# Defensive Security Project
# by: The Dream Team

# Table of Contents

This document contains the following resources:

01

**Monitoring Environment**

02

**Attack Analysis**

03

**Project Summary & Future Mitigations**

# Monitoring Environment

# Scenario

- SOC analysts at Virtual Space Industries (VSI) which designs virtual-reality programs for businesses which designs virtual-reality programs for businesses.
- VSI hear rumors the a competitor, JobeCorp, may launch cyberattacks to disrupt VSI’s businesses
- As SOC analysts, we were tasked with using Splunk to monitor against potential attacks on VSI’s systems and applications
- VSI products that we were tasked with monitoring include an administrative webpage, an Apache web server, and a Window’s OS
- We reviewed logs from the Windows Server and the Apache Server

# Logs Analyzed

1 Windows Logs

This server contains intellectual property of VSI's next-generation virtual reality programs

2 Apache Logs

This server is used for VSI's main public-facing website, vsi-company.com

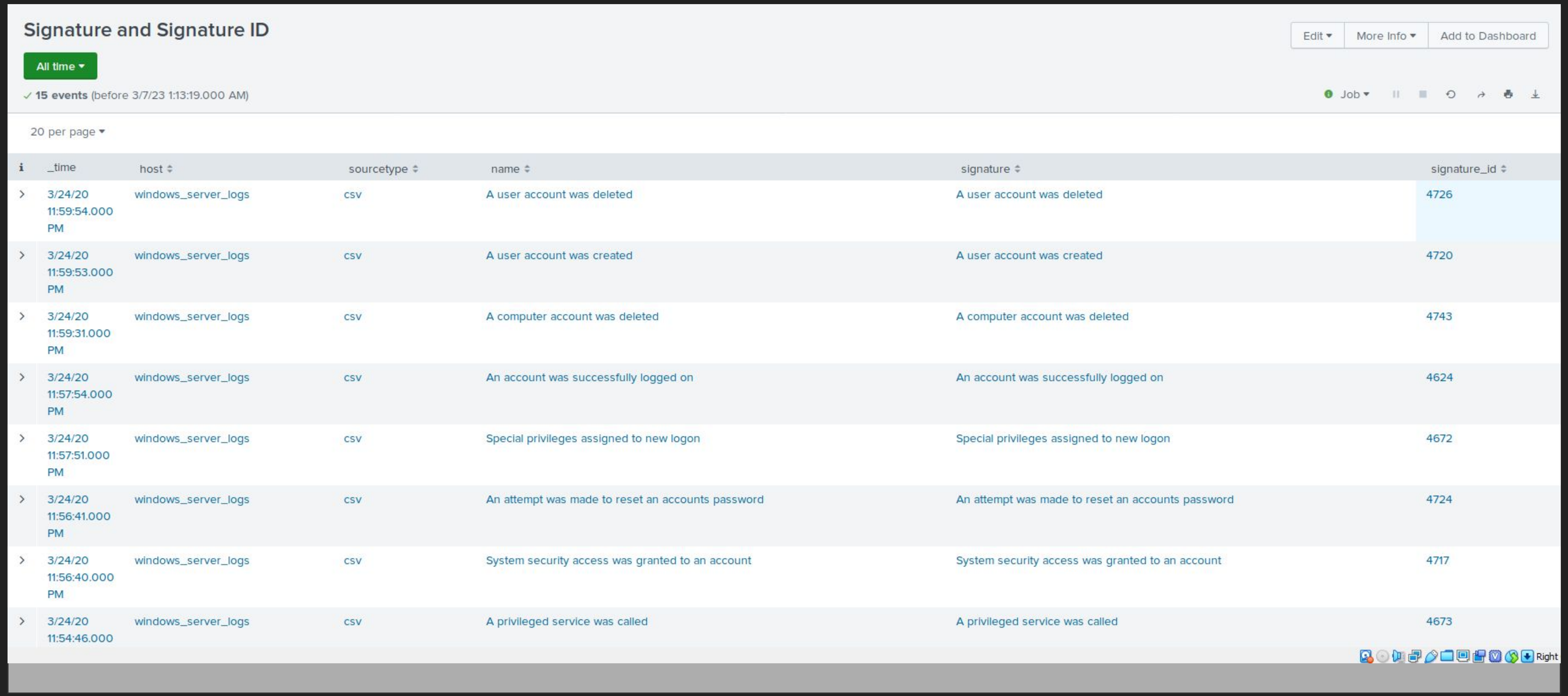
# Windows Logs

# Reports—Windows

Designed the following Reports:

| Report Name | Report Description |
|---|---|
| Signatures and associated signature IDs | To view reports that show the ID number associated with the specific signature for Windows activity. |
| Severity Levels Count and Percentage | To allow VSI to quickly understand the severity levels of the Windows logs being viewed. |
| Comparison Between Success and Failure | This report will allow VSI to monitor if there is a suspicious level of failed activities on their server. |

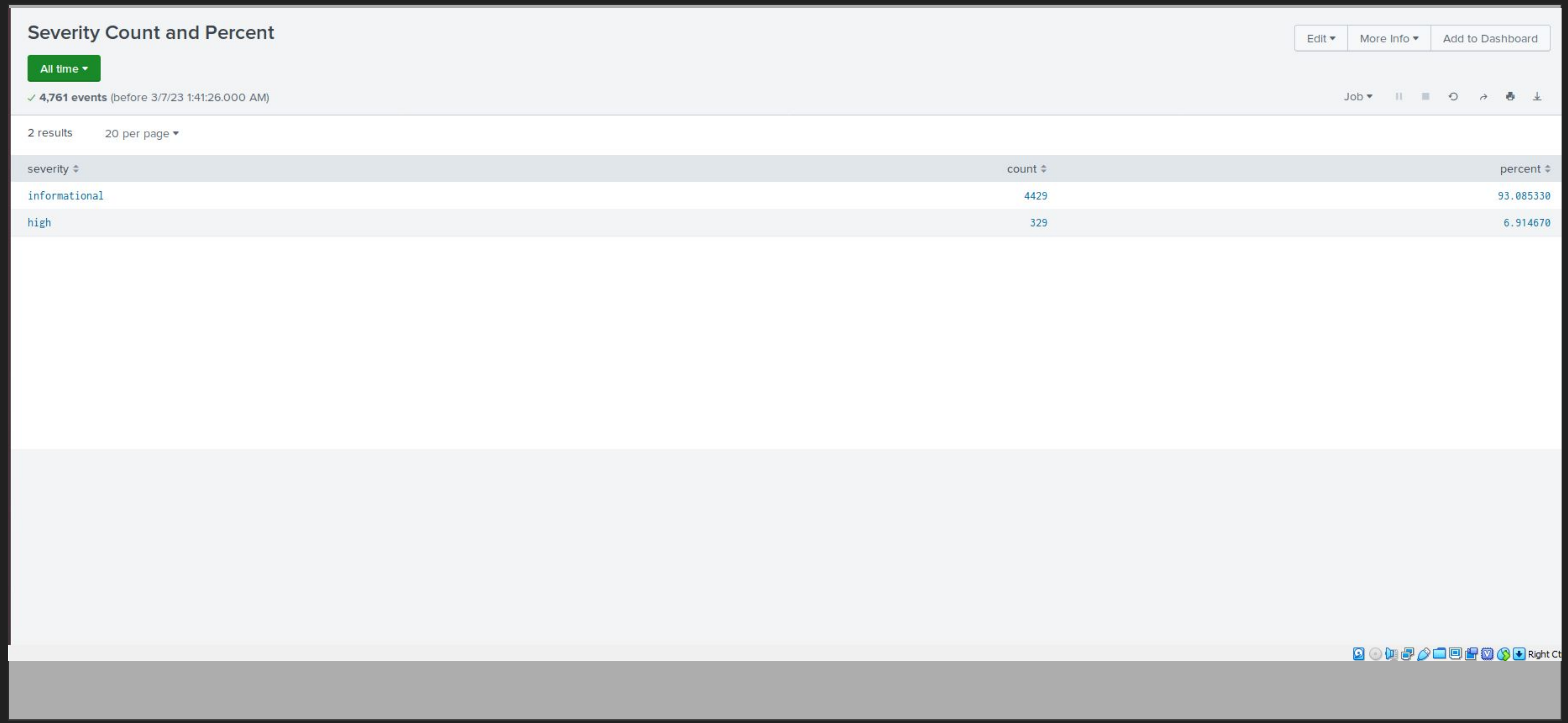
# Images of Reports—Windows



## Signature and Signature ID

✓ **15 events** (before 3/7/23 1:13:19.000 AM)

| i | _time | host | sourcetype | name | signature | signature_id |
|---|---|---|---|---|---|---|
| > | 3/24/20 11:59:54.000 PM | windows_server_logs | csv | A user account was deleted | A user account was deleted | 4726 |
| > | 3/24/20 11:59:53.000 PM | windows_server_logs | csv | A user account was created | A user account was created | 4720 |
| > | 3/24/20 11:59:31.000 PM | windows_server_logs | csv | A computer account was deleted | A computer account was deleted | 4743 |
| > | 3/24/20 11:57:54.000 PM | windows_server_logs | csv | An account was successfully logged on | An account was successfully logged on | 4624 |
| > | 3/24/20 11:57:51.000 PM | windows_server_logs | csv | Special privileges assigned to new logon | Special privileges assigned to new logon | 4672 |
| > | 3/24/20 11:56:41.000 PM | windows_server_logs | csv | An attempt was made to reset an accounts password | An attempt was made to reset an accounts password | 4724 |
| > | 3/24/20 11:56:40.000 PM | windows_server_logs | csv | System security access was granted to an account | System security access was granted to an account | 4717 |
| > | 3/24/20 11:54:46.000 | windows_server_logs | csv | A privileged service was called | A privileged service was called | 4673 |

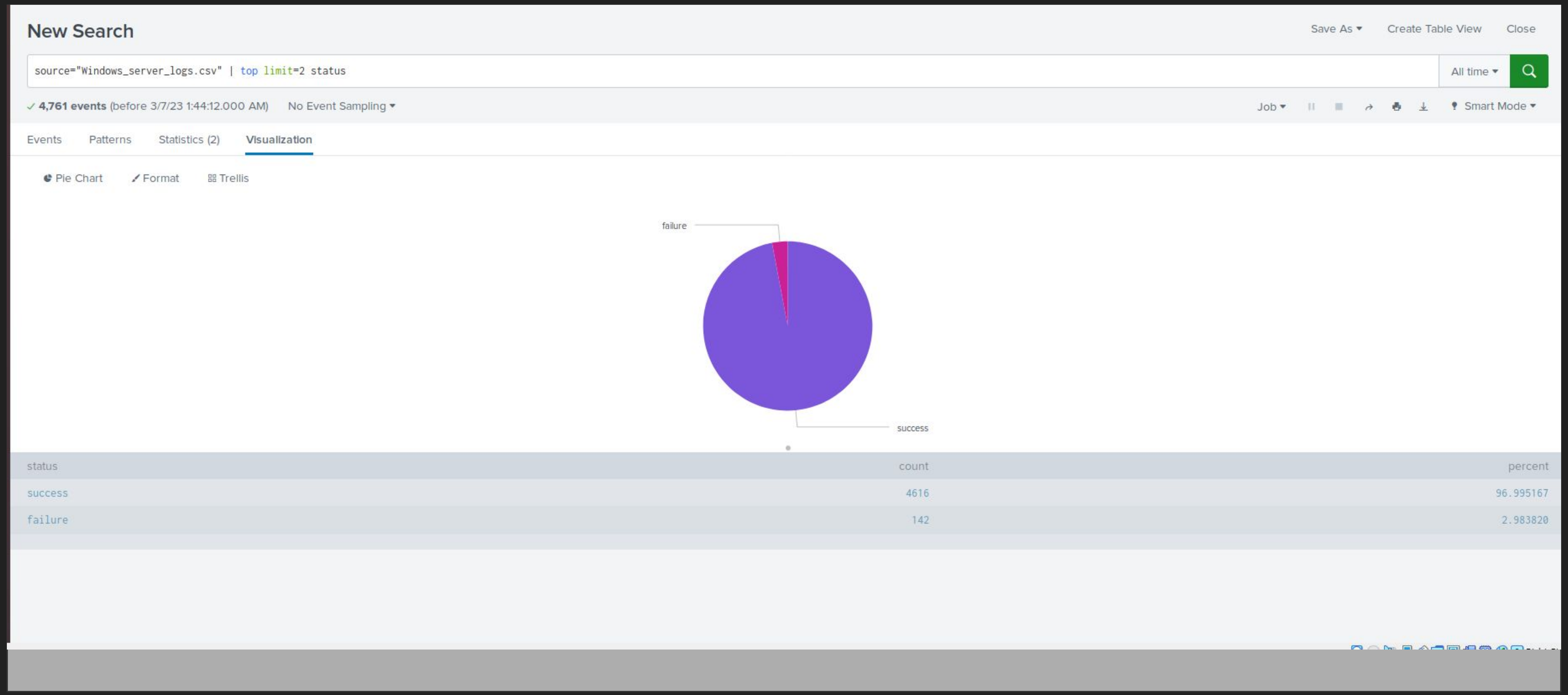


## Severity Count and Percent

✓ **4,761 events** (before 3/7/23 1:41:26.000 AM)

2 results

| severity | count | percent |
|---|---|---|
| informational | 4429 | 93.085330 |
| high | 329 | 6.914670 |



## New Search

```
source="Windows_server_logs.csv" | top limit=2 status
```

✓ **4,761 events** (before 3/7/23 1:44:12.000 AM) No Event Sampling ▾

| status | count | percent |
|---|---|---|
| success | 4616 | 96.995167 |
| failure | 142 | 2.983820 |

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Failed Windows Activity | Number of failed Windows activities by hour. | 11 | 20 |

**JUSTIFICATION: We took the average count by hour and made that figure our baseline. We then found the standard deviation of the counts and did the average plus two times the standard deviation to get our threshold.**

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| An Account Was Successfully Logged On | Alerts when an inordinate amount of logins occur in an hour. | 27 | 39 |

**JUSTIFICATION: We took the average count by hour and made that figure our baseline. We then found the standard deviation of the counts and did the average plus two times the standard deviation to get our threshold.**

