Defensive Security Project
by: Jaden Lassiter

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

Provide Virtual Space Industries (VSI) with a monitoring solution by assuming the position of a SOC analyst.

Monitor:

- Windows server
- Apache server
- Administrative Web page
  - This is a web page for administration: https://vsi-corporation.azurewebsites.net/
  - Hosted on an Apache web server.
  - VSI's back-end activities are primarily run on a Windows operating system.

Create

- Dashboards, Reports, and alerts

[“Add-On” App]

Barracuda Spam and Virus Firewall Add-On

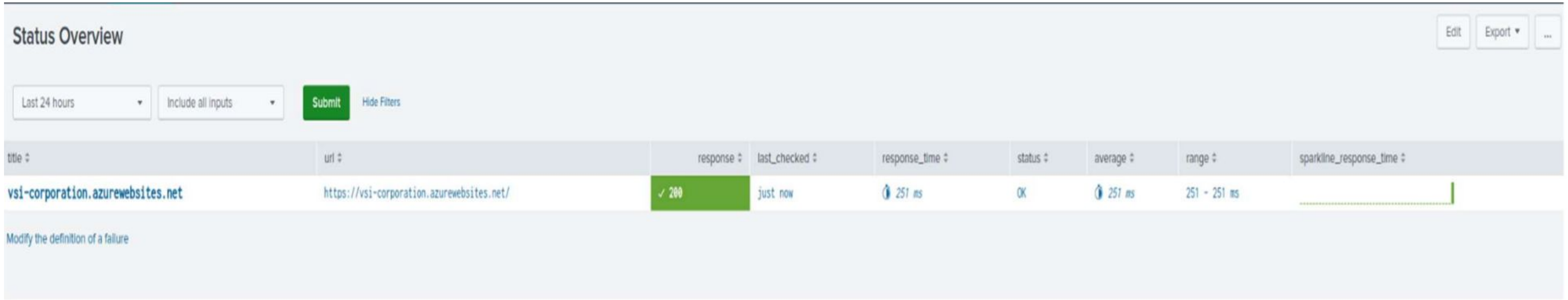
Barracuda Spam and Virus Firewall Add-On:

We decided to do the Barracuda Spam and Virus Firewall Add-on for it's benefits of parsing out firewall logs for our windows machine.

This Add-on The is a robust, enterprise-grade firewall engineered for seamless deployment in dynamic and secure network environments. It provides superior protection, enhances operational efficiency, and ensures network reliability by defending against line outages and quality issues.

The Barracuda NG Firewall app offers insights into matched access rules, detected applications, and applied URL filter policies, with both fixed and real-time data views.

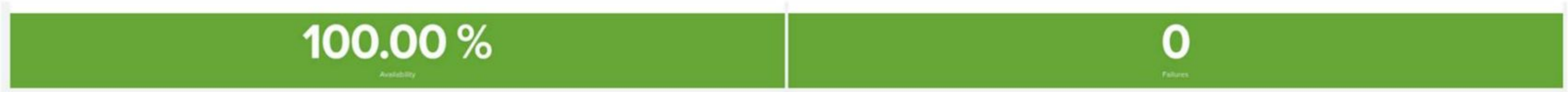
[Add-On App Name]

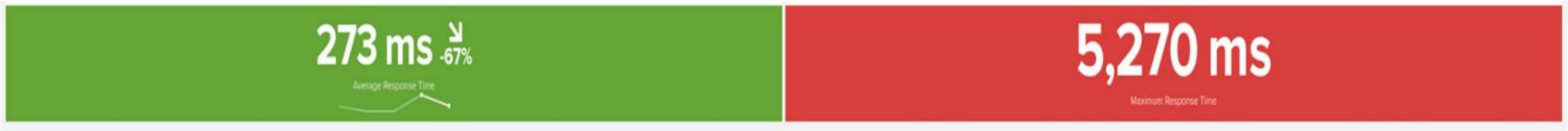


Status Overview

title ⇕	url ⇕	response ⇕	last_checked ⇕	response_time ⇕	status ⇕	average ⇕	range ⇕	sparkline_response_time ⇕
vsi-corporation.azurewebsites.net	https://vsi-corporation.azurewebsites.net/	✓ 200	just now	251 ms	OK	251 ms	251 - 251 ms	

Modify the definition of a failure





Logs Analyzed

1 Windows Logs

- Signature IDs
- Severity
- Users
- Signatures
- Status

2 Apache Logs

- Methods
- Referrer domains
- Status
- Client IPs
- User agents

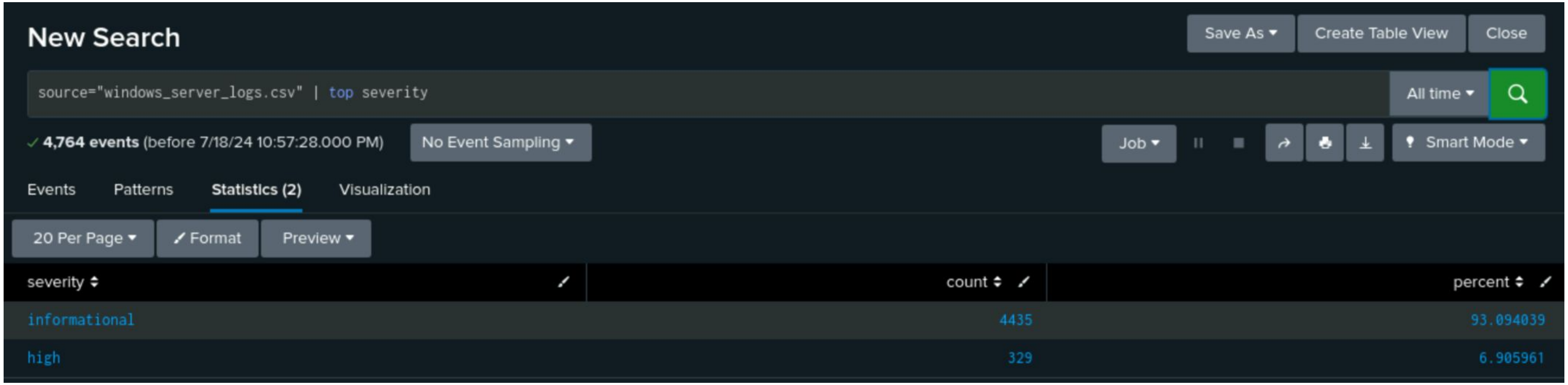
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Windows log Signature and Signature ID	A report that displays the ID number linked to a particular Windows activity signature.
Windows Logs Severity	Indicates whether the server's failure activity is at an unusually high level.
Windows Success and Failure Report	A report that indicates whether their server's failure rate is suspiciously high.

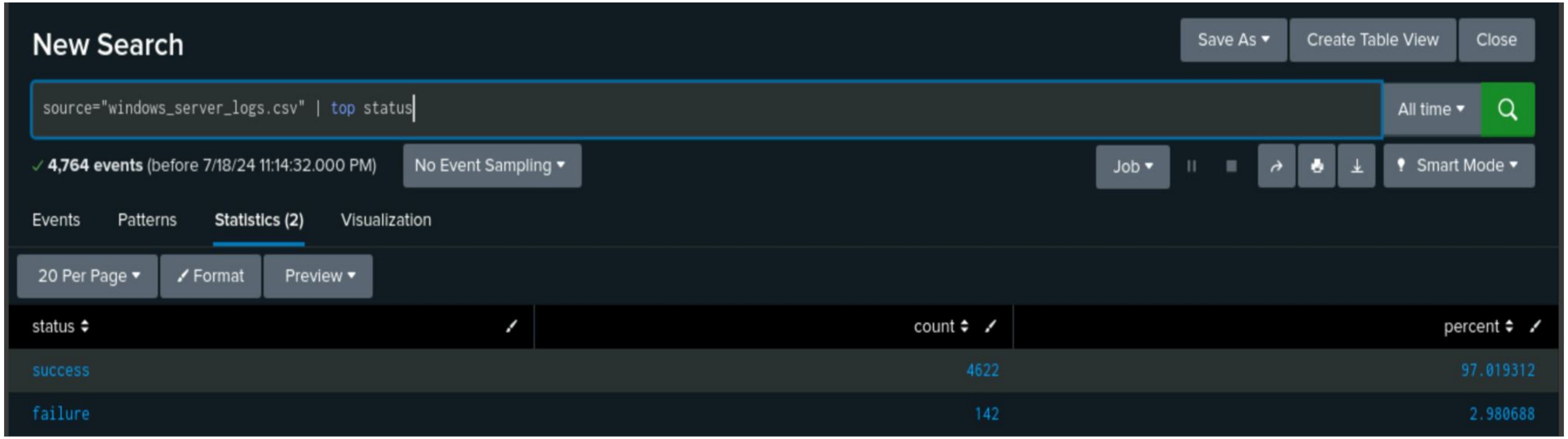
Images of Reports—Windows



```
source="windows_server_logs.csv" | top severity
```

