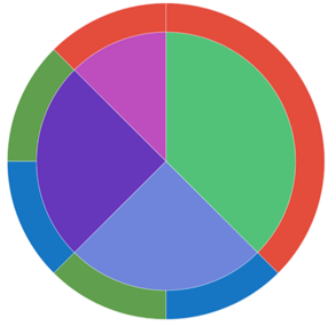


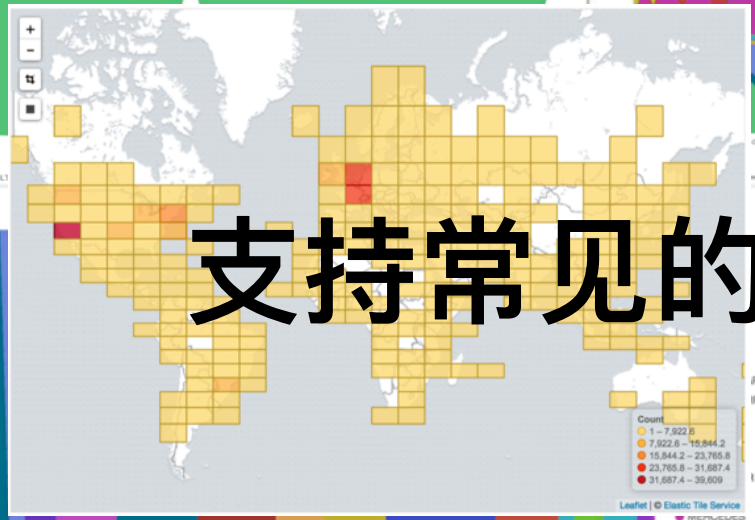
支持常见的可视化类型

elastic





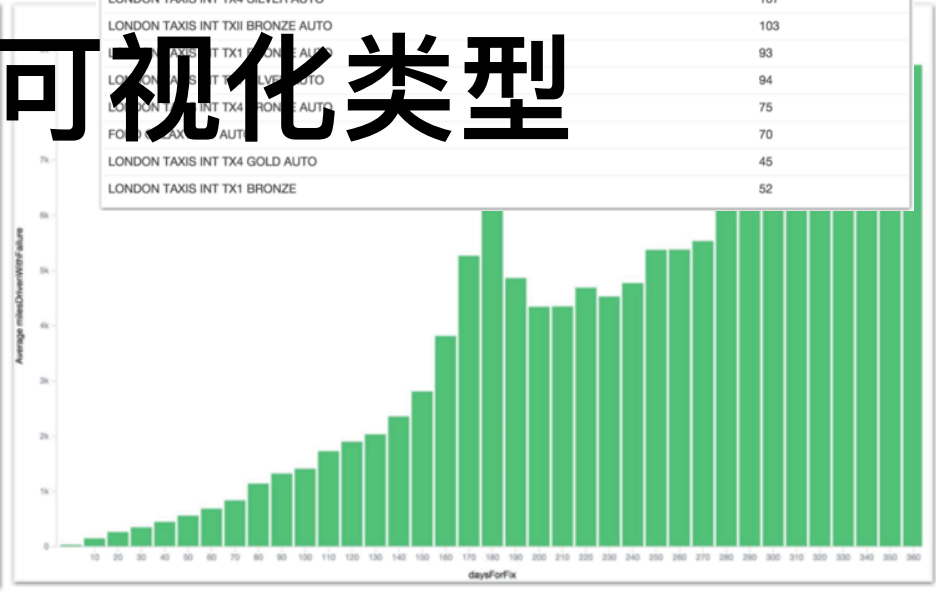




支持常见的可视化类型

Table of cars driven long distances after failures

Top 20 unusual terms in MakeModel.raw	Count of documents
VOLKSWAGEN SHARAN S TDI 115 AUTO	247
LONDON TAXIS INT TXII SILVER AUTO	125
LONDON TAXIS INT TX4 SILVER AUTO	107
LONDON TAXIS INT TXII BRONZE AUTO	103
[illegible]	93
[illegible]	94
[illegible]	75
[illegible]	70
LONDON TAXIS INT TX4 GOLD AUTO	45
LONDON TAXIS INT TX1 BRONZE	52

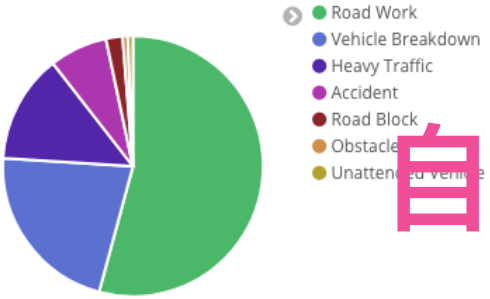


Total Incidents [Singapore LTA]

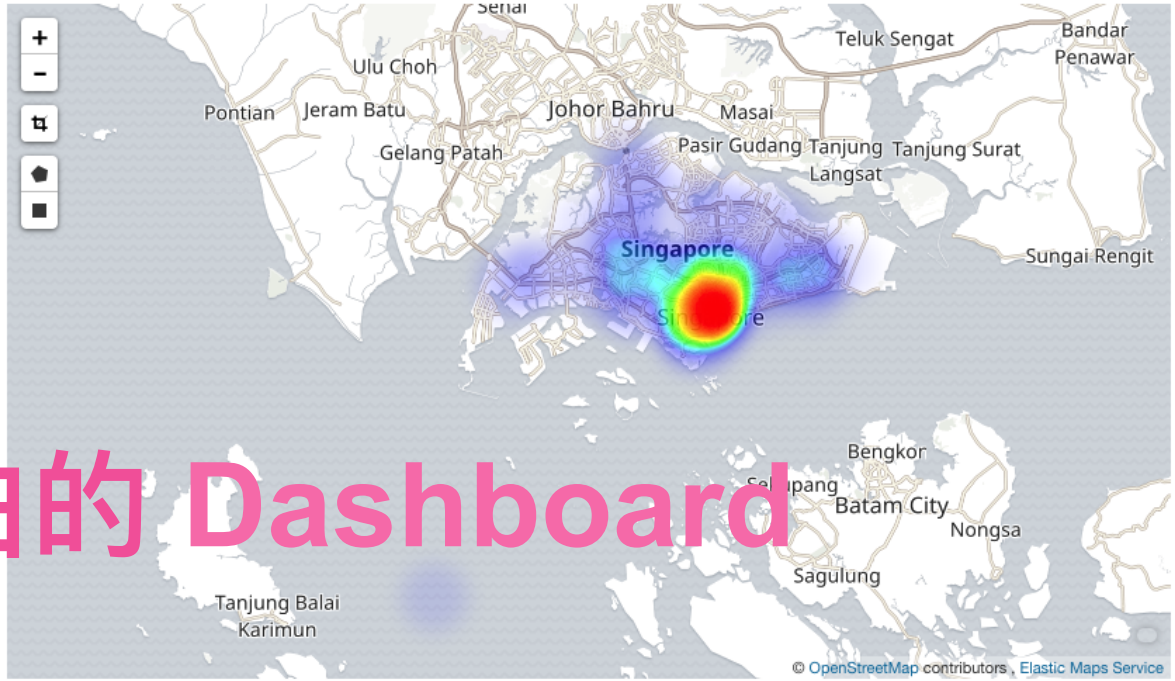
13,207

Unique Incidents

Incidents by Type [Singapore LTA]



Incidents Heatmap [Singapore LTA]

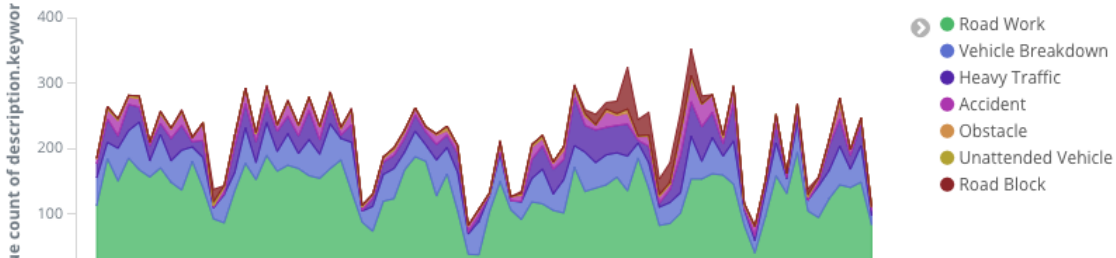


Overview [Singapore LTA]

