Defensive Security Project
by: Stephanie Ortega

Table of Contents

This document contains the following resources:

Monitoring Environment

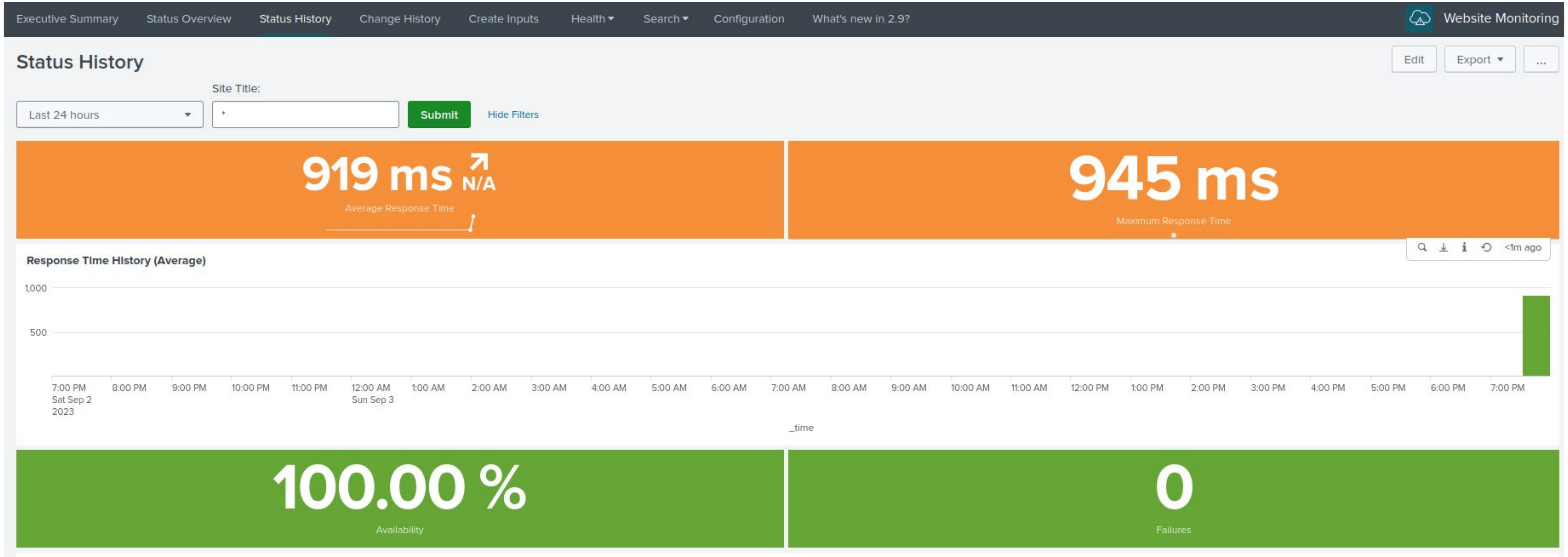
Scenario

- Virtual Space Industries (VSI) contracted us as a SOC based on rumors of an attack by the competitor JobeCorp.
- We were given normal conditions for VSI to establish baseline activities and create thresholds for potential attacks.
- Using the data VSI provided we were able to monitor a cybersecurity attack on their Windows and Apache servers.
- We were also given the attack logs which we used to analyze the attack

Website Monitoring App

Website Monitoring

This app monitors a website (URL inserted into a modular input) to detect downtime and performance problems. The add-on collects relevant data from websites / web applications like response times, server health, and error rates. It has pre-configured dashboards & visualizations for these values.



Status History

Last 24 hours

Site Title: *

919 ms N/A
Average Response Time

945 ms
Maximum Response Time

Response Time History (Average)

100.00 %
Availability

0
Failures

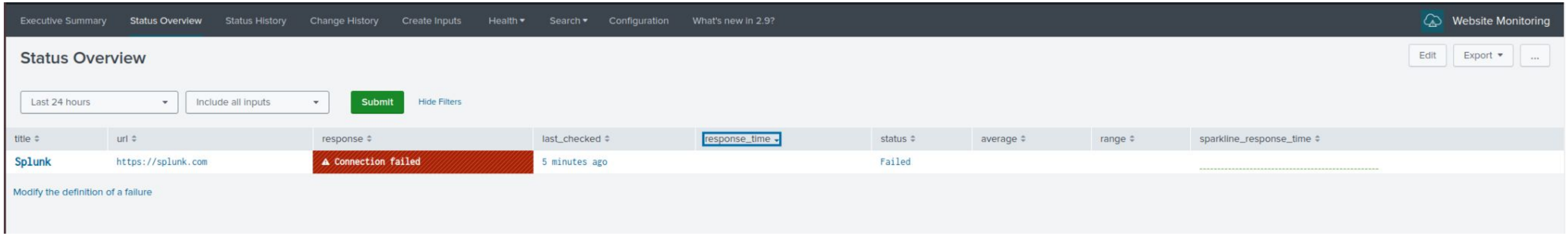
Website Monitoring

Who benefits from Website Monitoring add-on app

- Business websites, getting performance data on your website or web app is important because you want to make sure your website is healthy and clients are able to access it.
- SLA compliance

Website Monitoring

We can put inputs into the website monitoring add on which has many settings and fields that you can use to track more specifically what data you want to see. Here I used simply the default fields on the splunk url. This add on had many features such as dashboards



Status Overview

Last 24 hours ▾ | Include all inputs ▾

title	url	response	last_checked	response_time	status	average	range	sparkline_response_time
Splunk	https://splunk.com	⚠ Connection failed	5 minutes ago		Failed			

Modify the definition of a failure

Logs Analyzed

1 Windows Logs

Account names
Account domain
User account controls
Privileges
Password attributes
Changed attributes
Log on information
Security ID
Process ID and Name
Service Request Information
Service Name

2 Apache Logs

HTTP status code
HTTP request type
IP address of device making request
Date and time of request
Size of response in bytes
URL of page linked to request
Browser information of user

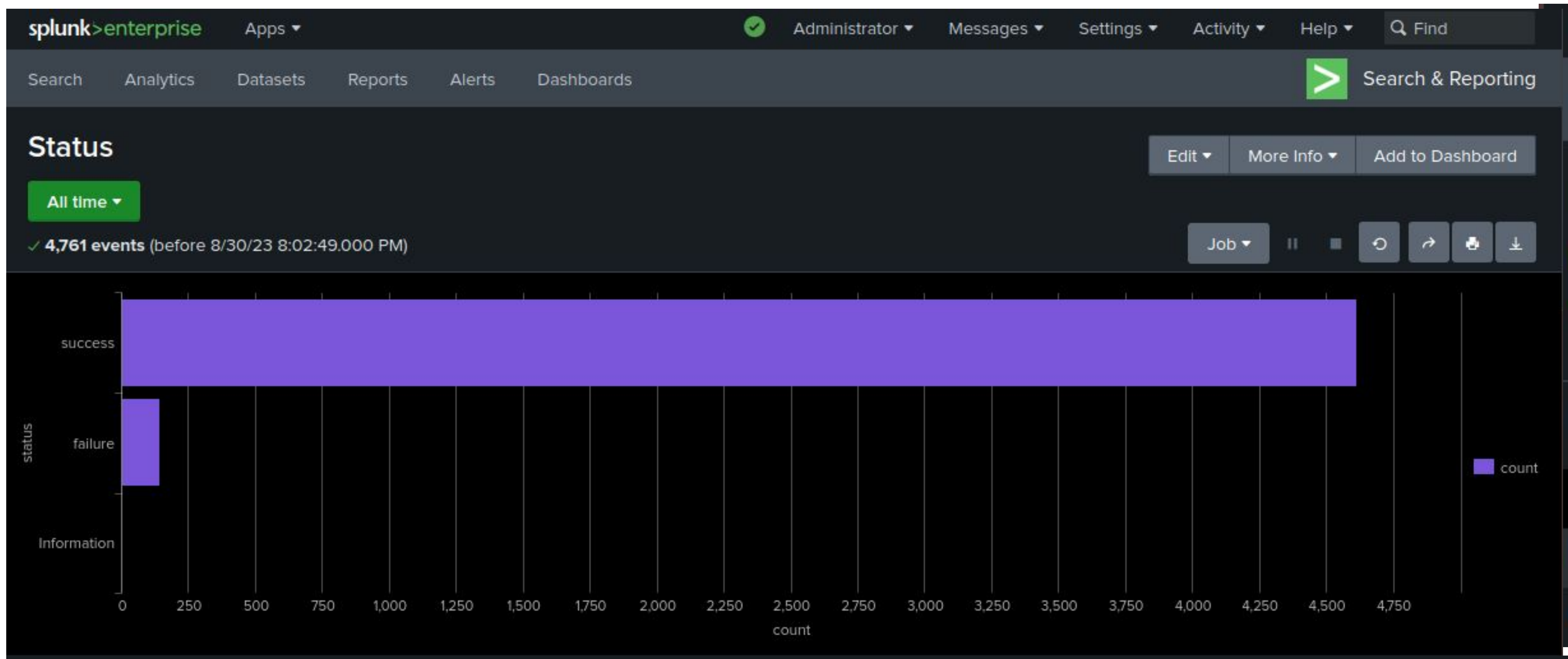
Windows Logs

Reports—Windows

Designed the following reports:

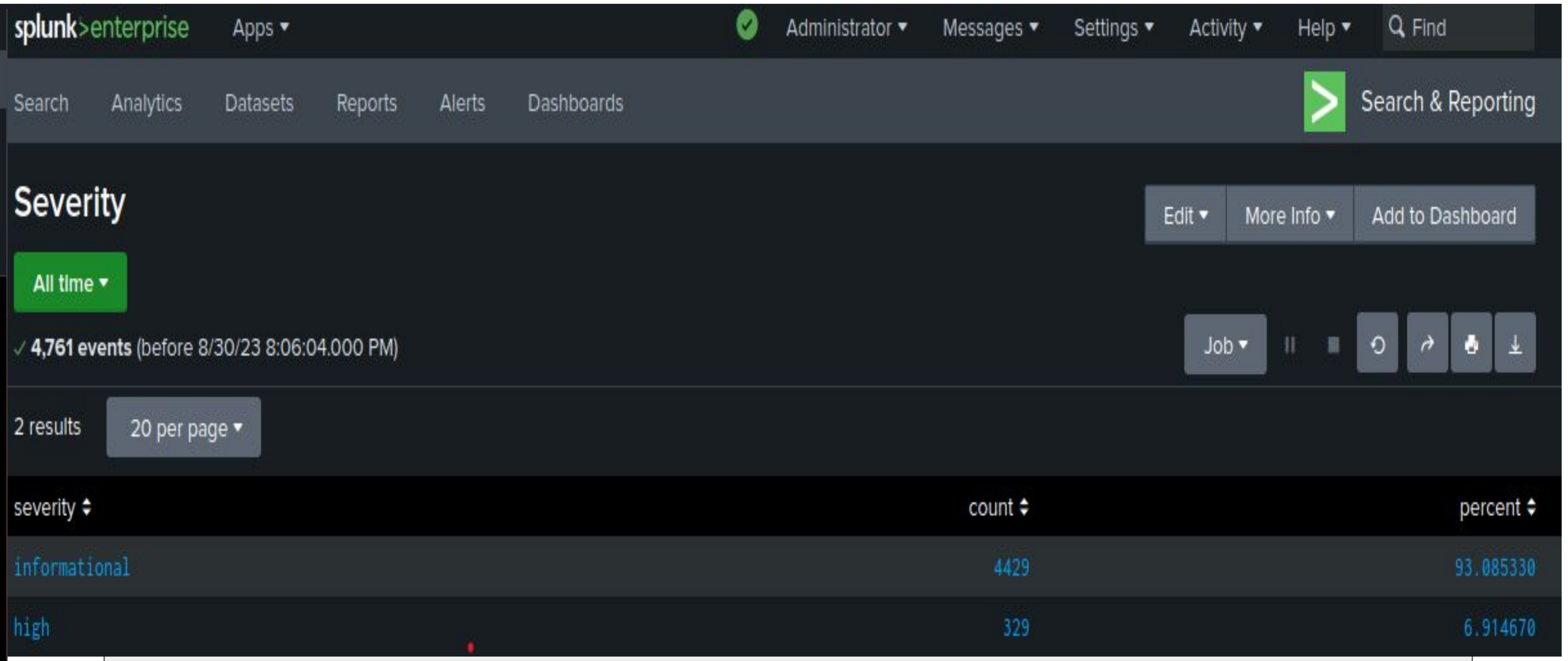
Report Name	Report Description
Signature and ID	Shows the ID number of a given signature
Severity	Gives an idea of the severity outlook
Status	Shows the success and failure status
User Count	Shows count of users and their logins

Images of Reports—Windows



Status

✓ **4,761 events** (before 8/30/23 8:02:49.000 PM)

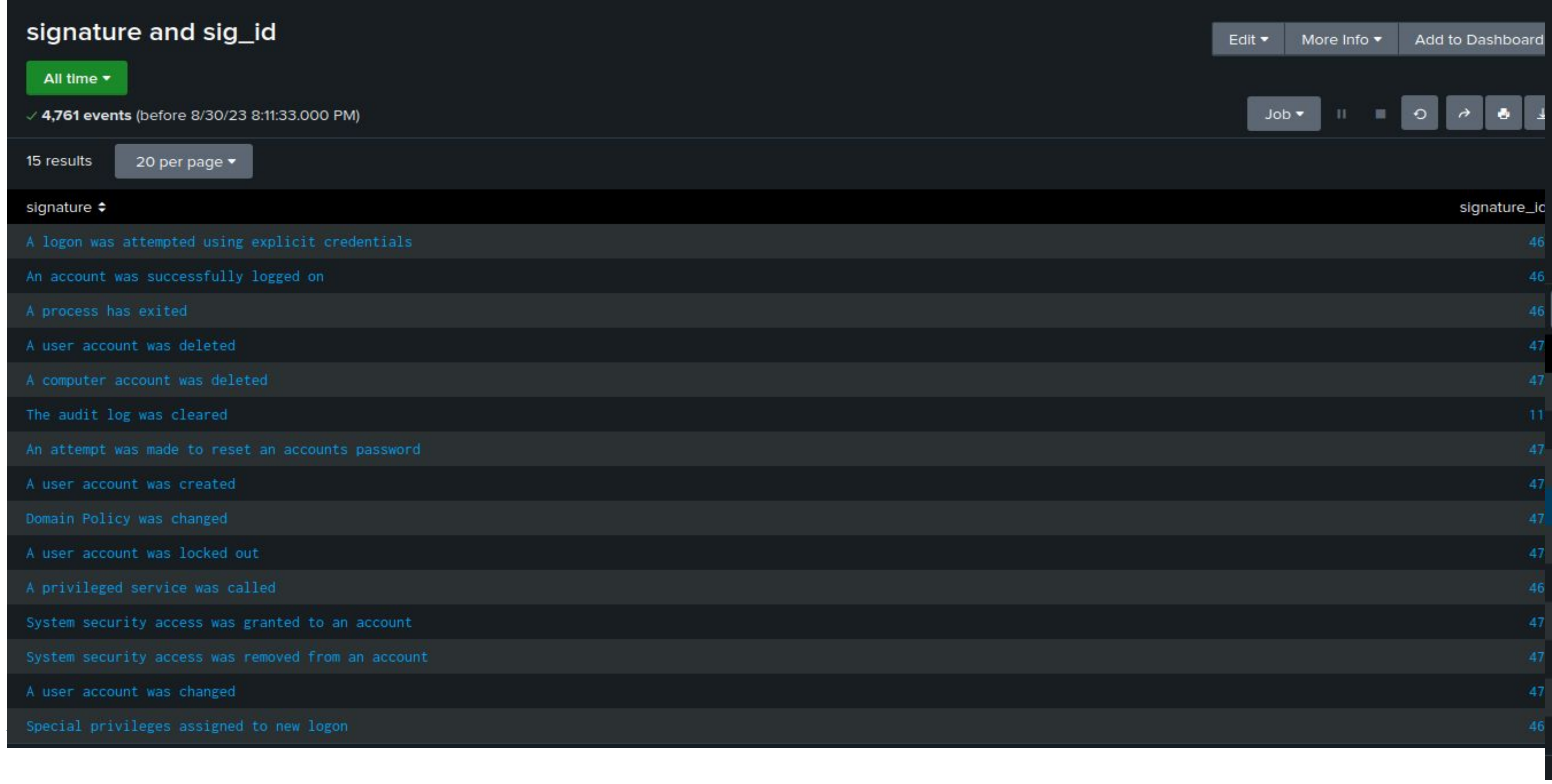


Severity

✓ **4,761 events** (before 8/30/23 8:06:04.000 PM)