✓ **4,764 events** (before 7/18/24 10:57:28.000 PM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961

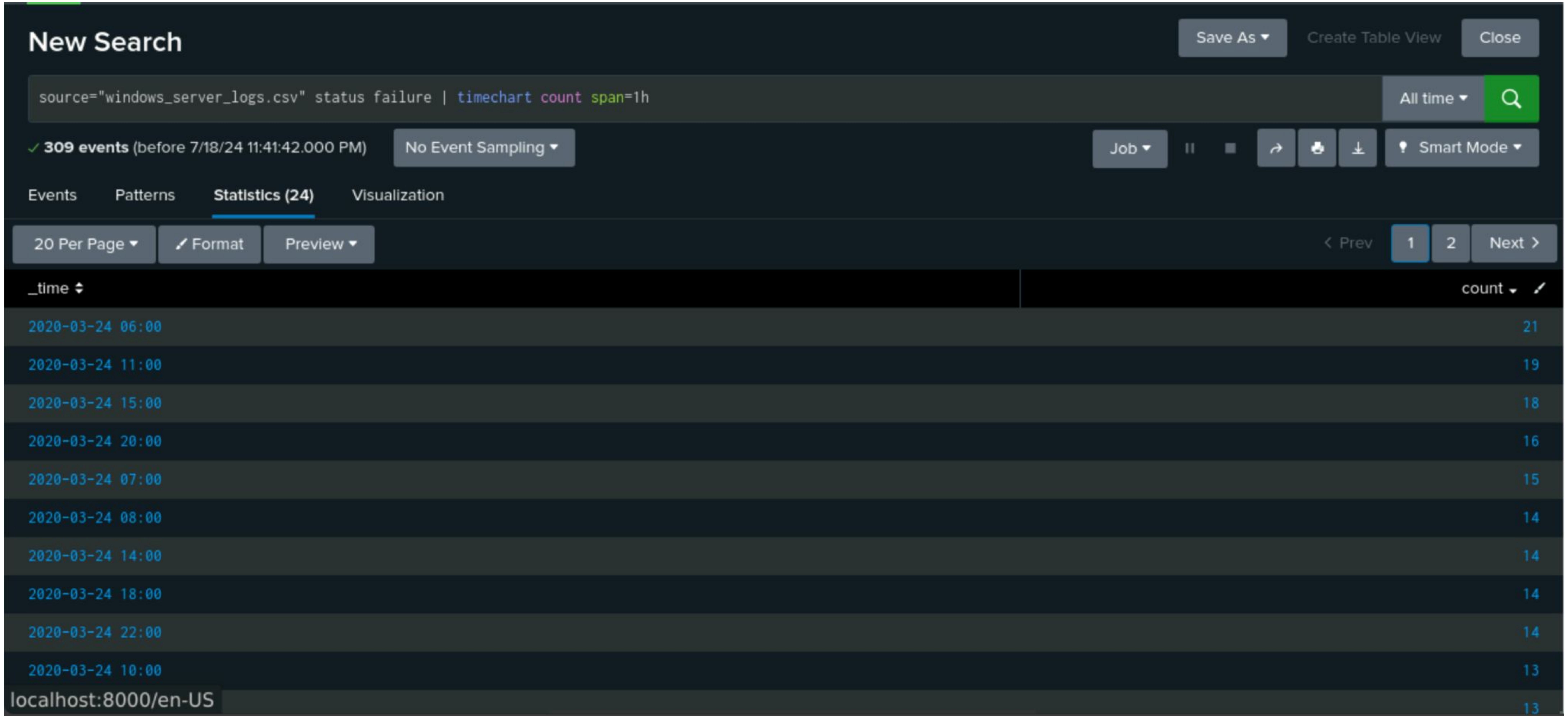


```
source="windows_server_logs.csv" | top status
```

✓ **4,764 events** (before 7/18/24 11:14:32.000 PM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

Images of Reports—Windows



```
source="windows_server_logs.csv" status failure | timechart count span=1h
```

✓ **309 events** (before 7/18/24 11:41:42.000 PM)

_time	count
2020-03-24 06:00	21
2020-03-24 11:00	19
2020-03-24 15:00	18
2020-03-24 20:00	16
2020-03-24 07:00	15
2020-03-24 08:00	14
2020-03-24 14:00	14
2020-03-24 18:00	14
2020-03-24 22:00	14
2020-03-24 10:00	13
	13

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Successfully logged in	An alert that is generated if the threshold for the number of successfully logged accounts is surpassed	12	21

JUSTIFICATION: To create our baseline, the average number of failed Windows activities was approximately 12, but it never above 21. Failings higher than 21 would undoubtedly point to questionable behavior.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity Alerts	An alert is generated after the threshold is exceeded by the number of unsuccessful activities.	6	10

JUSTIFICATION: To set our baseline, the average quantity of failed Windows activity was approximately 6, but it never above 10. Failings more than thirty would undoubtedly point to questionable behavior.

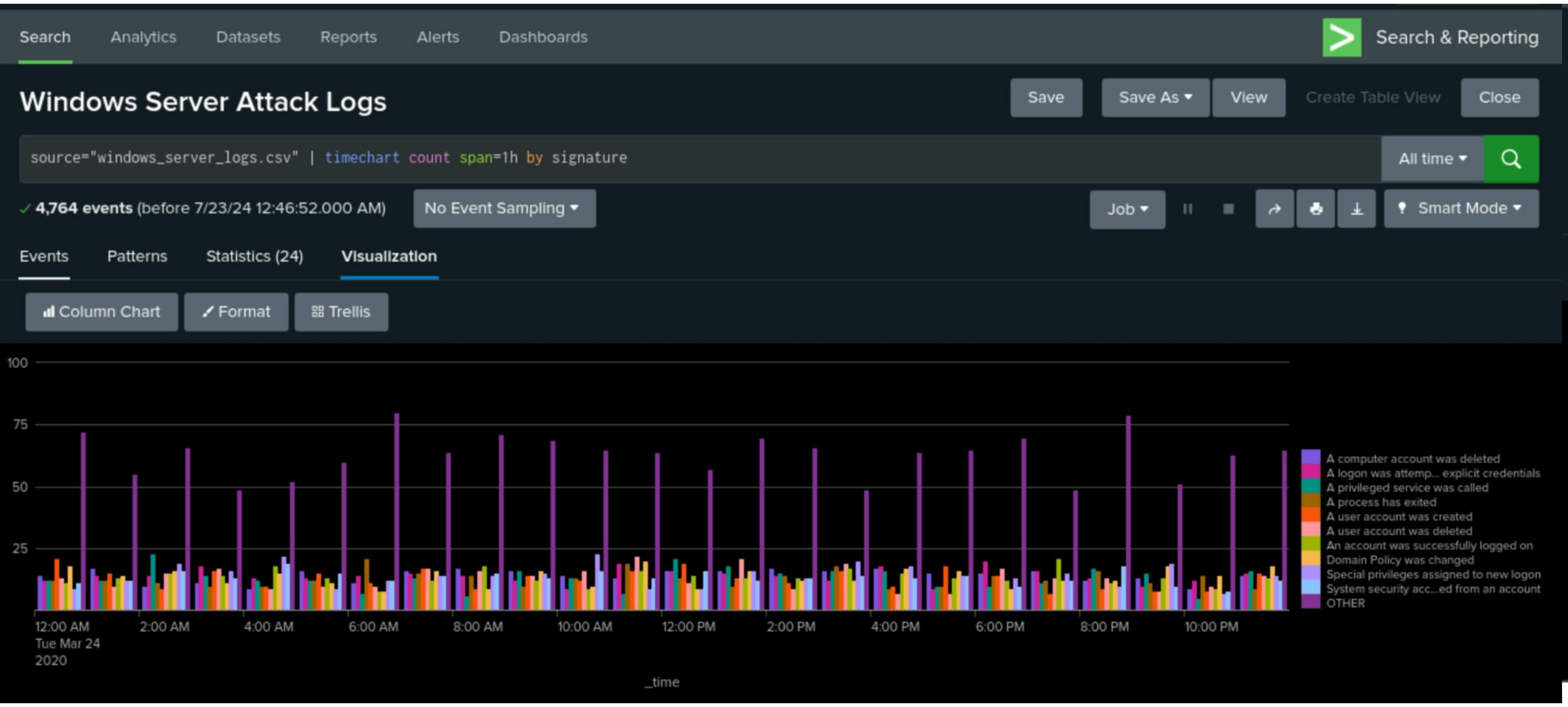
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deleted	An alert is generated in the event that an excessive number of deleted user accounts exist.	10	21

JUSTIFICATION: A 10 baseline seems to be comparable to a "normal" hour. Anything over 21 would be cause for concern and suggest an issue.