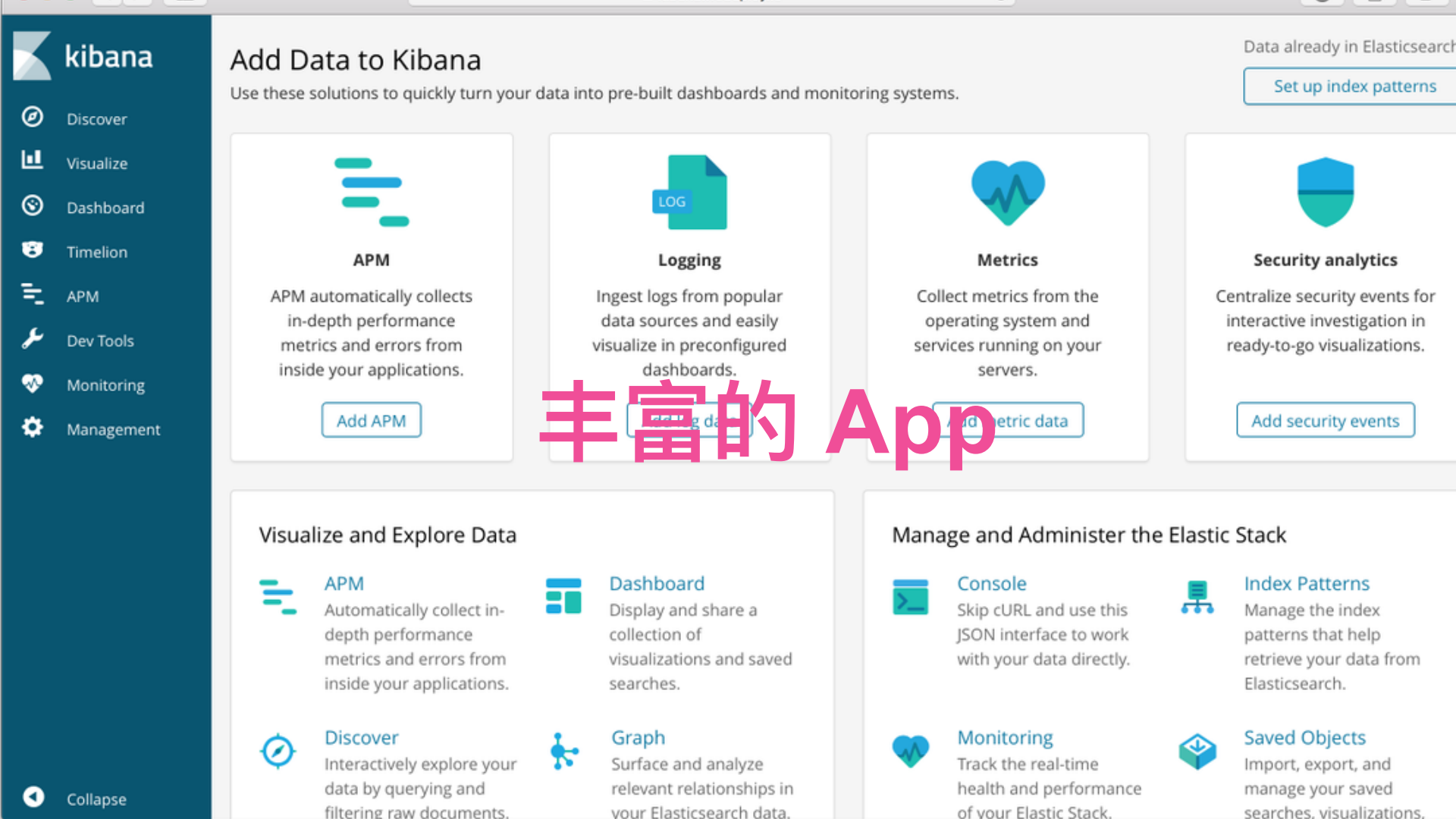
Source data provided by Singapore Land Transport Authority.

Terms and conditions here.

Incidents Timeline [Singapore LTA]



自由的 Dashboard


kibana
Discover
Visualize
Dashboard
Timelion
APM
Dev Tools
Monitoring
Management
Collapse
Add Data to Kibana
Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.
Data already in Elasticsearch
Set up index patterns
APM
APM automatically collects in-depth performance metrics and errors from inside your applications.
Add APM
LOG
Logging
Ingest logs from popular data sources and easily visualize in preconfigured dashboards.
Metrics
Collect metrics from the operating system and services running on your servers.
Security analytics
Centralize security events for interactive investigation in ready-to-go visualizations.
Add security events
丰富的 App
Visualize and Explore Data
APM
Automatically collect in-depth performance metrics and errors from inside your applications.
Dashboard
Display and share a collection of visualizations and saved searches.
Discover
Interactively explore your data by querying and
Graph
Surface and analyze relevant relationships in
Manage and Administer the Elastic Stack
Console
Skip cURL and use this JSON interface to work with your data directly.
Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.
Monitoring
Track the real-time health and performance
Saved Objects
Import, export, and manage your saved

kibana

0 hits

新建 保存 打开 分享

查询... (例如：status:200 AND extension:PHP)

使用Lucene查询语法

发现
可视化
仪表盘
时间线
开发工具
管理

get_type: "1"

添加筛选器 +

操作

所有筛选器: 启用 禁用 钉住 取消钉住 换位 开关 移除

logstash-scanlog

已选字段

? _source

可选字段

未查到数据 😐

抱歉，找不到符合查询条件的数据。以下是一些处理建议：

改善您的查询

顶部的搜索框使用Elasticsearch所支持的Lucene 查询字串语法。假设我们正在搜索已经解析成几个字段的Web服务器日志。

例如：

在任意字段中查找包含数字200的请求：

```
200
```

或者我们也可以在特定字段中查找，如：在status字段中查找200：

```
status:200
```

查找400-499之间所有状态码：

```
status:[400 TO 499]
```

查找状态码在400-499之间并且extension值为php的请求：

```
status:[400 TO 499] AND extension:PHP
```

