Visualize your threats

Philipp Krenn @xeraa

elastic

elastic

Infrastructure | Developer Advocate

Meetup

ViennaDB
Papers We Love Vienna

elastic

elasticsearch.

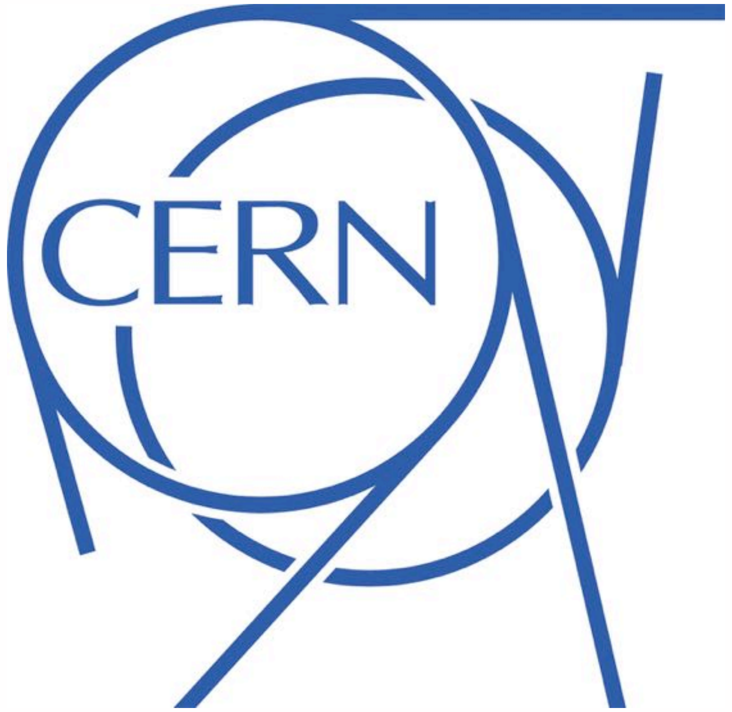
You Know, for Search

kibana

logstash

ELK Stack

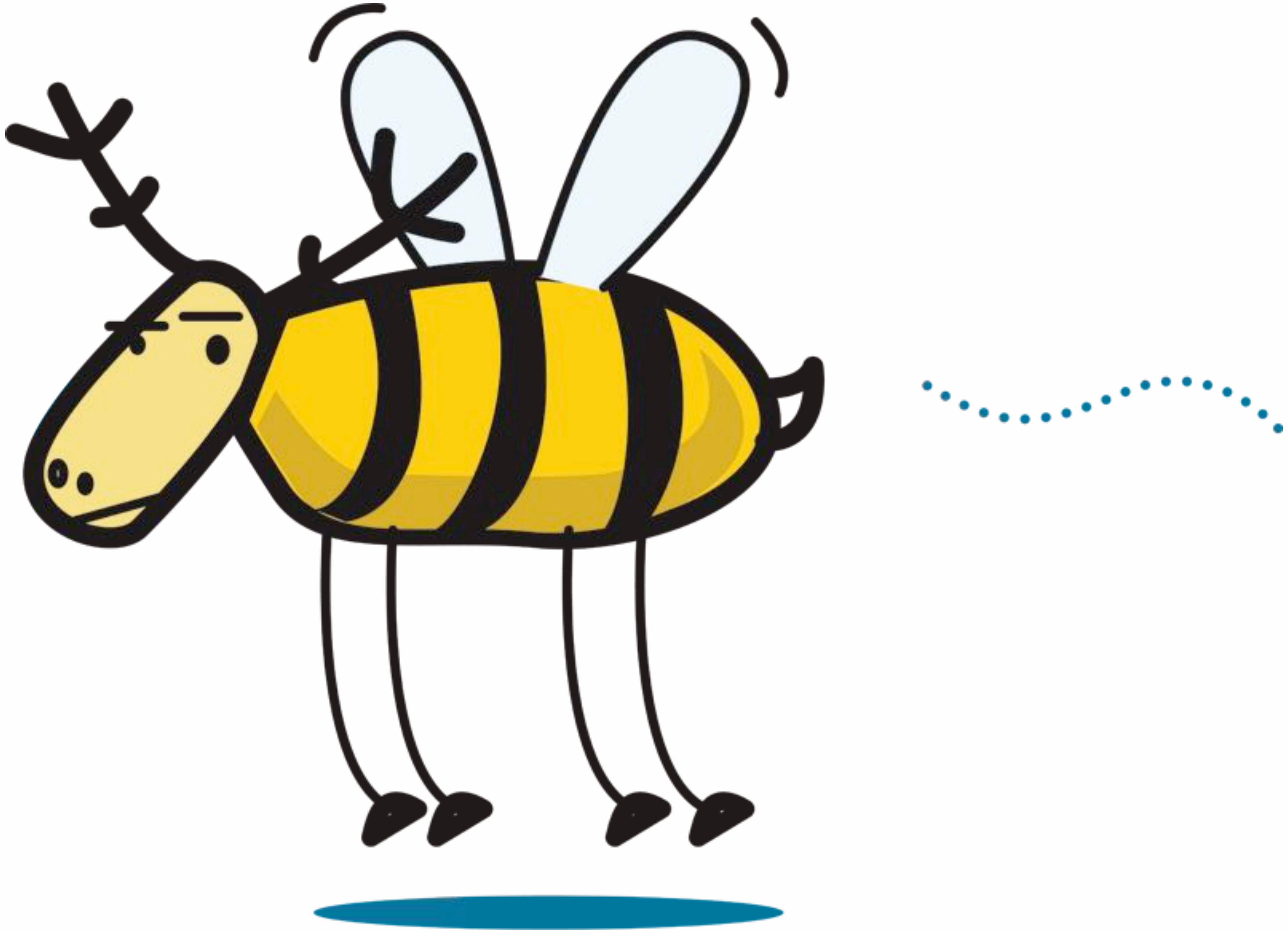
elastic


CERN

Goldman
Sachs

salesforce

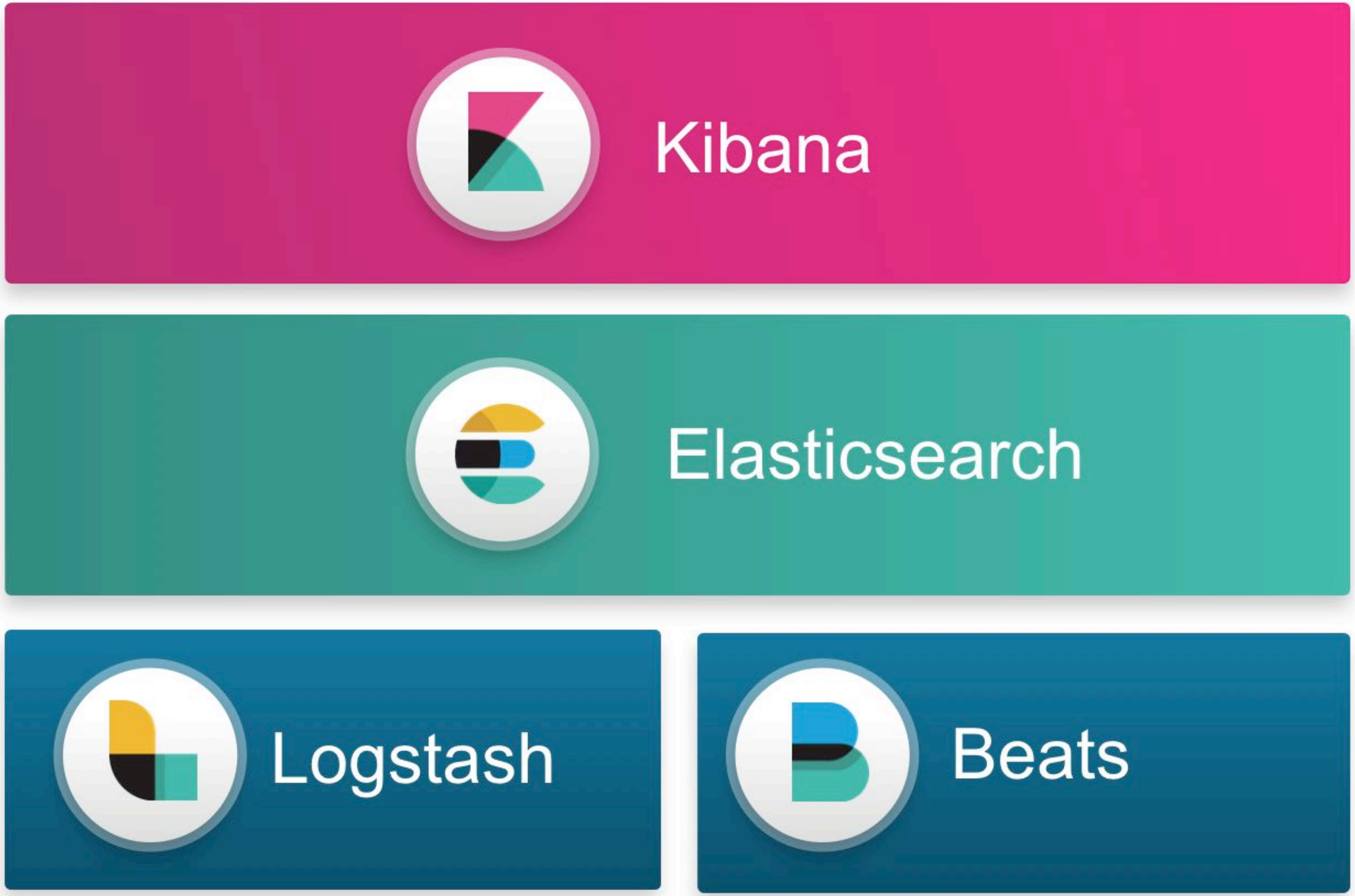
elastic



elastic

Elastic Stack

elastic



Kibana

Elasticsearch

Logstash

Beats

elastic

What about security?

Once upon a time...