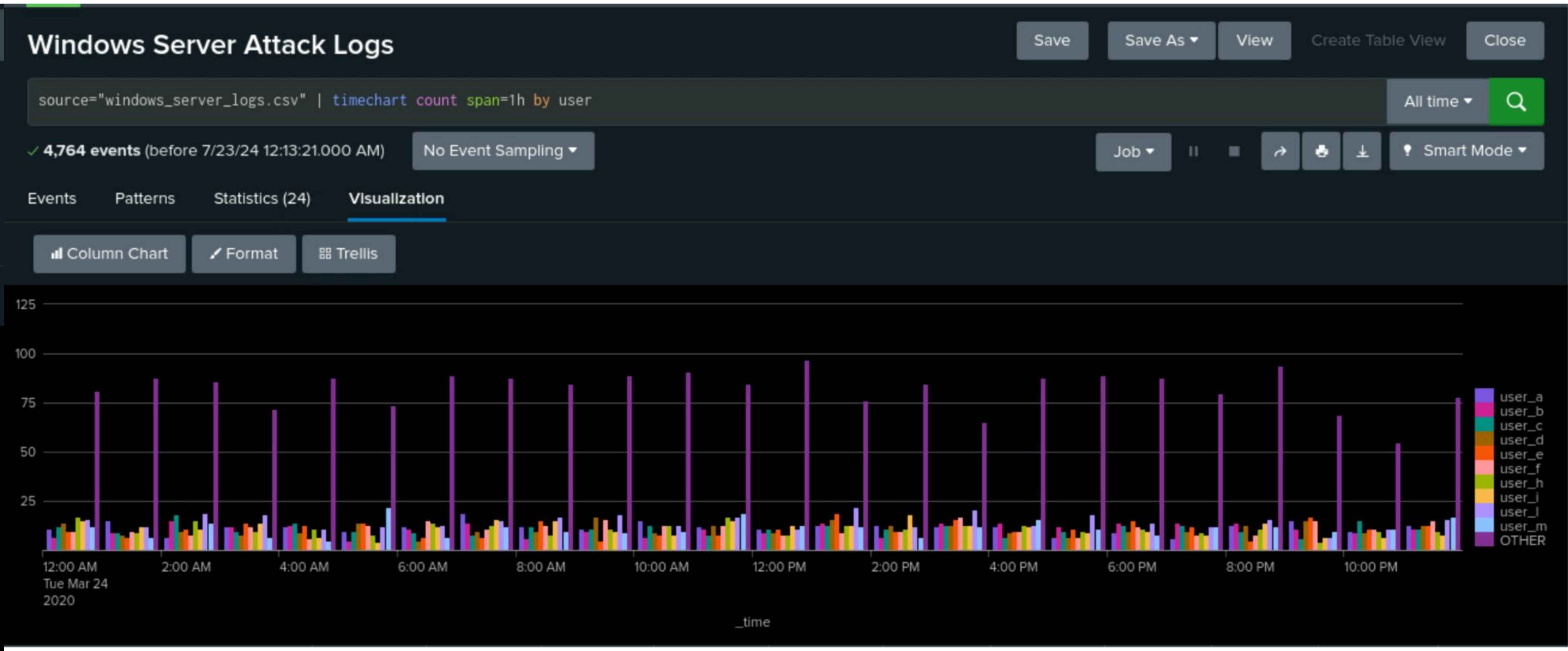
Dashboards—Windows



Windows Server Attack Logs

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

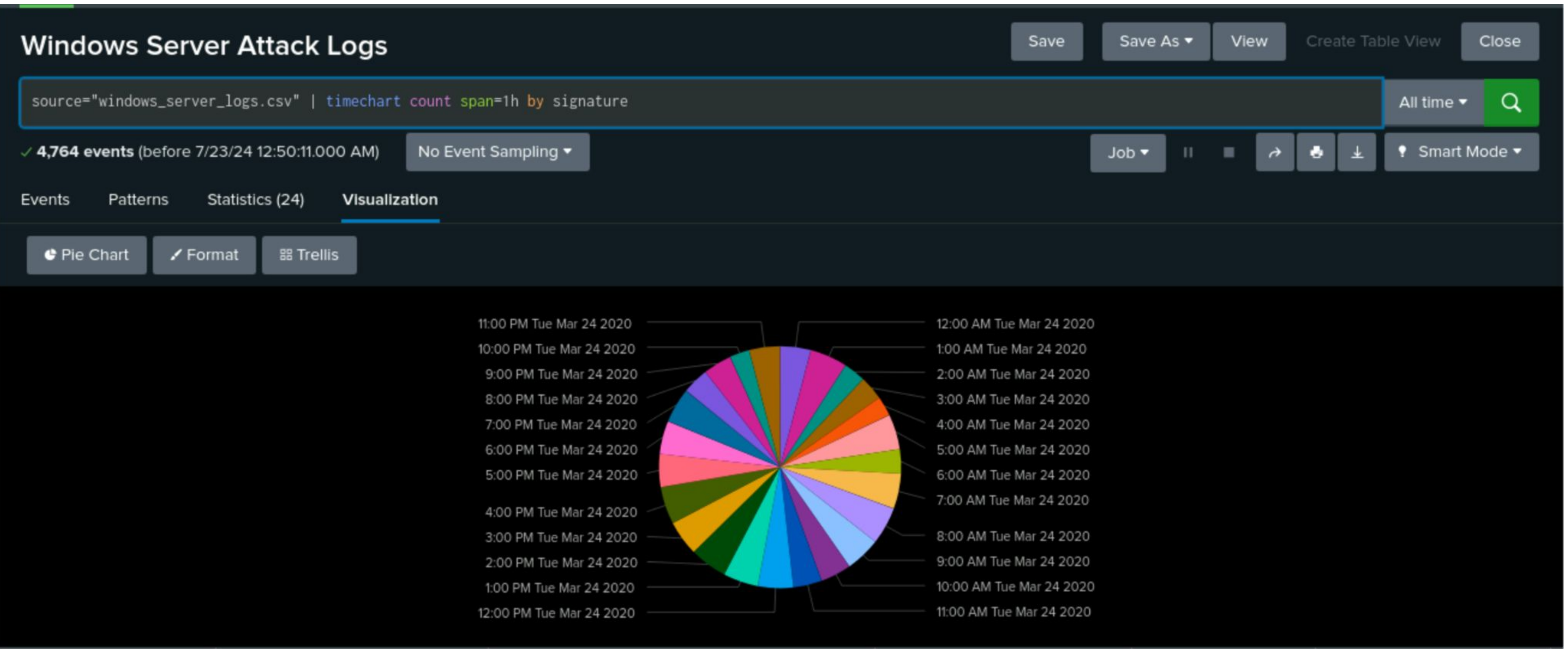
✓ **4,764 events** (before 7/23/24 12:46:52.000 AM)



Windows Server Attack Logs

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

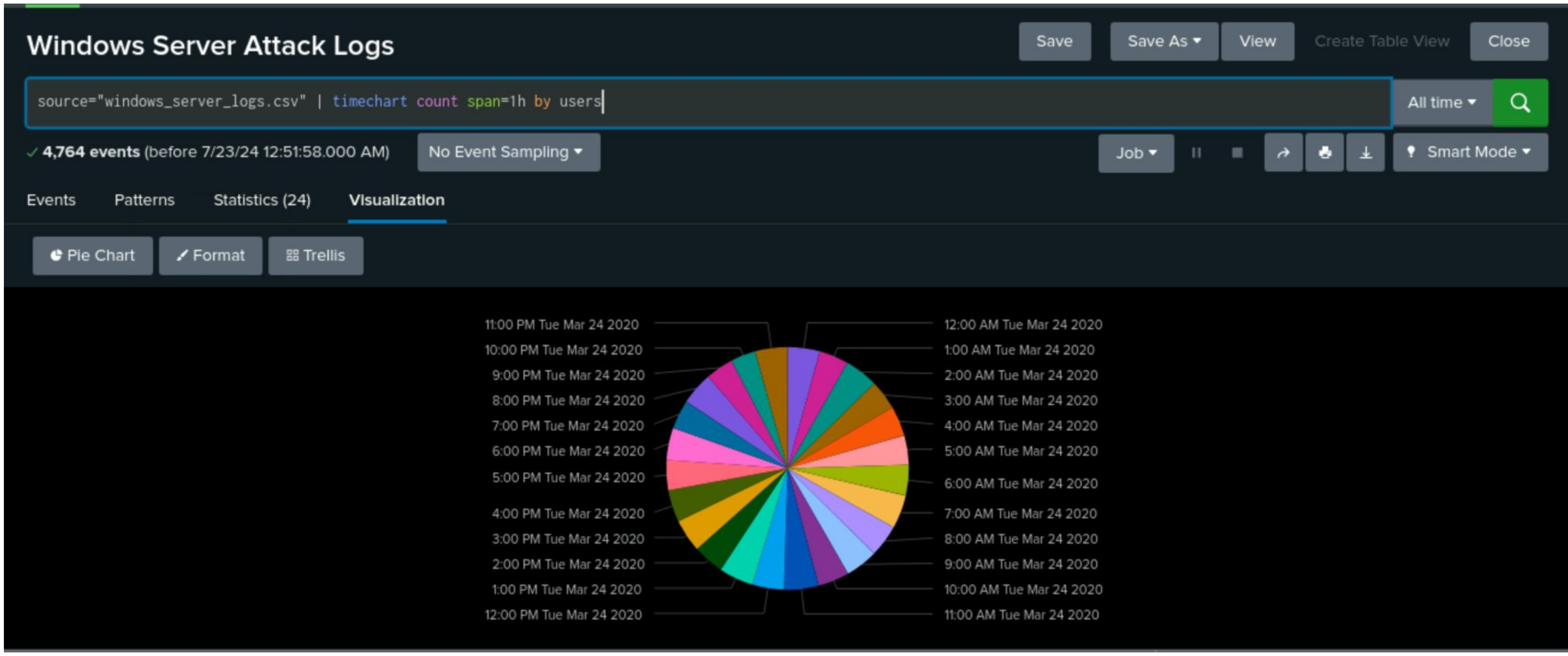
✓ **4,764 events** (before 7/23/24 12:13:21.000 AM)



