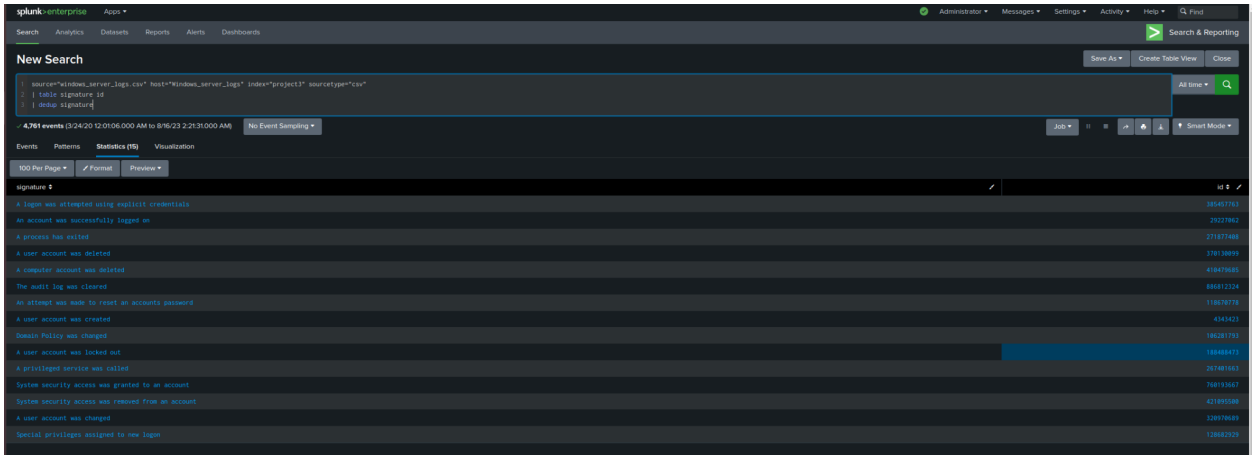
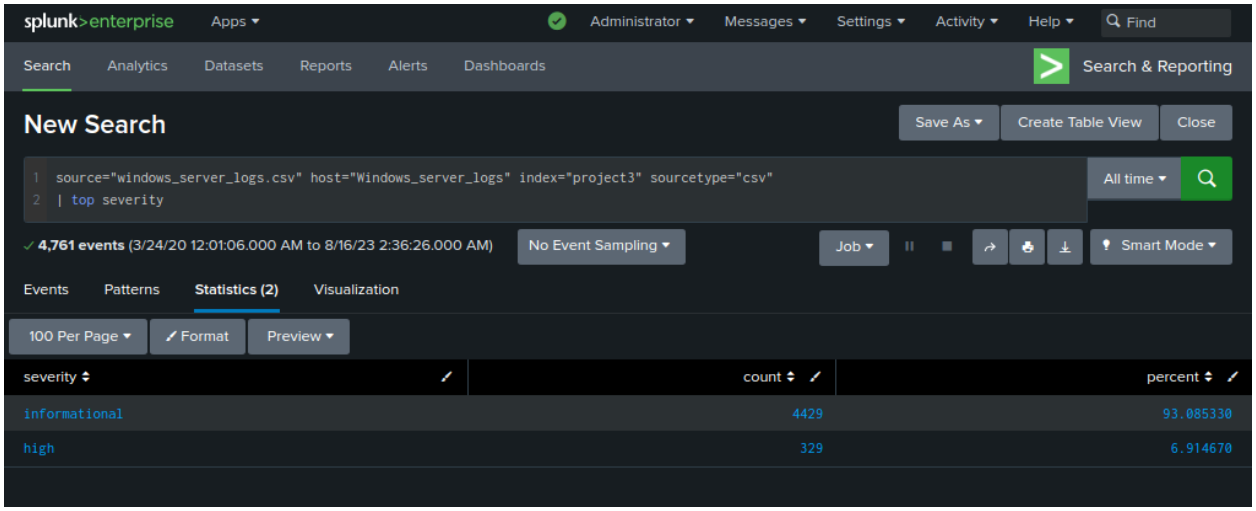
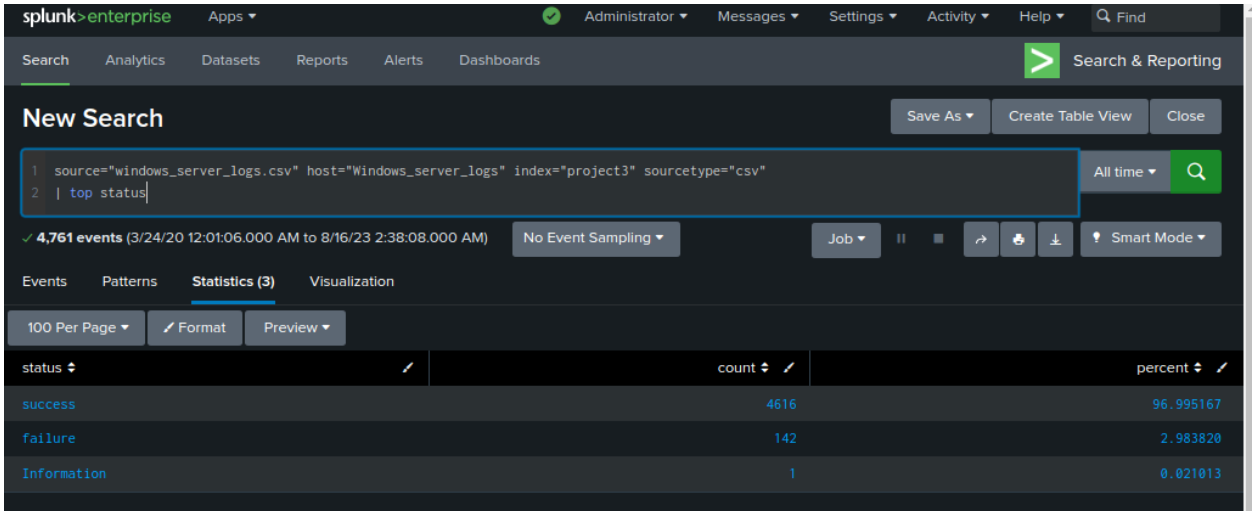
SPL Query (Signatures and IDs)