2 results

severity ⇕	count ⇕	percent ⇕
informational	4429	93.085330
high	329	6.914670

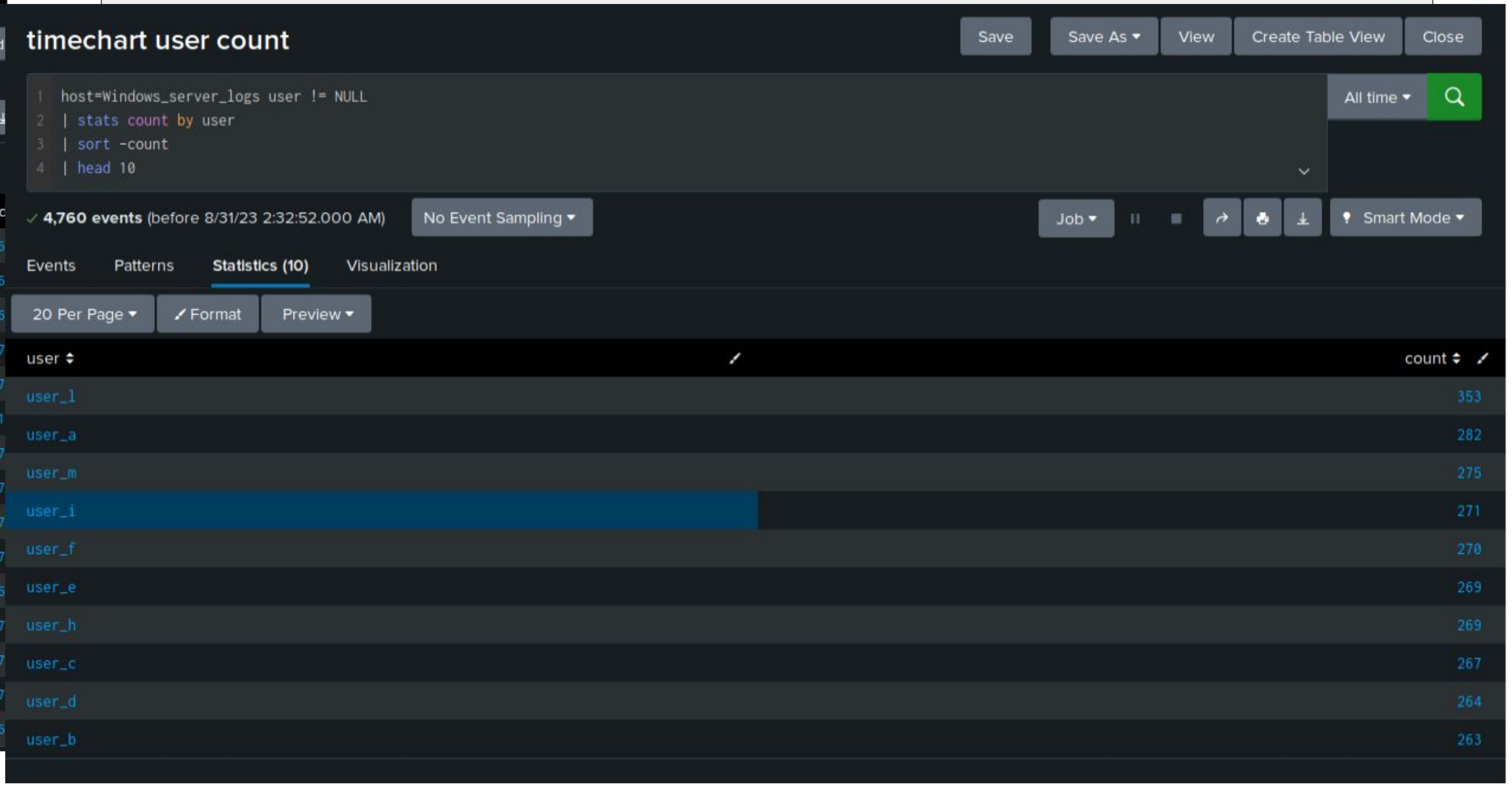


signature and sig_id

✓ **4,761 events** (before 8/30/23 8:11:33.000 PM)

15 results

signature ⇕	signature_ic
A logon was attempted using explicit credentials	46
An account was successfully logged on	46
A process has exited	46
A user account was deleted	47
A computer account was deleted	47
The audit log was cleared	11
An attempt was made to reset an accounts password	47
A user account was created	47
Domain Policy was changed	47
A user account was locked out	47
A privileged service was called	46
System security access was granted to an account	47
System security access was removed from an account	47
A user account was changed	47
Special privileges assigned to new logon	46



timechart user count

```
host=Windows_server_logs user != NULL
| stats count by user
| sort -count
| head 10
```

✓ **4,760 events** (before 8/31/23 2:32:52.000 AM)

user ⇕	count ⇕
user_l	353
user_a	282
user_m	275
user_i	271
user_f	270
user_e	269
user_h	269
user_c	267
user_d	264
user_b	263

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Suspicious Activity	Looks at the number of failed status	7-8 per hour	15 per hour

JUSTIFICATION: Based on the column chart normal hourly activity is 5 failure status plus or minus around 2-3. Therefore, A high baseline would be 8. Doubling the high base line gave me the threshold of 15 per hour.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Login	Counts the hourly number of successfully logins	around 15 per hour	40 per hour

JUSTIFICATION: The majority of successful logins per hour was around 15 which was what I determined was a baseline. The highest number of successful logins was 21 which I doubled and rounded down to get a threshold of 40 per hour.

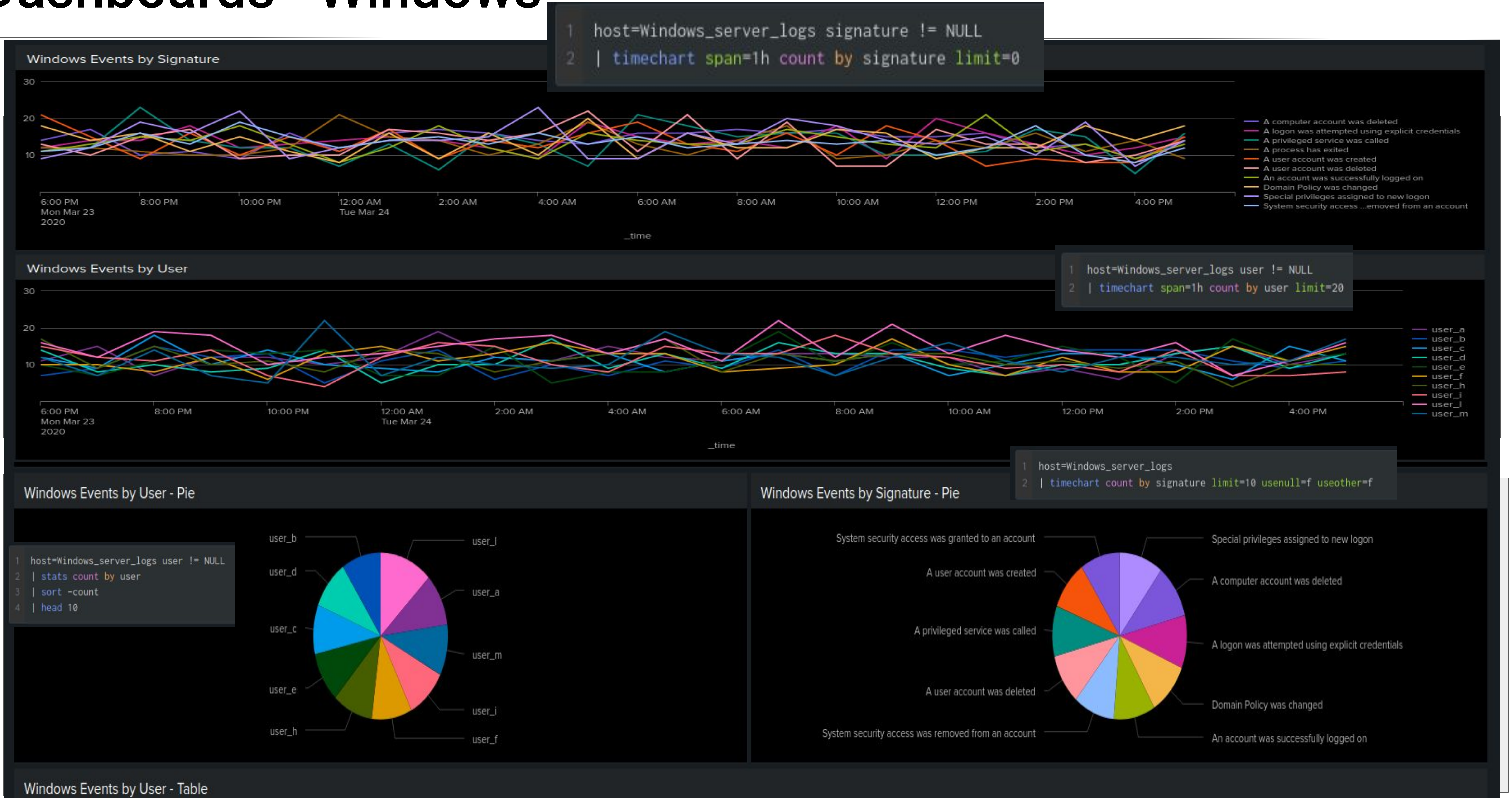
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Signature ID 4726	An event that pertains to a user account being deleted	[11]	[17]