Honeypot

elastic

Dataset

https://github.com/tcrug/marx_data

Condensed into one day

2016-01-12

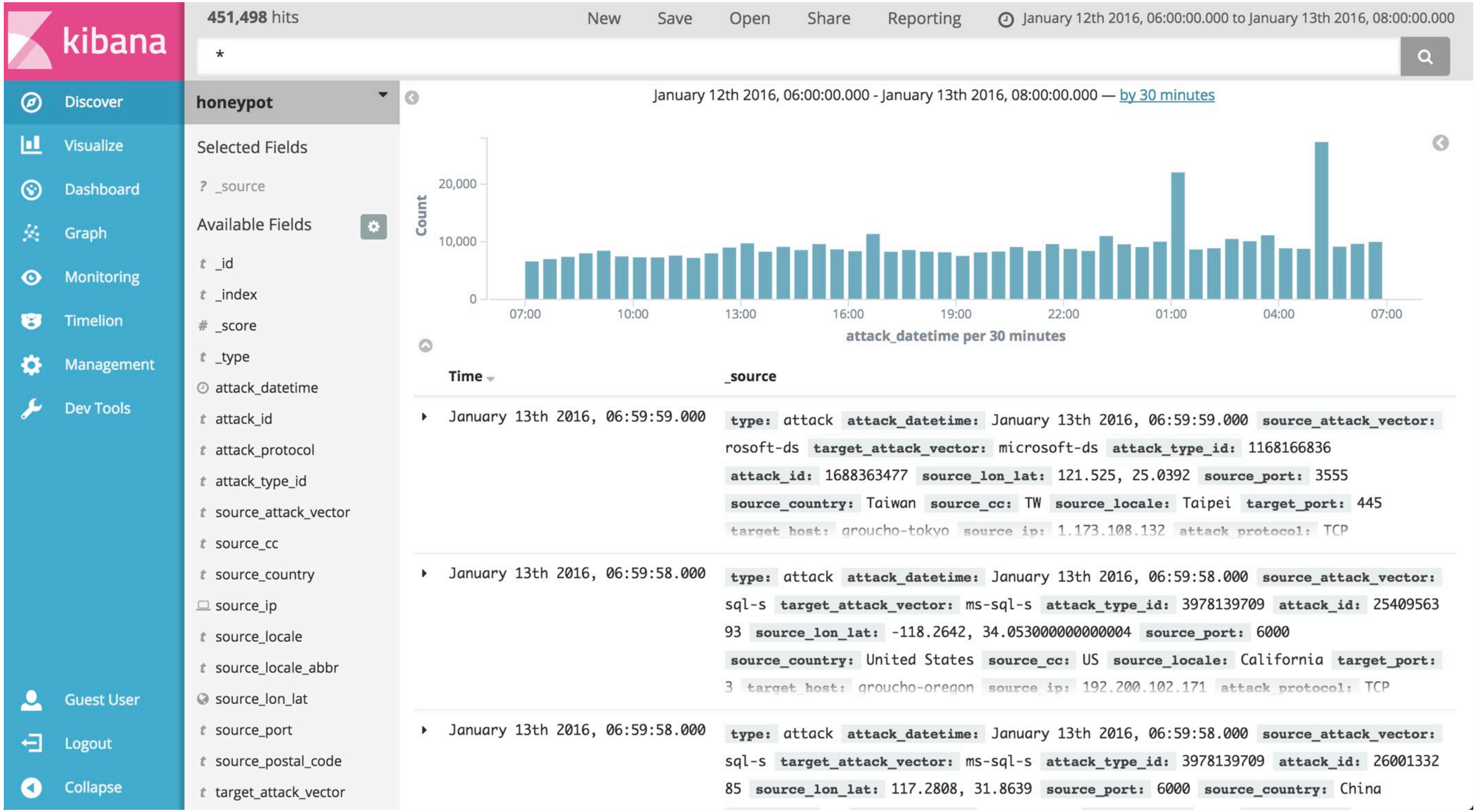
Enriched

Port numbers, unique attack types, individual attacks, GeoIP

Metrics

Generated

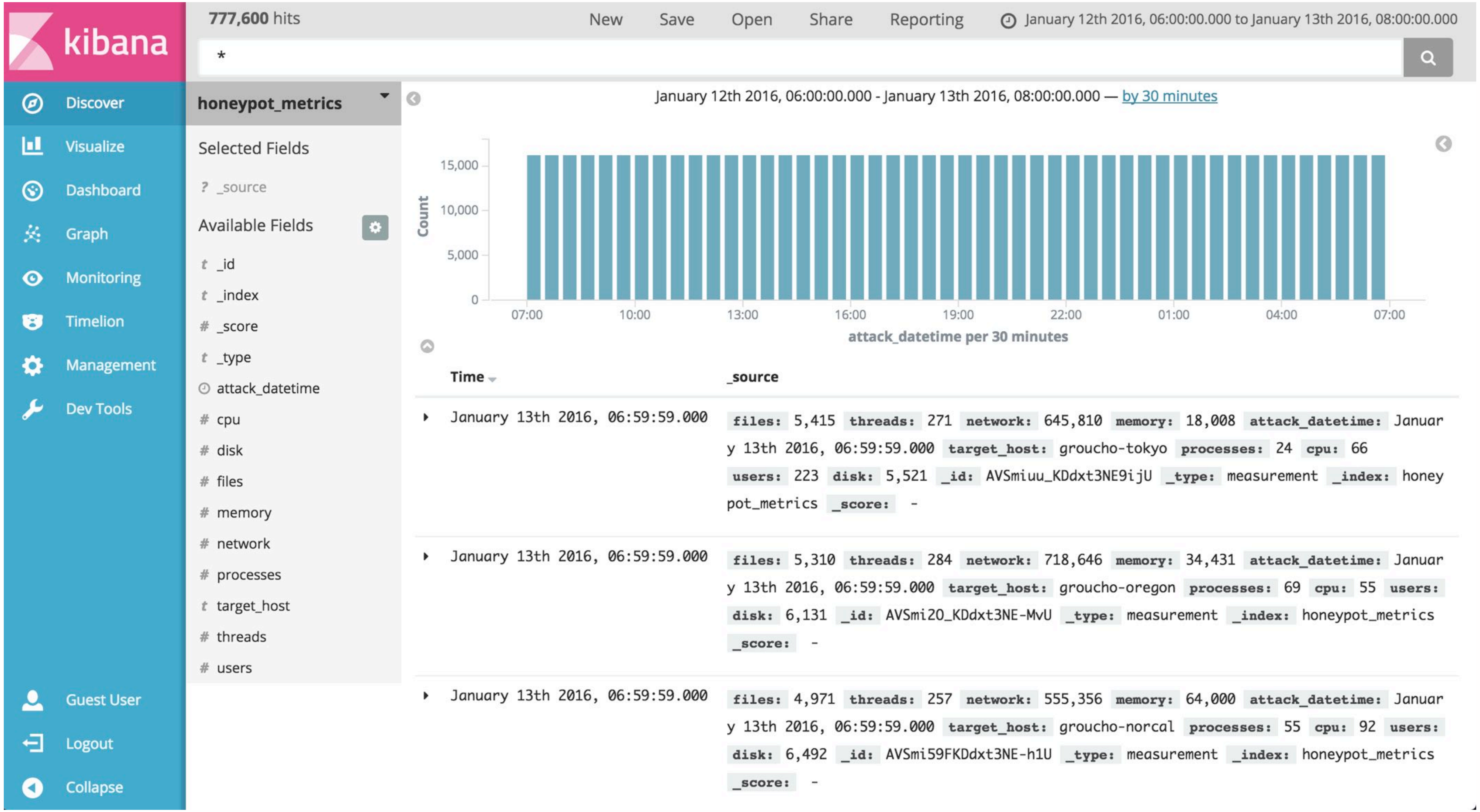
Discover



January 13th 2016, 06:59:59.000 type: attack attack_datetime: January 13th 2016, 06:59:59.000 source_attack_vector: rosoft-ds target_attack_vector: microsoft-ds attack_type_id: 1168166836 attack_id: 1688363477 source_lon_lat: 121.525, 25.0392 source_port: 3555 source_country: Taiwan source_cc: TW source_locale: Taipei target_port: 445 target_host: groucho-tokyo source_ip: 1.173.108.132 attack_protocol: TCP

January 13th 2016, 06:59:58.000 type: attack attack_datetime: January 13th 2016, 06:59:58.000 source_attack_vector: sql-s target_attack_vector: ms-sql-s attack_type_id: 3978139709 attack_id: 2540956393 source_lon_lat: -118.2642, 34.053000000000004 source_port: 6000 source_country: United States source_cc: US source_locale: California target_port: 3 target_host: groucho-oregon source_ip: 192.200.102.171 attack_protocol: TCP

January 13th 2016, 06:59:58.000 type: attack attack_datetime: January 13th 2016, 06:59:58.000 source_attack_vector: sql-s target_attack_vector: ms-sql-s attack_type_id: 3978139709 attack_id: 2600133285 source_lon_lat: 117.2808, 31.8639 source_port: 6000 source_country: China