或者HTML

```
status:[400 TO 499] AND (extension:php OR extension:html)
```



跨平台、多语言

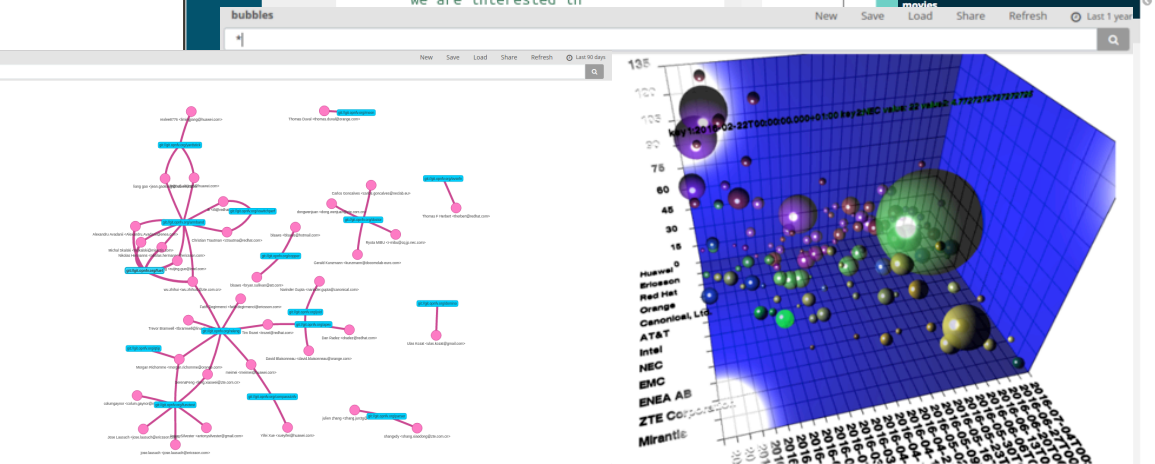
折叠

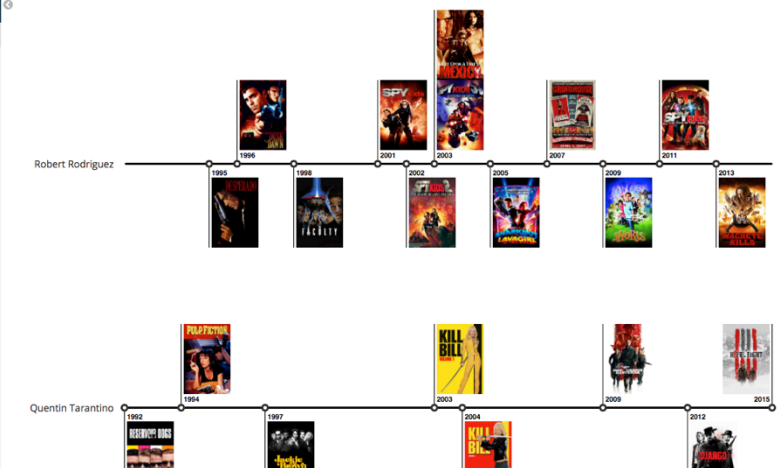
elastic



丰富的社区扩展

https://www.elastic.co/guide/en/kibana/current/known-plugins.html






ENOUGH TALK
SHOW ME THE DEMO!
memegenerator.net



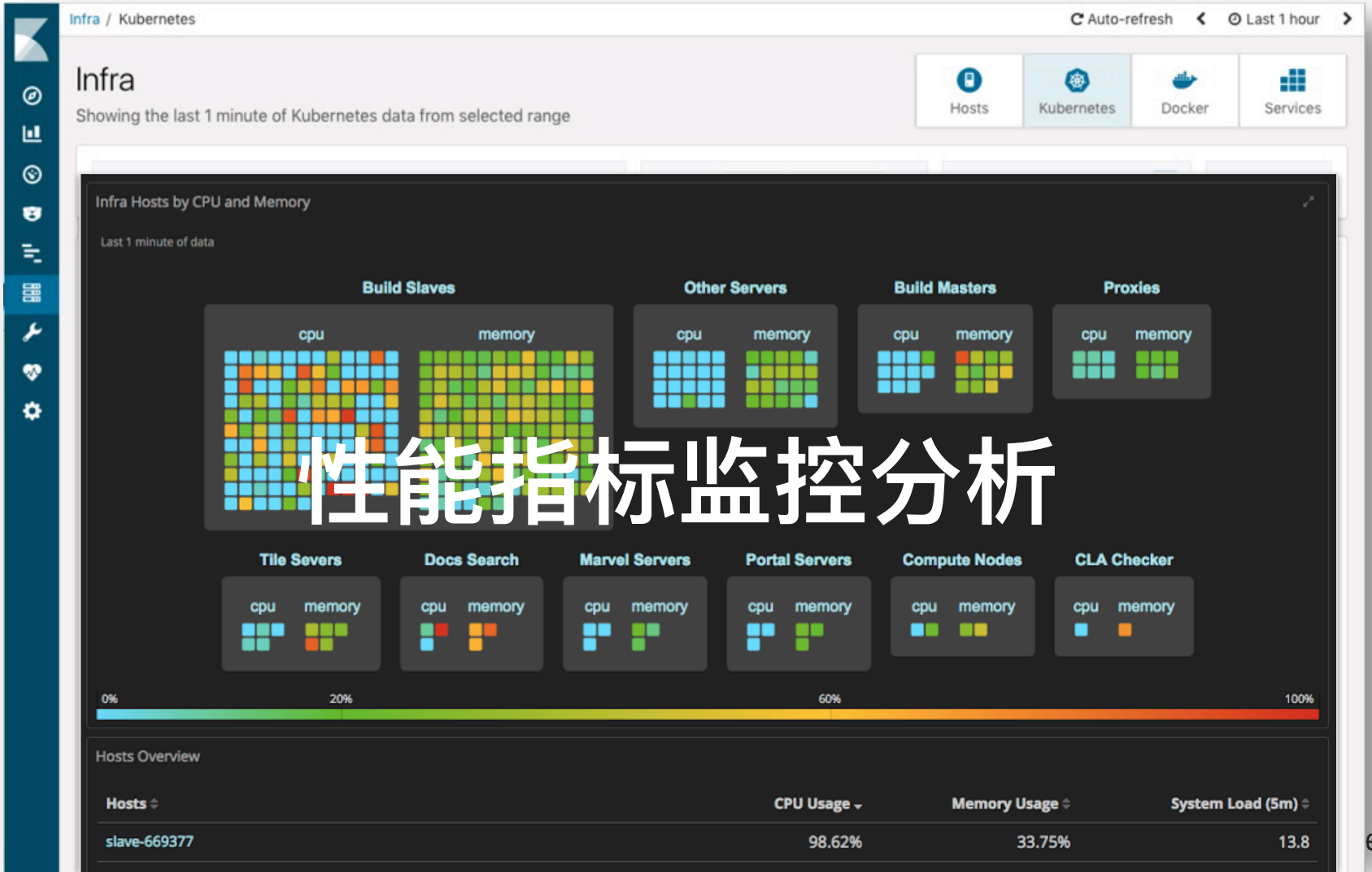
5 minutes demo


Kibana 的十八般武艺

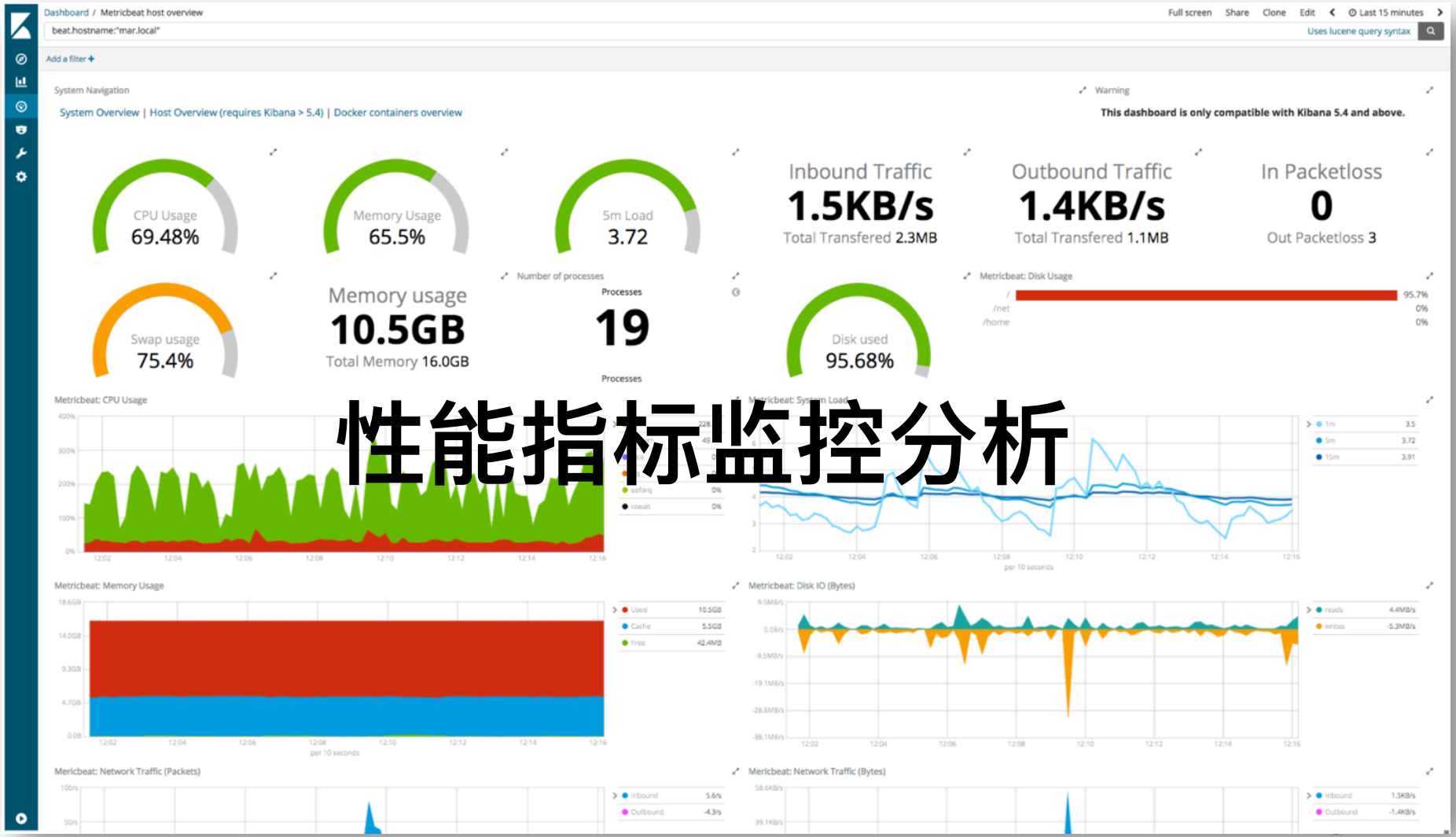


可用于**日志分析

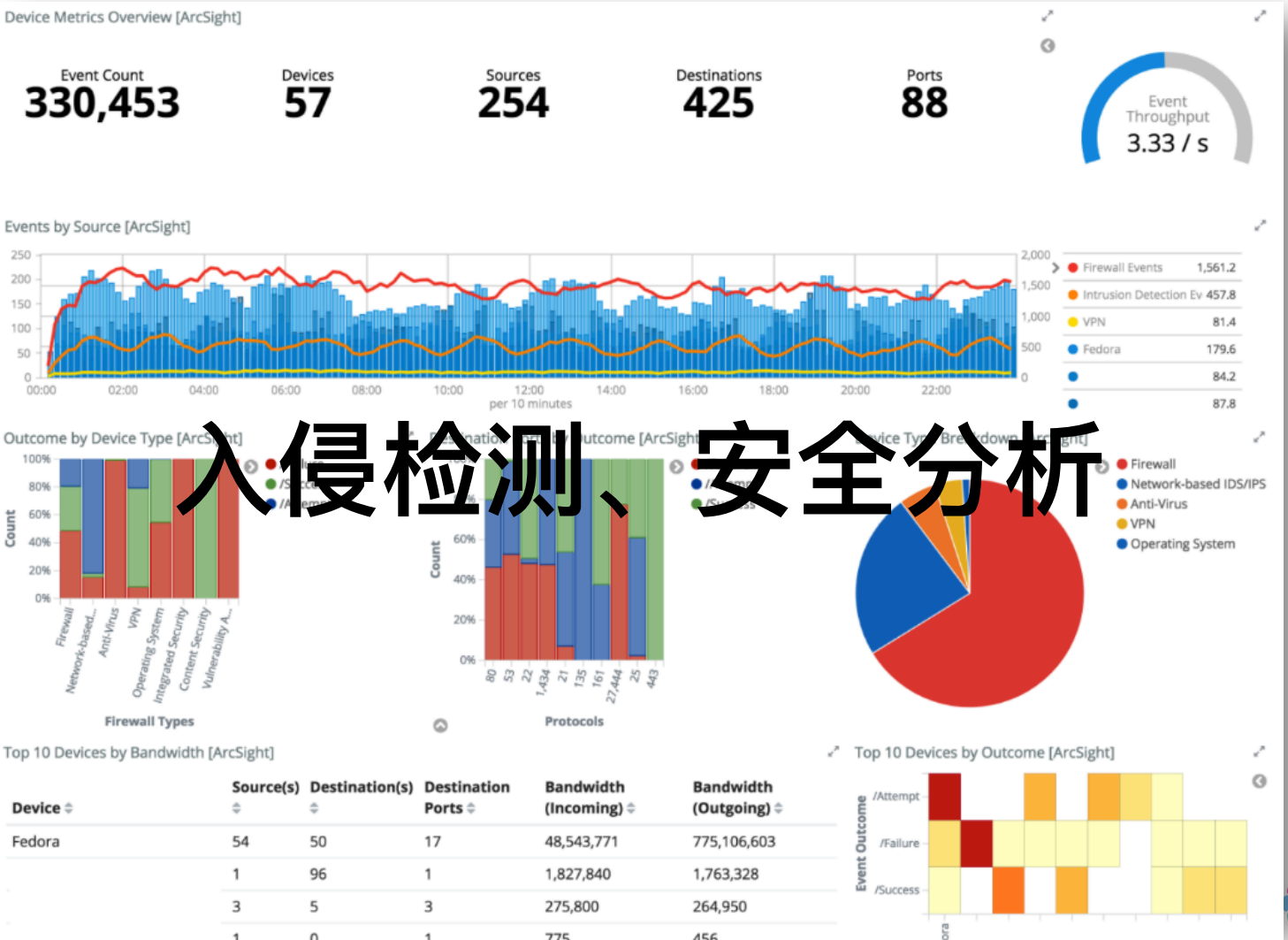
elastic


Infra / Kubernetes
Auto-refresh
Last 1 hour
Infra
Showing the last 1 minute of Kubernetes data from selected range
Hosts
Kubernetes
Docker
Services
Infra Hosts by CPU and Memory
Last 1 minute of data
Build Slaves
Other Servers
Build Masters
Proxies
cpu
memory
性能指标监控分析
Tile Severs
Docs Search
Marvel Servers
Portal Servers
Compute Nodes
CLA Checker
0%
20%
60%
100%
Hosts Overview
Hosts
CPU Usage
Memory Usage
System Load (5m)
slave-669377
98.62%
33.75%
13.8