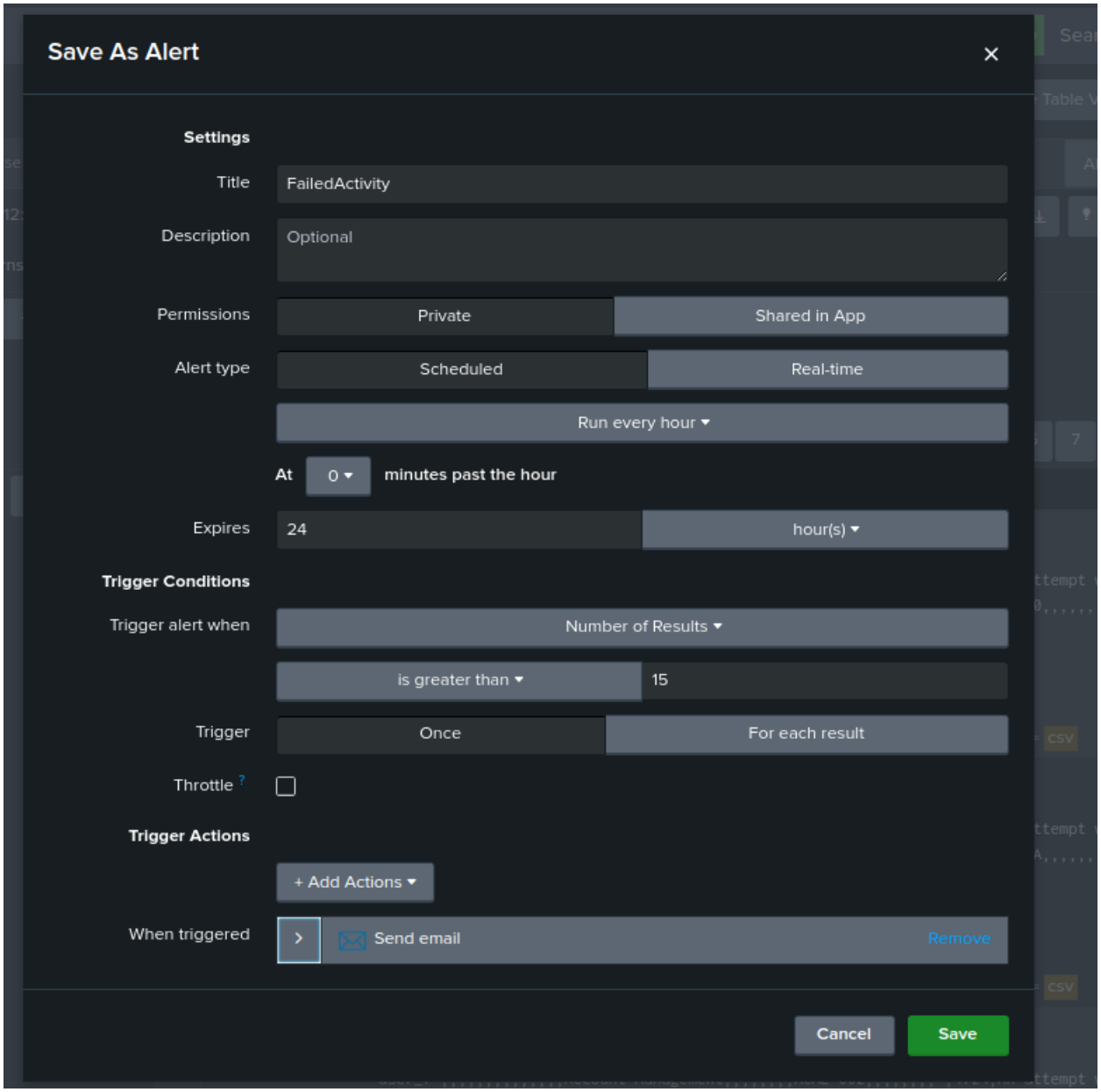
SPL Query (Sverity, count, percentage)



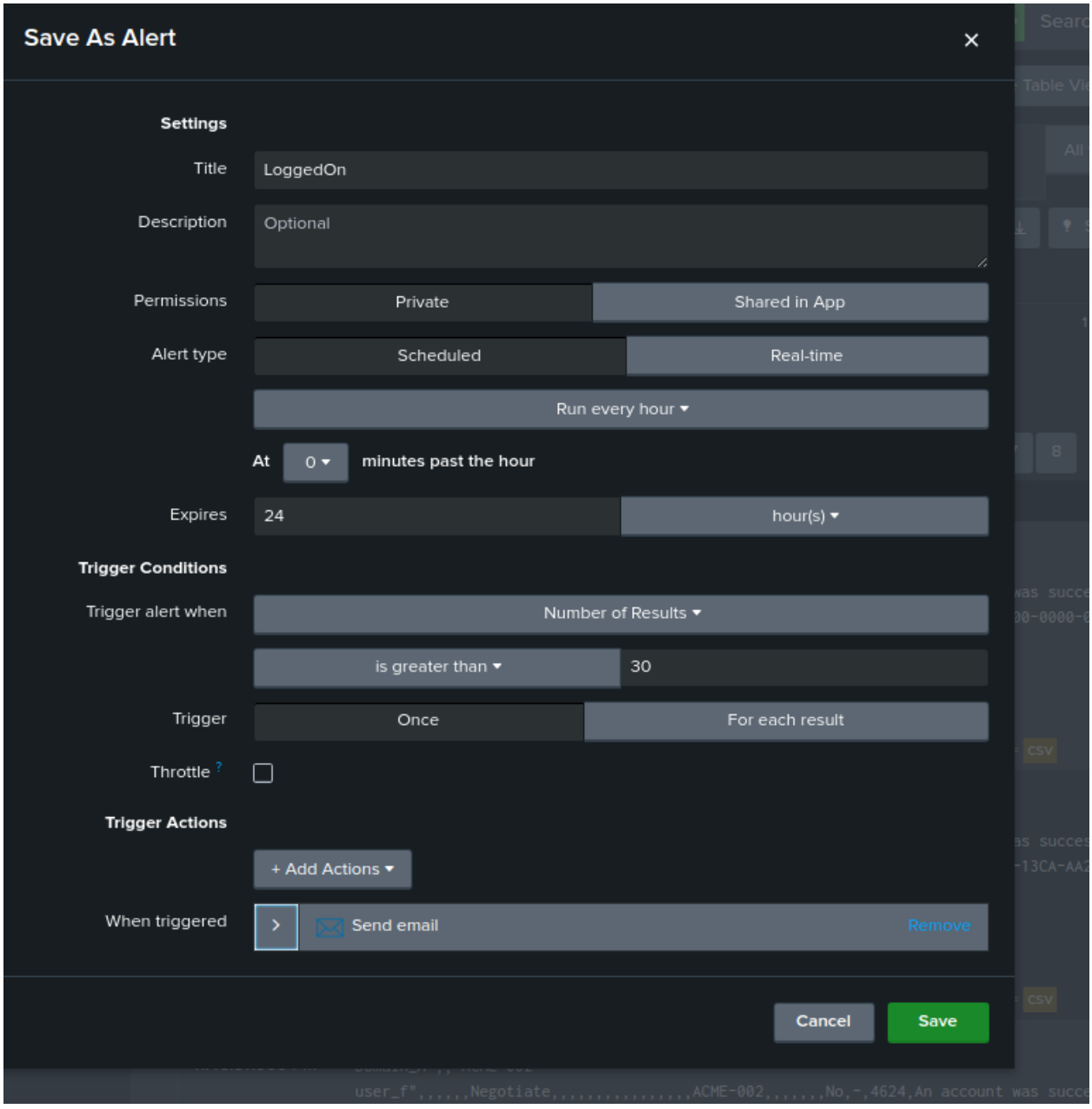
SPL Query (status)