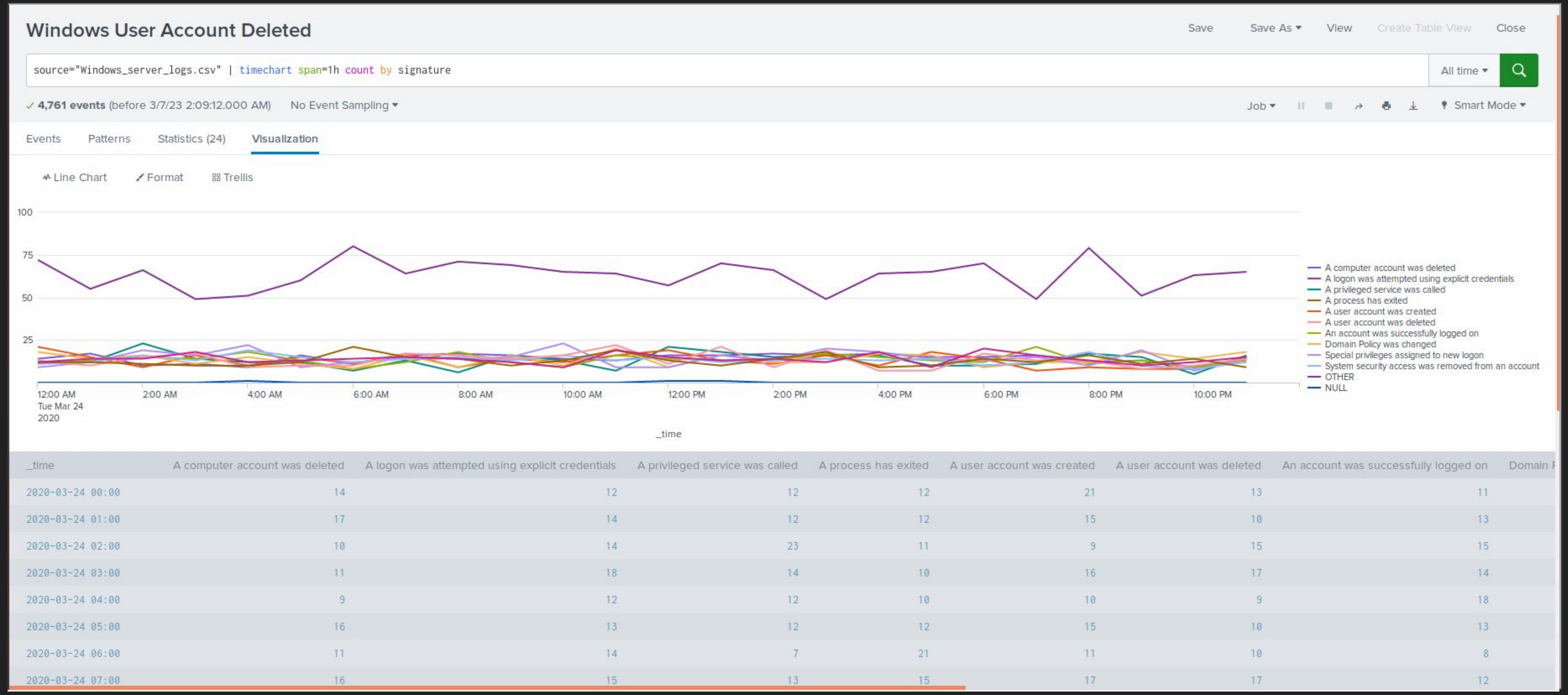
# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| User Accounts Deleted | Alerts when an inordinate amount of user accounts are deleted in an hour. | 27 | 44 |

**JUSTIFICATION: We took the average count by hour and made that figure our baseline. We then found the standard deviation of the counts and did the average plus two times the standard deviation to get our threshold.**

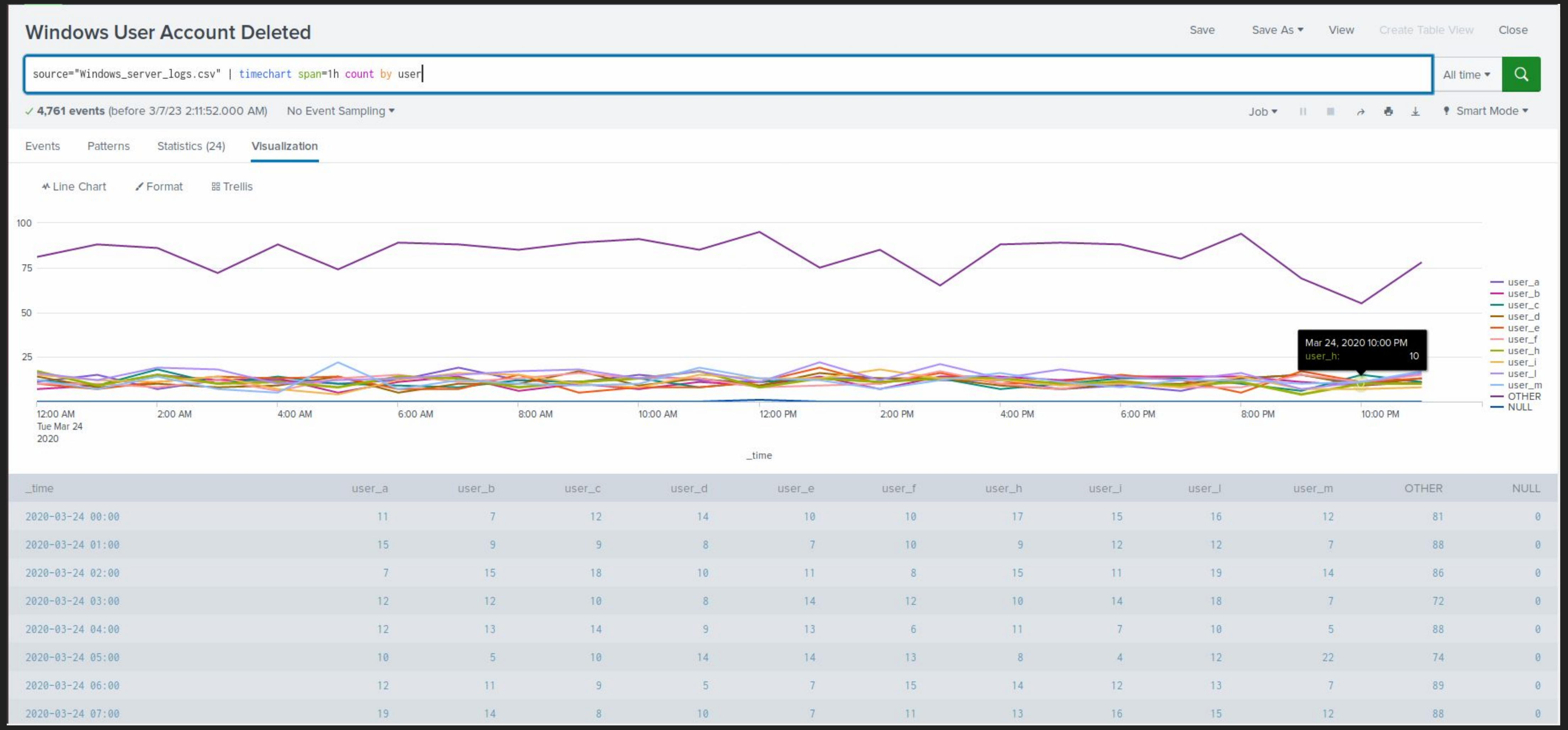
# Dashboards—Windows


Windows User Account Deleted
Save
Save As ▾
View
Create Table View
Close
All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (24)
Visualization
Line Chart
Format
Trellis
100
75
50
25
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
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 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

```
source="Windows_server_logs.csv" | timechart span=1h count by signature
```

✓ **4,761 events** (before 3/7/23 2:09:12.000 AM) No Event Sampling ▾

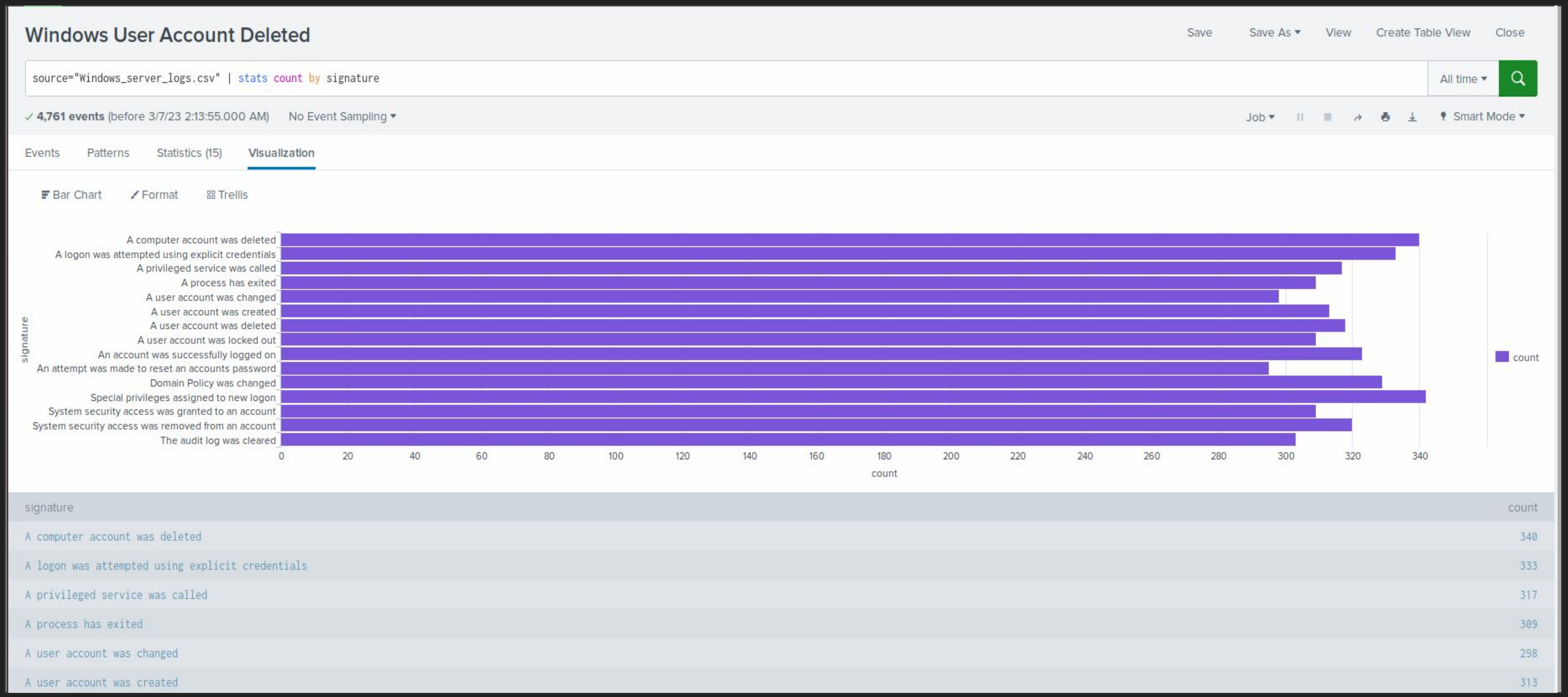
| _time | A computer account was deleted | A logon was attempted using explicit credentials | A privileged service was called | A process has exited | A user account was created | A user account was deleted | An account was successfully logged on | Domain |
|---|---|---|---|---|---|---|---|---|
| 2020-03-24 00:00 | 14 | 12 | 12 | 12 | 21 | 13 | 11 | |
| 2020-03-24 01:00 | 17 | 14 | 12 | 12 | 15 | 10 | 13 | |
| 2020-03-24 02:00 | 10 | 14 | 23 | 11 | 9 | 15 | 15 | |
| 2020-03-24 03:00 | 11 | 18 | 14 | 10 | 16 | 17 | 14 | |
| 2020-03-24 04:00 | 9 | 12 | 12 | 10 | 10 | 9 | 18 | |
| 2020-03-24 05:00 | 16 | 13 | 12 | 12 | 15 | 10 | 13 | |
| 2020-03-24 06:00 | 11 | 14 | 7 | 21 | 11 | 10 | 8 | |
| 2020-03-24 07:00 | 16 | 15 | 13 | 15 | 17 | 17 | 12 | |



```
source="Windows_server_logs.csv" | timechart span=1h count by user
```

✓ **4,761 events** (before 3/7/23 2:11:52.000 AM) No Event Sampling ▾

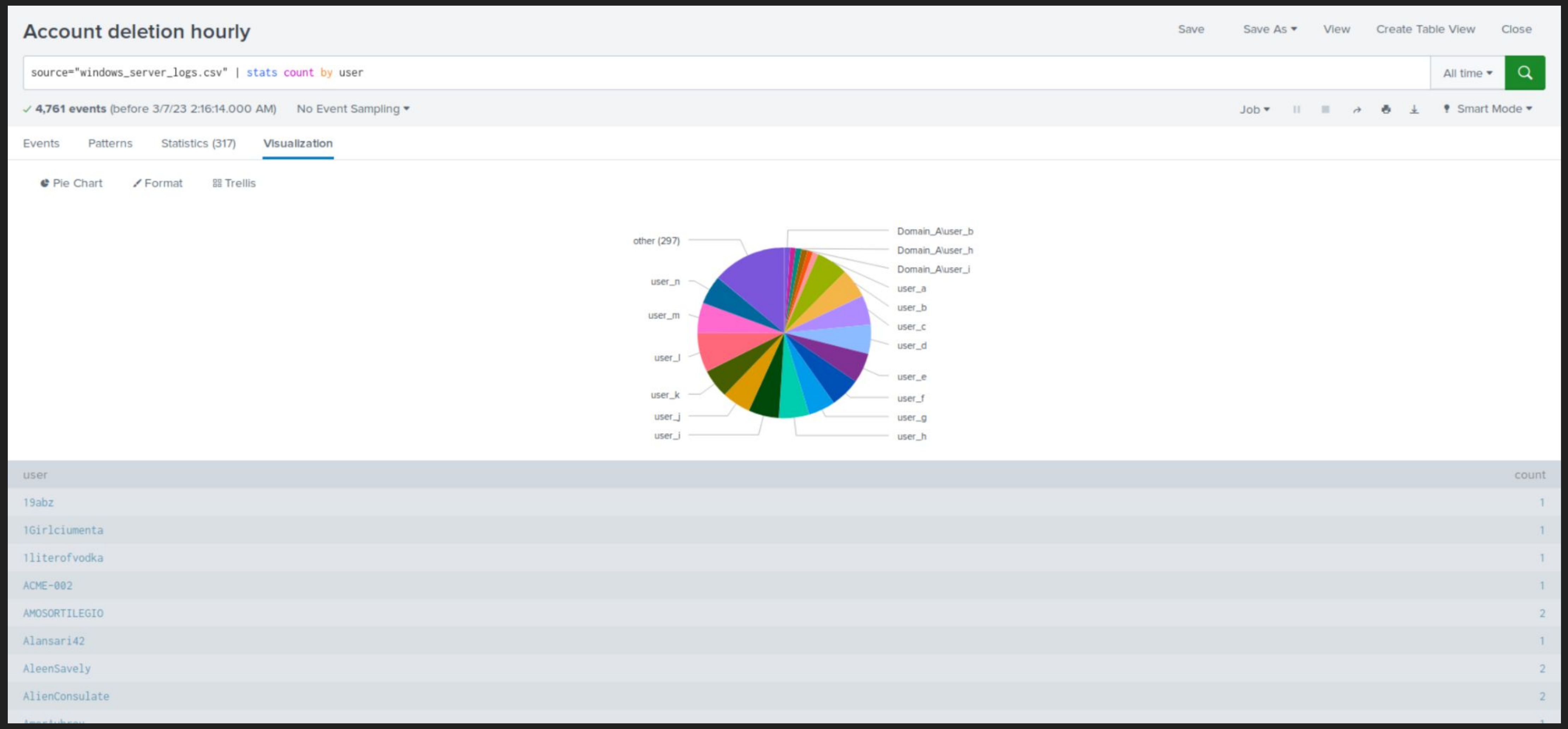
| _time | user_a | user_b | user_c | user_d | user_e | user_f | user_h | user_i | user_l | user_m | OTHER | NULL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2020-03-24 00:00 | 11 | 7 | 12 | 14 | 10 | 10 | 17 | 15 | 16 | 12 | 81 | 0 |
| 2020-03-24 01:00 | 15 | 9 | 9 | 8 | 7 | 10 | 9 | 12 | 12 | 7 | 88 | 0 |
| 2020-03-24 02:00 | 7 | 15 | 18 | 10 | 11 | 8 | 15 | 11 | 19 | 14 | 86 | 0 |
| 2020-03-24 03:00 | 12 | 12 | 10 | 8 | 14 | 12 | 10 | 14 | 18 | 7 | 72 | 0 |
| 2020-03-24 04:00 | 12 | 13 | 14 | 9 | 13 | 6 | 11 | 7 | 10 | 5 | 88 | 0 |
| 2020-03-24 05:00 | 10 | 5 | 10 | 14 | 14 | 13 | 8 | 4 | 12 | 22 | 74 | 0 |
| 2020-03-24 06:00 | 12 | 11 | 9 | 5 | 7 | 15 | 14 | 12 | 13 | 7 | 89 | 0 |
| 2020-03-24 07:00 | 19 | 14 | 8 | 10 | 7 | 11 | 13 | 16 | 15 | 12 | 88 | 0 |