777,600 hits

January 12th 2016, 06:00:00.000 to January 13th 2016, 08:00:00.000

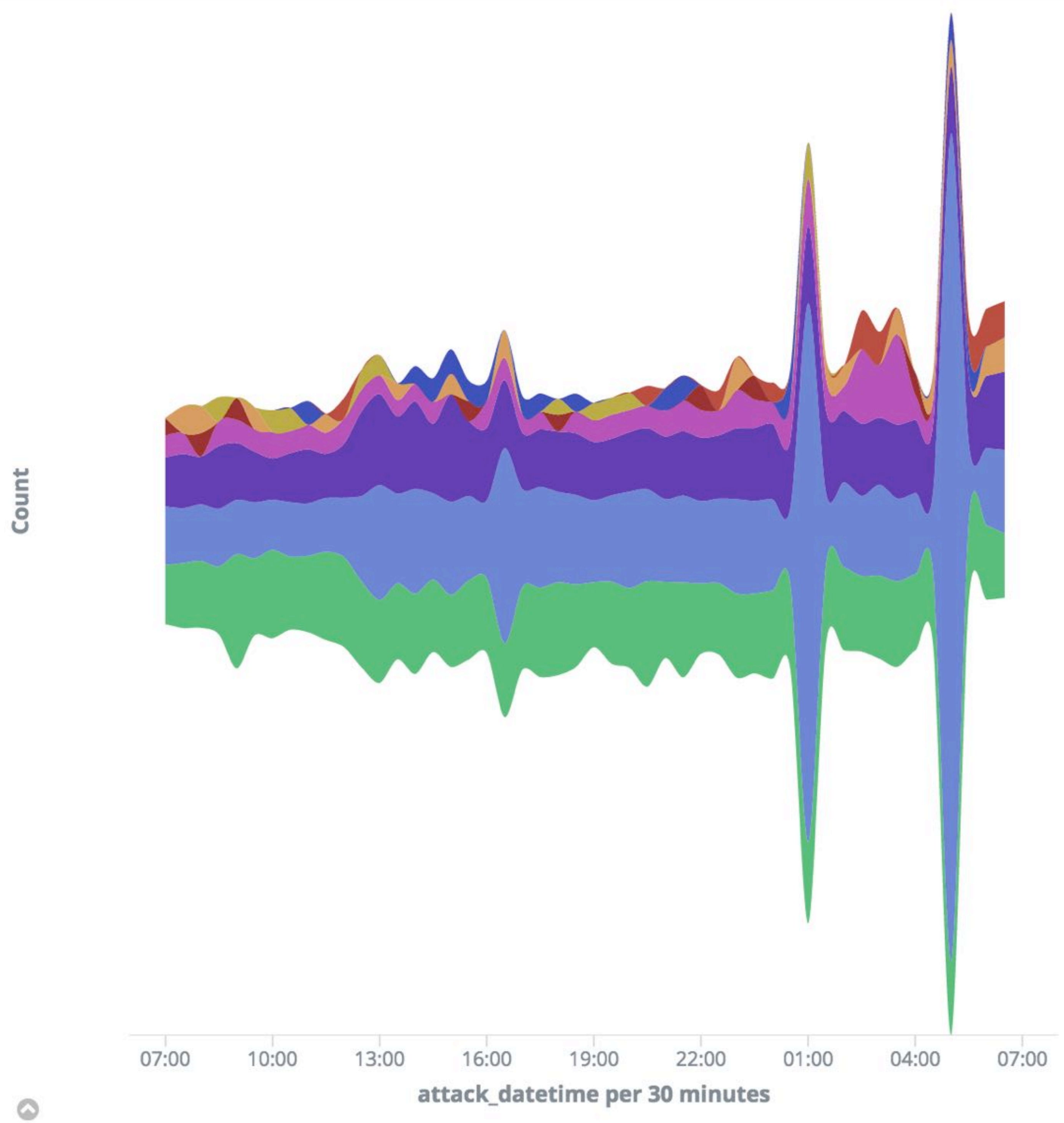
*

January 12th 2016, 06:00:00.000 - January 13th 2016, 08:00:00.000 — by 30 minutes

Time	_source
January 13th 2016, 06:59:59.000	**files:** 5,415 **threads:** 271 **network:** 645,810 **memory:** 18,008 **attack_datetime:** January 13th 2016, 06:59:59.000 **target_host:** groucho-tokyo **processes:** 24 **cpu:** 66 **users:** 223 **disk:** 5,521 **_id:** AVSmiuu_KDdxt3NE9ijU **_type:** measurement **_index:** honeypot_metrics **_score:** -
January 13th 2016, 06:59:59.000	**files:** 5,310 **threads:** 284 **network:** 718,646 **memory:** 34,431 **attack_datetime:** January 13th 2016, 06:59:59.000 **target_host:** groucho-oregon **processes:** 69 **cpu:** 55 **users:** **disk:** 6,131 **_id:** AVSmi2O_KDdxt3NE-MvU **_type:** measurement **_index:** honeypot_metrics **_score:** -
January 13th 2016, 06:59:59.000	**files:** 4,971 **threads:** 257 **network:** 555,356 **memory:** 64,000 **attack_datetime:** January 13th 2016, 06:59:59.000 **target_host:** groucho-norcal **processes:** 55 **cpu:** 92 **users:** **disk:** 6,492 **_id:** AVSmi59FKDdxt3NE-h1U **_type:** measurement **_index:** honeypot_metrics **_score:** -