Windows Server Attack Logs

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

✓ **4,764 events** (before 7/23/24 12:50:11.000 AM)

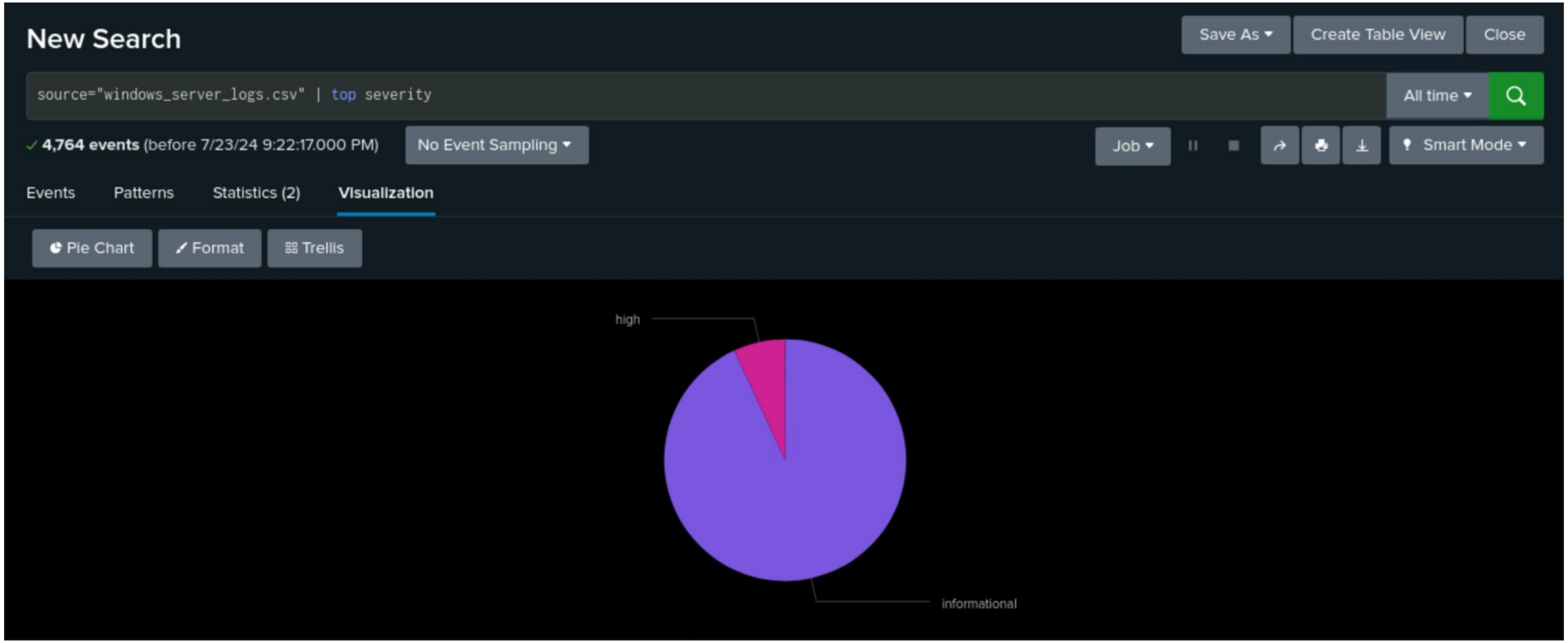


Windows Server Attack Logs

```
source="windows_server_logs.csv" | timechart count span=1h by users
```

✓ **4,764 events** (before 7/23/24 12:51:58.000 AM)

Dashboards—Windows



```
source="windows_server_logs.csv" | top severity
```

✓ **4,764 events** (before 7/23/24 9:22:17.000 PM)

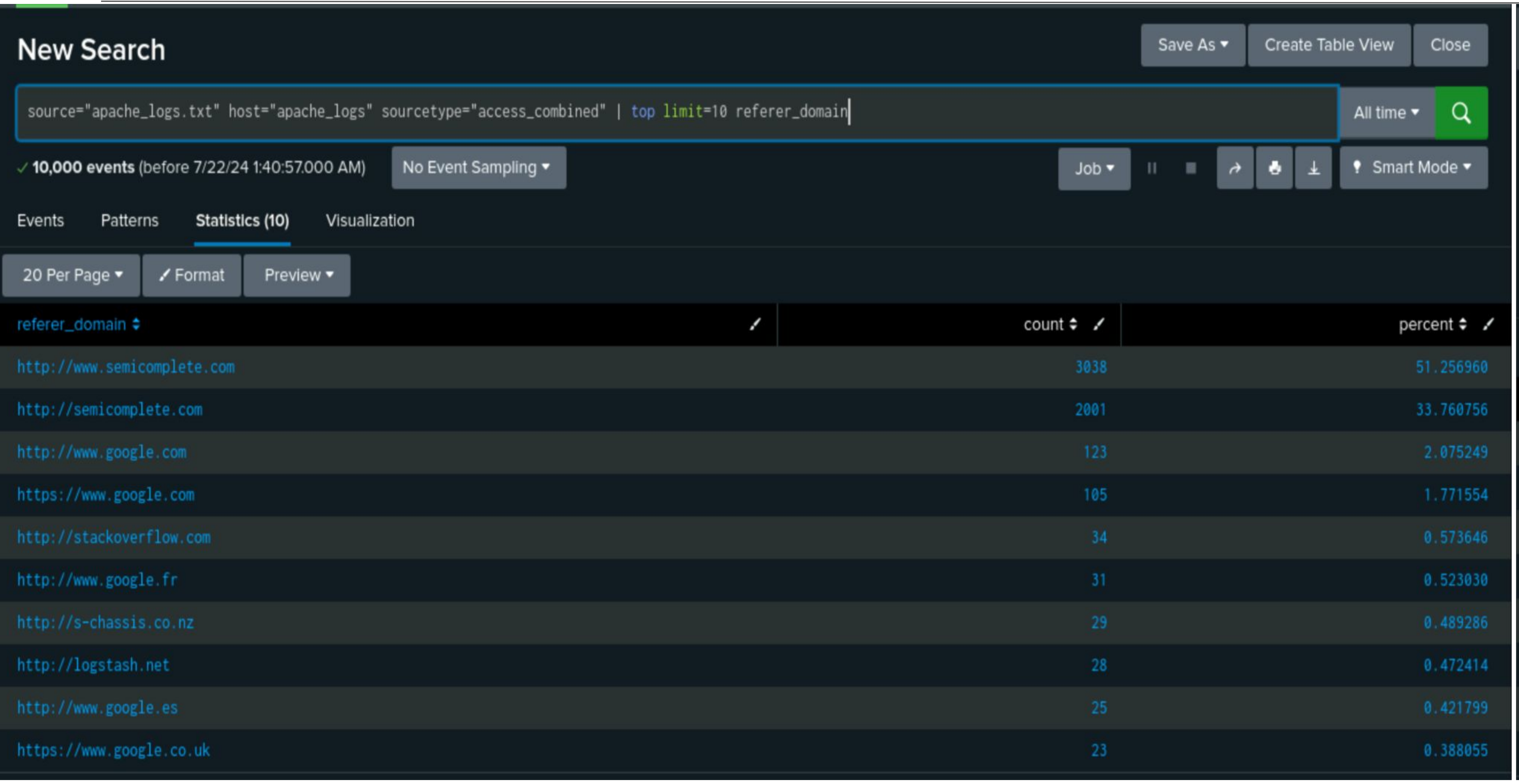
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP methods	Table that shows the count of GET, POST, HEAD and OPTIONS
Top 10 Domains	A report that shows the top 10 domains that refer to VSI's website
HTTP Response Code	Shows the count of HTTP response code