Windows User Account Deleted
Save
Save As ▾
View
Create Table View
Close
All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (15)
Visualization
Bar Chart
Format
Trellis
signature
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
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
Special privileges assigned to new logon
System security access was granted to an account
System security access was removed from an account
The audit log was cleared
0
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
320
340
count
count

```
source="Windows_server_logs.csv" | stats count by signature
```

✓ **4,761 events** (before 3/7/23 2:13:55.000 AM) No Event Sampling ▾

| signature | count |
|---|---|
| A computer account was deleted | 340 |
| A logon was attempted using explicit credentials | 333 |
| A privileged service was called | 317 |
| A process has exited | 309 |
| A user account was changed | 298 |
| A user account was created | 313 |

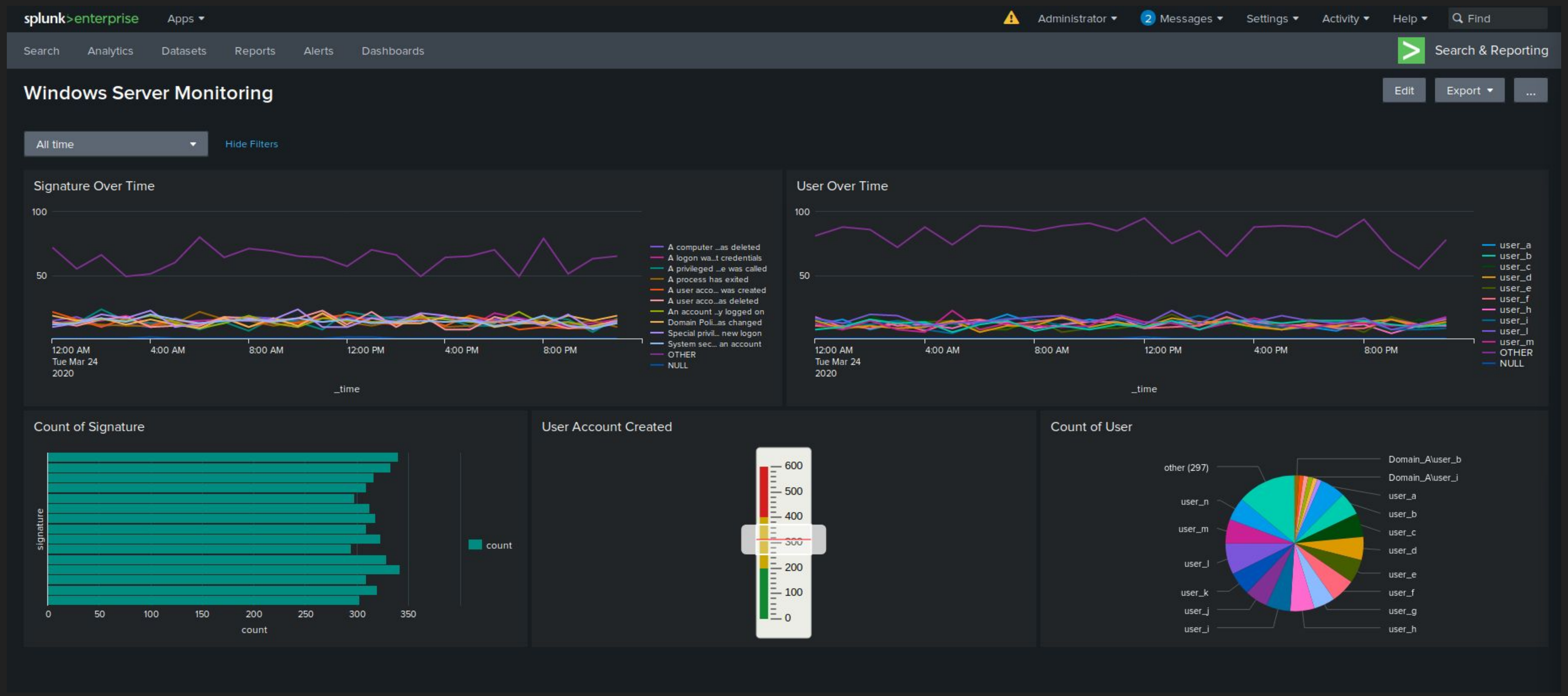


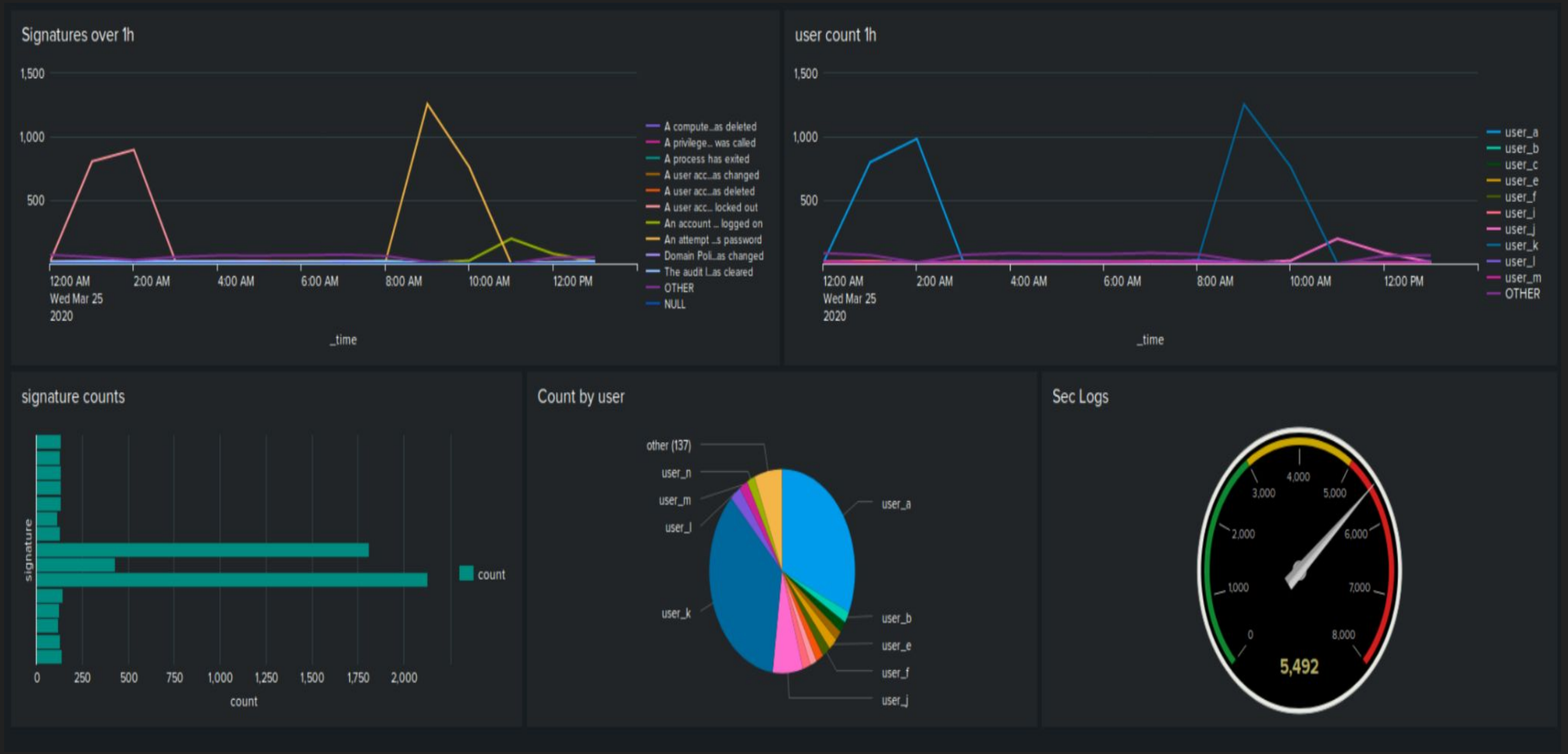
```
source="windows_server_logs.csv" | stats count by user
```

✓ **4,761 events** (before 3/7/23 2:16:14.000 AM) No Event Sampling ▾

| user | count |
|---|---|
| 19abz | 1 |
| 1Girlciumenta | 1 |
| 1literofvodka | 1 |
| ACME-002 | 1 |
| AMOSORTILEGIO | 2 |
| Alansari42 | 1 |
| AleenSavely | 2 |
| AlienConsulate | 2 |

# Dashboards—Windows





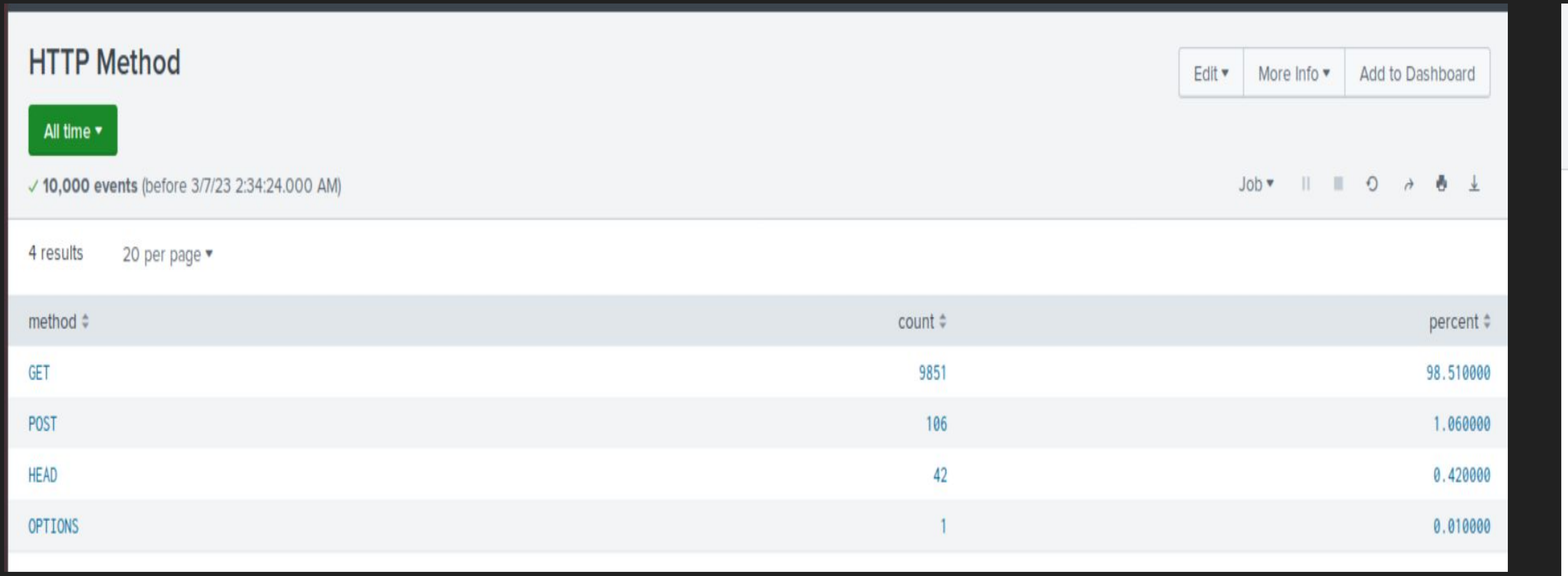
# Apache Logs

# Reports—Apache

Designed the following reports:

| Report Name | Report Description |
|---|---|
| HTTP Method | This will provide insight into the type of HTTP activity being requested against VSI's web server |
| Top 10 Domains | This will assist VSI with identifying suspicious referrers |
| Top HTTP Codes | This will provide insight into any suspicious levels of HTTP responses |

# Images of Reports—Apache

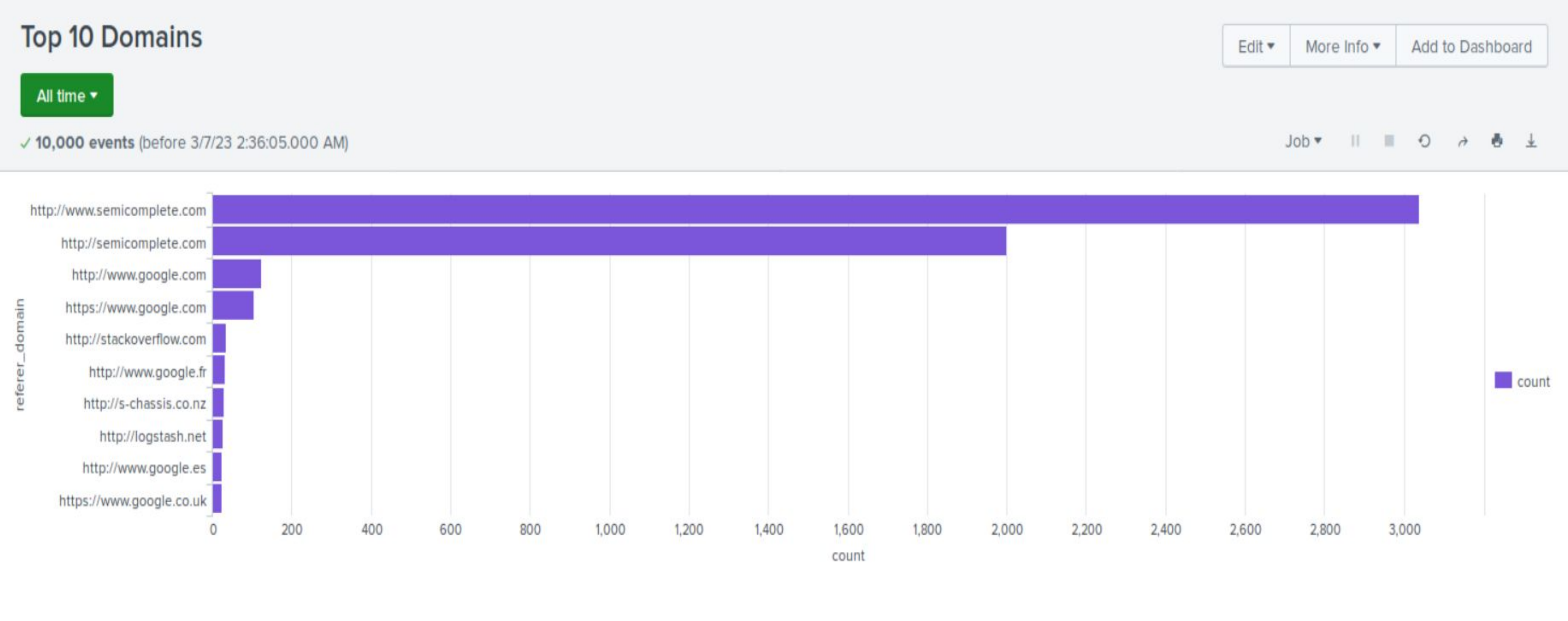


## HTTP Method

✓ **10,000 events** (before 3/7/23 2:34:24.000 AM)