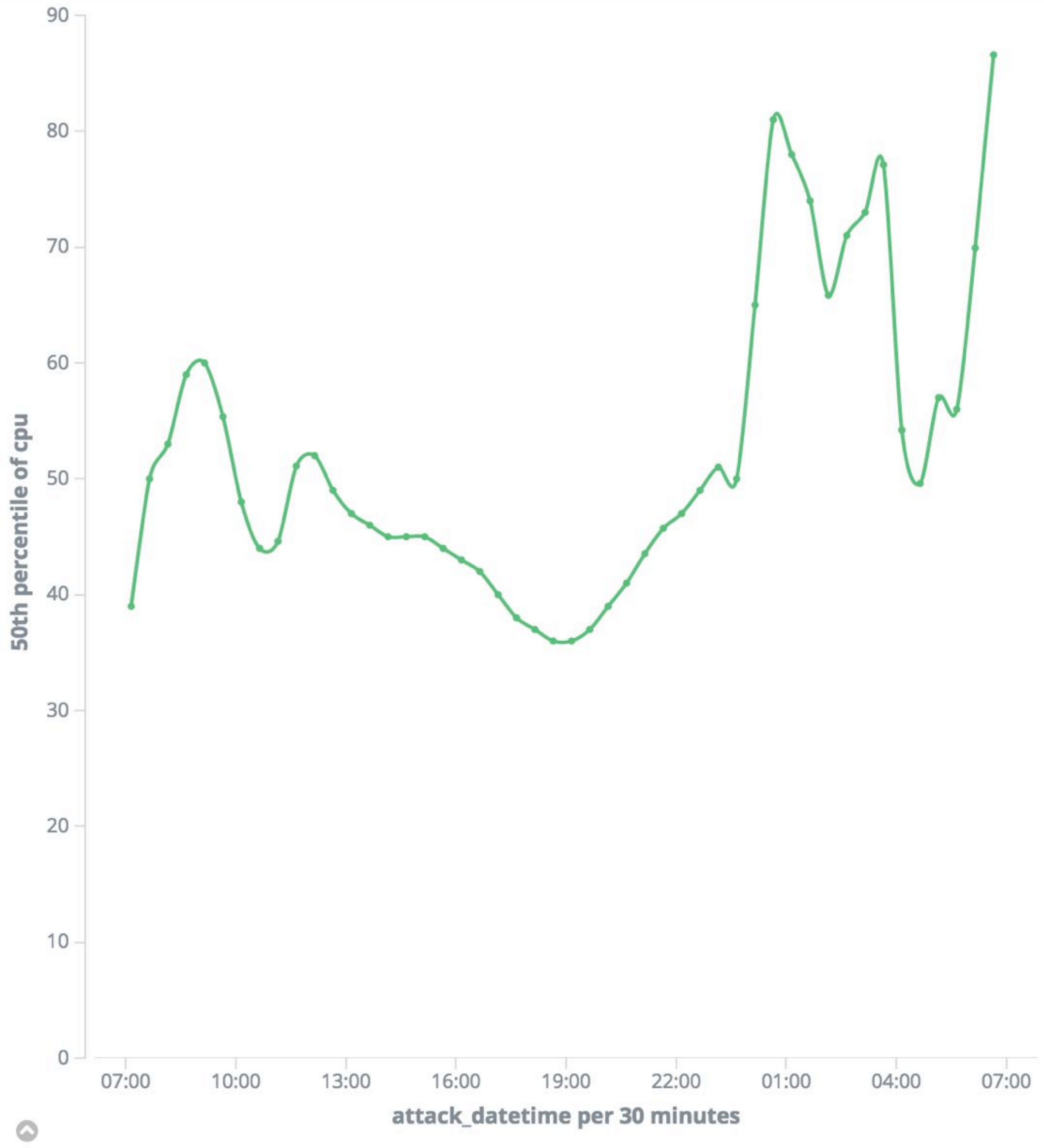
Visualize

Attacks by host and time

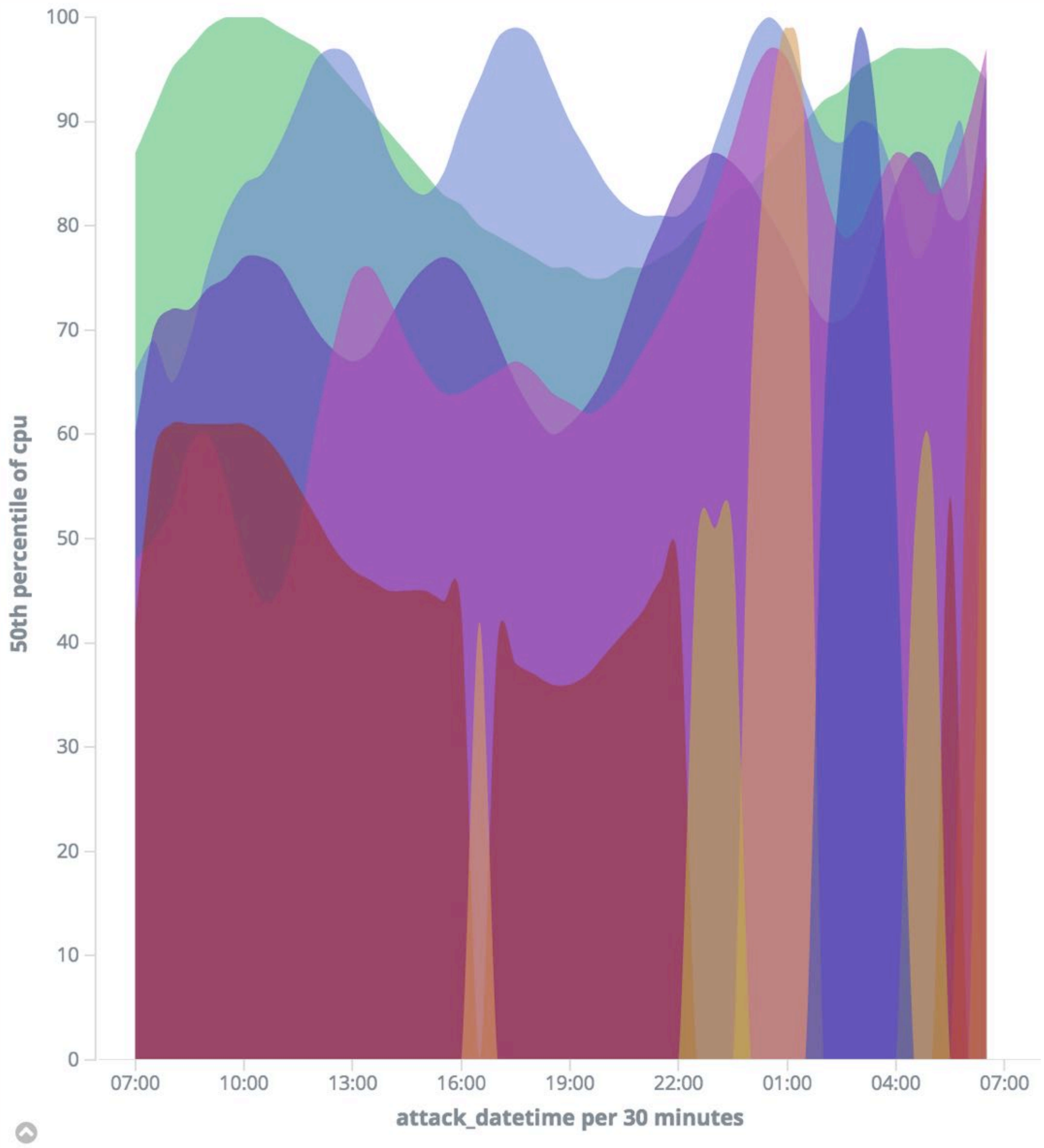

Count
07:00
10:00
13:00
16:00
19:00
22:00
01:00
04:00
07:00
attack_datetime per 30 minutes

elastic

CPU over time


90
80
70
60
50
40
30
20
10
0
50th percentile of cpu
07:00
10:00
13:00
16:00
19:00
22:00
01:00
04:00
07:00
attack_datetime per 30 minutes