JUSTIFICATION: [Account deletion happened between 7-22 times and with most of them happening around 9-11 times. The highest being 22, so we set our alerts at 11 and 17.]

Dashboards—Windows



```
host=Windows_server_logs signature != NULL
| timechart span=1h count by signature limit=0
```

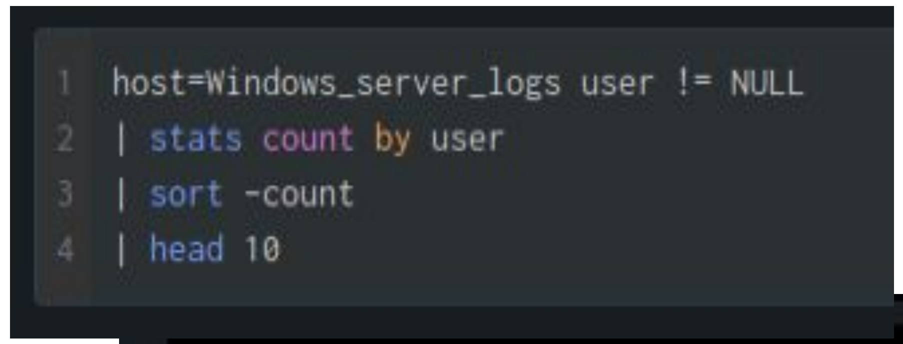
```
host=Windows_server_logs user != NULL
| timechart span=1h count by user limit=20
```

```
host=Windows_server_logs
| timechart count by signature limit=10 usenull=f useother=f
```

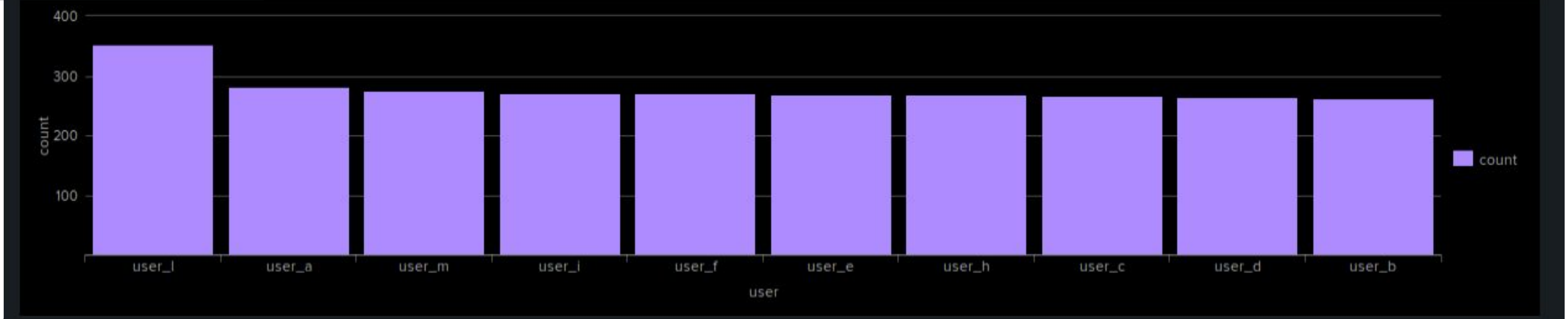
```
host=Windows_server_logs user != NULL
| stats count by user
| sort -count
| head 10
```

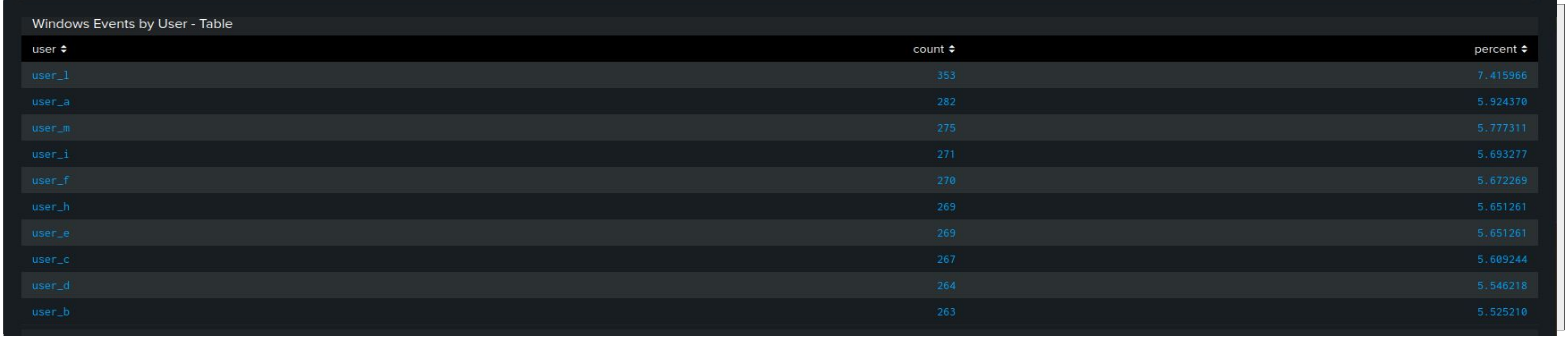
Windows Events by Signature
30
20
10
6:00 PM
Mon Mar 23
2020
8:00 PM
10:00 PM
12:00 AM
Tue Mar 24
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
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 ...emoved from an account
Windows Events by User
30
20
10
6:00 PM
Mon Mar 23
2020
8:00 PM
10:00 PM
12:00 AM
Tue Mar 24
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
_time
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_l
user_m
Windows Events by User - Pie
user_b
user_d
user_c
user_e
user_h
user_l
user_a
user_m
user_i
user_f
Windows Events by Signature - Pie
System security access was granted to an account
A user account was created
A privileged service was called
A user account was deleted
System security access was removed from an account
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
Windows Events by User - Table

Dashboards—Windows



```
host=Windows_server_logs user != NULL
| stats count by user
| sort -count
| head 10
```





Windows Events by User - Table

user ⇕	count ⇕	percent ⇕
user_l	353	7.415966
user_a	282	5.924370
user_m	275	5.777311
user_i	271	5.693277
user_f	270	5.672269
user_h	269	5.651261
user_e	269	5.651261
user_c	267	5.609244
user_d	264	5.546218
user_b	263	5.525210