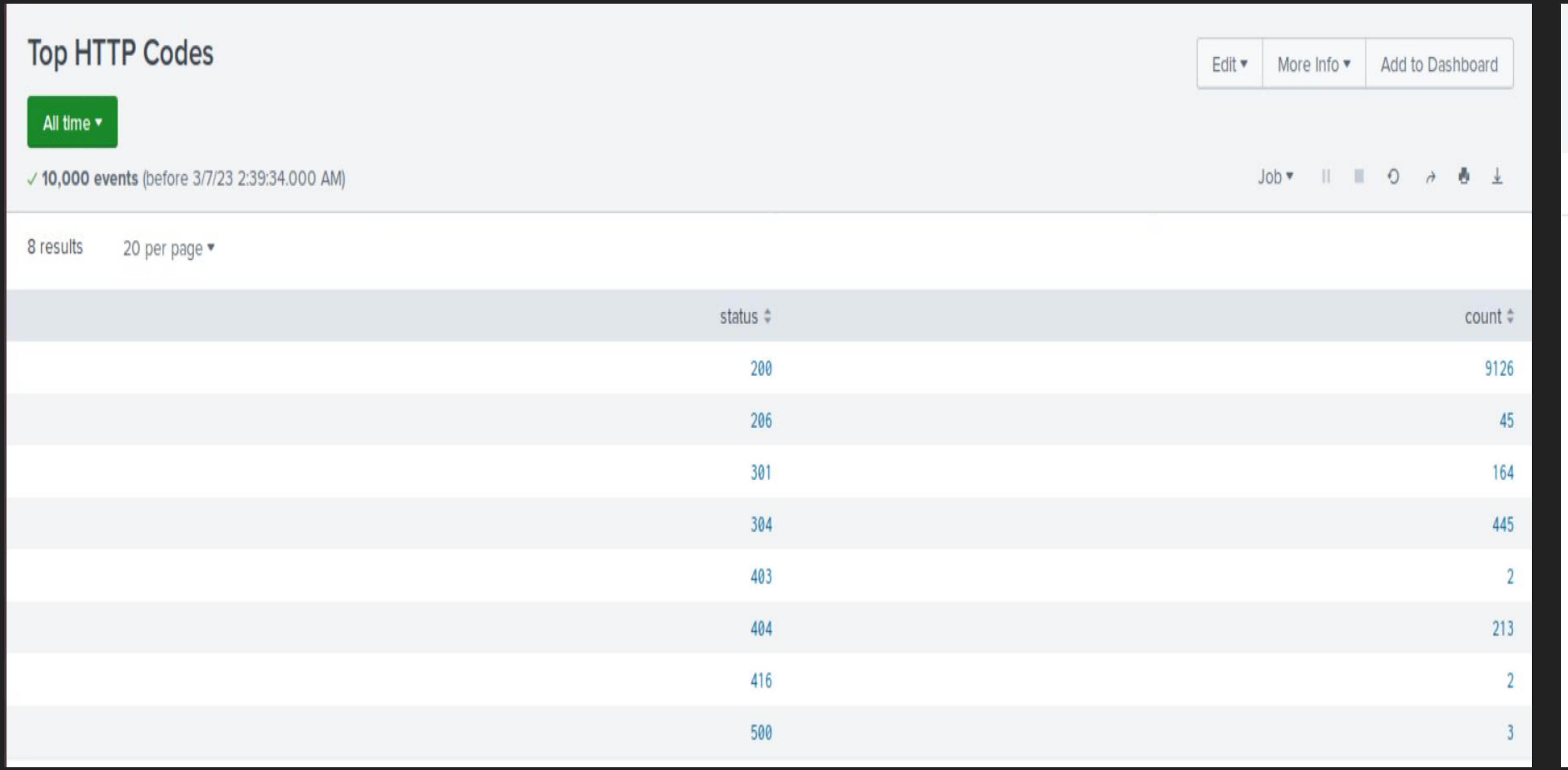
4 results   20 per page ▾

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



## Top 10 Domains

✓ **10,000 events** (before 3/7/23 2:36:05.000 AM)

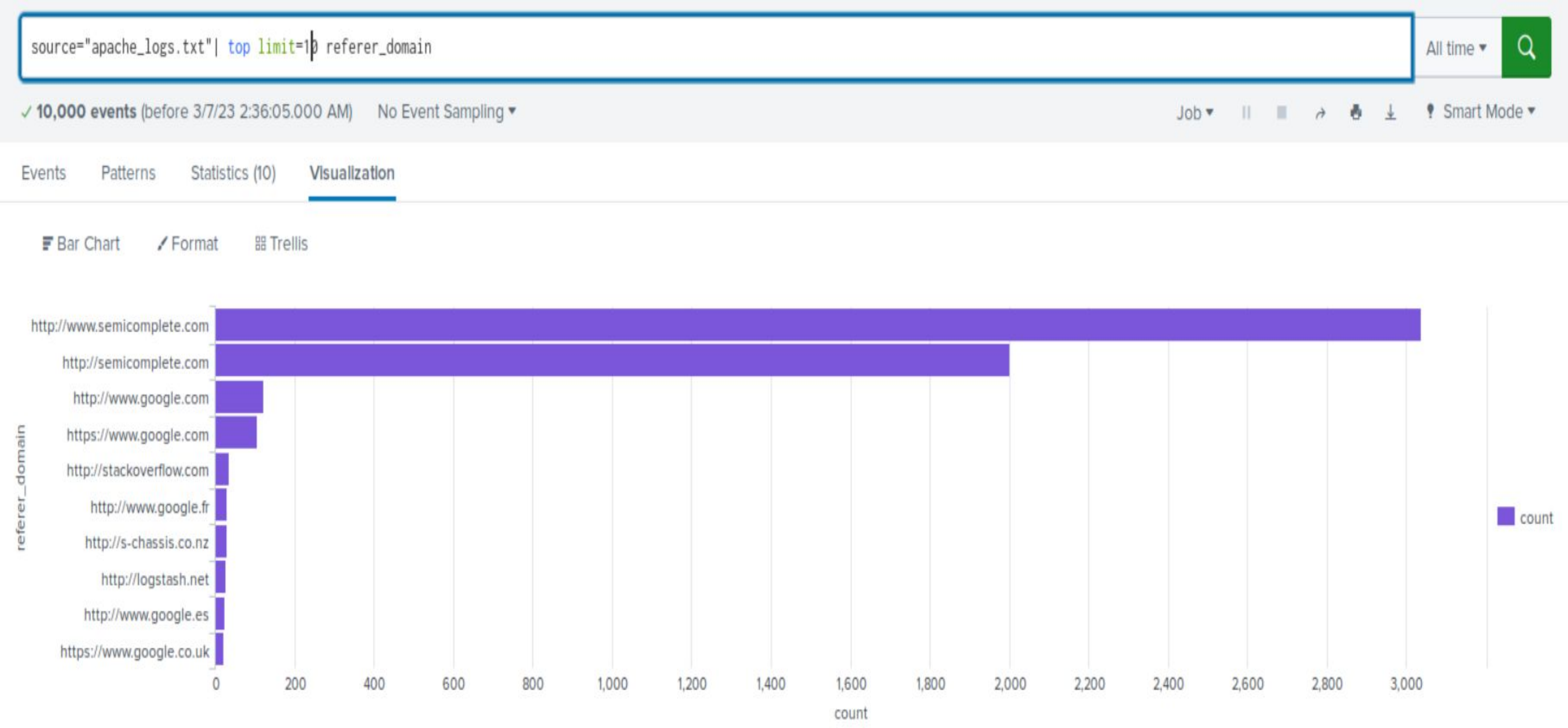


## Top HTTP Codes

✓ **10,000 events** (before 3/7/23 2:39:34.000 AM)

8 results   20 per page ▾

| 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
```

All time ▾

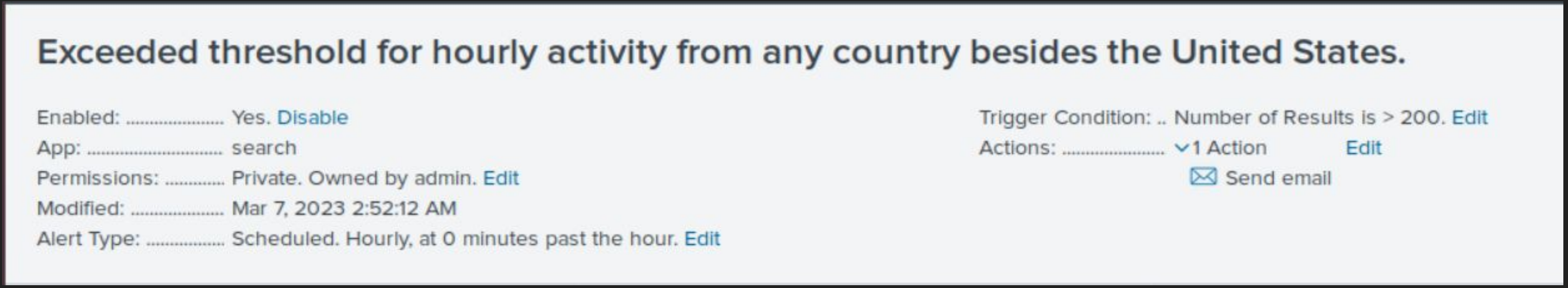
✓ **10,000 events** (before 3/7/23 2:36:05.000 AM)   No Event Sampling ▾

# Alerts—Apache

Designed the following alerts:

| **Alert Name** | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Exceeded threshold for hourly activity from any country besides the US | Alert emails SOC@VSI-company.com when threshold reached | 128 | 200 |

**JUSTIFICATION: Rough second standard deviation calculation to determine the threshold**



Exceeded threshold for hourly activity from any country besides the United States.

Enabled: ..................... Yes. Disable
App: ............................. search
Permissions: ............ Private. Owned by admin. Edit
Modified: ..................... Mar 7, 2023 2:52:12 AM
Alert Type: ................ Scheduled. Hourly, at 0 minutes past the hour. Edit

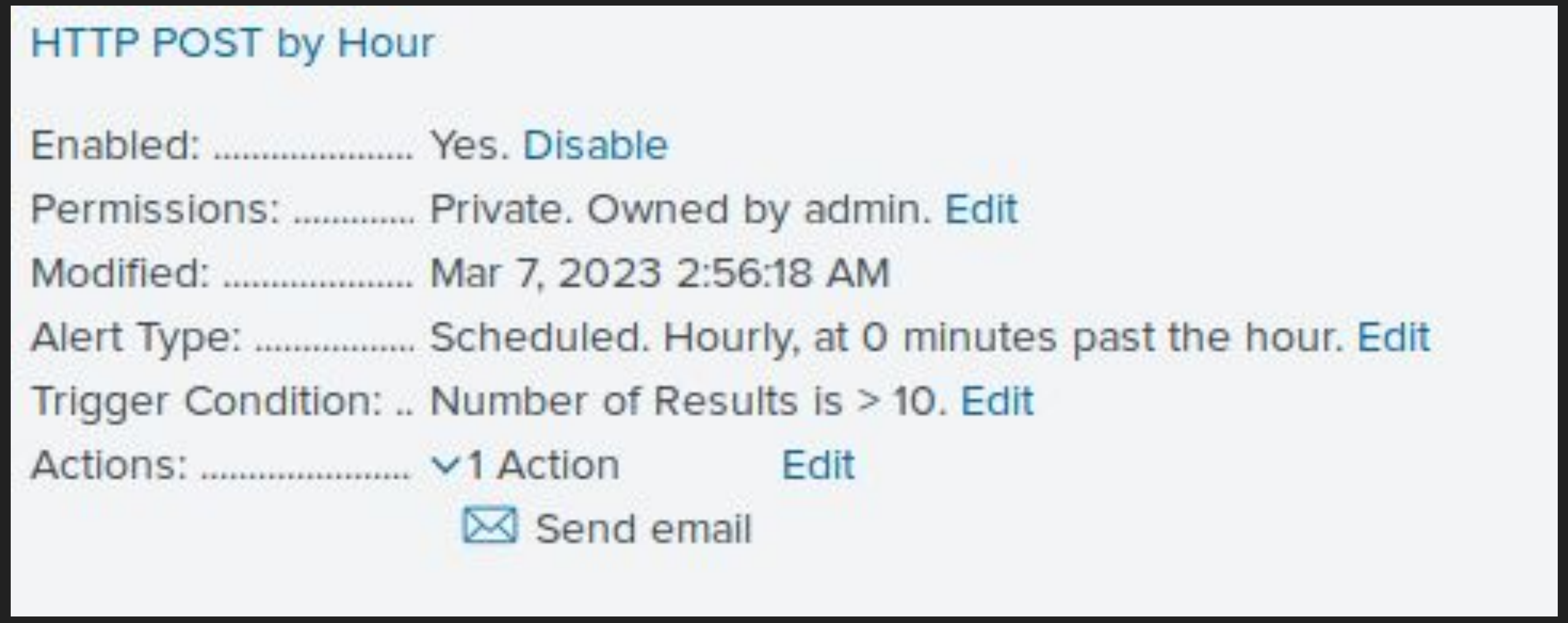
Trigger Condition: .. Number of Results is > 200. Edit
Actions: ..................... 1 Action Edit
Send email

# Alerts—Apache

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Abnormal amount of hourly HTTP POST requests | This alert will notify a VSI SOC Analyst if there are an abnormal amount of HTTP POST requests in an hour | 5 | 10 |

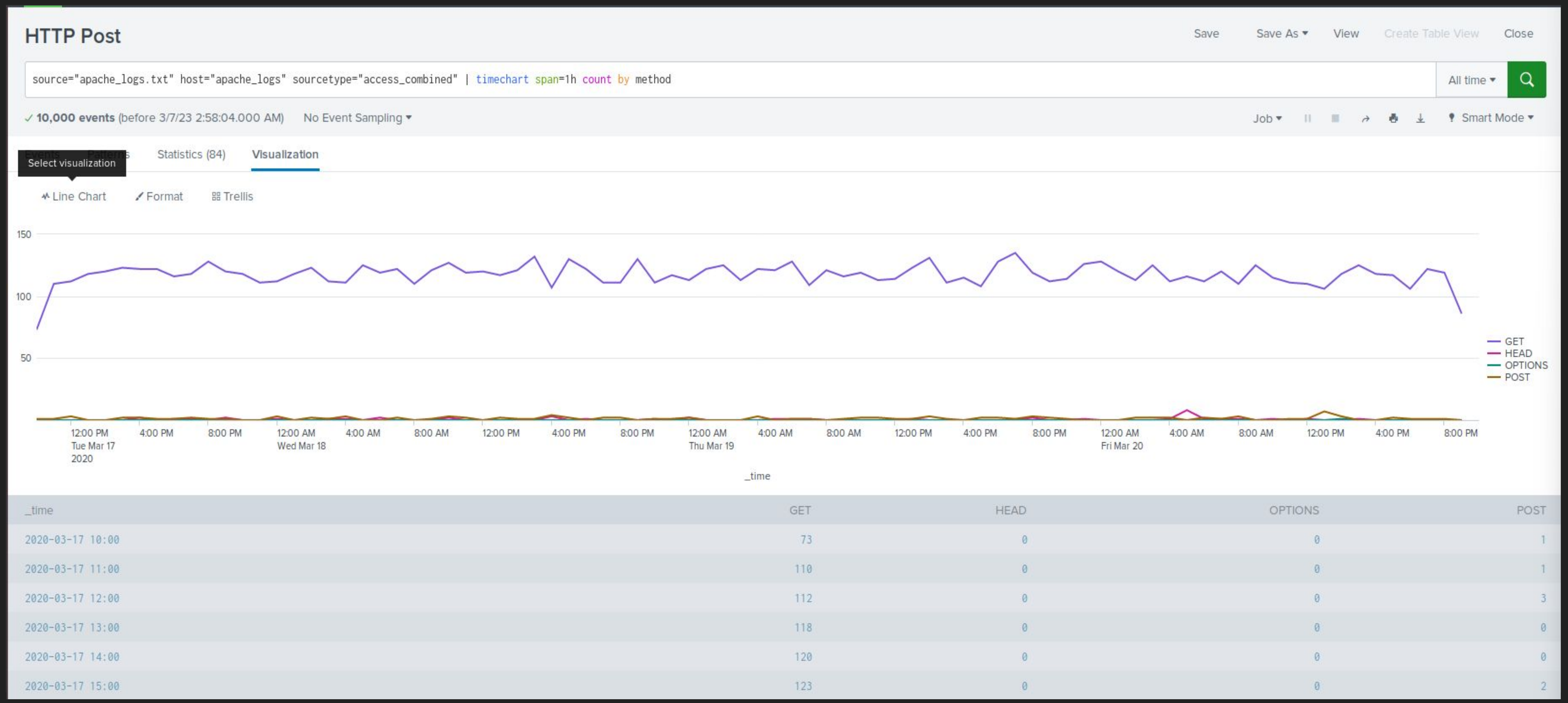
**JUSTIFICATION: Rough second standard deviation calculation to determine the threshold**



HTTP POST by Hour

Enabled: .................... Yes. Disable
Permissions: ............ Private. Owned by admin. Edit
Modified: .................... Mar 7, 2023 2:56:18 AM
Alert Type: ................ Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: .. Number of Results is > 10. Edit
Actions: ...................... 1 Action Edit
Send email

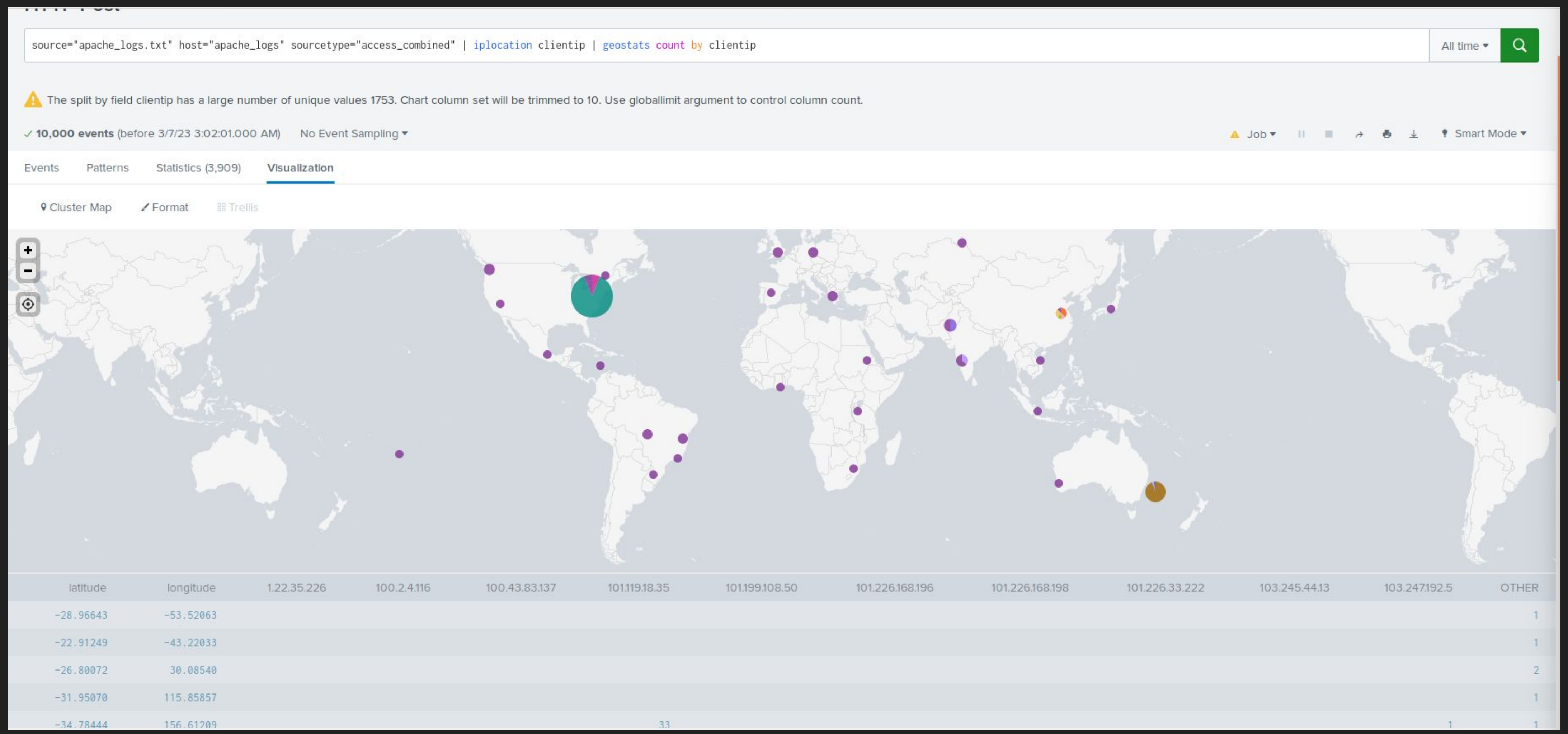
# Dashboards—Apache