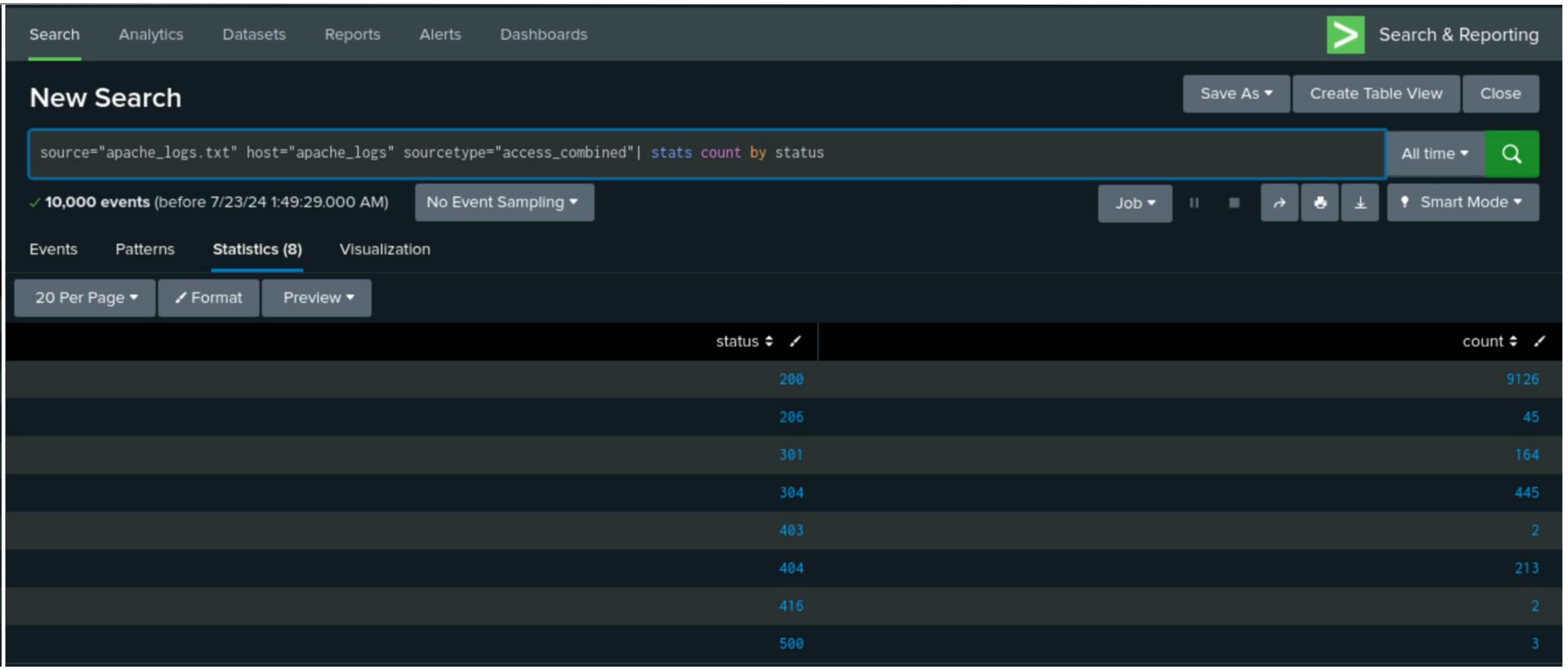
Images of Reports—Apache



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

✓ **10,000 events** (before 7/22/24 1:40:57.000 AM) No Event Sampling ▾

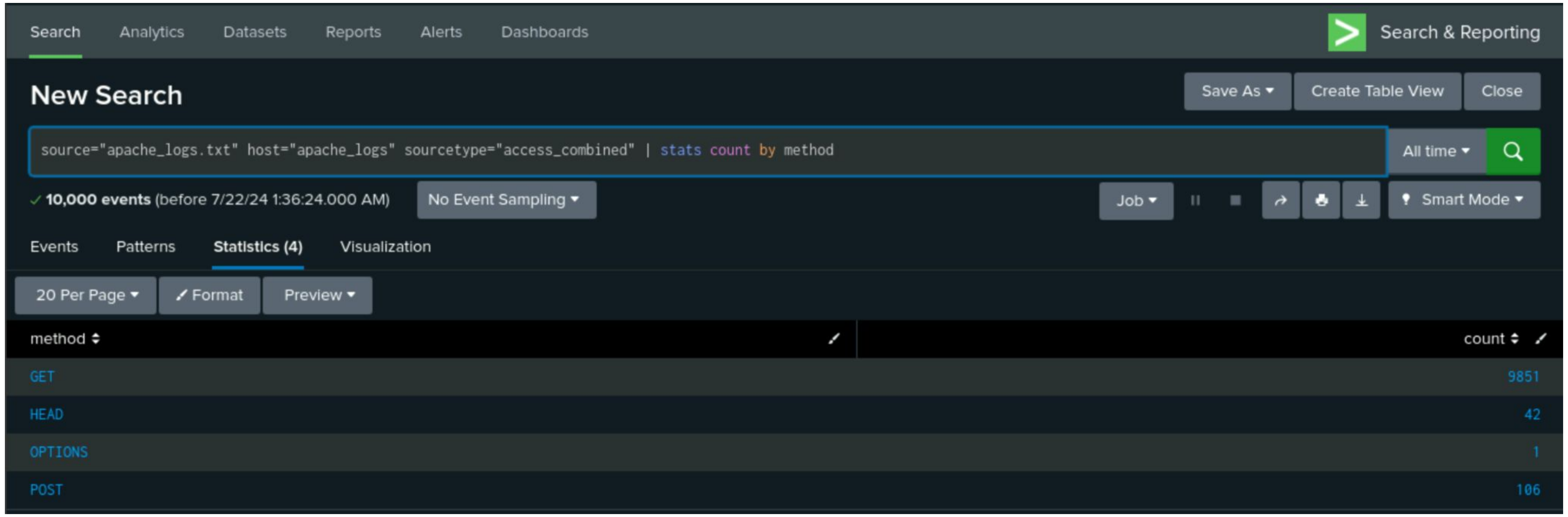
referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net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



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

✓ **10,000 events** (before 7/23/24 1:49:29.000 AM) No Event Sampling ▾

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



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

✓ **10,000 events** (before 7/22/24 1:36:24.000 AM) No Event Sampling ▾

method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Non-USA Activity	If the hourly activity from any nation other than the US surpasses the threshold, send out an alert.	80	180

JUSTIFICATION: The logs indicated that 80 incidents per hour was typical, but more than 180 appeared improbable on a typical day. Any number of incidents above the threshold would suggest a problem.

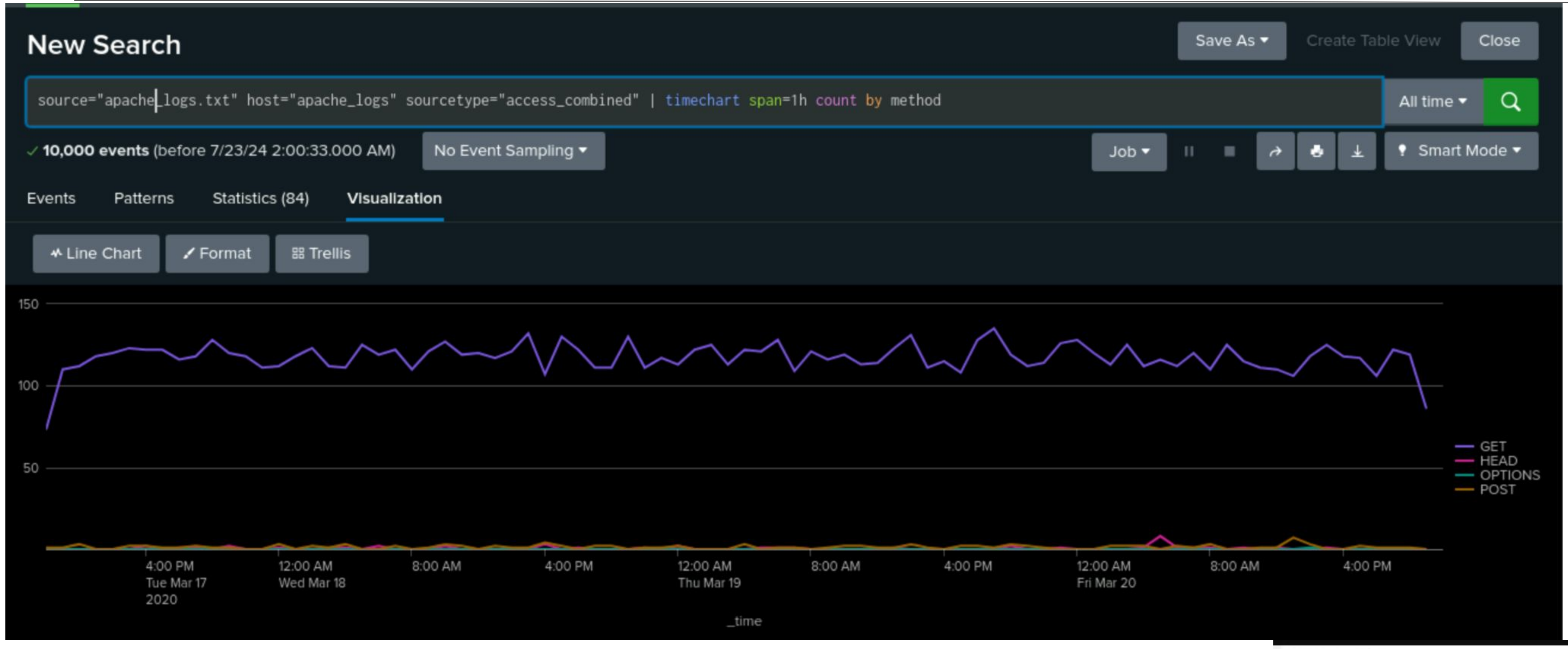
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST Method Count	Alert if the HTTP POST method's hourly count surpasses the predetermined threshold.	3	12

JUSTIFICATION: Since there were approximately 3 http post counts every hour on average, I thought that 12 would be a nice place to start.