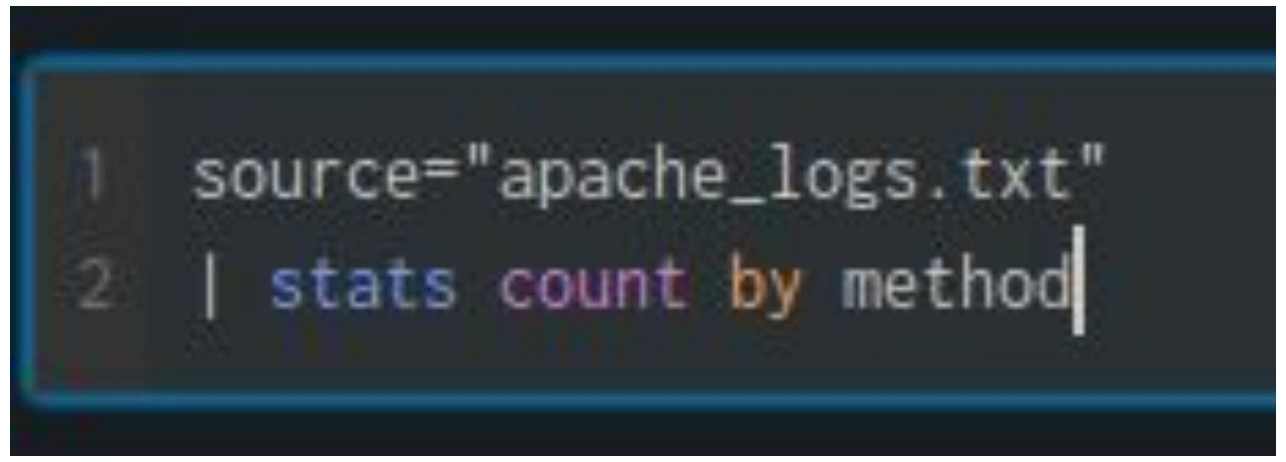
Apache Logs

Reports—Apache

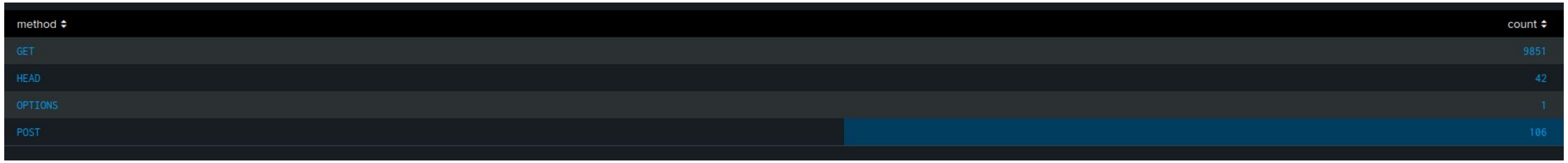
Designed the following reports:

Report Name	Report Description
HTTP Methods	Gives insight into the different HTTP request activity against the web server.
HTTP Response Code Count	Shows any abnormal counts of HTTP responses.
Top 10 Domains	This report shows the top 10 domains that referred to the VSI website.

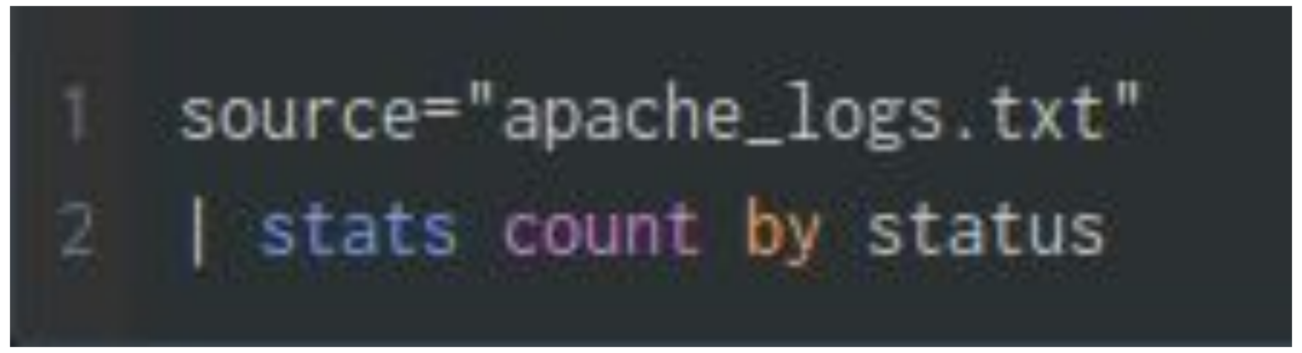
Images of Reports—Apache



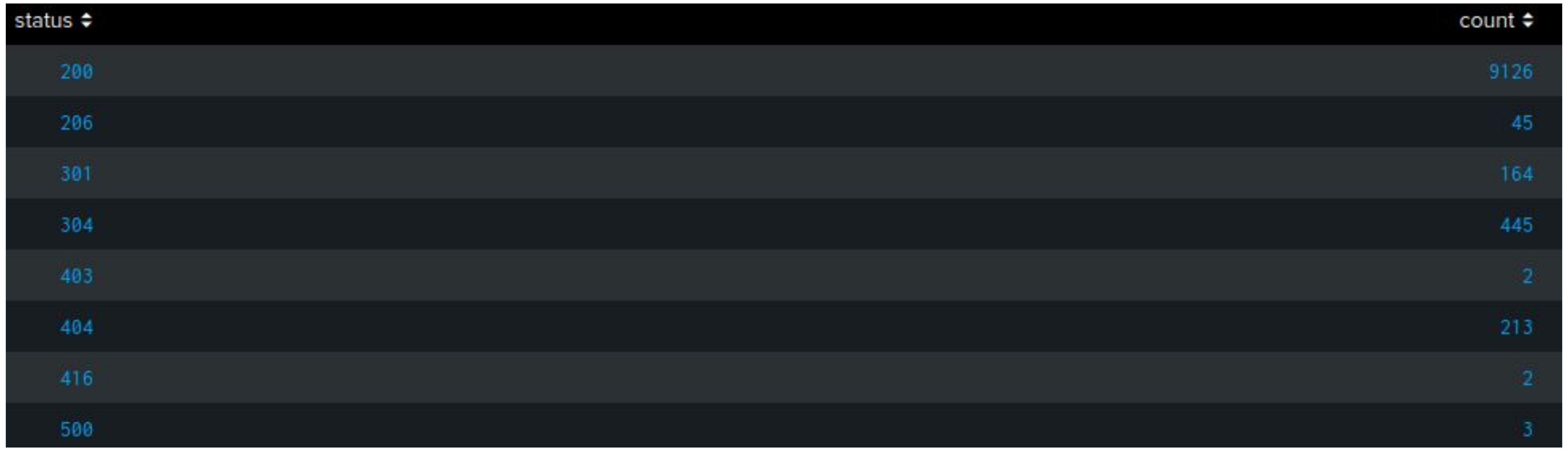
```
source="apache_logs.txt"
| stats count by method
```



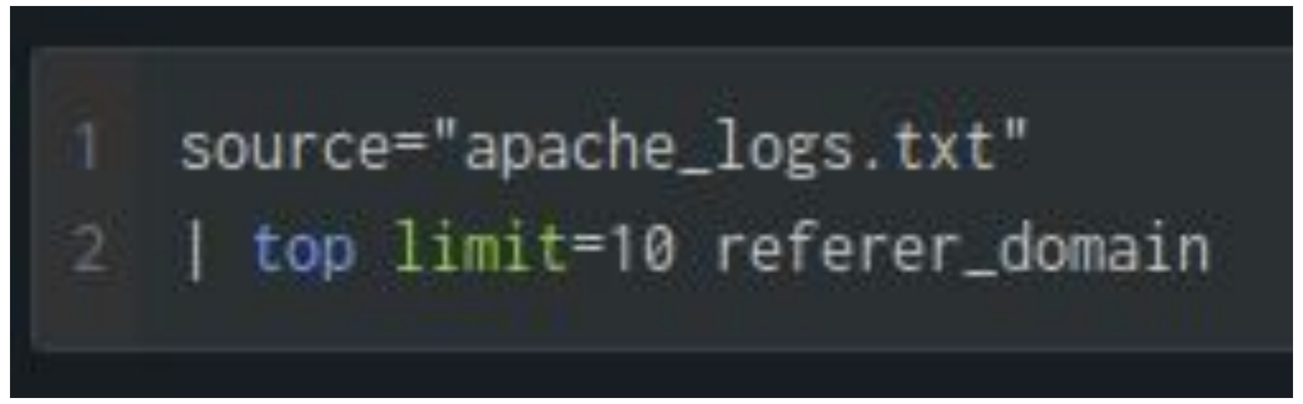
method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106