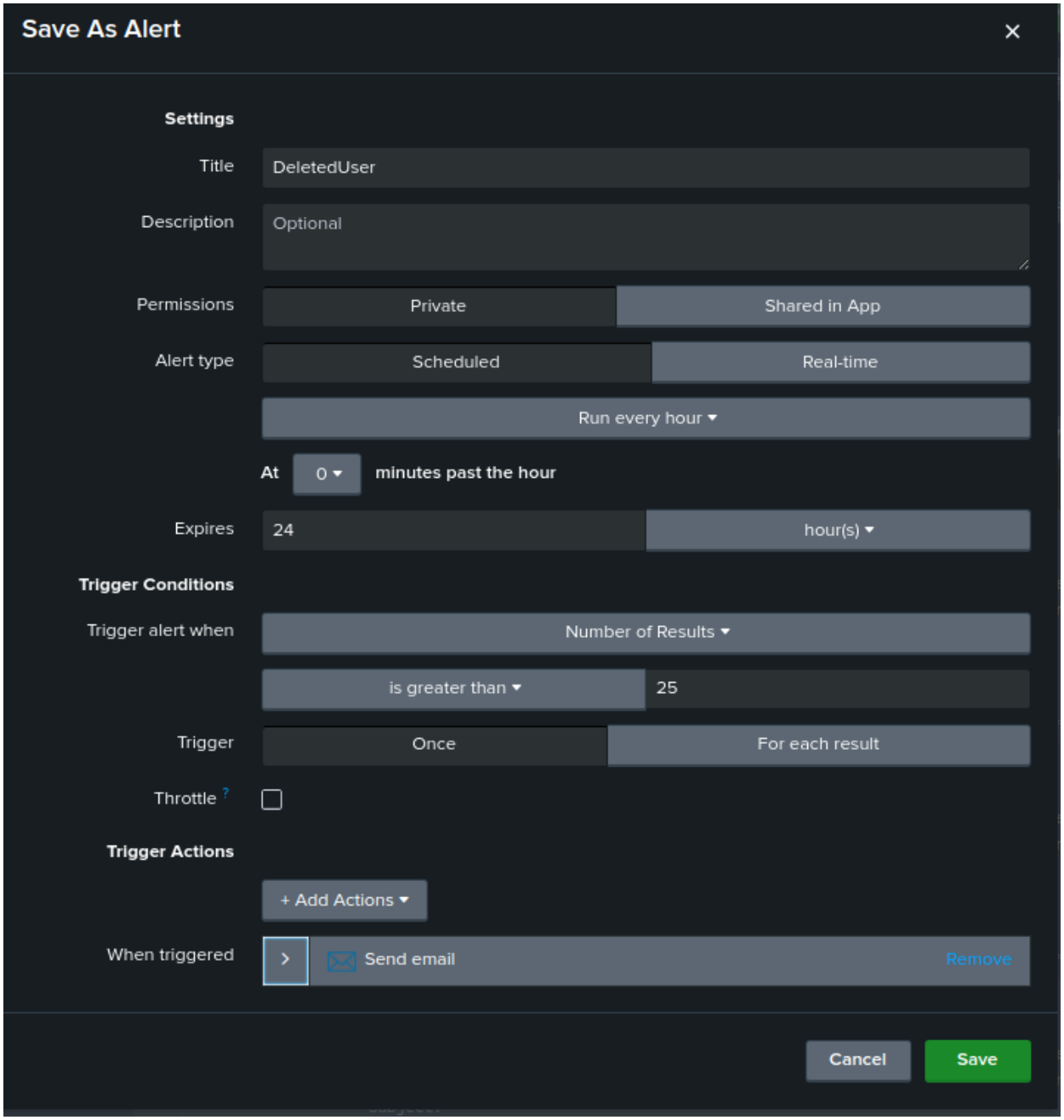
Alert (Failed Activity) status=failure



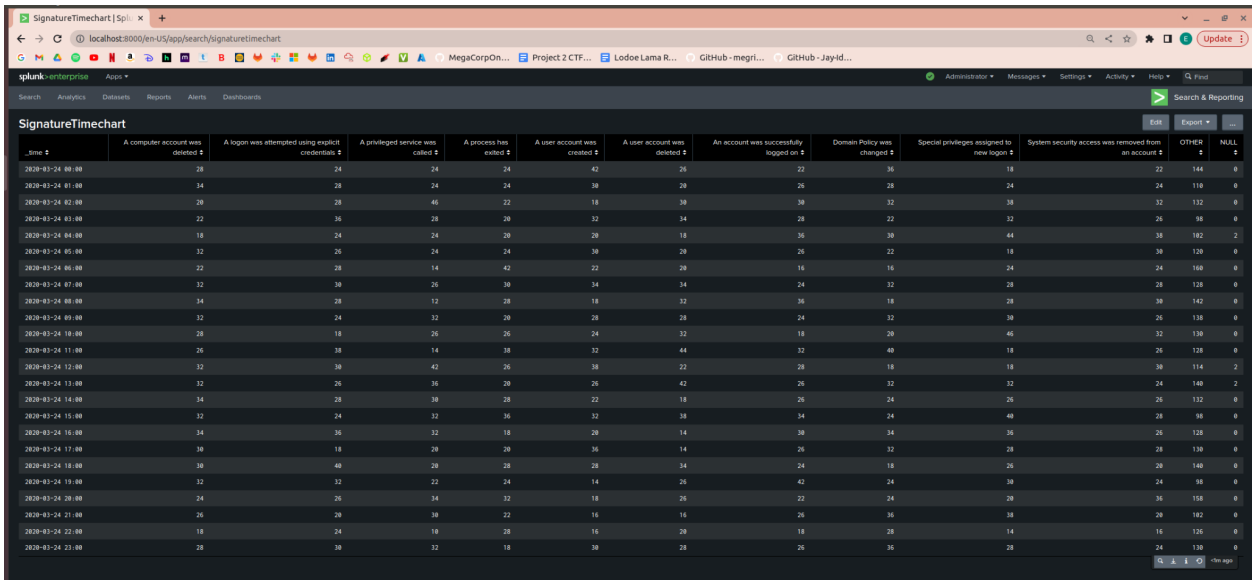
Alert (LoggedOn) signature=”An account was successfully logged on”



Alert (Deleted account) signature_id="4726"



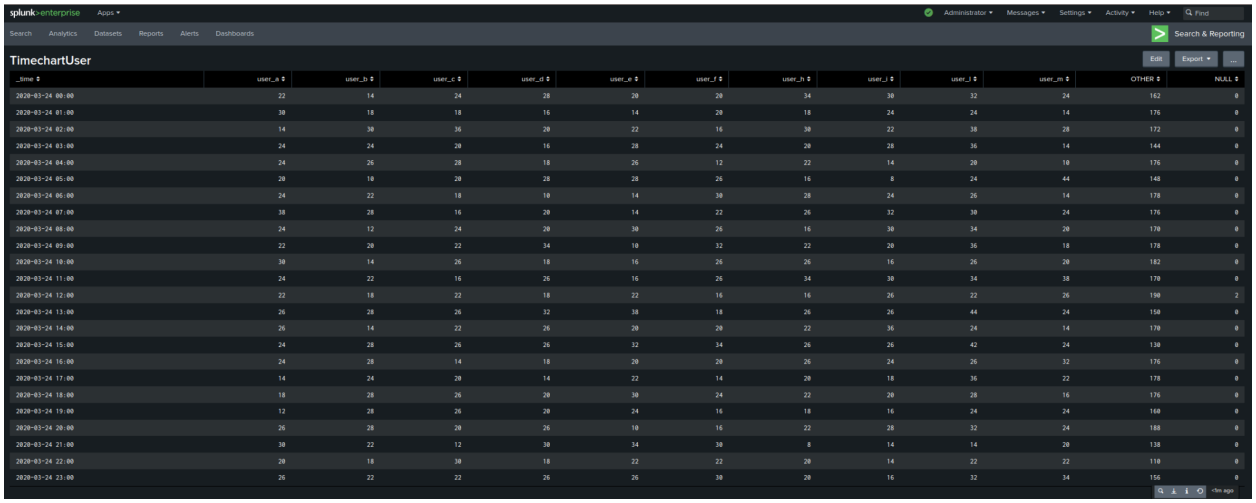
Linechart Signature timechart span=1h count by signature



SignatureTimechart

_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was created	A user account was deleted	An account was successfully logged on	Domain Policy was changed	Special privileges assigned to new logon	System security access was removed from an account	OTHER	NULL
2020-03-24 00:00	28	24	24	24	42	26	22	36	18	22	144	0
2020-03-24 01:00	34	28	24	24	30	20	26	28	24	24	110	0
2020-03-24 02:00	20	28	46	22	18	30	30	32	38	32	132	0
2020-03-24 03:00	22	36	28	20	32	34	28	22	32	26	98	0
2020-03-24 04:00	18	24	24	20	20	18	36	30	44	38	102	2
2020-03-24 05:00	32	26	24	24	30	20	26	22	18	30	120	0