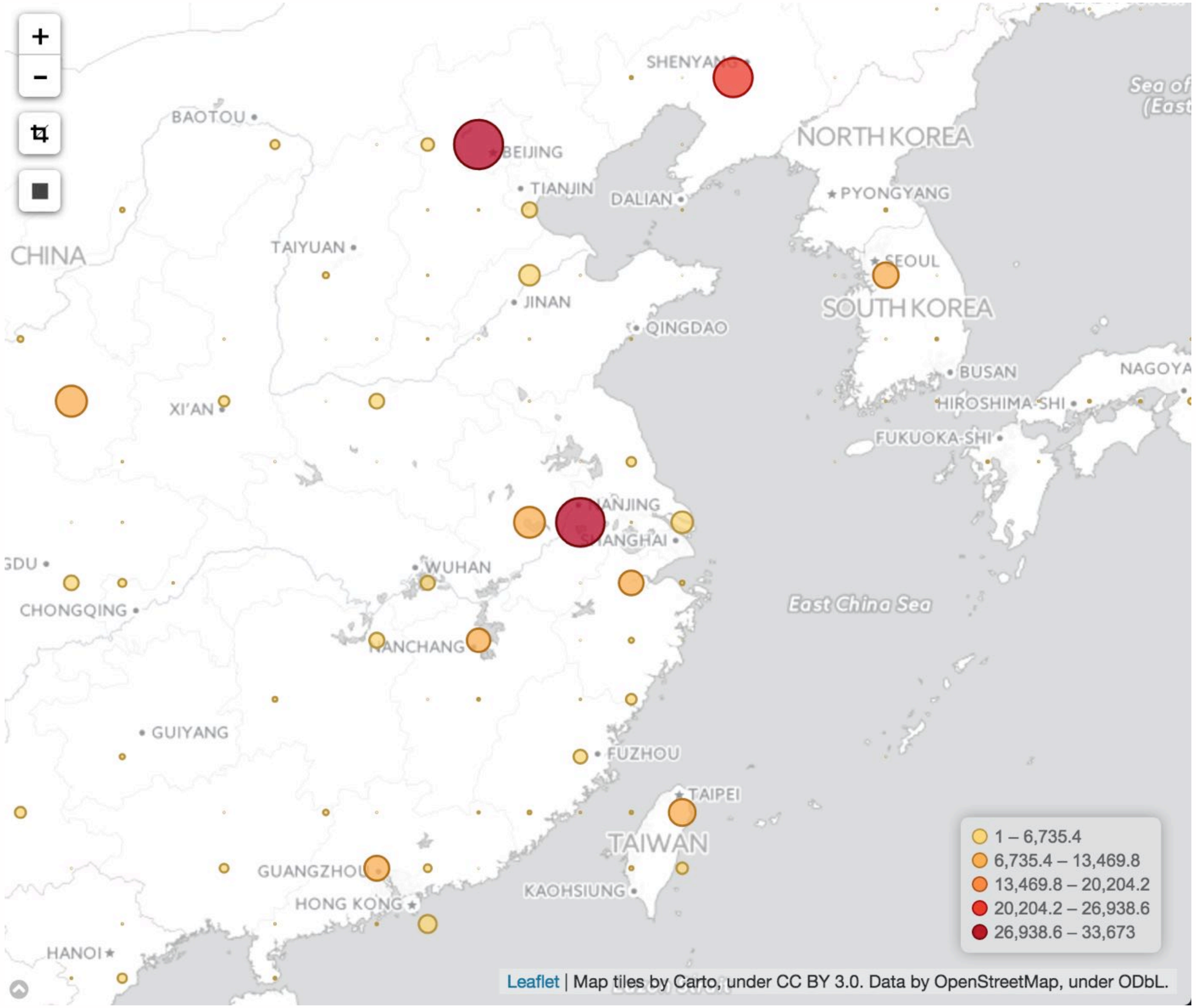
CPU over time by host



100
90
80
70
60
50
40
30
20
10
0
50th percentile of cpu
07:00
10:00
13:00
16:00
19:00
22:00
01:00
04:00
07:00
attack_datetime per 30 minutes

elastic

Geolocation of attacks

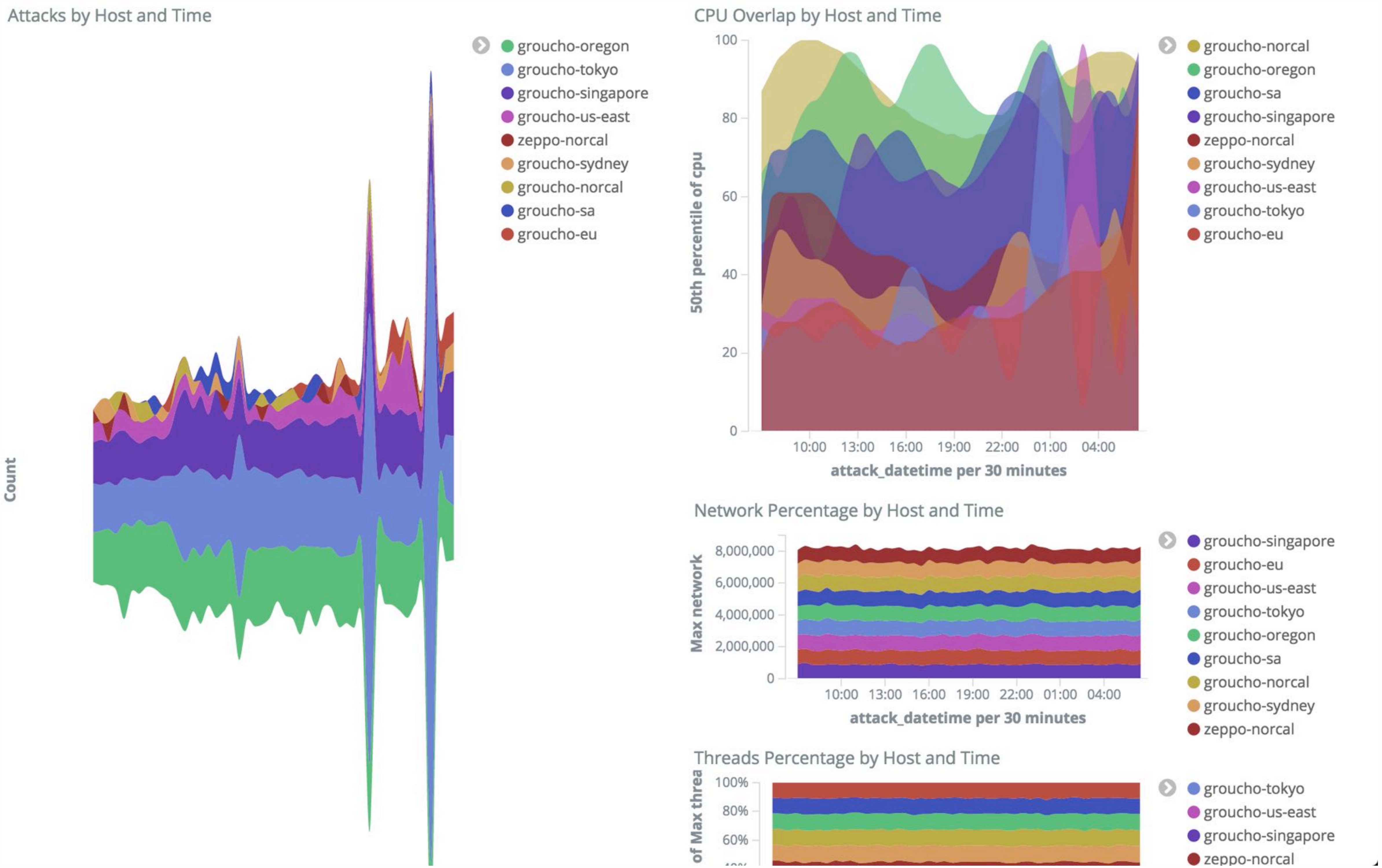


Leaflet | Map tiles by Carto, under CC BY 3.0. Data by OpenStreetMap, under ODbL.