```
source="apache_logs.txt" host="apache_logs" sourcetype="access_combined" | timechart span=1h count by method
```

✓ 10,000 events (before 3/7/23 2:58:04.000 AM) No Event Sampling ▾

| _time | GET | HEAD | OPTIONS | POST |
|---|---|---|---|---|
| 2020-03-17 10:00 | 73 | 0 | 0 | 1 |
| 2020-03-17 11:00 | 110 | 0 | 0 | 1 |
| 2020-03-17 12:00 | 112 | 0 | 0 | 3 |
| 2020-03-17 13:00 | 118 | 0 | 0 | 0 |
| 2020-03-17 14:00 | 120 | 0 | 0 | 0 |
| 2020-03-17 15:00 | 123 | 0 | 0 | 2 |

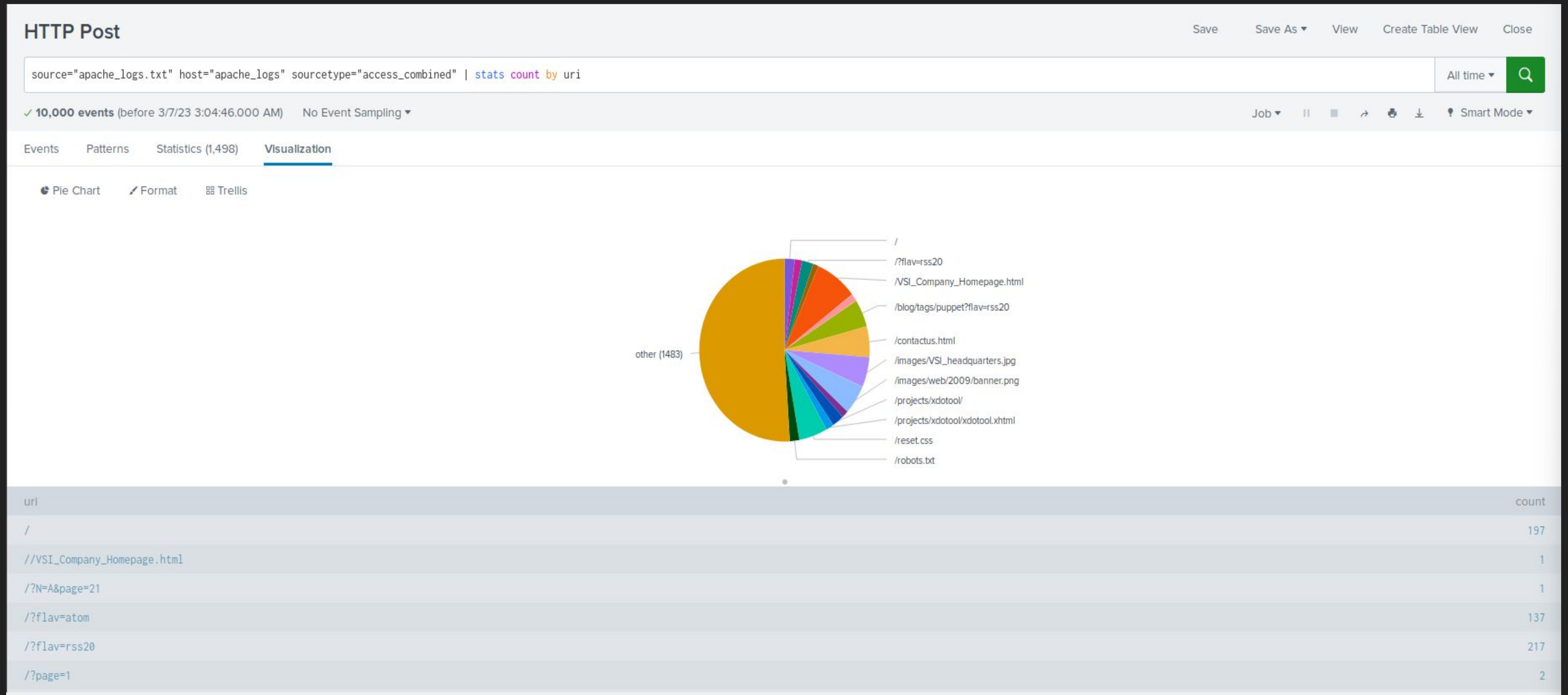


```
source="apache_logs.txt" host="apache_logs" sourcetype="access_combined" | iplocation clientip | geostats count by clientip
```

⚠ The split by field clientip has a large number of unique values 1753. Chart column set will be trimmed to 10. Use globallimit argument to control column count.

✓ 10,000 events (before 3/7/23 3:02:01.000 AM) No Event Sampling ▾

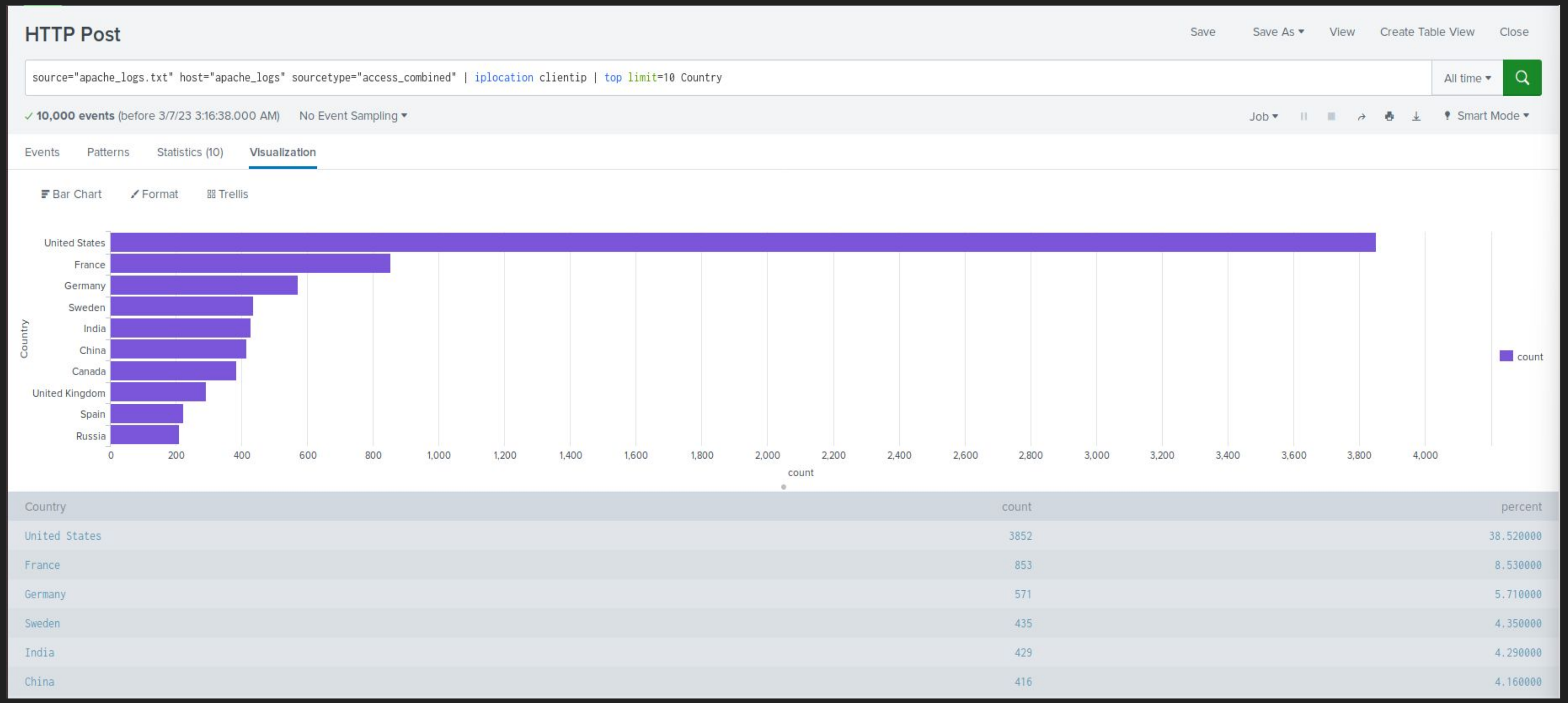
| latitude | longitude | 1.22.35.226 | 100.2.4.116 | 100.43.83.137 | 101.119.18.35 | 101.199.108.50 | 101.226.168.196 | 101.226.168.198 | 101.226.33.222 | 103.245.44.13 | 103.247.192.5 | OTHER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| -28.96643 | -53.52063 | | | | | | | | | | | 1 |
| -22.91249 | -43.22033 | | | | | | | | | | | 1 |
| -26.80072 | 30.08540 | | | | | | | | | | | 2 |
| -31.95070 | 115.85857 | | | | | | | | | | | 1 |
| -34.78444 | 156.61209 | | | | 33 | | | | | | 1 | 1 |