elastic

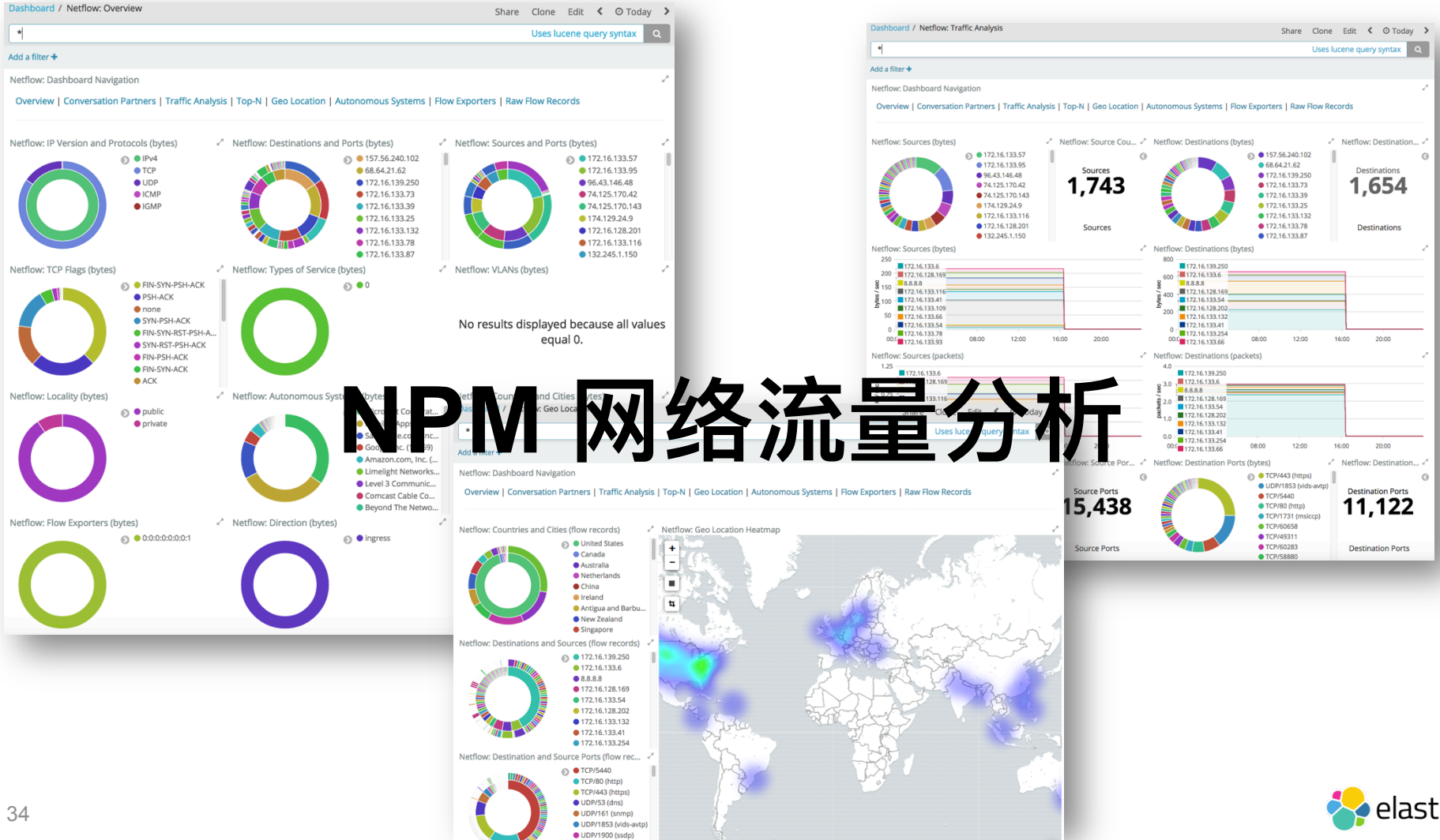

Dashboard / Metricbeat host overview
Full screen
Share
Clone
Edit
Last 15 minutes
beat.hostname:"mar.local"
Uses lucene query syntax
Add a filter
System Navigation
System Overview | Host Overview (requires Kibana > 5.4) | Docker containers overview
Warning
This dashboard is only compatible with Kibana 5.4 and above.
CPU Usage
69.48%
Memory Usage
65.5%
5m Load
3.72
Inbound Traffic
1.5KB/s
Total Transfered 2.3MB
Outbound Traffic
1.4KB/s
Total Transfered 1.1MB
In Packetloss
0
Out Packetloss 3
Swap usage
75.4%
Memory usage
10.5GB
Total Memory 16.0GB
Number of processes
Processes
19
Processes
Disk used
95.68%
Metricbeat: Disk Usage
/
/net
/home
95.7%
0%
0%
Metricbeat: CPU Usage
Metricbeat: System Load
Metricbeat: Memory Usage
Metricbeat: Disk IO (Bytes)
Mericbeat: Network Traffic (Packets)
Mericbeat: Network Traffic (Bytes)

