

- find 5 most frequent source IPs:

Top values

66.249.73.135	4.9%	<input type="button" value="+"/>	<input type="button" value="-"/>
46.105.14.53	3.7%	<input type="button" value="+"/>	<input type="button" value="-"/>
130.237.218.86	2.1%	<input type="button" value="+"/>	<input type="button" value="-"/>
75.97.9.59	1.3%	<input type="button" value="+"/>	<input type="button" value="-"/>
50.16.19.13	1.1%	<input type="button" value="+"/>	<input type="button" value="-"/>

66[.]249[.]73[.]135

46[.]105[.]14[.]53

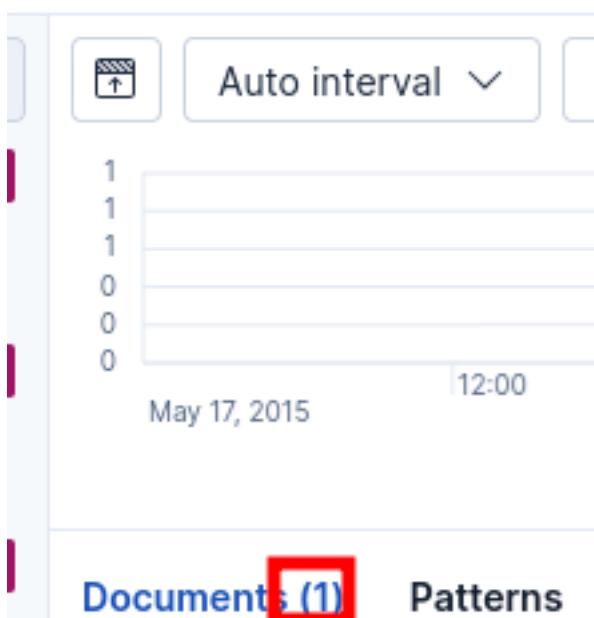
130[.]237[.]218[.]86

75[.]97[.]9[.]59

50[.]16[.]19[.]13

- how many connections are from 5[.]9[.]143[.]150?

Q source.ip: "5.9.143.150"



1

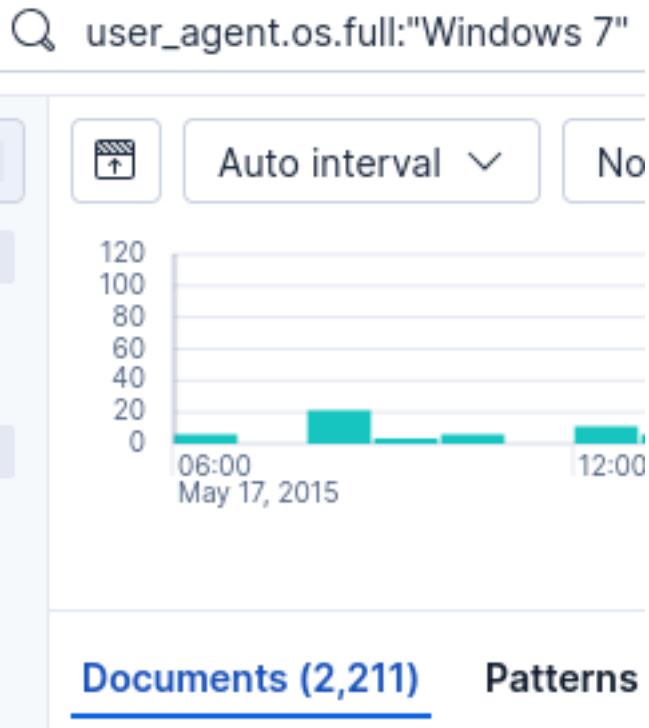
- what is the HTTP request method from

130[.]88[.]99[.]231?

@timestamp ⓘ http.request.method source.ip
May 19, 2015 @ 13:05:09.000 GET 130.88.99.231

GET

- how many connections from Windows 7 user agents?



2211

- how many HTTP request methods that are either HEAD or POST?

Q http.request.method:"HEAD" OR http.request.method:"POST"

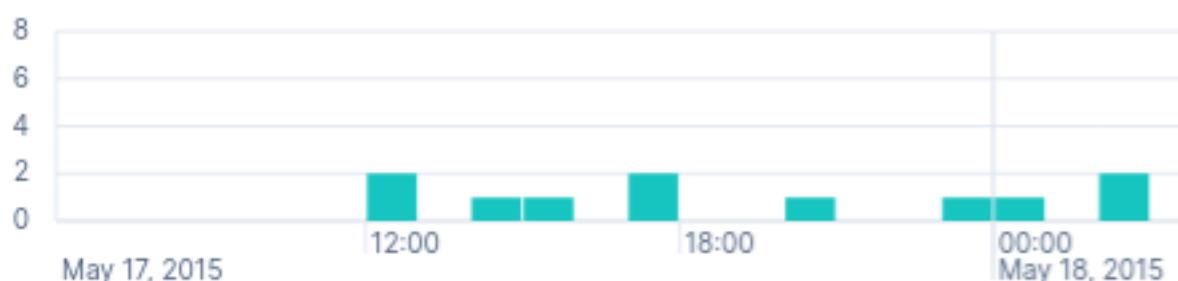
0



Auto interval ▾

No breakdown ▾

8



Documents (47)

Patterns

Field statistics

47

- how many documents with request method POST and response status code not 200?