2020-03-24 06:00	22	28	14	42	22	20	16	16	24	24	160	0
2020-03-24 07:00	32	30	26	30	34	34	24	32	28	28	128	0
2020-03-24 08:00	34	28	12	28	18	32	36	18	28	30	142	0
2020-03-24 09:00	32	24	32	20	28	28	24	32	30	26	138	0
2020-03-24 10:00	28	18	26	26	24	32	18	20	46	32	130	0
2020-03-24 11:00	26	38	14	38	32	44	32	40	18	26	128	0
2020-03-24 12:00	32	30	42	26	38	22	28	18	18	30	114	2
2020-03-24 13:00	32	26	36	20	26	42	26	32	32	24	140	2
2020-03-24 14:00	34	28	30	28	22	18	26	24	26	26	132	0
2020-03-24 15:00	32	24	32	36	32	38	34	24	40	28	98	0
2020-03-24 16:00	34	36	32	18	20	14	30	34	36	26	128	0
2020-03-24 17:00	30	18	20	20	36	14	26	32	28	28	130	0
2020-03-24 18:00	30	40	20	28	28	34	24	18	26	20	140	0
2020-03-24 19:00	32	32	22	24	14	26	42	24	30	24	98	0
2020-03-24 20:00	24	26	34	32	18	26	22	24	20	36	158	0
2020-03-24 21:00	26	20	30	22	16	16	26	36	38	20	102	0
2020-03-24 22:00	18	24	10	28	16	20	18	28	14	16	126	0
2020-03-24 23:00	28	30	32	18	30	28	26	36	28	24	130	0