性能指标监控分析



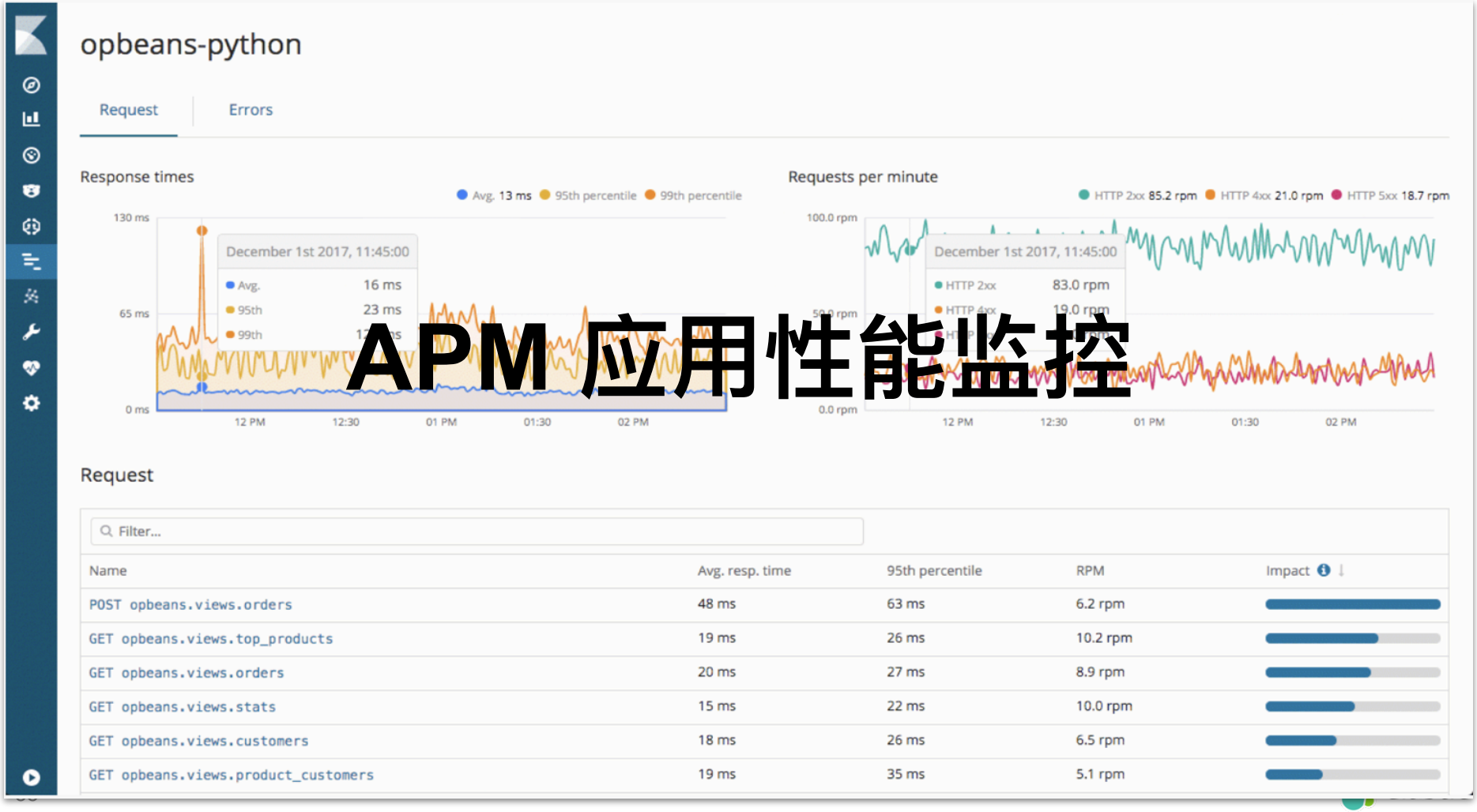
入侵检测、安全分析

elastic

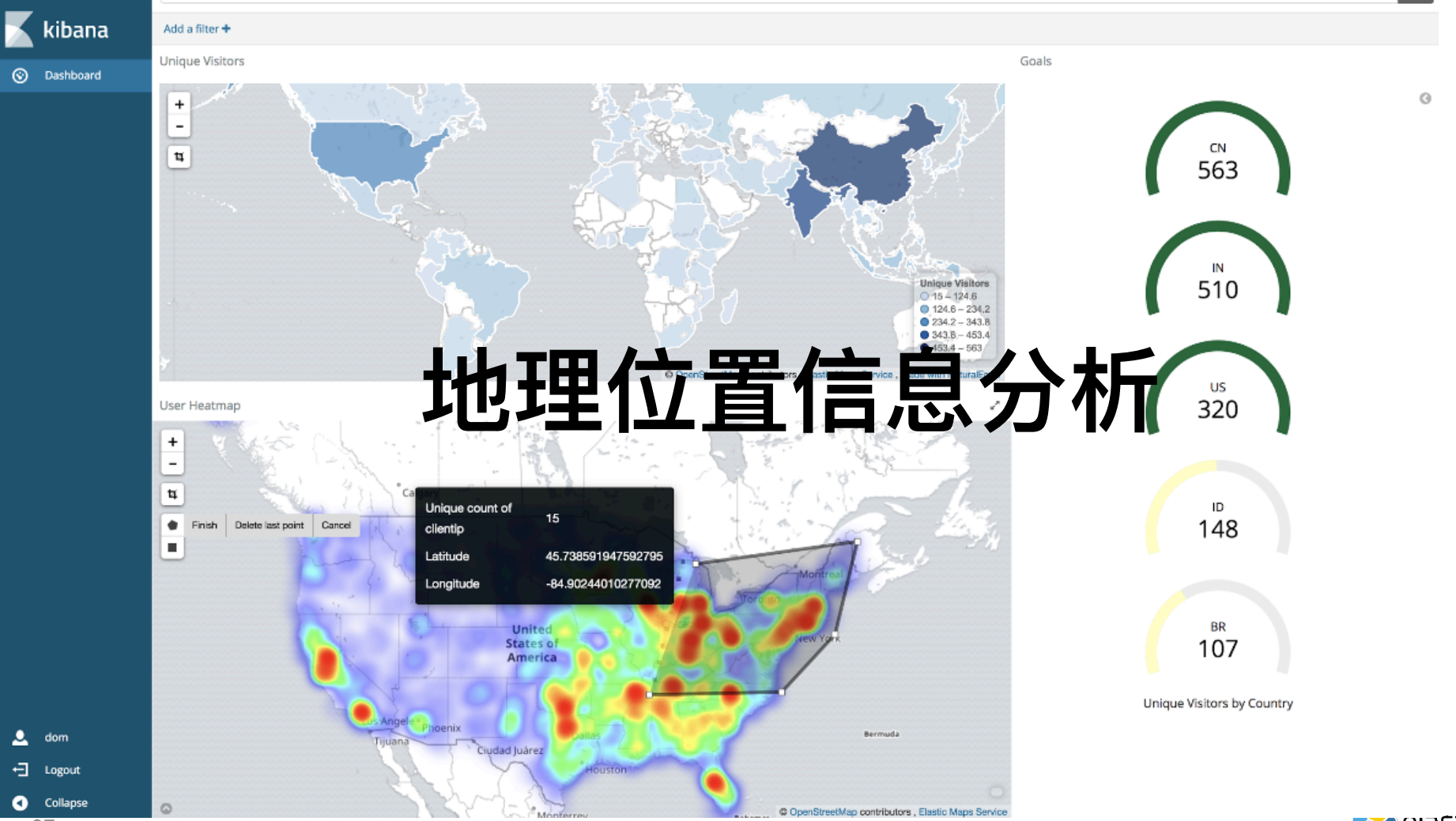


NPM 网络流量分析

elastic 3


opbeans-python
Request
Errors
Response times
Avg. 13 ms
95th percentile
99th percentile
130 ms
65 ms
0 ms
December 1st 2017, 11:45:00
Avg. 16 ms
95th 23 ms
99th
12 PM
12:30
01 PM
01:30
02 PM
Requests per minute
HTTP 2xx 85.2 rpm
HTTP 4xx 21.0 rpm
HTTP 5xx 18.7 rpm
100.0 rpm
0.0 rpm
December 1st 2017, 11:45:00
HTTP 2xx 83.0 rpm
12 PM
12:30
01 PM
01:30
02 PM
APM 应用性能监控
Request
Filter...
Name
Avg. resp. time
95th percentile
RPM
Impact
POST opbeans.views.orders
48 ms
63 ms
6.2 rpm
GET opbeans.views.top_products
19 ms
26 ms
10.2 rpm
GET opbeans.views.orders
20 ms
27 ms
8.9 rpm
GET opbeans.views.stats
15 ms
22 ms
10.0 rpm
GET opbeans.views.customers
18 ms
26 ms
6.5 rpm
GET opbeans.views.product_customers
19 ms
35 ms
5.1 rpm

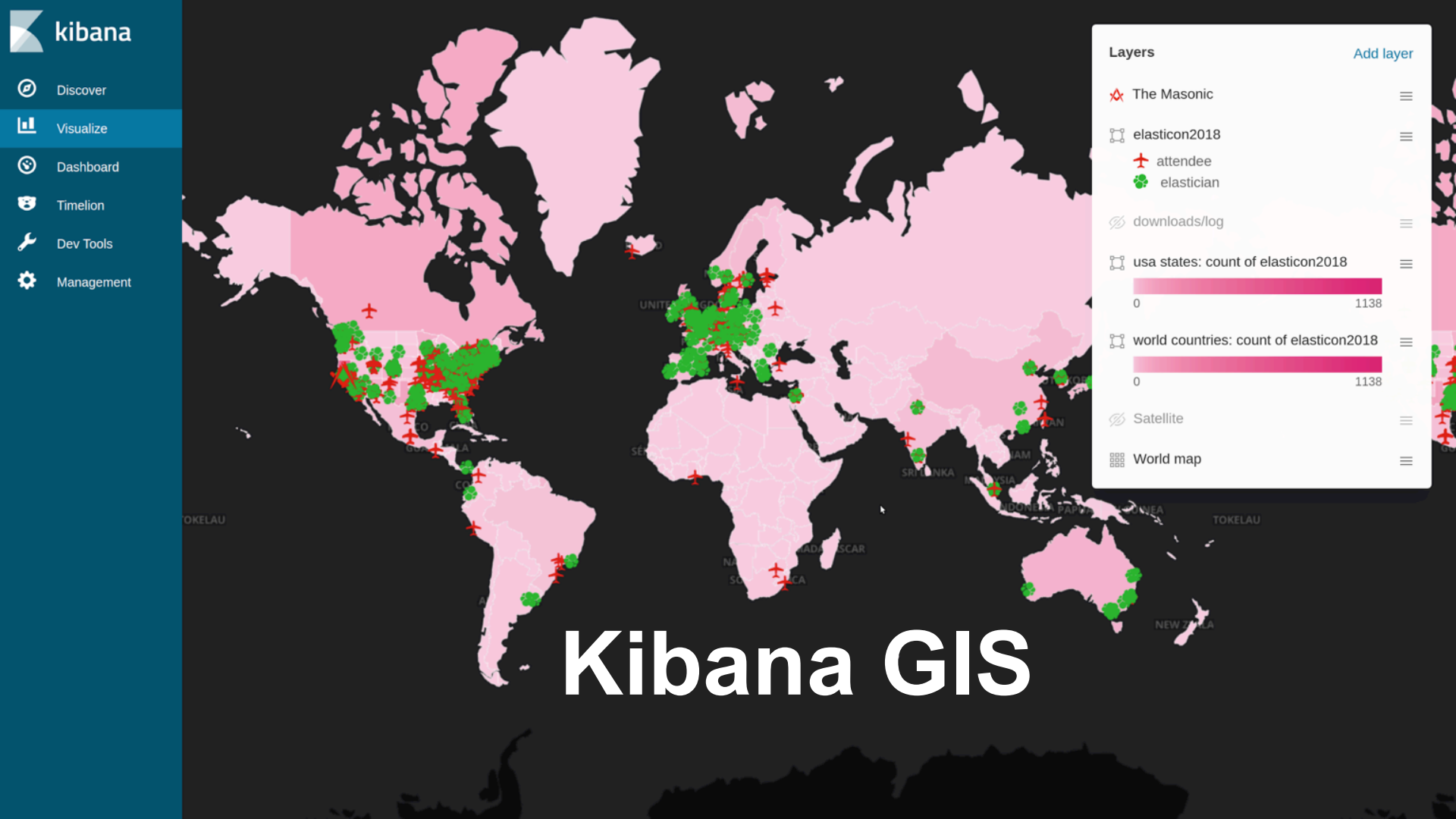

Visualize / Hit Map - US
Save
Share
Refresh
Reporting
September 15th 2017, 00:00:00.000 to October 21st 2017, 23:59:59.999
apache2.access.geoip.country_iso_code:US
Uses lucene query syntax
apache2.access.geoip.country_iso_code: "US"
Add a filter +
Actions
地理位置信息分析
Calgary
United States of America
Chicago
New York
Phoenix
Dallas
Tijuana
Ciudad Juárez
Houston
Monterrey
Mexico
Mexico City
Bermuda
Bahamas
Cuba
Turks and Caicos Islands
Cayman Islands
Haiti
Jamaica
Port-au-Prince
Sint Maarten
Belize
Number of Requests
252 – 63,107
63,107 – 125,962
125,962 – 188,817
188,817 – 251,672
251,672 – 314,527
© OpenStreetMap contributors , Elastic Maps Service , Made with NaturalEarth