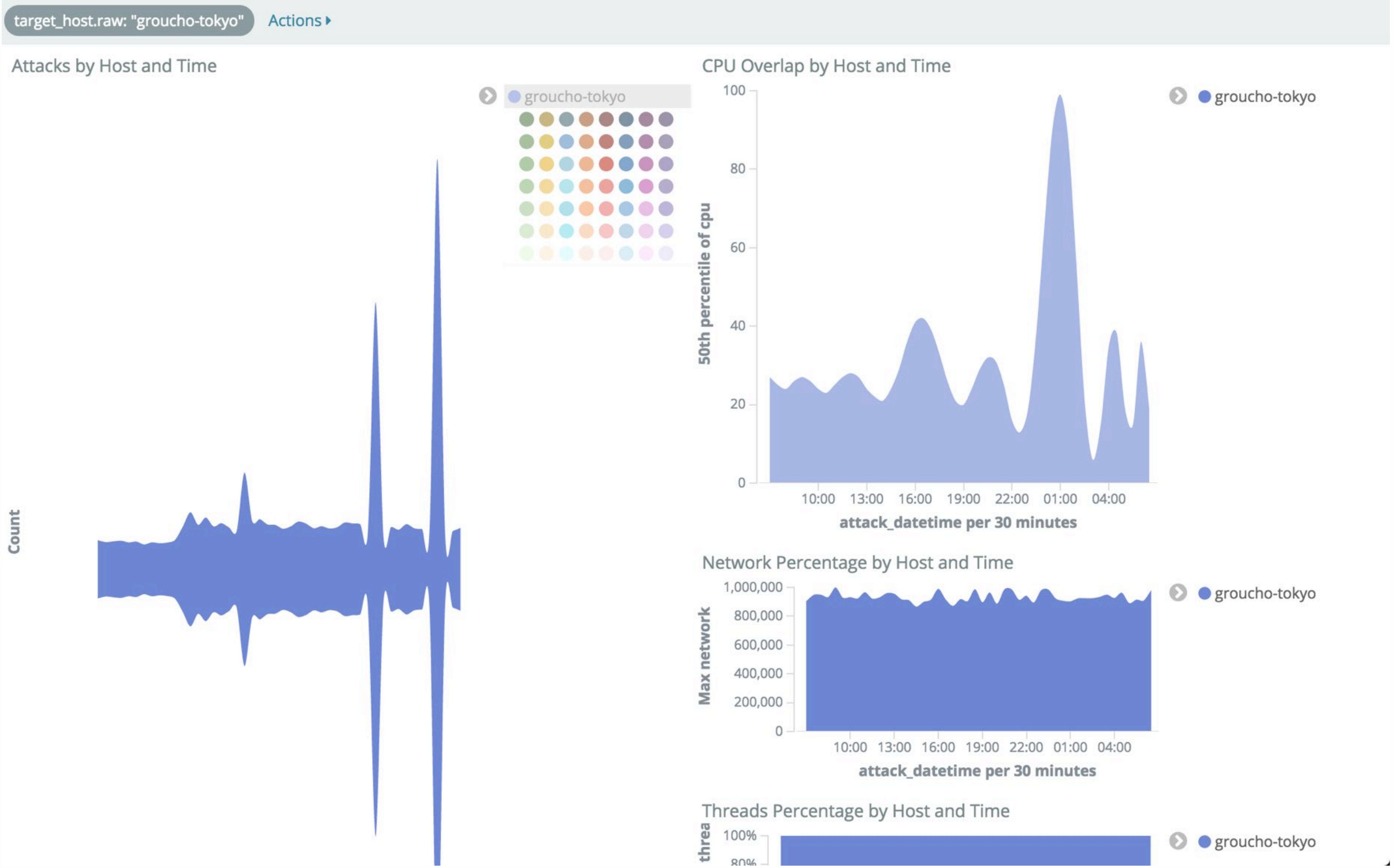
Dashboard

elastic

Putting it together


Attacks by Host and Time
Count
groucho-oregon
groucho-tokyo
groucho-singapore
groucho-us-east
zeppo-norcal
groucho-sydney
groucho-norcal
groucho-sa
groucho-eu
CPU Overlap by Host and Time
50th percentile of cpu
100
80
60
40
20
0
10:00
13:00
16:00
19:00
22:00
01:00
04:00
attack_datetime per 30 minutes
groucho-norcal
groucho-oregon
groucho-sa
groucho-singapore
zeppo-norcal
groucho-sydney
groucho-us-east
groucho-tokyo
groucho-eu
Network Percentage by Host and Time
Max network
8,000,000
6,000,000
4,000,000
2,000,000
0
10:00
13:00
16:00
19:00
22:00
01:00
04:00
attack_datetime per 30 minutes
groucho-singapore
groucho-eu
groucho-us-east
groucho-tokyo
groucho-oregon
groucho-sa
groucho-norcal
groucho-sydney
zeppo-norcal
Threads Percentage by Host and Time
of Max threa
100%
80%
60%
groucho-tokyo
groucho-us-east
groucho-singapore
zeppo-norcal

elastic



target_host.raw: "groucho-tokyo"