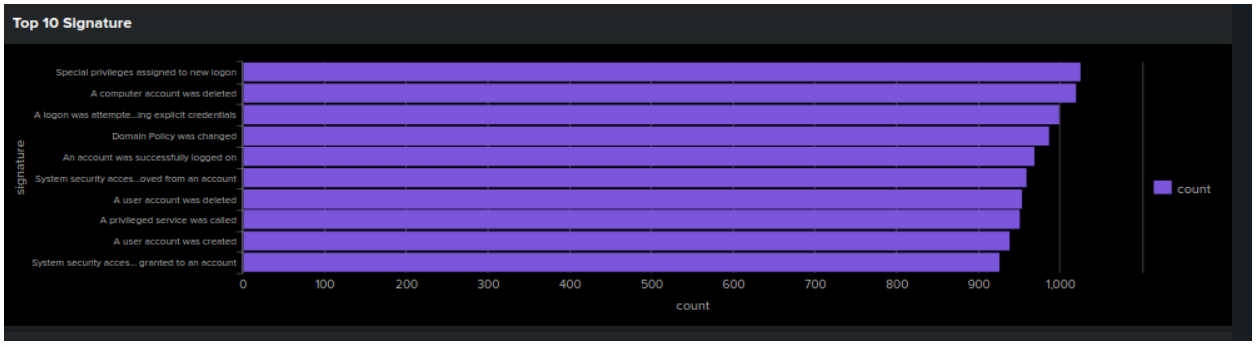
Linechart User timechart span=1h count by user



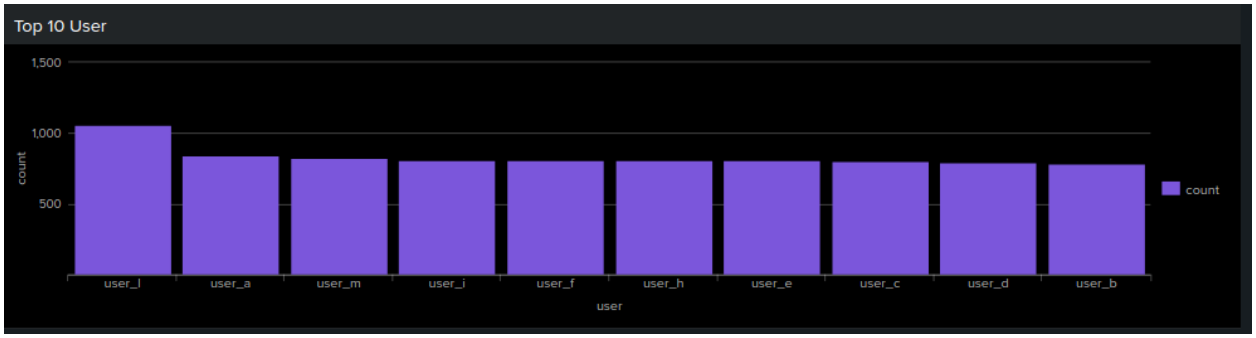
TimechartUser

_time	user_a	user_b	user_c	user_d	user_e	user_f	user_h	user_i	user_l	user_m	OTHER	NULL
2020-03-24 00:00	22	14	24	28	20	20	34	30	32	24	162	0
2020-03-24 01:00	30	18	18	16	14	20	18	24	24	14	176	0
2020-03-24 02:00	14	30	36	20	22	16	30	22	38	28	172	0
2020-03-24 03:00	24	24	20	16	28	24	20	28	36	14	144	0
2020-03-24 04:00	24	26	28	18	26	12	22	14	20	10	176	0
2020-03-24 05:00	20	10	20	28	28	26	16	8	24	44	148	0
2020-03-24 06:00	24	22	18	10	14	30	28	24	26	14	178	0
2020-03-24 07:00	38	28	16	20	14	22	26	32	30	24	176	0
2020-03-24 08:00	24	12	24	20	30	26	16	30	34	20	170	0
2020-03-24 09:00	22	20	22	34	10	32	22	20	36	18	178	0
2020-03-24 10:00	30	14	26	18	16	26	26	16	26	20	182	0
2020-03-24 11:00	24	22	16	26	16	26	34	30	34	38	170	0
2020-03-24 12:00	22	18	22	18	22	16	16	26	22	26	190	2
2020-03-24 13:00	26	28	26	32	38	18	26	26	44	24	150	0
2020-03-24 14:00	26	14	22	26	20	20	22	36	24	14	170	0
2020-03-24 15:00	24	28	26	26	32	34	26	26	42	24	130	0
2020-03-24 16:00	24	28	14	18	20	20	26	24	26	32	176	0
2020-03-24 17:00	14	24	20	14	22	14	20	18	36	22	178	0
2020-03-24 18:00	18	28	26	20	30	24	22	20	28	16	176	0
2020-03-24 19:00	12	28	26	20	24	16	18	16	24	24	160	0
2020-03-24 20:00	26	28	20	26	10	16	22	28	32	24	188	0
2020-03-24 21:00	30	22	12	30	34	30	8	14	14	20	138	0
2020-03-24 22:00	20	18	30	18	22	22	20	14	22	22	110	0
2020-03-24 23:00	26	22	22	26	26	30	20	16	32	34	156	0