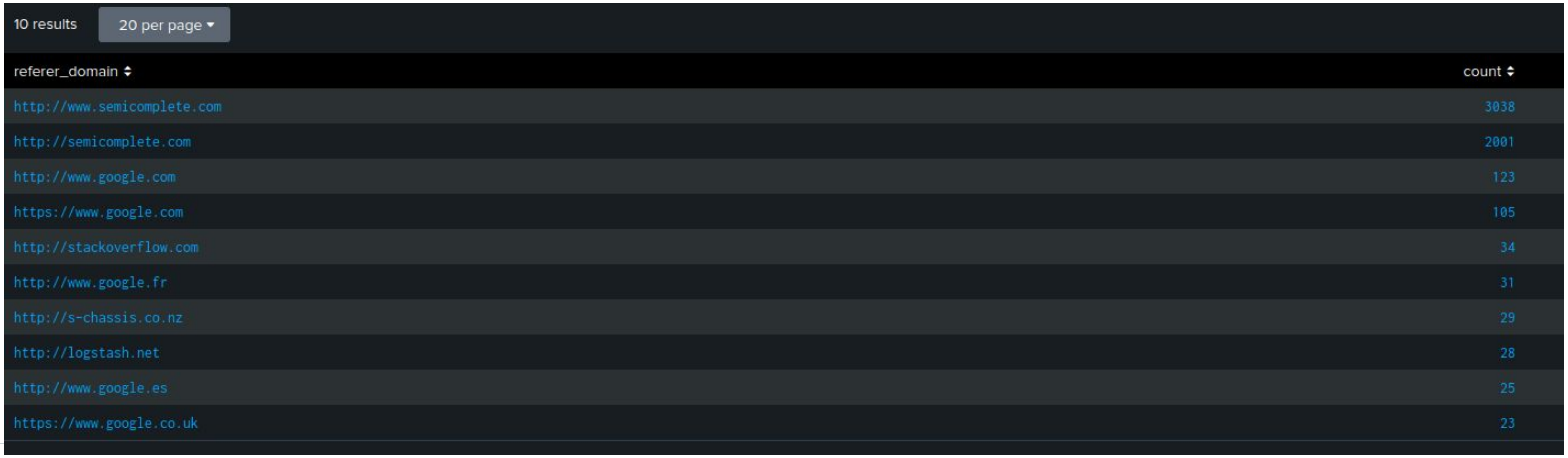
```
source="apache_logs.txt"
| stats count by status
```



status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3



```
source="apache_logs.txt"
| top limit=10 referer_domain
```



10 results   20 per page ▾

referer_domain	count
http://www.semicomplete.com	3038
http://semicomplete.com	2001
http://www.google.com	123
https://www.google.com	105
http://stackoverflow.com	34
http://www.google.fr	31
http://s-chassis.co.nz	29
http://logstash.net	28
http://www.google.es	25
https://www.google.co.uk	23

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Count	Counts the number of HTTP POST requests.	0-8 per hour	<10 per hour

JUSTIFICATION: After analyzing the linear timeline on apache_logs.txt, it was determined that there was a normal range of anywhere between 0 and 8 events in a given hour, by setting the threshold to 10 we can assume that anything at or above would be considered irregular activity.

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity Outside US	Counts hourly activity from a country other than the United States.	60-120 per hour	<150 per hour

JUSTIFICATION: After analyzing the linear timeline on apache_logs.txt, it was determined that the average activity per hour was anywhere from 60-120. Allowing for a slight variance in activity, the alert threshold was established at 150 to trigger any abnormal activity above that value.

Dashboards—Apache

Apache Web Server Monitoring

Apache Logs by HTTP Method

Apache Logs by URI

Apache Logs Count by Country

Apache Logs Count by HTTP Status 404

Edit
Export ▾
...
All time
Hide Filters
150
100
50
GET
HEAD
OPTIONS
POST
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 PM
12:00 AM Thu Mar 19
12:00 PM
12:00 AM Fri Mar 20
12:00 PM
_time
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg
/images/web/2009/banner.png
/blog/tags/puppet?flav=rss20
/projects/xdotool/
/?flav=rss20
/
/robots.txt
uri
0
100
200
300
400
500
600
700
800
count
count
United States
France
Germany
Sweden
India
China
United Kingdom
Canada
Netherlands
Spain
Country
0
500
1,000
1,500
2,000
2,500
3,000
3,500
4,000
count
count
0
50
100
150
200
250
300
350
400
450
213

Dashboards—Apache (continued)

Apache Logs by Client IP

Apache Logs by Count of User Agents

useragent	count	percent
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1044	10.441044
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	369	3.690369
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364	3.640364
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	296	2.960296
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	271	2.710271
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268	2.680268
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237	2.370237
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	236	2.360236
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	229	2.290229
Tiny Tiny RSS/1.11 (http://tt-rss.org/)	198	1.980198

Attack Analysis

Attack Summary—Windows

Summarize your findings from your reports when analyzing the attack logs.

- The percentage of events with a high severity flag went from 6.9% to 20.2%
- The ratio of failed action to successful ones surprisingly decreased from 0.03 on the 24 to 0.0158 on the 25 (Day of the Attack)
- The number of events in general on the 25 did increase by 1189

Attack Summary—Windows

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- The Alert for failed windows activities was set for 15 in an hour, this would trigger at 8 am on the 25th with 35 failed activities
- Alert for successful logins was set for 40, this alert would trigger at 11:00 am when there were 196 successful logins
- Alert for deleted user accounts was set for 40, this alert would not have been triggered

Attack Summary—Windows

Summarize your findings from your dashboards when analyzing the attack logs.

- There was a spike in events where an attempt was made to lock a user account from 12:00 am to 3:00 am on the 25th
- suspicious amount of attempts to reset account passwords were made from 8:00 am to 11:00 am on the 25th
- suspiciously high user activity was reported from user_a, user_k, and user_j
- The timecharts for users activities and windows activities line up to show that user_a was locking account, user_k was attempting to reset account passwords, and user_j was logging in to user accounts at a suspicious rate.

Attack Dashboard Screenshots 24th

Windows Server Monitoring
Actions ▾
Edit
Global Time Range
Mar 23, 2020 8:00 P... ▾
Number Of Users
user_b
user_d
user_c
user_e
user_h
user_l
user_a
user_m
user_i
user_f
Action Totals
500
250
count
A c...ted
A lo...tials
A pr...lled
A pr...ited
A u...ged
A u...ted
A u...ted
A u... out
An ... on
An ...ord
Do...ged
Spe...gon
Syst...unt
Syst...unt
The ...red
signature
count
Windows Account Activity
40
20
12:00 AM Tue Mar 24 2020
2:00 AM
4:00 AM Tue Mar 24
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_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 changed
A user account was created
A user account was deleted
A user account was locked out
▲ 1/2 ▼
User Activity
50
25
12:00 AM Tue Mar 24 2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM Tue Mar 24
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
2:00 PM
3:00 PM
4:00 PM
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
10:00 PM
11:00 PM
_time
Domain_A\user_b
Domain_A\user_c
Domain_A\user_h
Domain_A\user_i
Domain_A\user_j
Domain_A\user_k
user_a
user_b
user_c
user_d
user_e
▲ 1/3 ▼