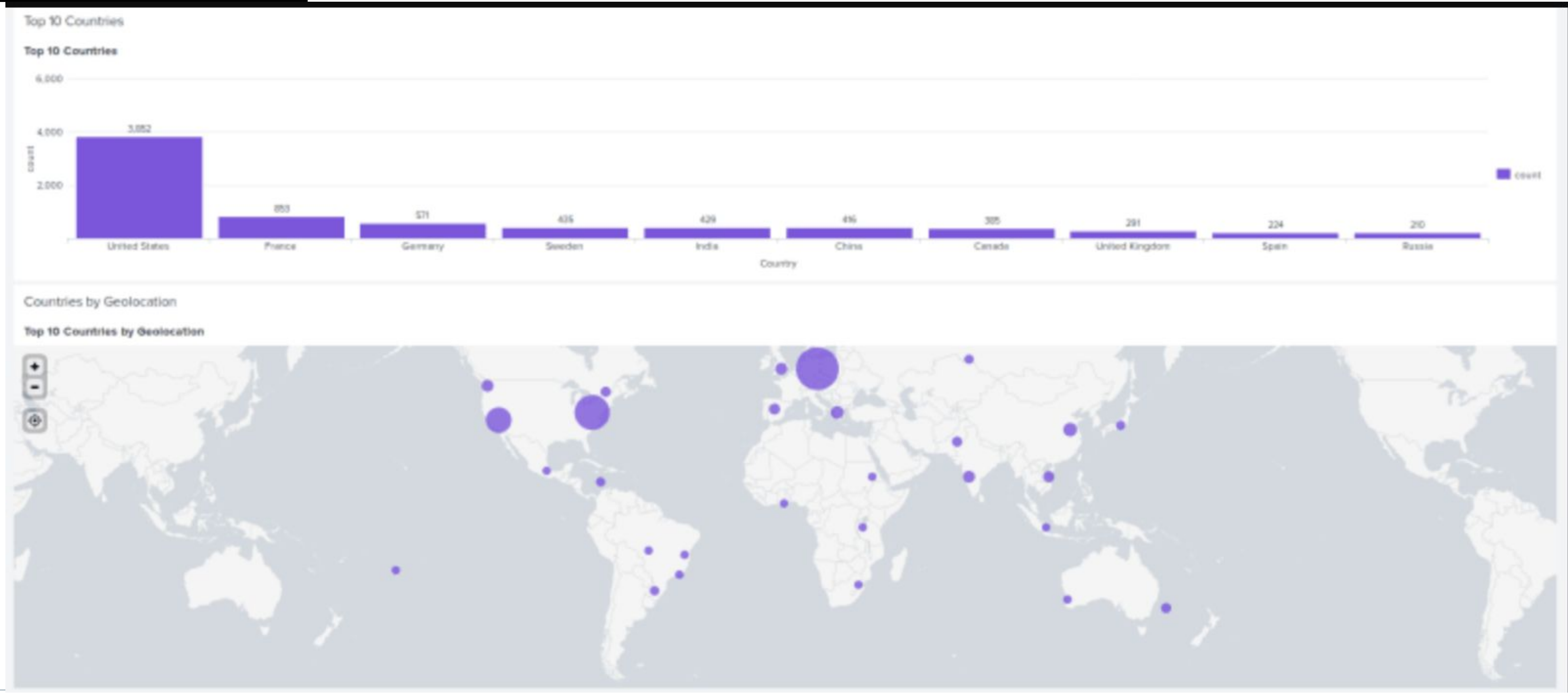
Dashboards—Apache



New Search

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

✓ **10,000 events** (before 7/23/24 2:00:33.000 AM)