Barchart top 10 signature top limit=10 signature



Barchart top 10 user top limit=10 user



Apache

Top method

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

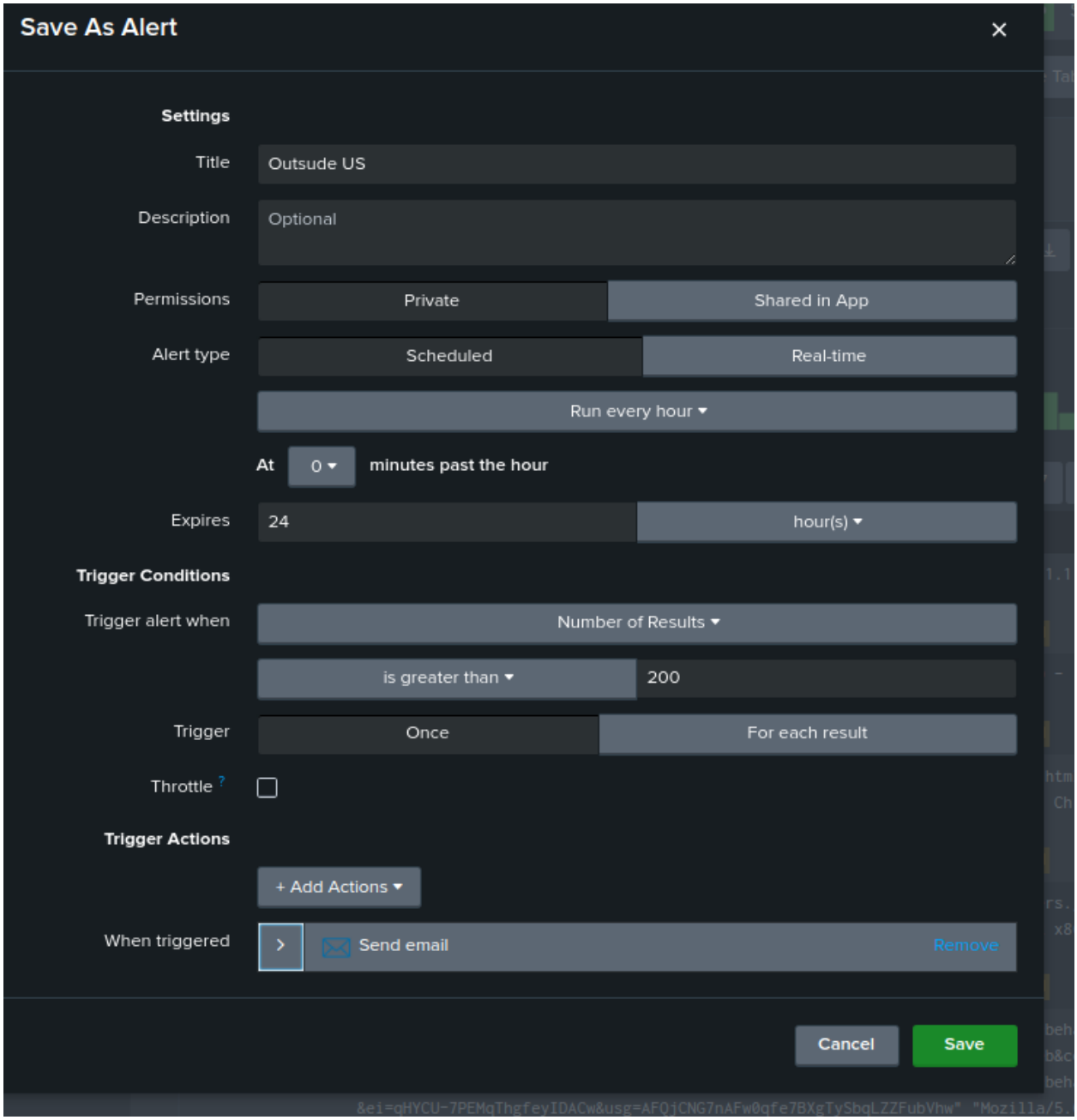
Top limit=10 referrer_domain

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

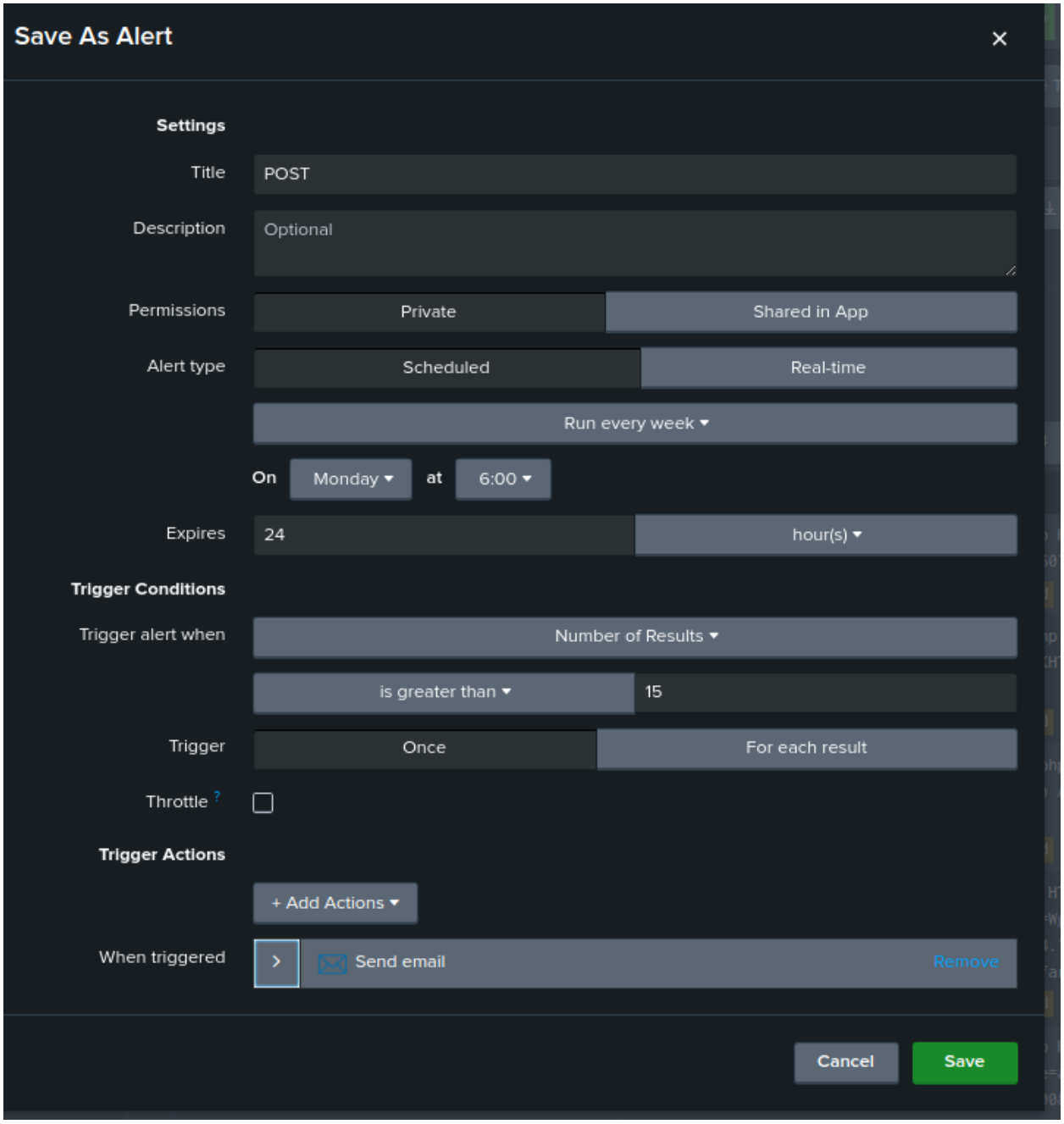
Top status