```
source="apache_logs.txt" host="apache_logs" sourcetype="access_combined" | stats count by uri
```

✓ 10,000 events (before 3/7/23 3:04:46.000 AM) No Event Sampling ▾

| uri | count |
|---|---|
| / | 197 |
| //VSI_Company_Homepage.html | 1 |
| /?N=A&page=21 | 1 |
| /?flav=atom | 137 |
| /?flav=rss20 | 217 |
| /?page=1 | 2 |

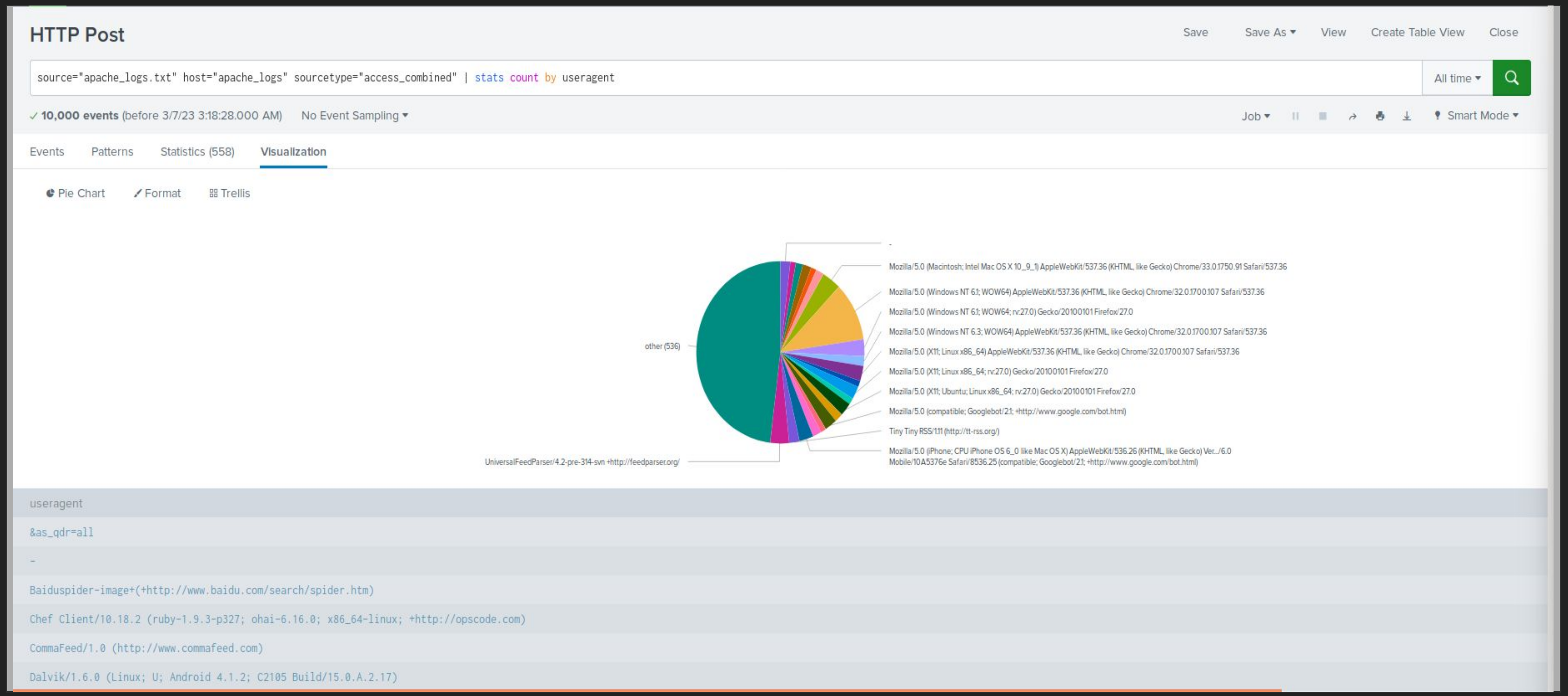


```
source="apache_logs.txt" host="apache_logs" sourcetype="access_combined" | iplocation clientip | top limit=10 Country
```

✓ 10,000 events (before 3/7/23 3:16:38.000 AM) No Event Sampling ▾

| Country | count | percent |
|---|---|---|
| United States | 3852 | 38.520000 |
| France | 853 | 8.530000 |
| Germany | 571 | 5.710000 |
| Sweden | 435 | 4.350000 |
| India | 429 | 4.290000 |
| China | 416 | 4.160000 |

# Dashboards—Apache

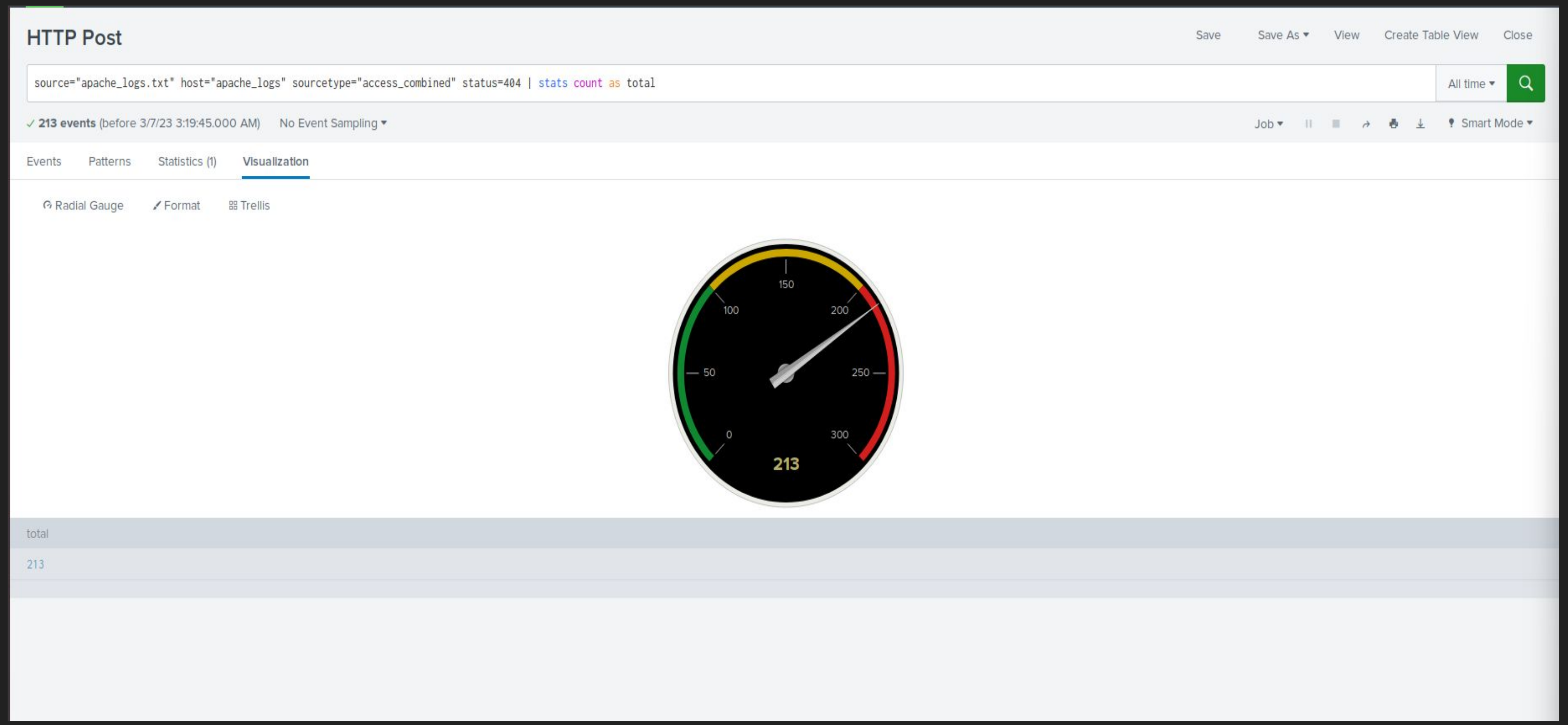

Save
Save As ▾
View
Create Table View
Close
All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (558)
Visualization
Pie Chart
Format
Trellis
-
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Ver.../6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
other (536)
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/

HTTP Post