Attacks by Host and Time

CPU Overlap by Host and Time

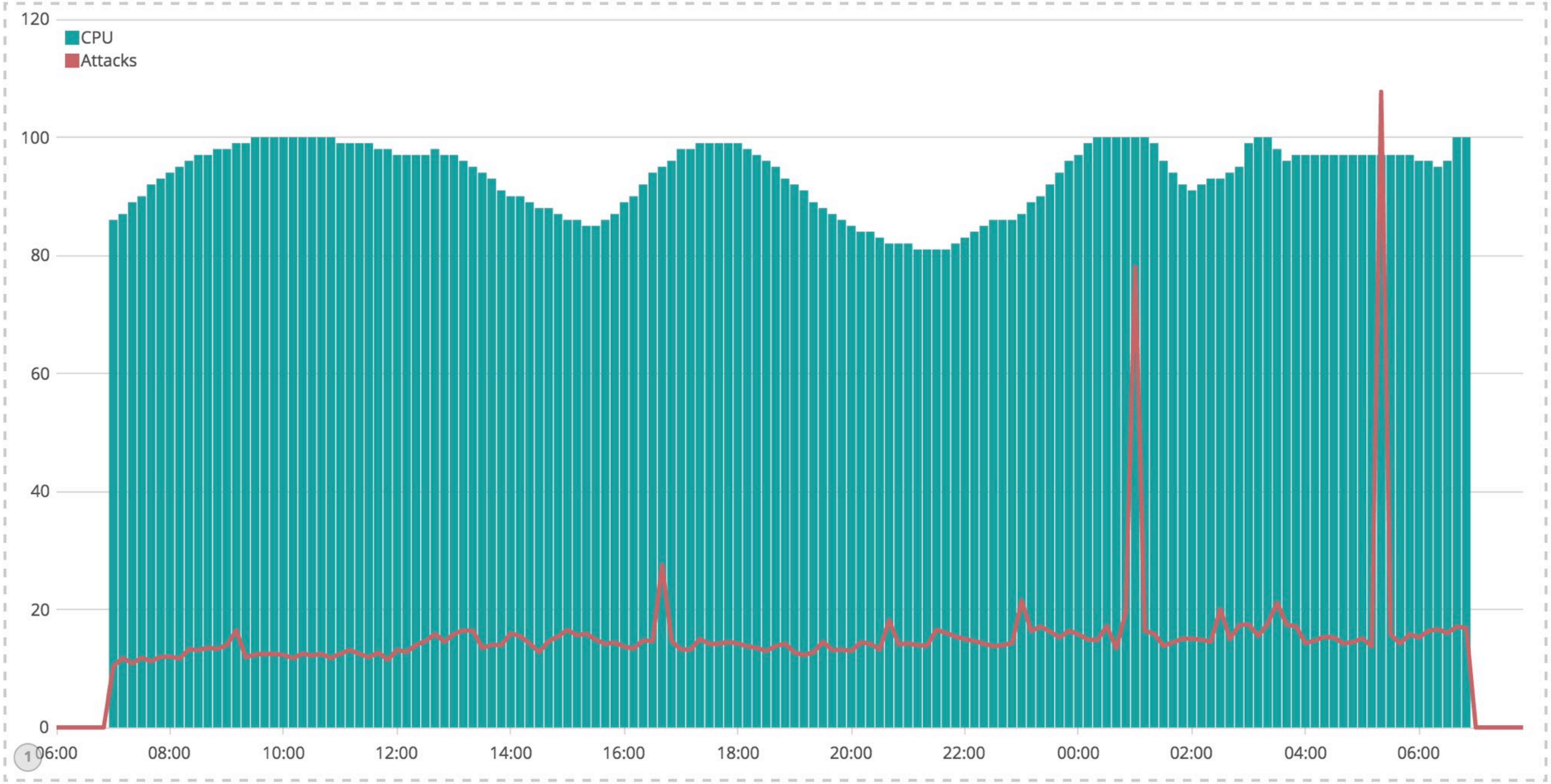
Network Percentage by Host and Time

Threads Percentage by Host and Time

Timelion

elastic

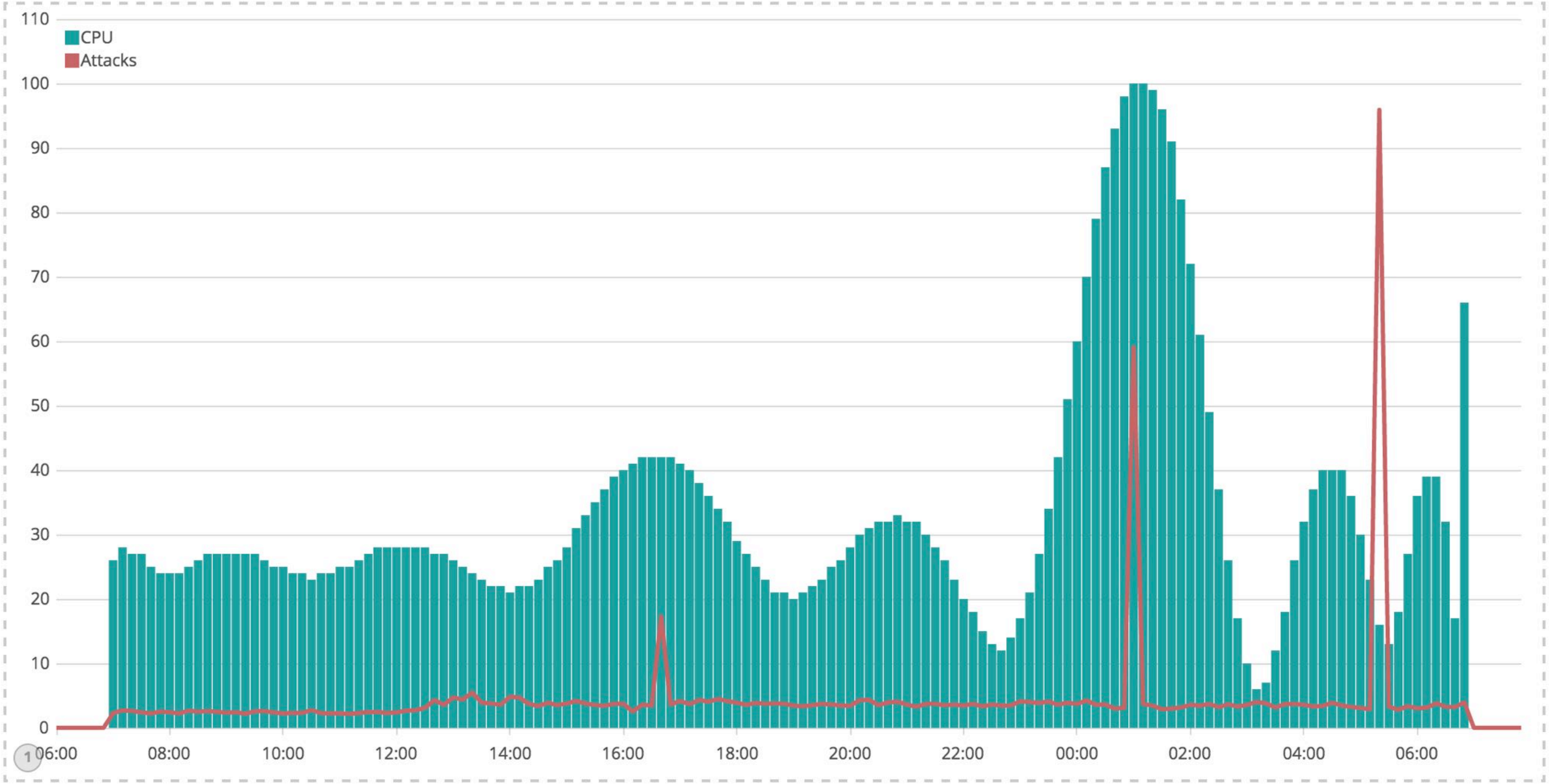
Compare honey data and metrics



120
100
80
60
40
20
0
🟩 CPU
🟥 Attacks
1
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00

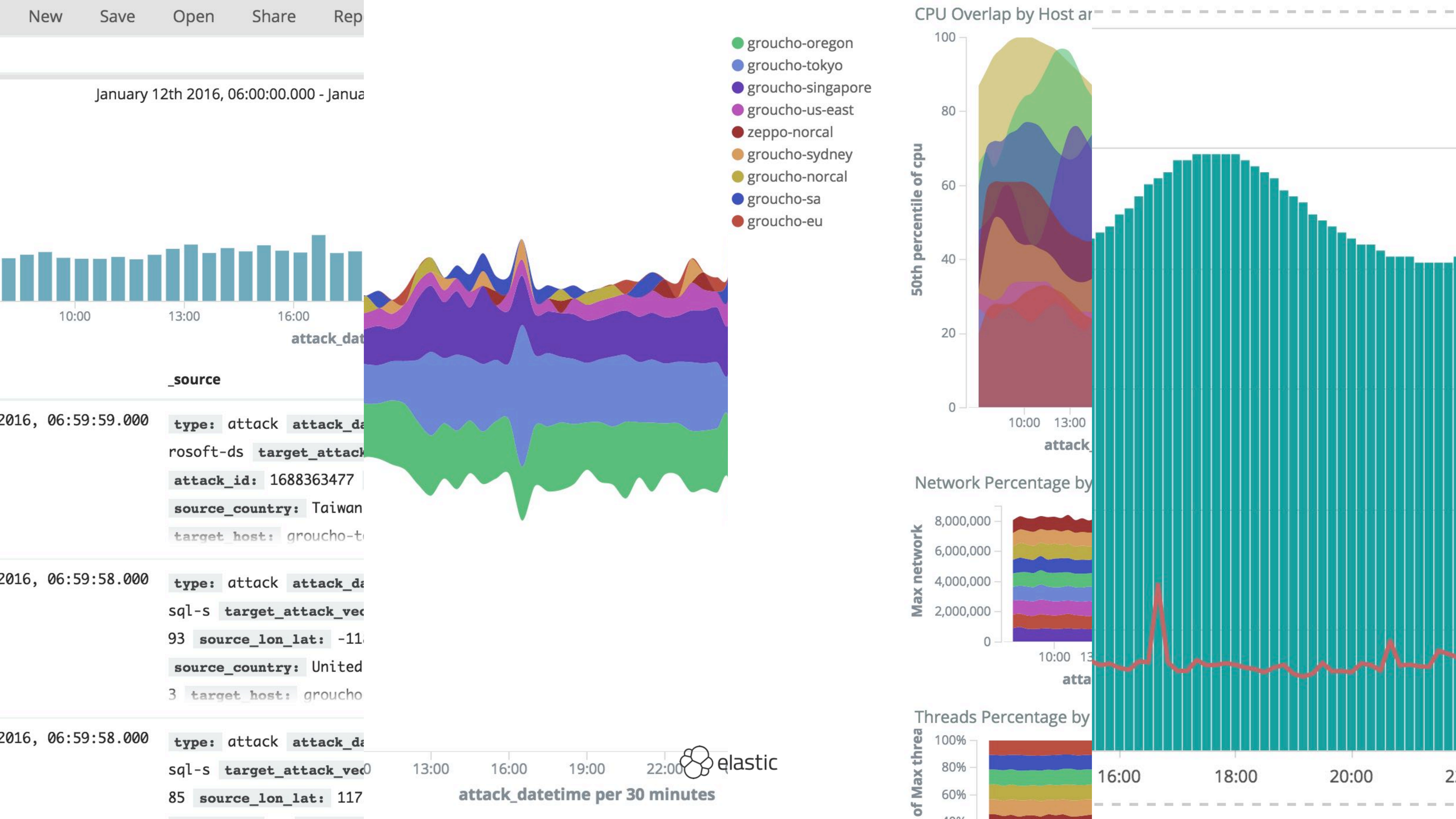
elastic

Compare honey data and metrics for Tokyo


110
100
90
80
70
60
50
40
30
20
10
0
🟩CPU
🟥Attacks
1
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00