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

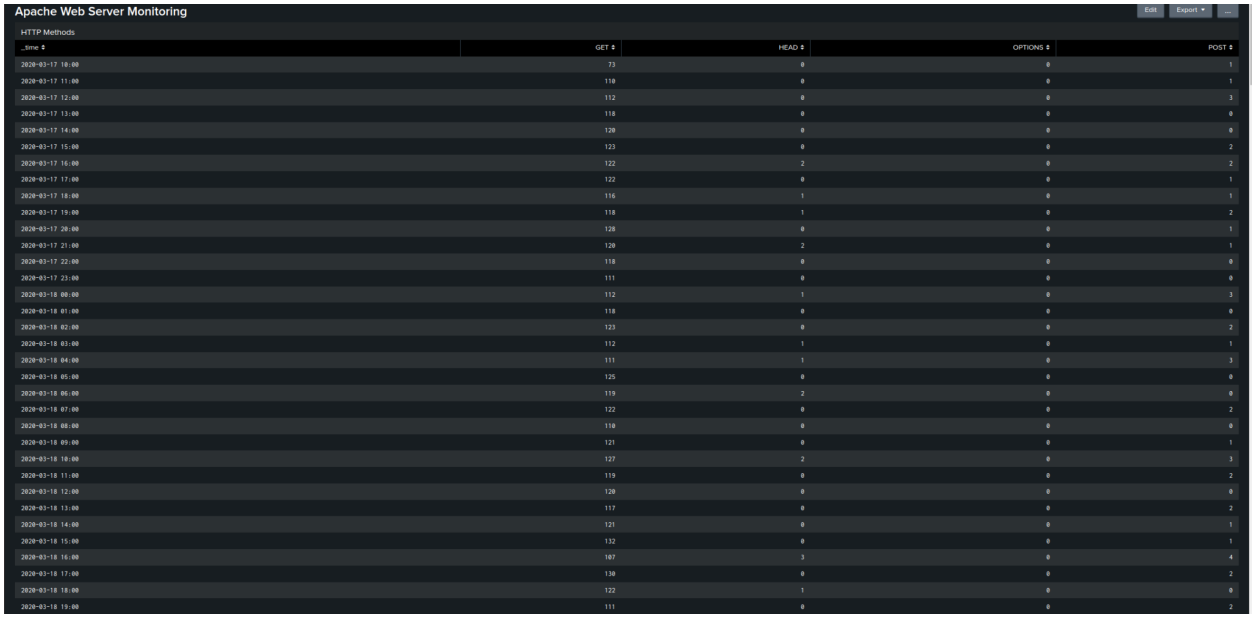
Alert Outside US: iplocation clientip | where Country !=”United States”



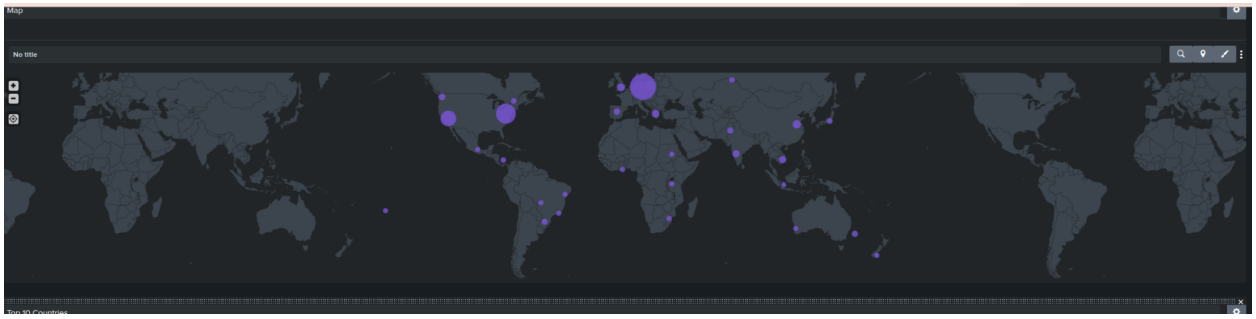
Alert method="POST" |


Save As Alert
Settings
Title
POST
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
15
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
Cancel
Save