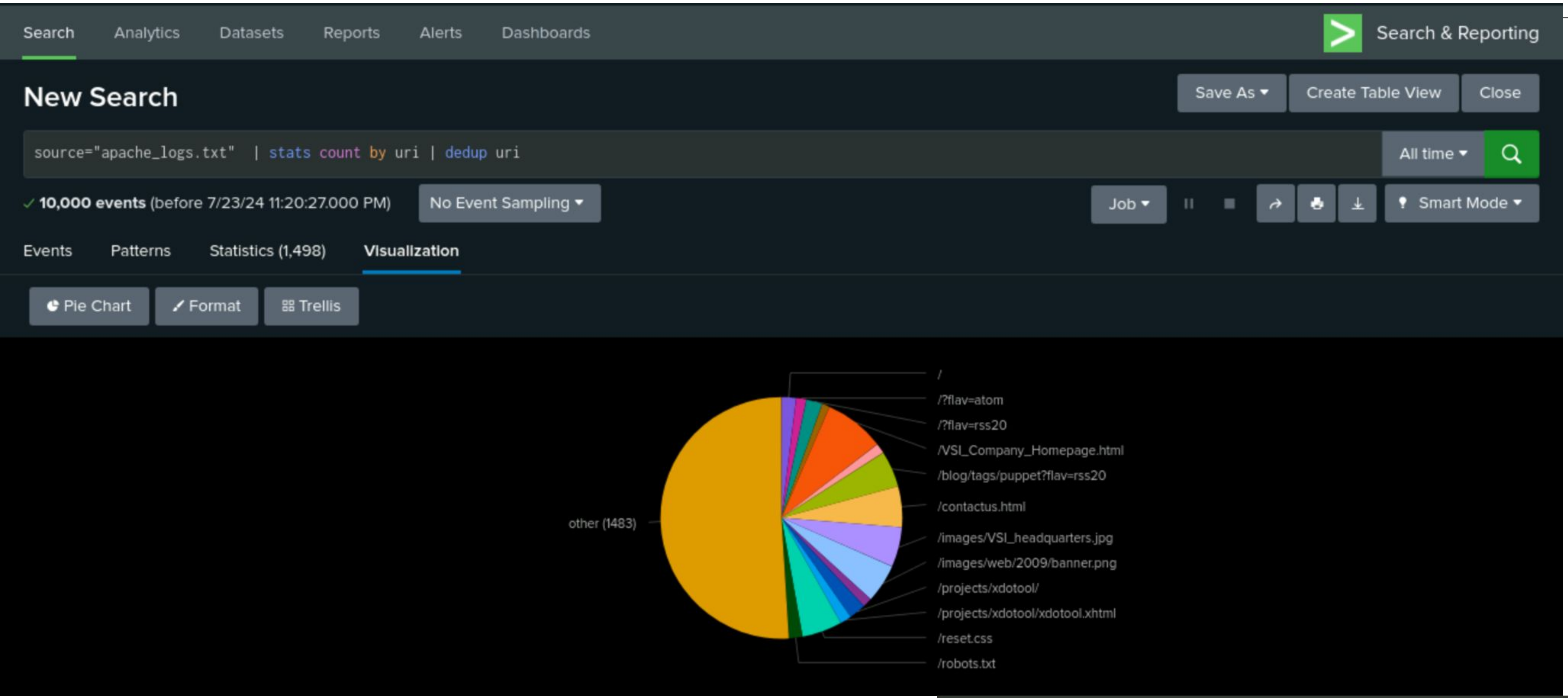
Top 10 Countries

Top 10 Countries

Countries by Geolocation

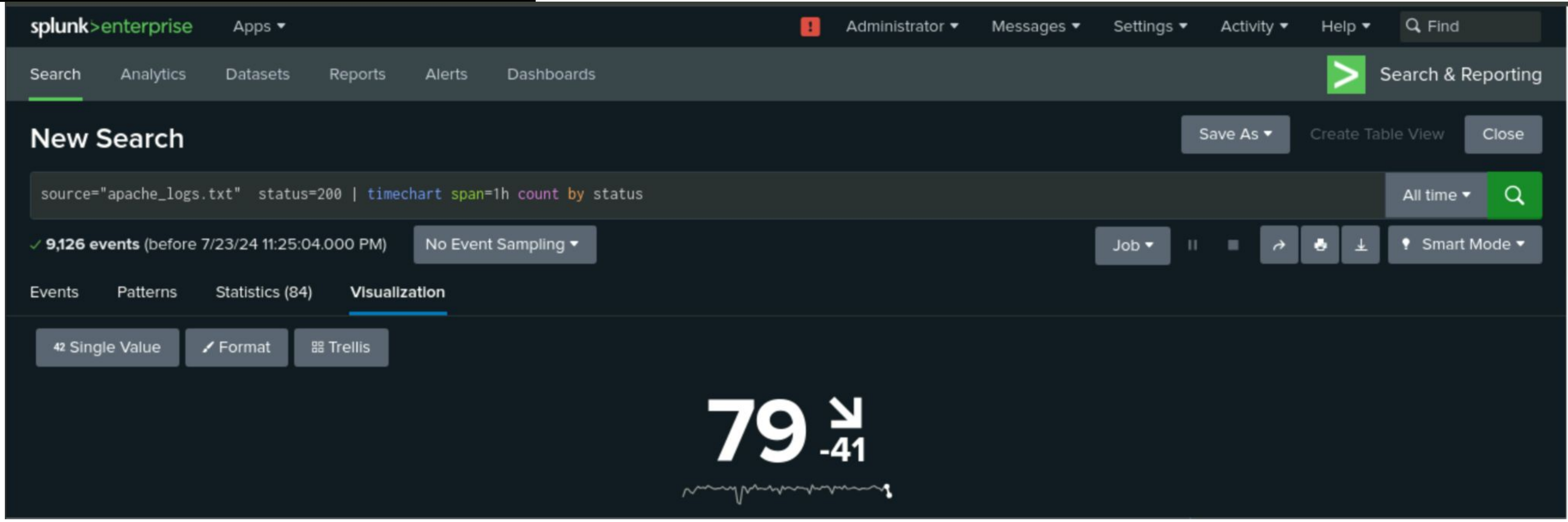
Top 10 Countries by Geolocation

Dashboards—Apache



```
source="apache_logs.txt"  | stats count by uri | dedup uri
```

✓ 10,000 events (before 7/23/24 11:20:27.000 PM)



```
source="apache_logs.txt"  status=200 | timechart span=1h count by status
```

✓ 9,126 events (before 7/23/24 11:25:04.000 PM)

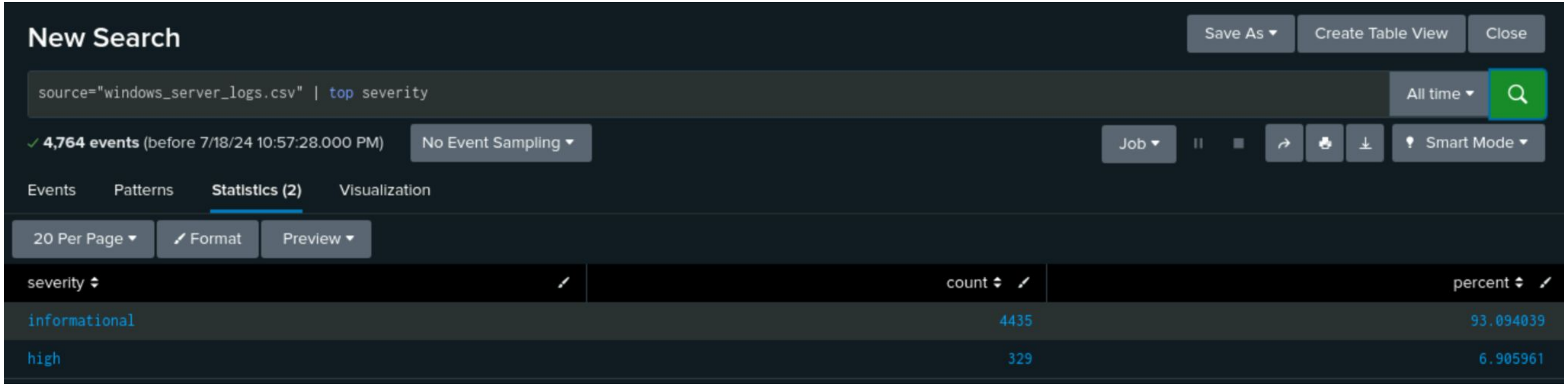
Attack Analysis

Attack Summary—Windows

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

- Compared to the over 93.1% "informational" and 7% “high” severity levels seen prior to the attack, the Windows attack system had more severity levels in the 20.2% "high" and 79.77% “informational” category. After the strike, more successes than failures were also recognized. The alert analysis revealed a concerning amount of unsuccessful attempts.
- On the severity dashboard, there were 13% more events categorized as high.
- Successful logins: An unusually high number of successful logins was found.

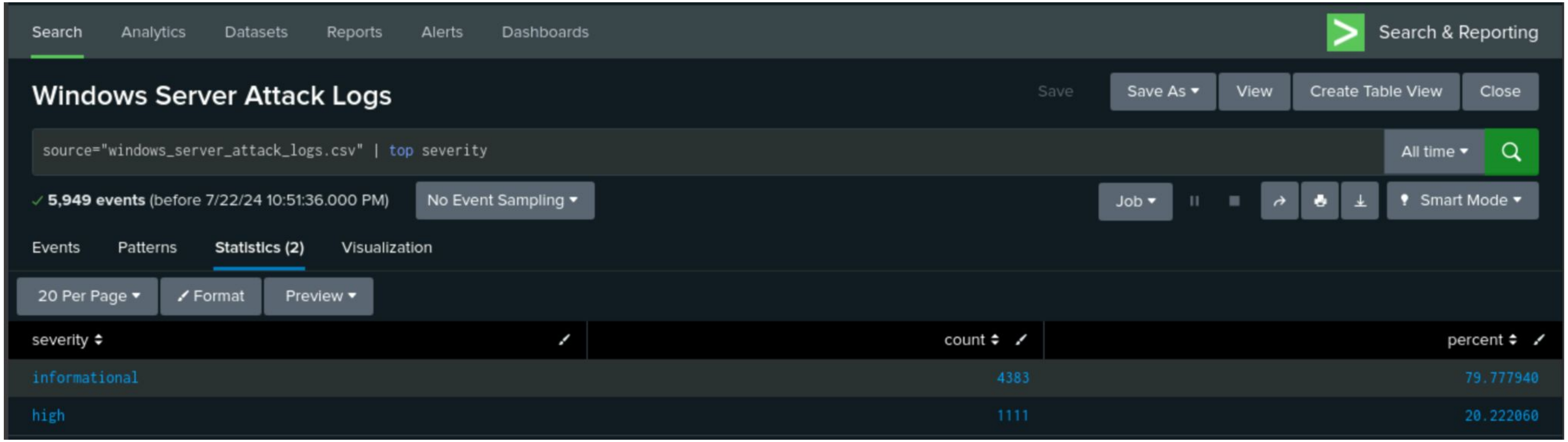
Screenshots of Attack Logs



```
source="windows_server_logs.csv" | top severity
```

✓ **4,764 events** (before 7/18/24 10:57:28.000 PM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961



```
source="windows_server_attack_logs.csv" | top severity
```

✓ **5,949 events** (before 7/22/24 10:51:36.000 PM)

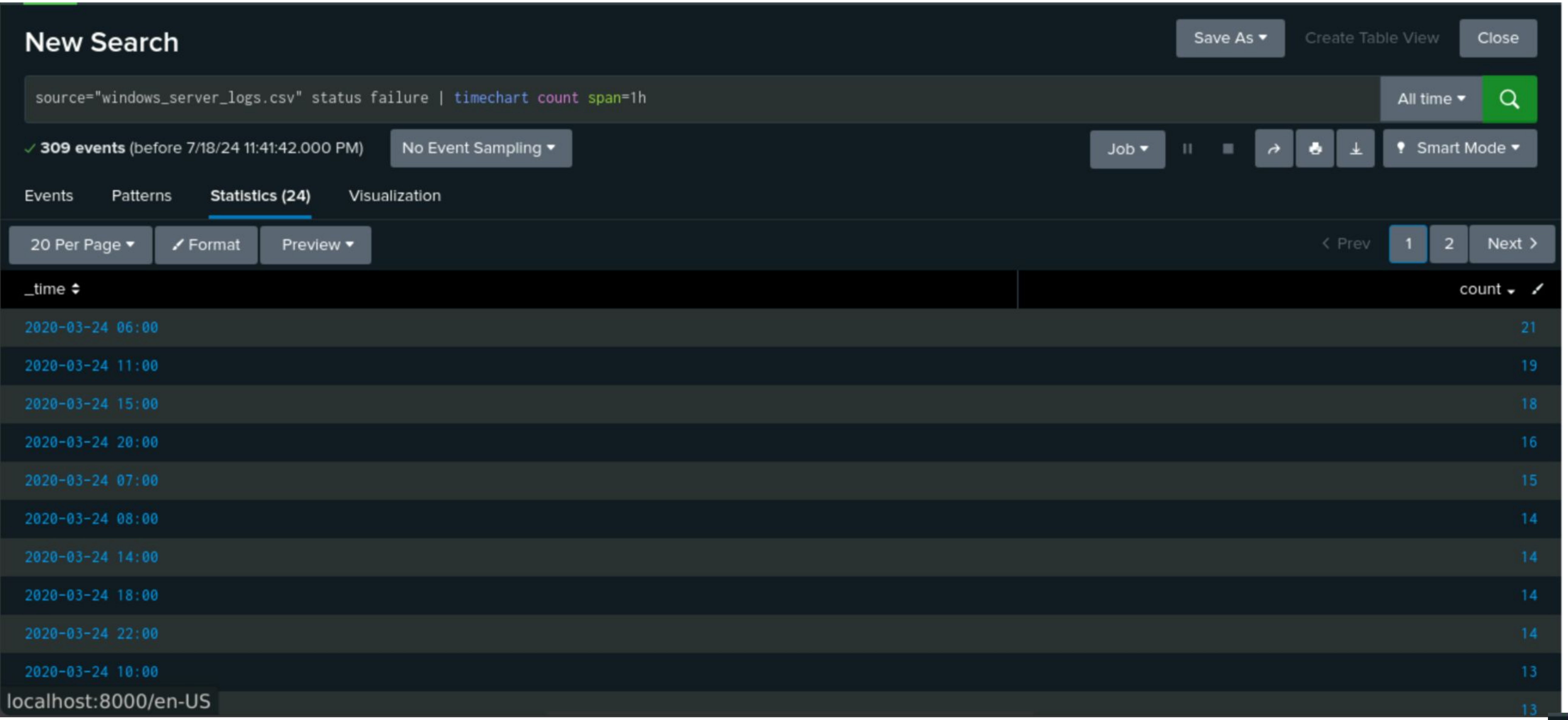
severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Attack Summary—Windows