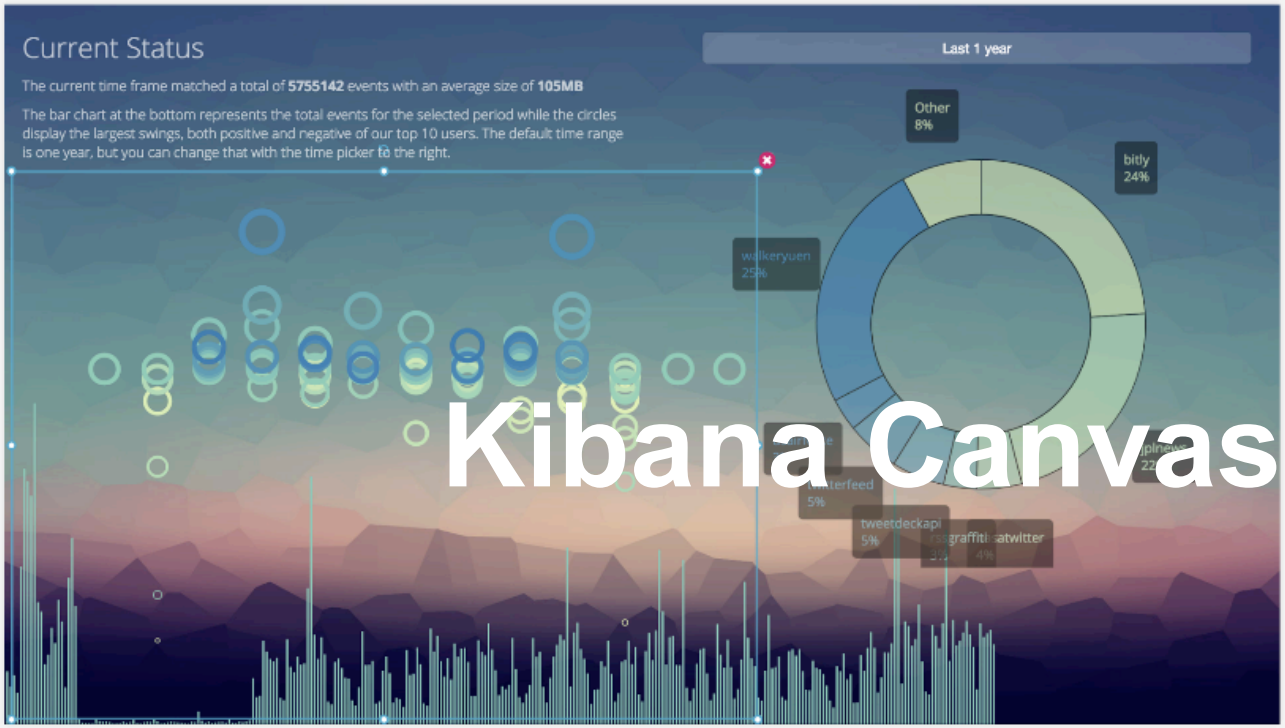


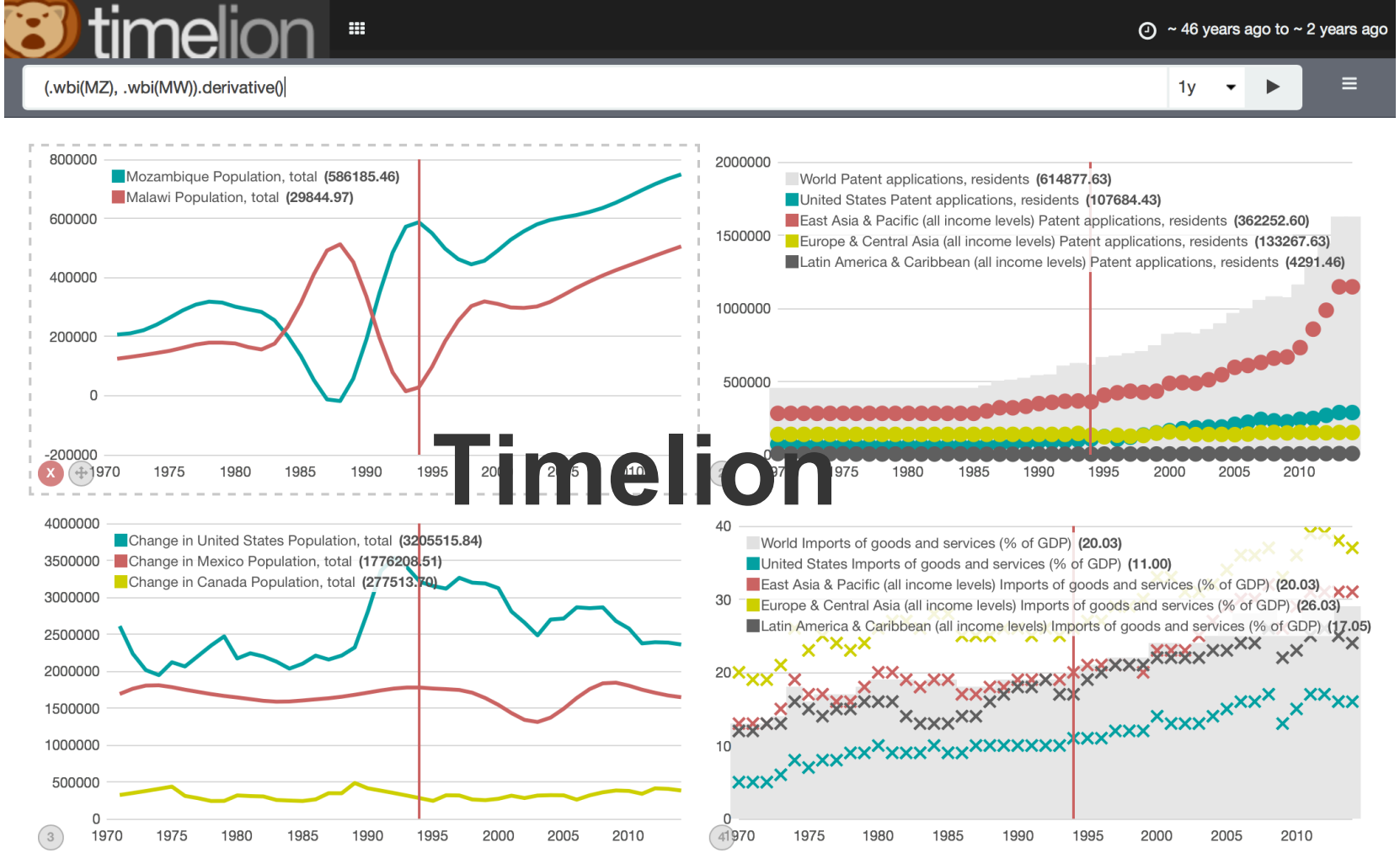
地理位置信息分析

elastic

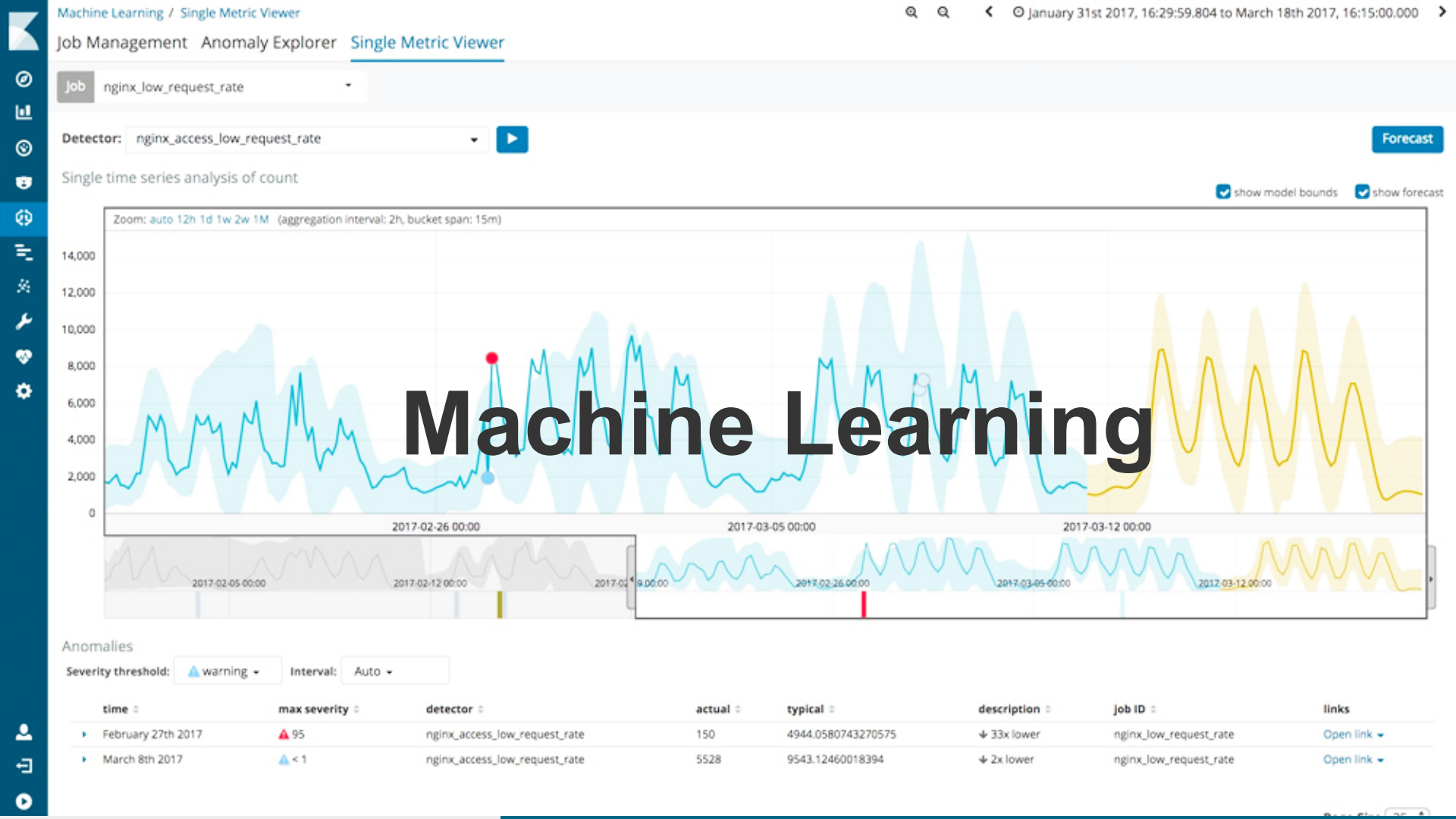

Kibana 的独门绝技

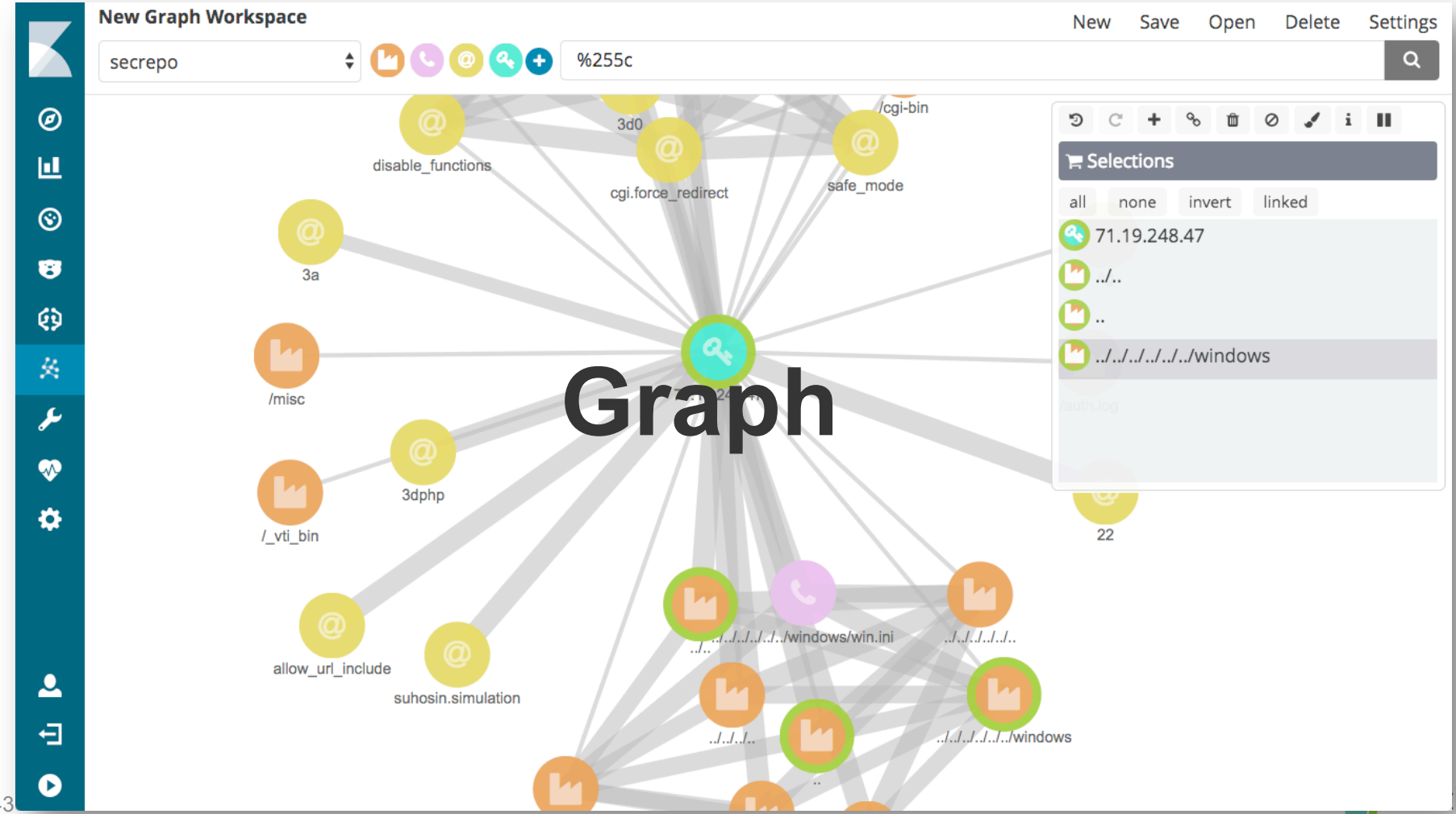

kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Layers
Add layer
The Masonic
elasticon2018
attendee
elastician
downloads/log
usa states: count of elasticon2018
0
1138
world countries: count of elasticon2018
0
1138
Satellite
World map
TOKELAU
TOKELAU
Kibana GIS


Users
Current Status
The current time frame matched a total of 5755142 events with an average size of 105MB
The bar chart at the bottom represents the total events for the selected period while the circles display the largest swings, both positive and negative of our top 10 users. The default time range is one year, but you can change that with the time picker to the right.
Last 1 year
Other 8%
bitly 24%
walkeryuen 25%
tweetdeckapi 5%
Kibana Canvas
Dimensions & Measures
X-axis value @timestamp
Y-axis value value
Color sum value
Size sum value
Chart Style
Color palette
Default style
Auto
Element Style
Custom CSS
.flot-tick-label {
color: #fff;
opacity: 0.5;
font-size: 1.5em;
font-family: Courier;
display: none;
}
Apply Stylesheet
Workpads
Pages
Elements
Assets
Datasource
Code



{Re}search astic


Machine Learning / Single Metric Viewer
January 31st 2017, 16:29:59.804 to March 18th 2017, 16:15:00.000