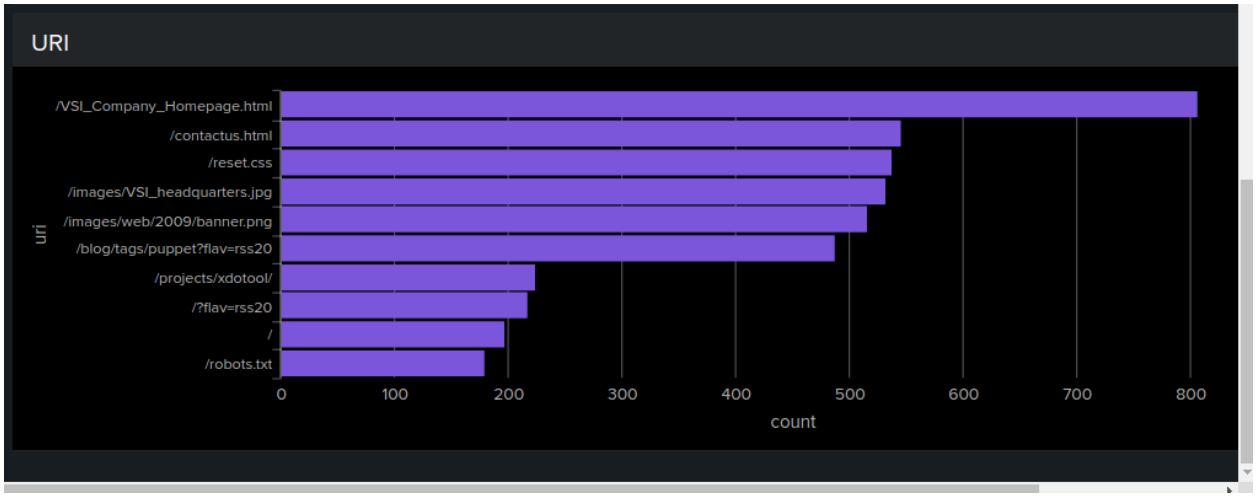
HTTP



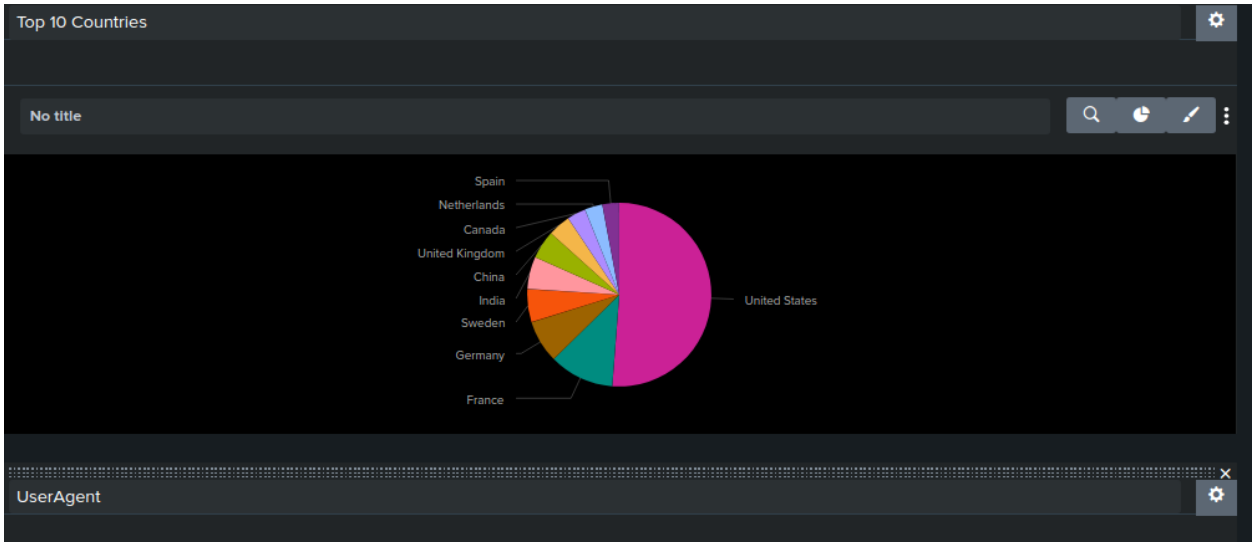
Map



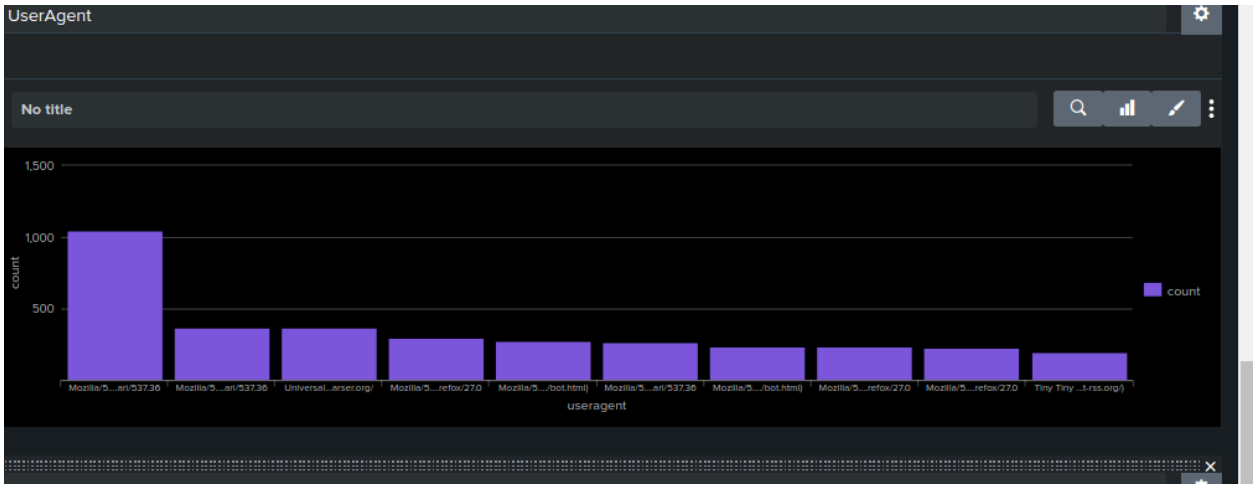
URI



Top 10 countries


Top 10 Countries
No title
Spain
Netherlands
Canada
United Kingdom
China
India
Sweden
Germany
France
United States
UserAgent

User Agent


UserAgent
No title
1,500
1,000
500
count
count
useragent