Windows DashBoard Day of Attack

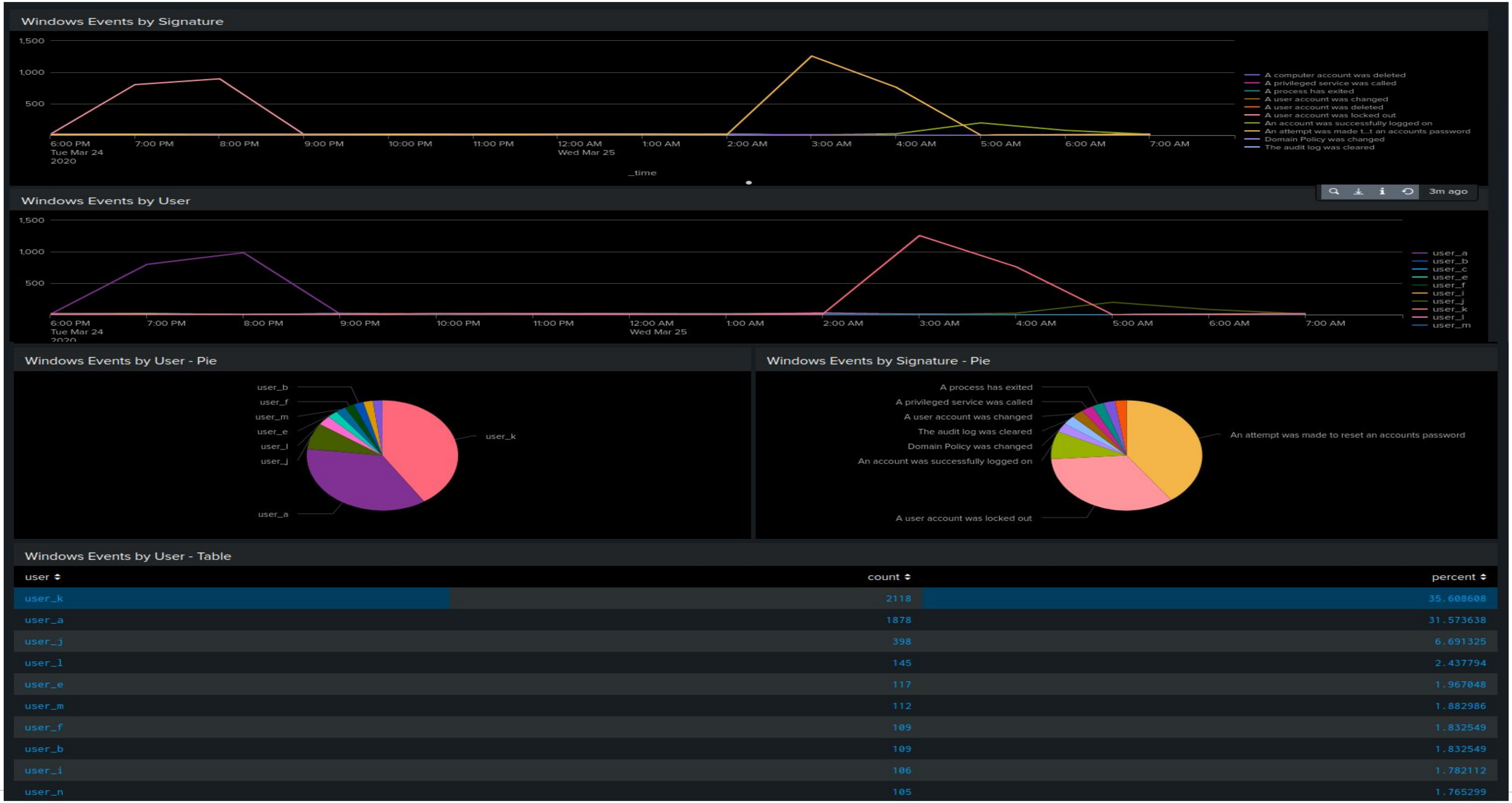
Windows Server Monitoring

Global Time Range

Mar 23, 2020 8:00 P...

Actions
Edit
Save
Number Of Users
user_m
user_e
user_l
user_j
user_a
user_k
Action Totals
4K
2K
count
count
A c...ted
A lo...tials
A pr...lled
A pr...ited
A us...ged
A us...ted
A us...ted
A us... out
An ... on
An ...ord
Do...ged
Spe...gon
Syst...unt
Syst...unt
The ...red
signature
Windows Account Activity
2K
1K
12:00 AM Tue Mar 24 2020
4:00 AM Tue Mar 24
8:00 AM
12:00 PM
4:00 PM
8:00 PM
12:00 AM
4:00 AM Wed Mar 25
8:00 AM
12:00 PM
4:00 PM
8:00 PM
12:00 AM
4:00 AM Thu Mar 26
8:00 AM
12:00 PM
4:00 PM
8:00 PM
_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 changed
A user account was created
A user account was deleted
A user account was locked out
1/2
User Activity
2K
1K
12:00 AM Wed Mar 25 2020
2:00 AM
4:00 AM Wed Mar 25
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM Thu Mar 26
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
Domain_A\user_d
Domain_A\user_e
Domain_A\user_f
Domain_A\user_g
Domain_A\user_m
Domain_A\user_n
user_a
user_b
user_c
user_d
user_e
1/3

Screenshots of Attack Logs


Windows Events by Signature
1,500
1,000
500
6:00 PM
Tue Mar 24
2020
7:00 PM
8:00 PM
9:00 PM
10:00 PM
11:00 PM
12:00 AM
Wed Mar 25
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was successfully logged on
An attempt was made t...t an accounts password
Domain Policy was changed
The audit log was cleared
3m ago
Windows Events by User
1,500
1,000
500
6:00 PM
Tue Mar 24
2020
7:00 PM
8:00 PM
9:00 PM
10:00 PM
11:00 PM
12:00 AM
Wed Mar 25
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
user_a
user_b
user_c
user_e
user_f
user_i
user_j
user_k
user_l
user_m
Windows Events by User - Pie
user_b
user_f
user_m
user_e
user_l
user_j
user_k
user_a
Windows Events by Signature - Pie
A process has exited
A privileged service was called
A user account was changed
The audit log was cleared
Domain Policy was changed
An account was successfully logged on
An attempt was made to reset an accounts password
A user account was locked out

Windows Events by User - Table

user ⇕	count ⇕	percent ⇕
user_k	2118	35.608608
user_a	1878	31.573638
user_j	398	6.691325
user_l	145	2.437794
user_e	117	1.967048
user_m	112	1.882986
user_f	109	1.832549
user_b	109	1.832549
user_i	106	1.782112
user_n	105	1.765299

Attack Summary—Apache (Reports)

- Post requests (ex: logging onto a website, making a comment, uploading a document) increased from 1% of HTTP methods used to 29.4%.
- 404 response codes increased from 2.1% of requests to 15% of requests.
- 304 responses went down from 4.45% to 0.8%
- There was no significant difference in the referrer domains used.

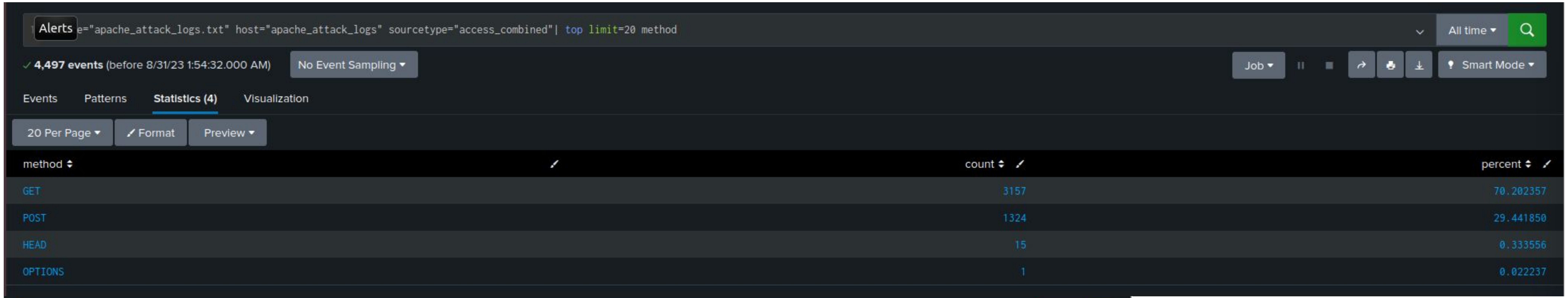
Attack Summary—Apache (Alerts)

- There was a suspicious spike in international traffic around 8:00PM that would've set off our alert. There is no need to change the threshold since activity for the rest of the day was within the established baseline.
- Also at 8:00PM HTTP POST request activity spiked to 1,296 requests in an hour. There is no need to change the threshold of 10 requests in an hour as the activity for the rest of the day was within the set baseline of 0-8 requests an hour.

Attack Summary—Apache (Dashboards)

- The number of GET requests to the server spikes at 6:00PM with a total of 729 requests. The GET requests at 5:00PM and 7:00PM were below the established threshold. The number of POST requests spikes at 8:00PM with a total of 1296 requests. The POST requests at 7:00PM and 9:00PM are below the established threshold.
- Activity within Ukraine spikes on the day of the attack, mostly in the cities of Kiev and Kharkiv. Activity from Kiev spikes from 30 to 439. In Kharkiv it spikes from 35 to 432.
- Based off this information it can be inferred that attackers from Ukraine attempted a brute force attack on the website between the hours of 7:00 and 9:00PM.