```
source="apache_logs.txt" host="apache_logs" sourcetype="access_combined" | stats count by useragent
```

✓ **10,000 events** (before 3/7/23 3:18:28.000 AM) No Event Sampling ▾

| useragent |
|---|
| &as_qdr=all |
| - |
| Baiduspider-image+(+http://www.baidu.com/search/spider.htm) |
| Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com) |
| CommaFeed/1.0 (http://www.commafeed.com) |
| Dalvik/1.6.0 (Linux; U; Android 4.1.2; C2105 Build/15.0.A.2.17) |

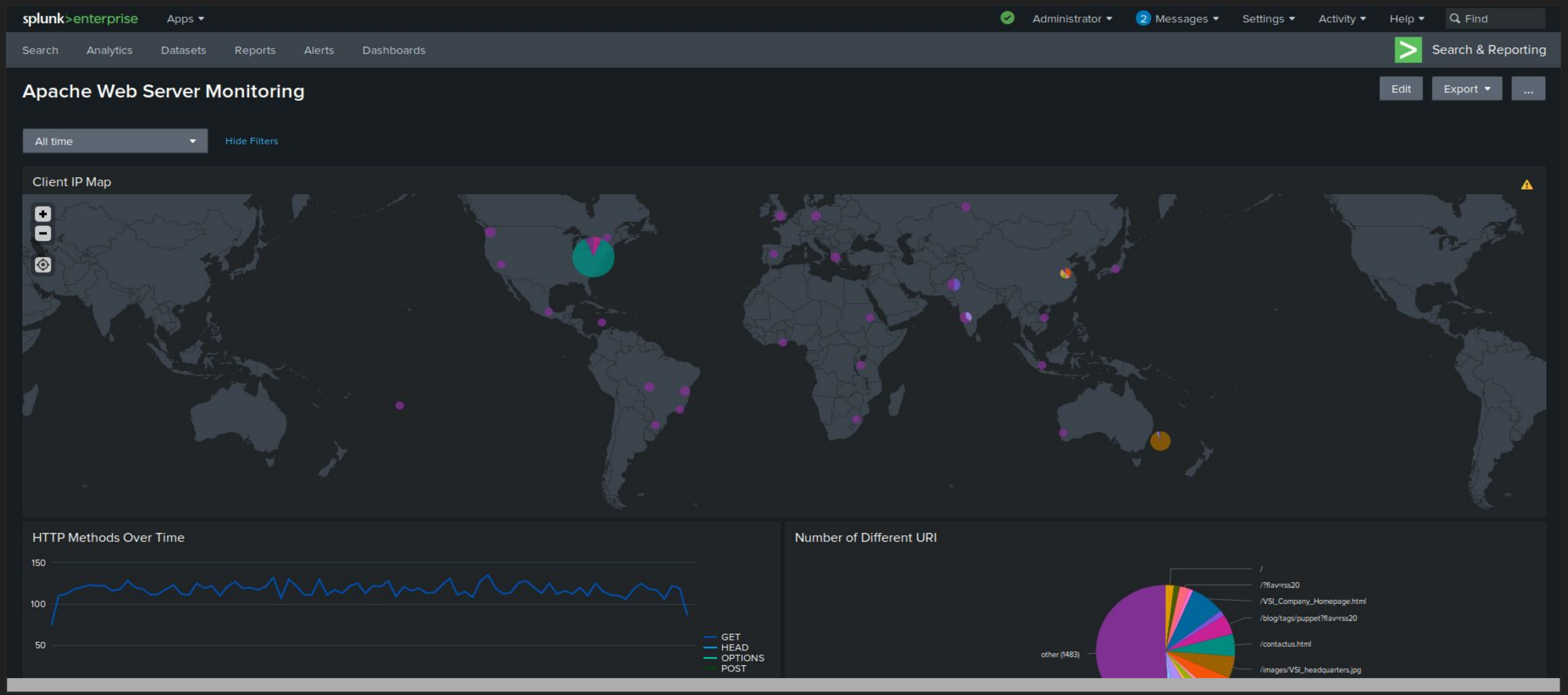


HTTP Post

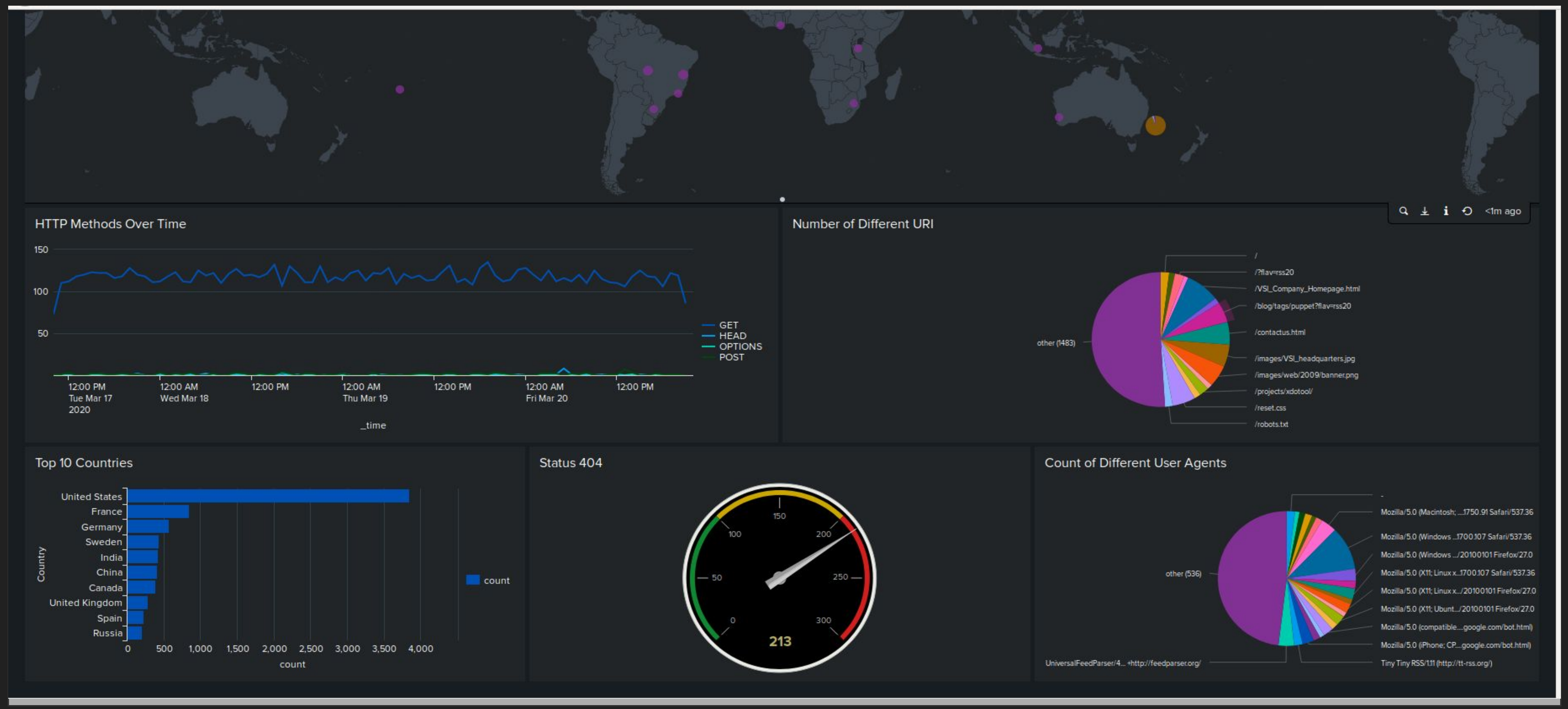
```
source="apache_logs.txt" host="apache_logs" sourcetype="access_combined" status=404 | stats count as total
```

✓ **213 events** (before 3/7/23 3:19:45.000 AM) No Event Sampling ▾

| total |
|---|
| 213 |



Apache Web Server Monitoring

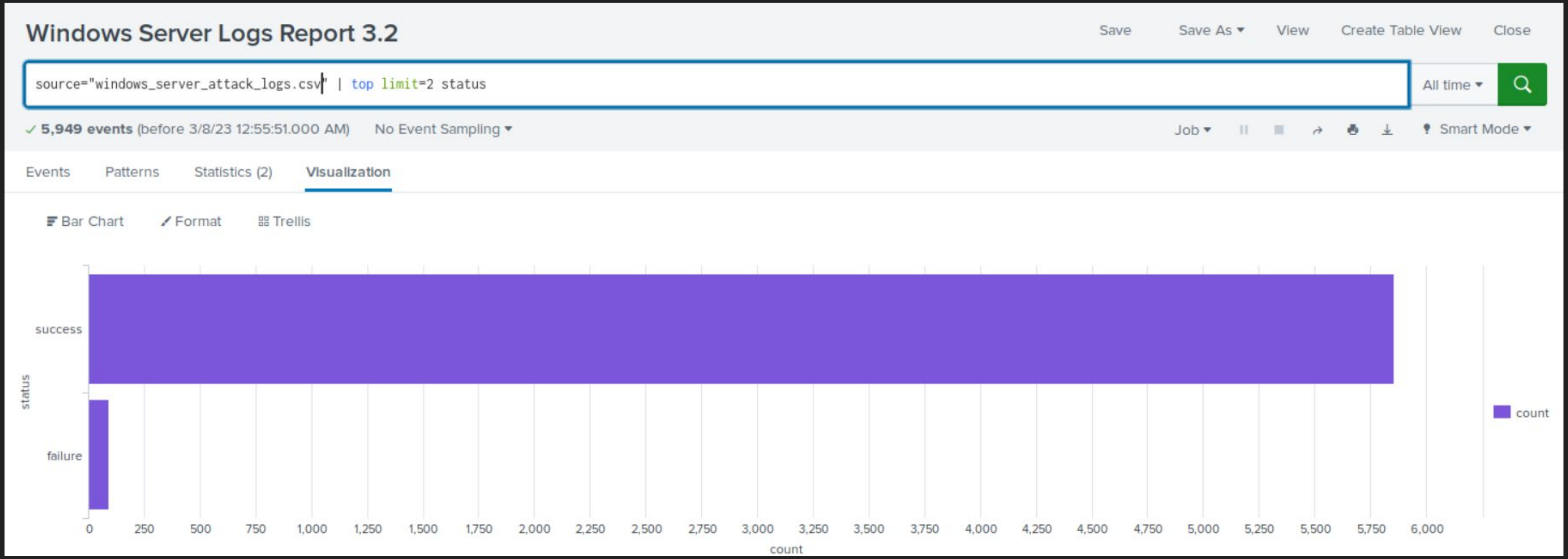

<1m ago
HTTP Methods Over Time
150
100
50
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 PM
12:00 AM Thu Mar 19
12:00 PM
12:00 AM Fri Mar 20
12:00 PM
_time
GET
HEAD
OPTIONS
POST
Number of Different URI
/
/?flav=rss20
/VSI_Company_Homepage.html
/blog/tags/puppet?flav=rss20
/contactus.html
/images/VSI_headquarters.jpg
/images/web/2009/banner.png
/projects/xdotool/
/reset.css
/robots.txt
other (1483)
Top 10 Countries
United States
France
Germany
Sweden
India
China
Canada
United Kingdom
Spain
Russia
Country
0
500
1,000
1,500
2,000
2,500
3,000
3,500
4,000
count
count
Status 404
0
50
100
150
200
250
300
213
Count of Different User Agents
-
Mozilla/5.0 (Macintosh; ...1750.91 Safari/537.36
Mozilla/5.0 (Windows ...1700.107 Safari/537.36
Mozilla/5.0 (Windows .../20100101 Firefox/27.0
Mozilla/5.0 (X11; Linux x...1700.107 Safari/537.36
Mozilla/5.0 (X11; Linux x.../20100101 Firefox/27.0
Mozilla/5.0 (X11; Ubunt.../20100101 Firefox/27.0
Mozilla/5.0 (compatible....google.com/bot.html)
Mozilla/5.0 (iPhone; CP...google.com/bot.html)
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
other (536)
UniversalFeedParser/4... +http://feedparser.org/

# Attack Analysis

# Attack Summary—Windows

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

- IT severity count decreased (93% to 80%), while the high severity account increased (7% to 20%)
- Notable changes in failed activities, increase in successes 4616 to 5854 and decrease in fails from 142 to 93.



Windows Server Logs Report 3.2

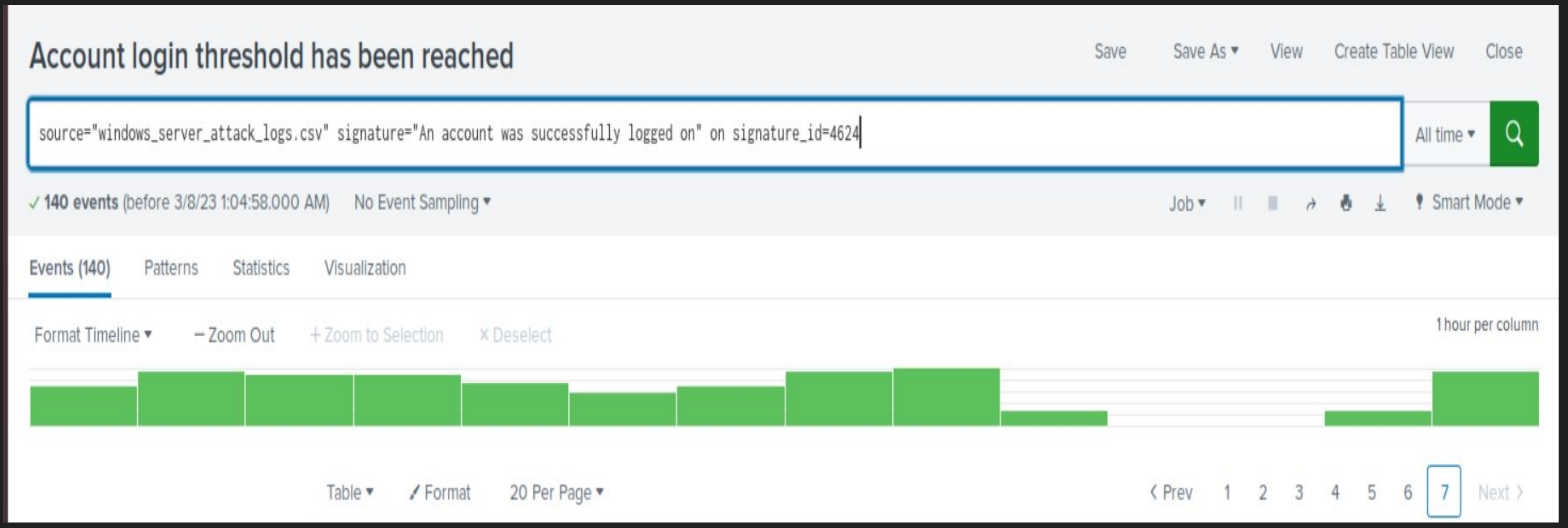
```
source="windows_server_attack_logs.csv" | top limit=2 status
```

✓ 5,949 events (before 3/8/23 12:55:51.000 AM) No Event Sampling ▾

# Attack Summary—Windows

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

- Alert for suspicious volume of failed activities failed
  - Signature_id 4624 prevents the alert being triggered
- Alert for suspicious volume of deleted accounts succeeded



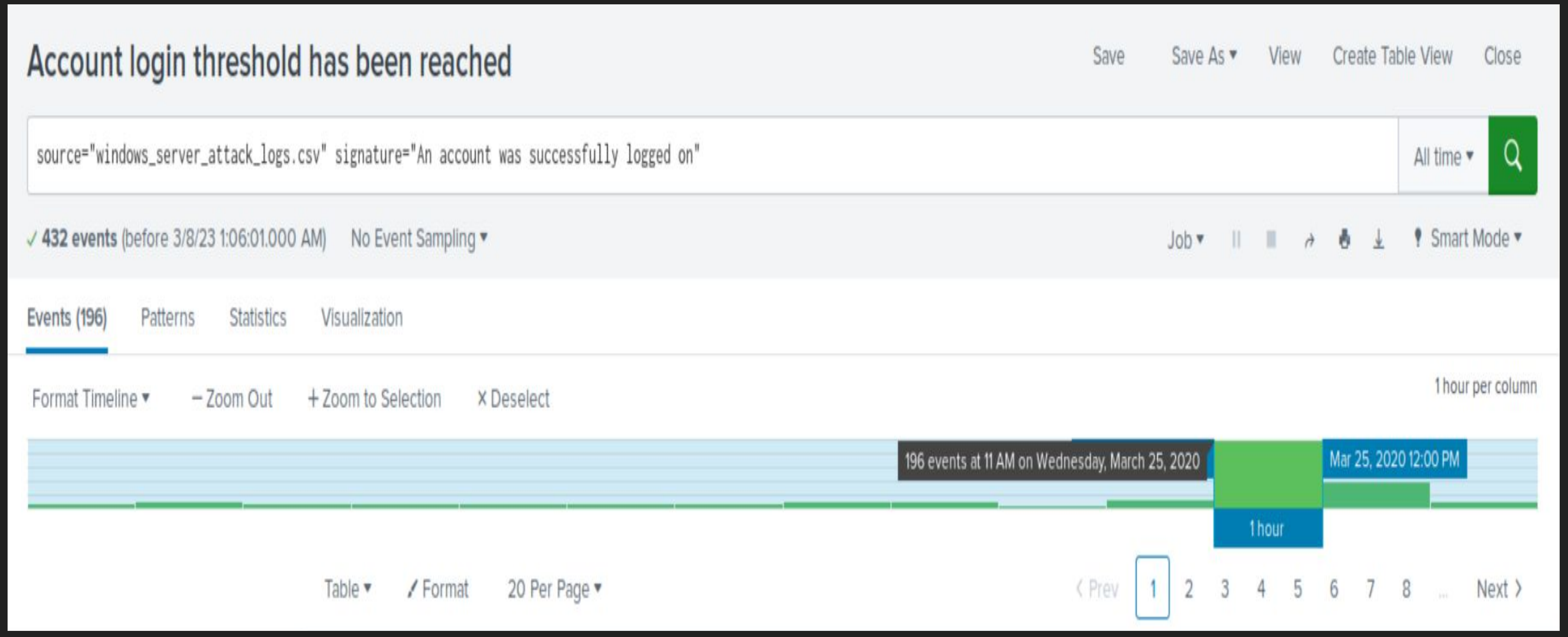
Account login threshold has been reached

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on" on signature_id=4624
```

✓ 140 events (before 3/8/23 1:04:58.000 AM) No Event Sampling ▾

Events (140)