Job Management
Anomaly Explorer
Single Metric Viewer
Job
nginx_low_request_rate
Detector:
nginx_access_low_request_rate
Forecast
Single time series analysis of count
show model bounds
show forecast
Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 2h, bucket span: 15m)
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
2017-02-26 00:00
2017-03-05 00:00
2017-03-12 00:00
2017-02-05 00:00
2017-02-12 00:00
2017-02-26 00:00
2017-03-05 00:00
2017-03-12 00:00
Machine Learning
Anomalies
Severity threshold:
warning
Interval:
Auto
time
max severity
detector
actual
typical
description
job ID
links
February 27th 2017
95
nginx_access_low_request_rate
150
4944.0580743270575
33x lower
nginx_low_request_rate
Open link
March 8th 2017
< 1
nginx_access_low_request_rate
5528
9543.12460018394
2x lower
nginx_low_request_rate
Open link


New Graph Workspace
New
Save
Open
Delete
Settings
secrepo
%255c
Graph
Selections
all
none
invert
linked
71.19.248.47
../..
..
../../../../../../windows
disable_functions
3d0
cgi.force_redirect
safe_mode
/cgi-bin
3a
/misc
3dphp
/_vti_bin
allow_url_include
suhosin.simulation
22
../../../../../../windows/win.ini
../../../../../..
../../../../../../windows

继续学习

https://elastic.co

https://github.com/elastic

https://elasticsearch.cn

https://www.elastic.co/guide/cn/kibana/


elastic
elastic
elastic



THANK YOU

medcl@elastic.co
www.elastic.co