Conclusion

Visualize all the things

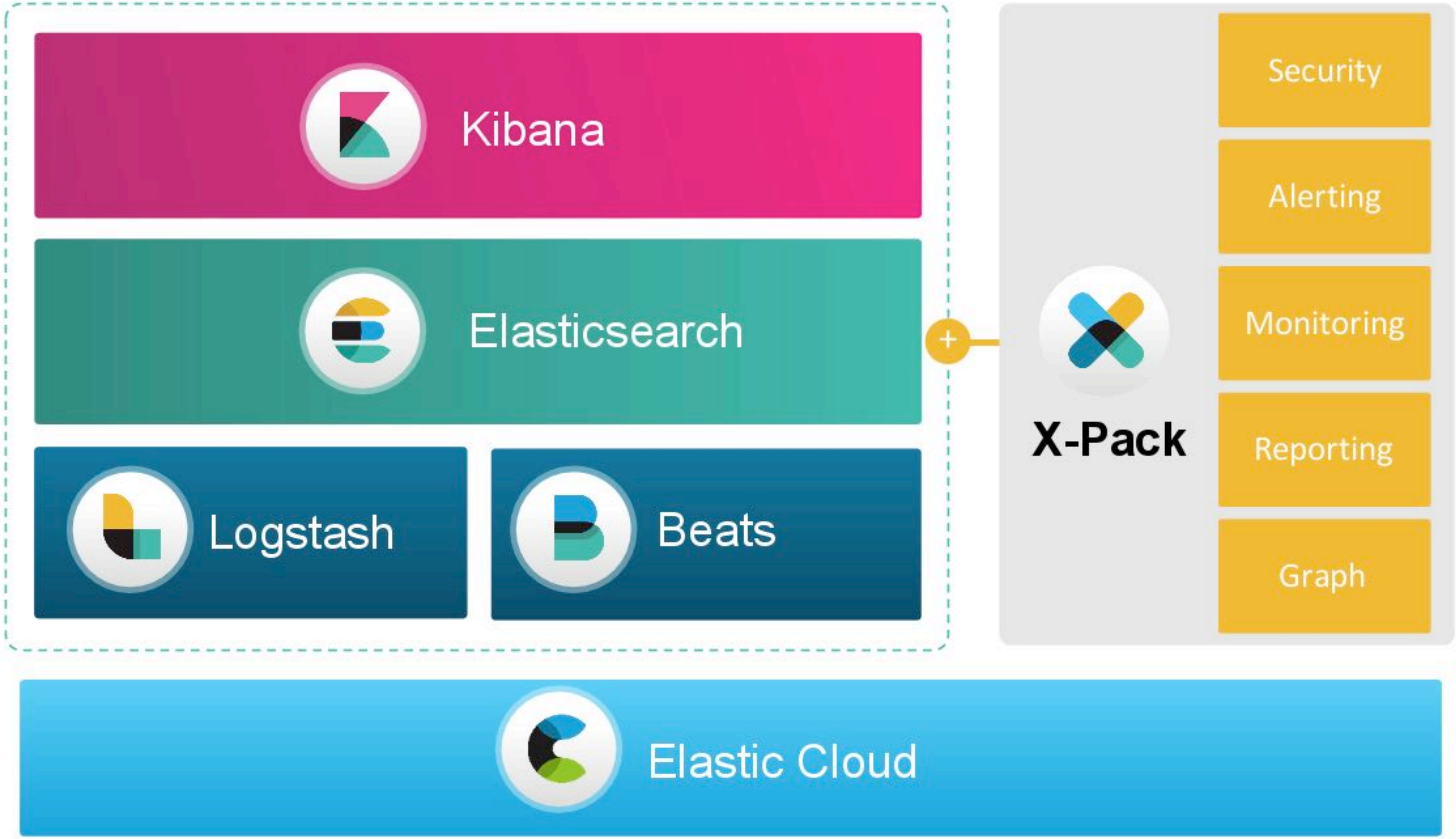


2016, 06:59:59.000 **type:** attack **attack_da**
rosoft-ds **target_attack**
attack_id: 1688363477
source_country: Taiwan
target_host: groucho-t

2016, 06:59:58.000 **type:** attack **attack_da**
sql-s **target_attack_vec**
93 **source_lon_lat:** -11
source_country: United
3 **target_host:** groucho

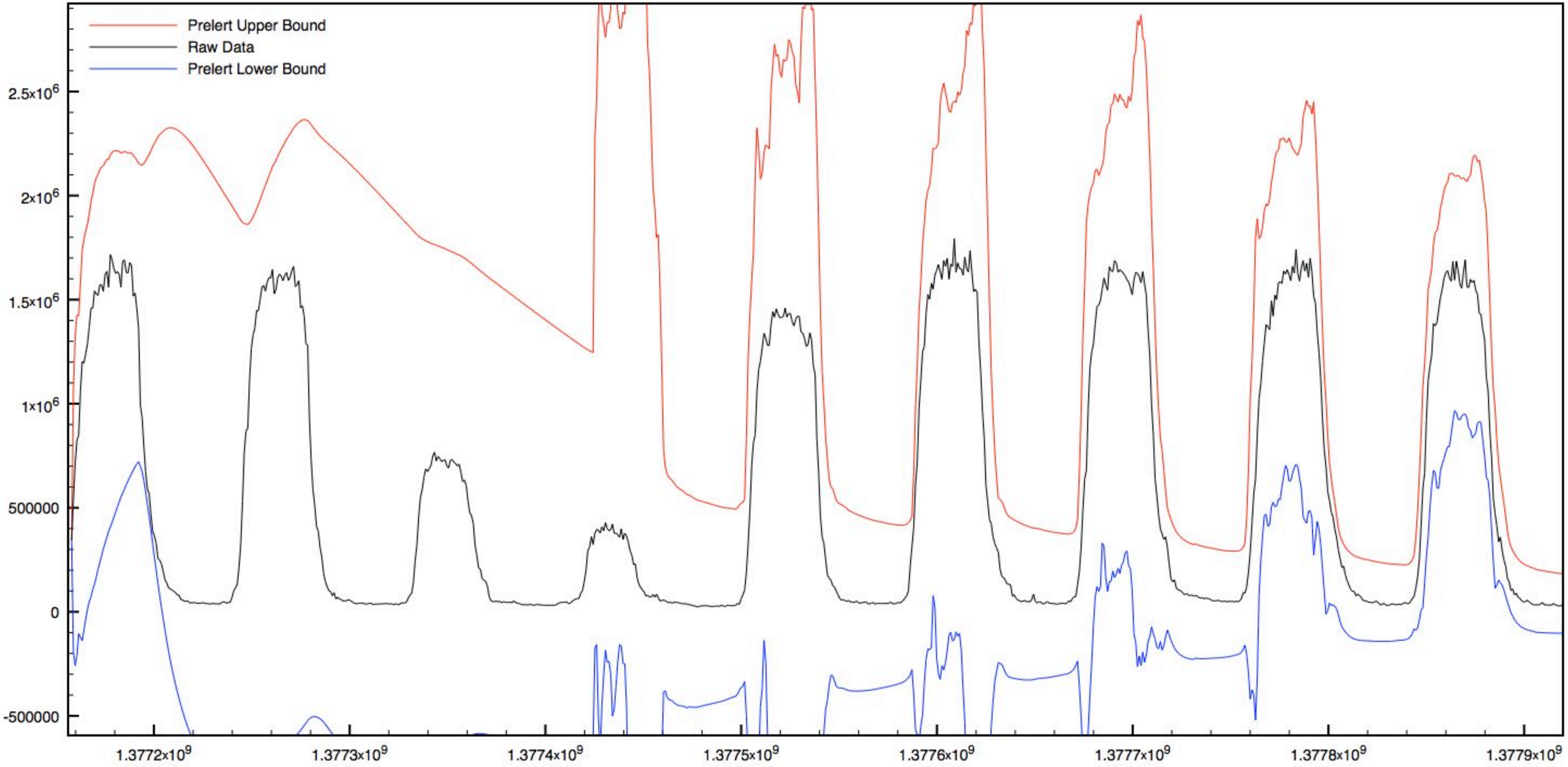
2016, 06:59:58.000 **type:** attack **attack_da**
sql-s **target_attack_vec**
85 **source_lon_lat:** 117

But wait, there is more


Kibana
Elasticsearch
Logstash
Beats
X-Pack
Security
Alerting
Monitoring
Reporting
Graph
Elastic Cloud

elastic

Prelert is coming


Prelert Upper Bound
Raw Data
Prelert Lower Bound
2.5x10^6
2x10^6
1.5x10^6
1x10^6
500000
0
-500000
1.3772x10^9
1.3773x10^9
1.3774x10^9
1.3775x10^9
1.3776x10^9
1.3777x10^9
1.3778x10^9
1.3779x10^9

elastic

Try it

https://github.com/xeraa/vagrant-elastic-stack

QUESTIONS?

Philipp Krenn @xeraa

PS: Sticker