1 hour per column



Account login threshold has been reached

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"
```

✓ 432 events (before 3/8/23 1:06:01.000 AM) No Event Sampling ▾

Events (196)

1 hour per column

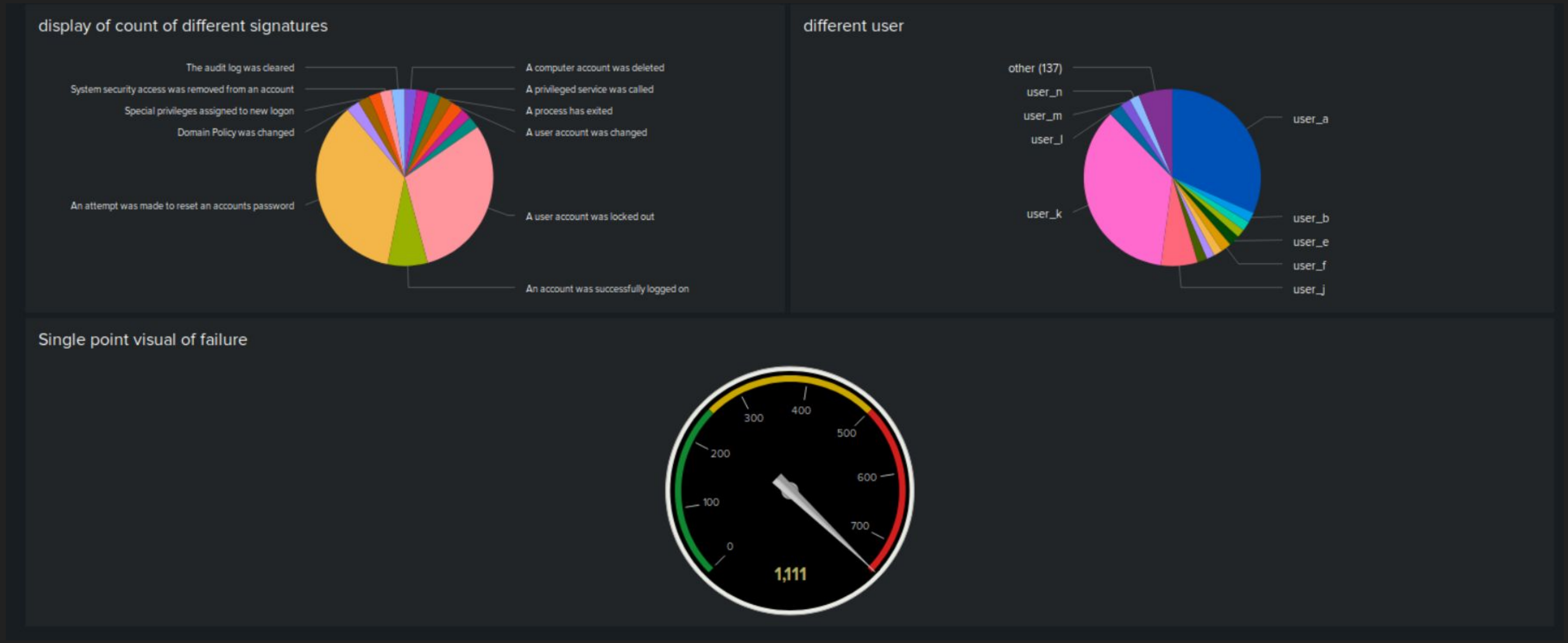
196 events at 11 AM on Wednesday, March 25, 2020

Mar 25, 2020 12:00 PM

# Attack Summary—Windows

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

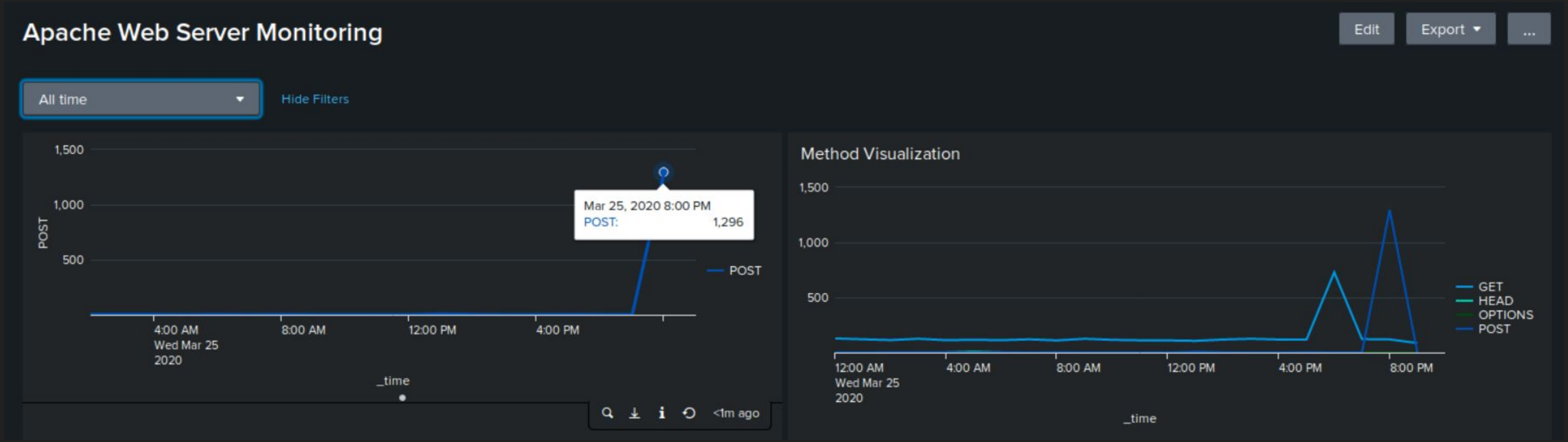
- Suspicious user activity – excessive login attempts by user_a, user_k, and user_j
- High number of attempts to reset account passwords (2128)
- High number of accounts locked out (1811)


display of count of different signatures
The audit log was cleared
System security access was removed from an account
Special privileges assigned to new logon
Domain Policy was changed
An attempt was made to reset an accounts password
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
different user
other (137)
user_n
user_m
user_l
user_k
user_a
user_b
user_e
user_f
user_j
Single point visual of failure
0
100
200
300
400
500
600
700
1,111

# Attack Summary—Apache

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

- There were a significant increase in POST requests (from 104 to 1324)
- There was a significant decline in referrals from websites
- The amount of 404 status code responses increased by 466 responses while all other response codes decreased



Apache Web Server Monitoring

All time

Mar 25, 2020 8:00 PM
POST: 1,296

Method Visualization

# Attack Summary—Apache

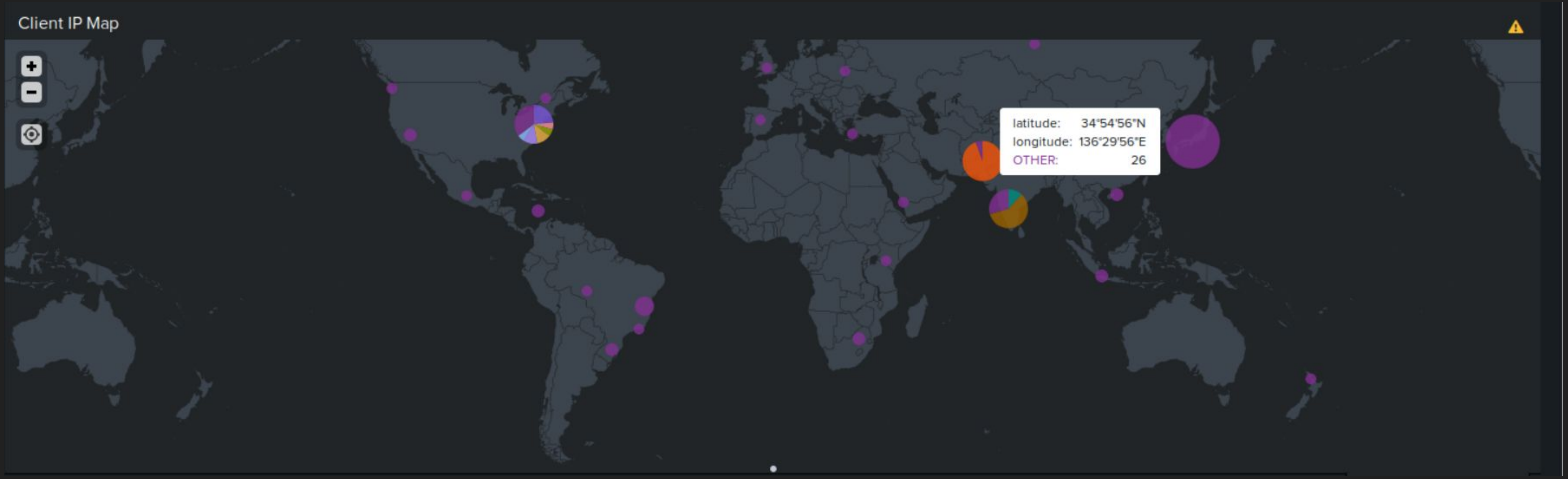
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- There was a stark increase in **international** activity at 20:00 on Wednesday March 25, 2020; 939 activities. The threshold of 334 would have successfully notified us of the suspicious activity.
- A suspicious volume of HTTP **POST** requests were detected on 20:00 on Wednesday March 25, 2020. There were 1296 POST requests made. Our threshold was set to 10, and it would have detected this volume of POST requests.

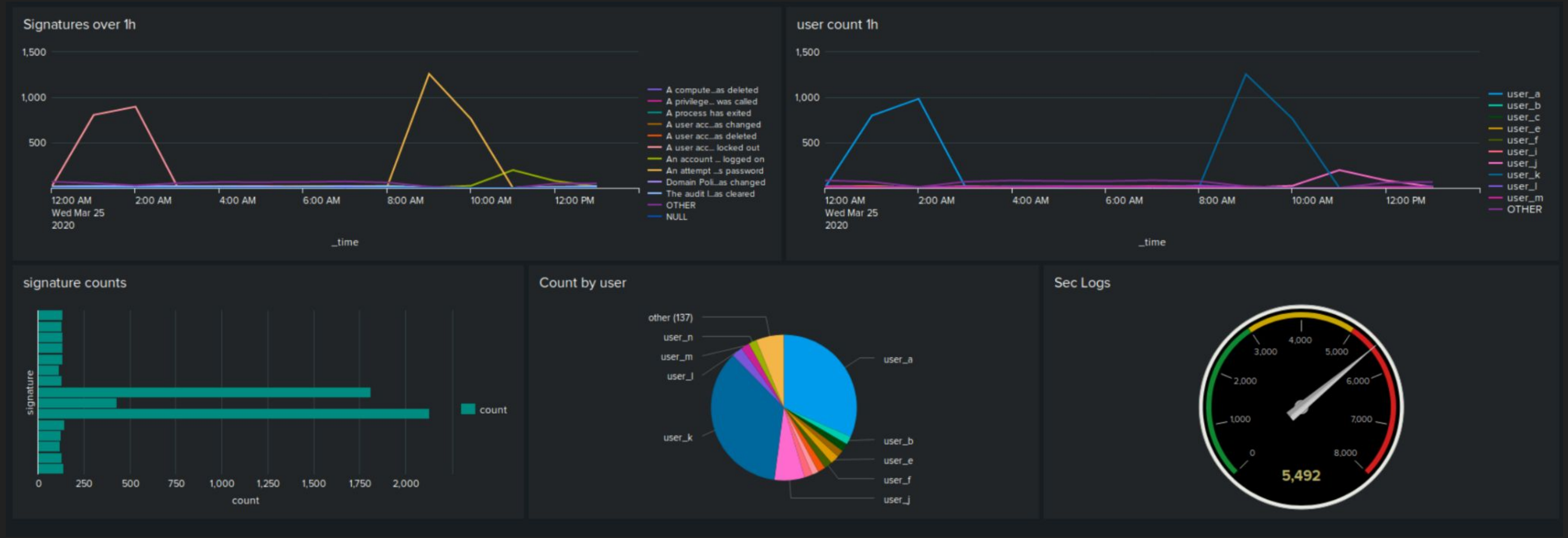
# Attack Summary—Apache

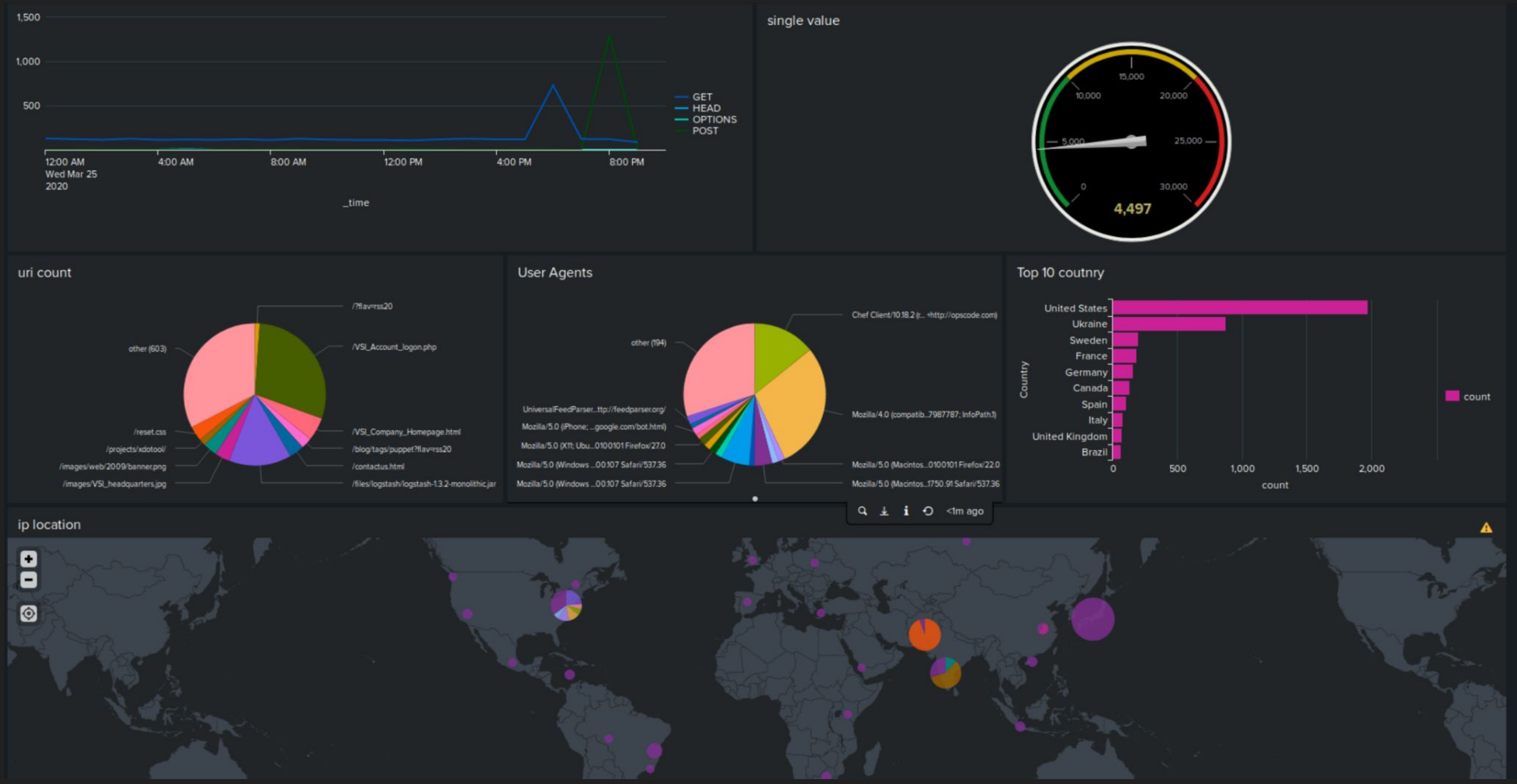
Summarize your findings from your dashboards when analyzing the attack logs.

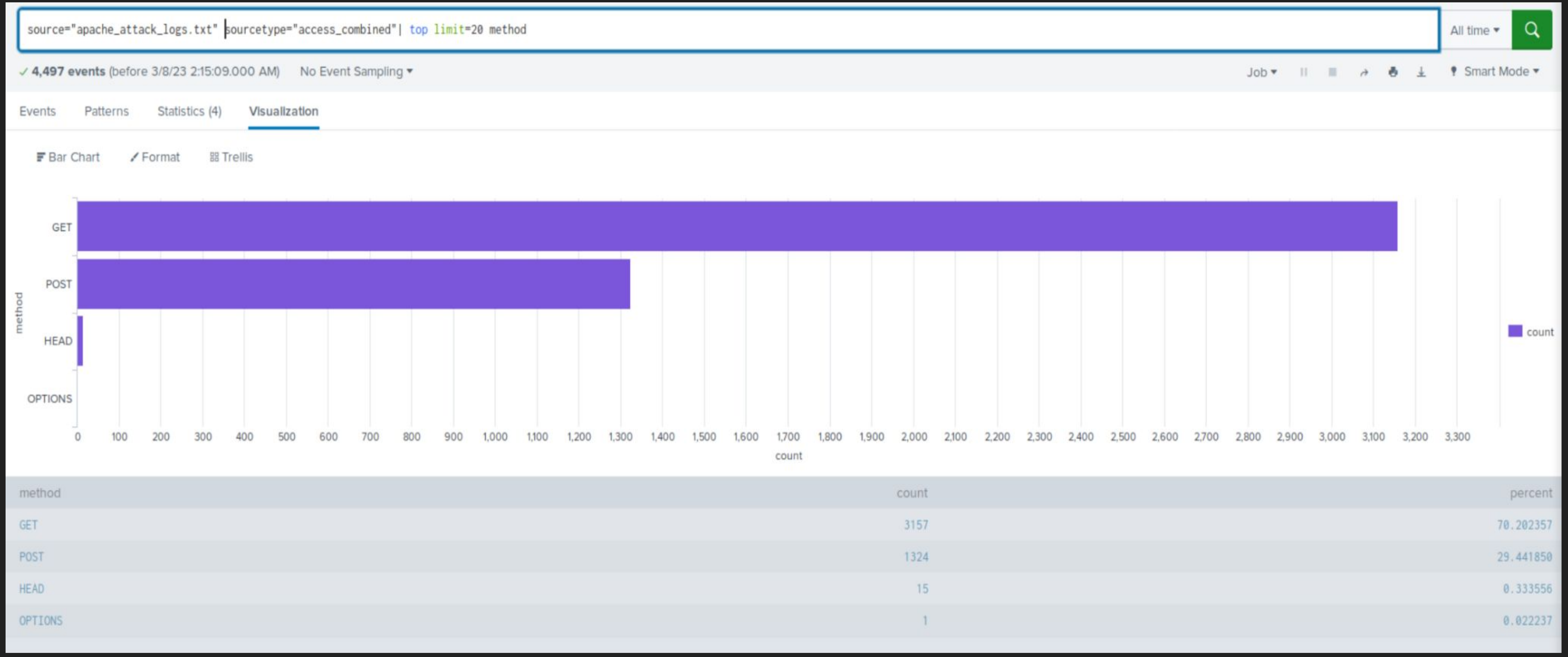
- Suspicious spike in POST and GET requests on 03/25/20
- Non-US country login attempts with high rates in Kiev and Kharkiv, Ukraine
- High rates of VSI account logon (1323)



# Screenshots of Attack Logs







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

✓ **4,497 events** (before 3/8/23 2:15:09.000 AM) No Event Sampling ▾

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

# Summary and Future Mitigations

# Project 3 Summary

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

  Windows Server:

  - Unusual account logins from users a, k, and j
  - Suspicious attempts to reset passwords and user lockout
  - Brute Force Attack

  Apache Server:

  - Attacker in Ukraine attempting DoS (404 errors)

- To protect VSI from future attacks, what future mitigations would you recommend?
  - Restrict high levels of account login attempts
  - Password reset policies
  - MFA