↳ http.request.method:"POST" AND NOT http.response.status_code:"200"



Auto interval ▾

No breakdown ▾

1

1

1

0

0

0

May 17, 2015

12:00

18:00

00:00

May 18, 2015

Documents (3)

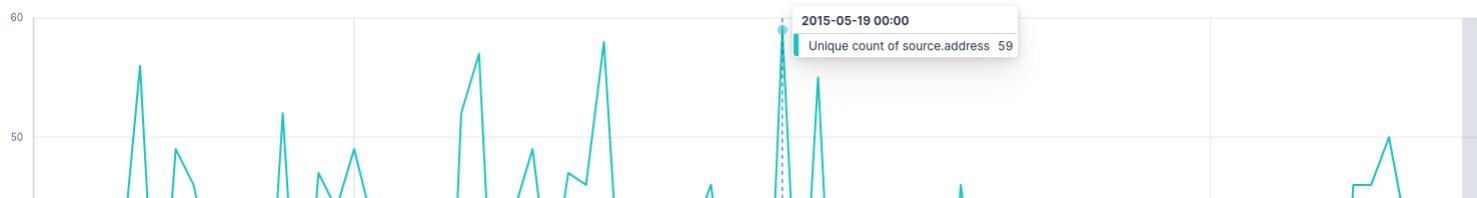
Patterns

Field statistics

3

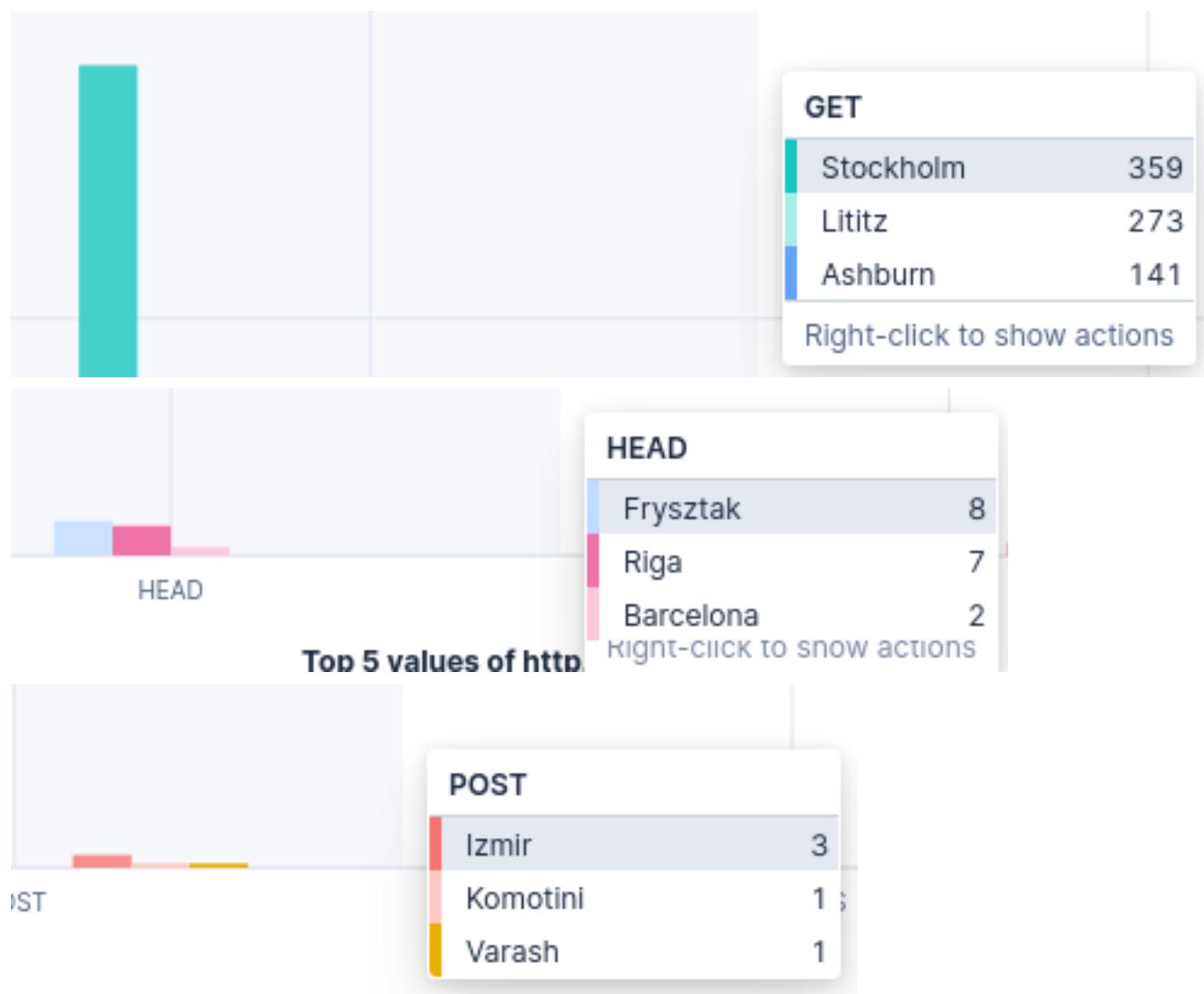
ADVANCED:

- between May 17, 2015 06:05 and May 20, 2015 14:05:59, using @timestamp per hour, what hour has the highest unique count of source.address with how many?



2015-05-19 00:00 with 59 unique source addresses

- which cities sent the most requests for GET, HEAD, and POST methods?



 Bar

Unstacked



filebeat-*



Horizontal axis

Optional

Top 5 values of http.request.method

Vertical axis

Count of http.request.method

+ Add or drag-and-drop a field

Breakdown

Optional

  Top 3 values of source.geo.city_name

Stockholm, Frysztak, Izmir