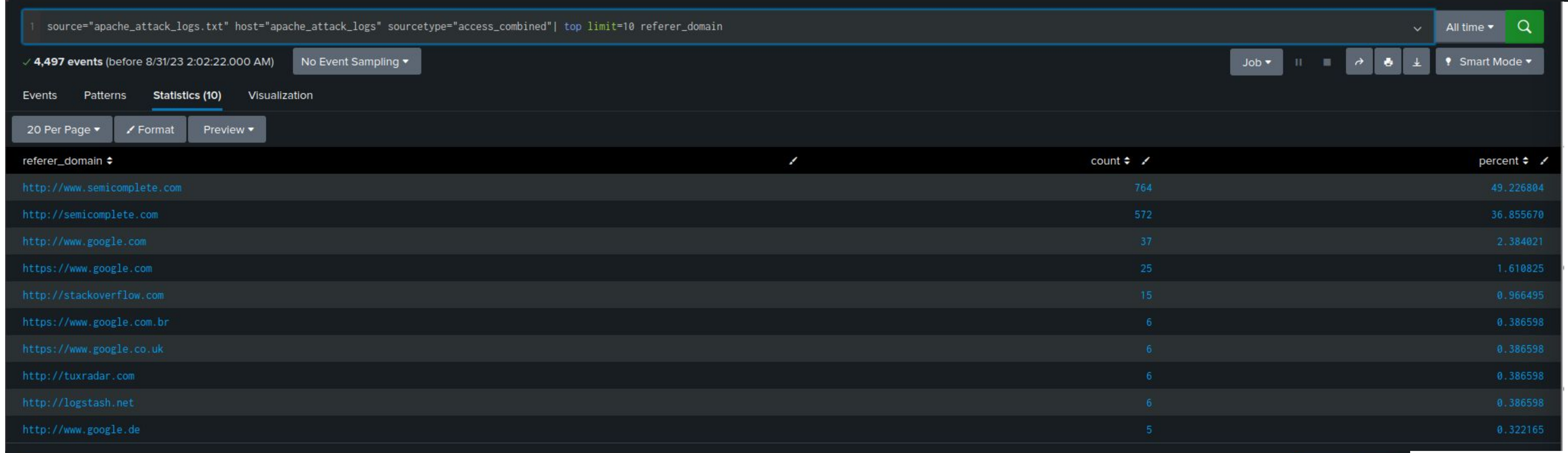
Screenshots of Attack Logs



```
e="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined"| top limit=20 method
```

✓ **4,497 events** (before 8/31/23 1:54:32.000 AM) No Event Sampling

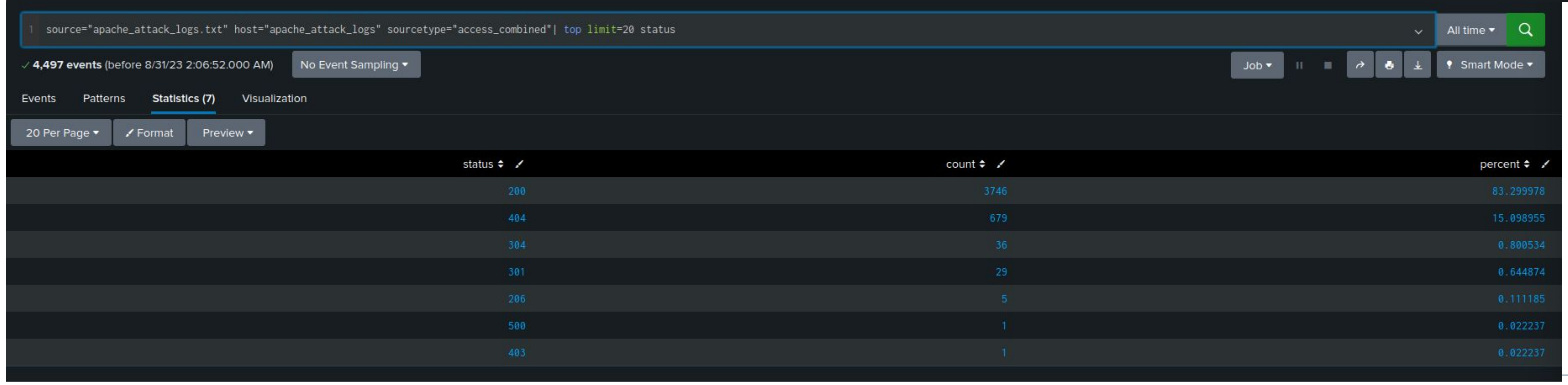
method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237



```
source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ **4,497 events** (before 8/31/23 2:02:22.000 AM) No Event Sampling

referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

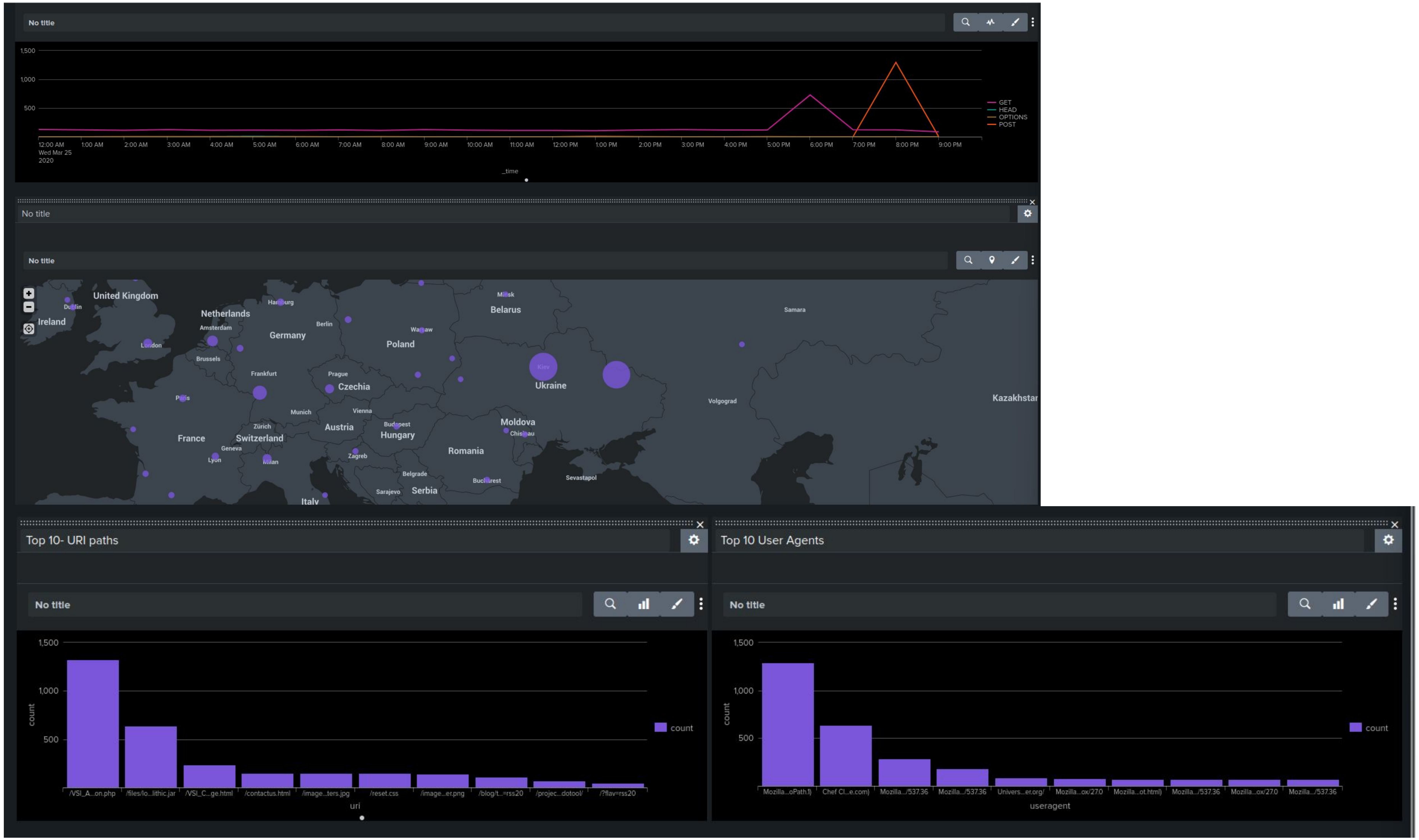


```
source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined"| top limit=20 status
```

✓ **4,497 events** (before 8/31/23 2:06:52.000 AM) No Event Sampling

status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?

  It looks like an attack happened with the attack coming from Ukraine, potential brute force or cross site scripting.

- To protect VSI from future attacks, what future mitigations would you recommend?

Set a limit for failed logins so that it times out for them or temporarily blocking them if they continuously fail to login. Implemented a Web Application Firewall that then you could potentially consider blocking certain IP addresses coming from Ukraine this would help with cross site scripting as well. Also ensuring strong passwords are used.