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

- The alert for the quantity of unsuccessful activities in an hour was turned on. Normally, there are less than 10 failed occurrences every hour, but on March 25, at 8:00 a.m., there were 35.
- No alerts were produced on the quantity of accounts that were deleted or the hourly number of successful logins.
- It appears that every alert threshold has been adjusted to a suitable range.

Screenshots of Attack Logs

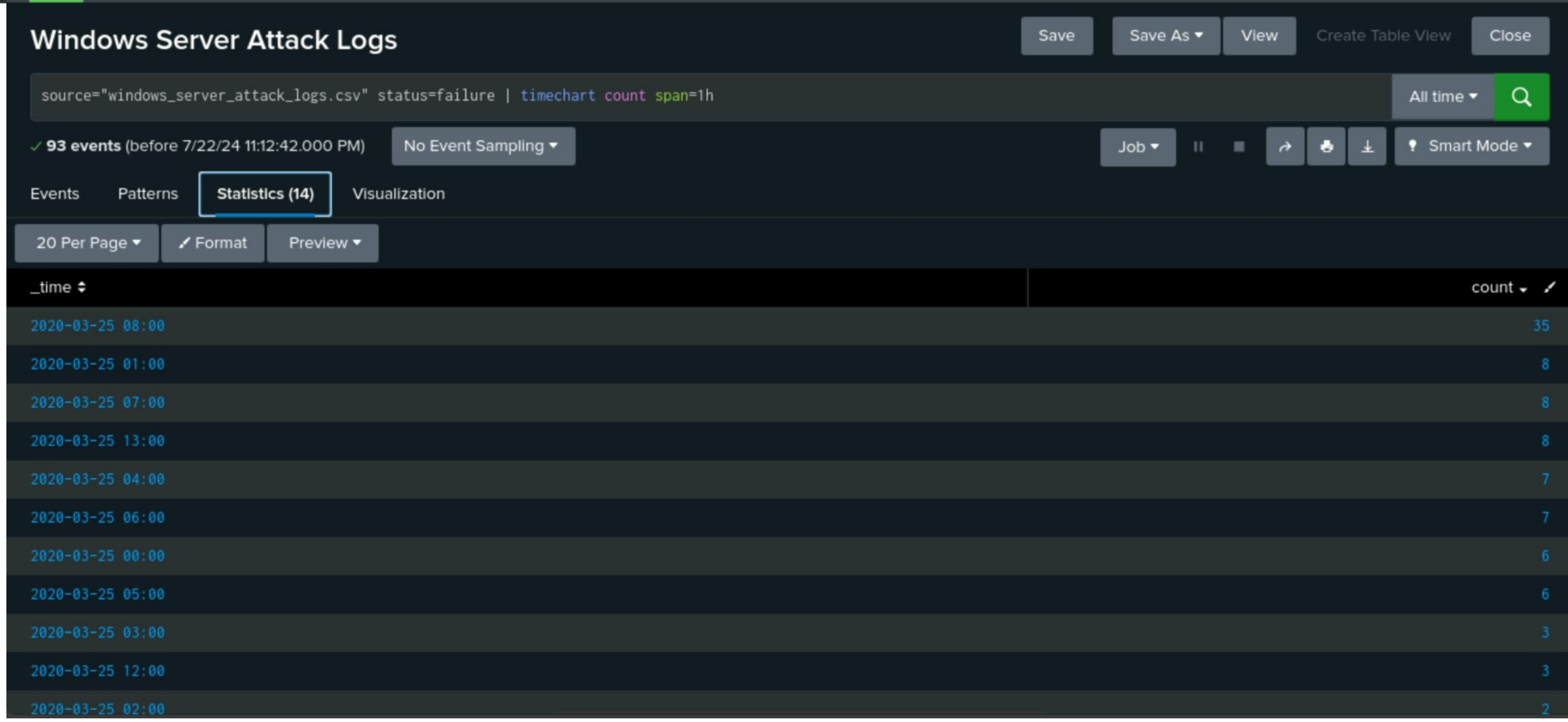


New Search

```
source="windows_server_logs.csv" status failure | timechart count span=1h
```

✓ **309 events** (before 7/18/24 11:41:42.000 PM)

_time	count
2020-03-24 06:00	21
2020-03-24 11:00	19
2020-03-24 15:00	18
2020-03-24 20:00	16
2020-03-24 07:00	15
2020-03-24 08:00	14
2020-03-24 14:00	14
2020-03-24 18:00	14
2020-03-24 22:00	14
2020-03-24 10:00	13
localhost:8000/en-US	13



Windows Server Attack Logs

```
source="windows_server_attack_logs.csv" status=failure | timechart count span=1h
```

✓ **93 events** (before 7/22/24 11:12:42.000 PM)

_time	count
2020-03-25 08:00	35
2020-03-25 01:00	8
2020-03-25 07:00	8
2020-03-25 13:00	8
2020-03-25 04:00	7
2020-03-25 06:00	7
2020-03-25 00:00	6
2020-03-25 05:00	6
2020-03-25 03:00	3
2020-03-25 12:00	3
2020-03-25 02:00	2

Attack Summary—Windows

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

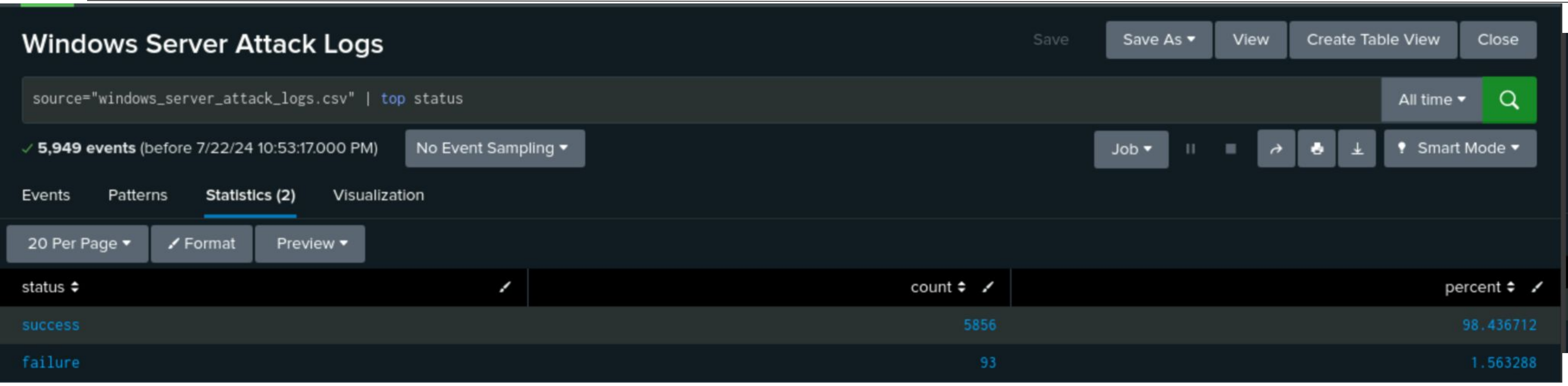
- There were notable shifts in the activity on the signatures for the Dashboard items that tracked signatures by time and total.
  - An attempt was made to reset the password for an account; 1258 incidents took place on 2020-03-25 at 09:00 a.m.
  - Locked user account 896 incidents happened on 2020-03-25 at 02:00 a.m.
  - Account successfully logged in. On 2020-03-25 at 11 a.m., 196 events took place.

Attack Summary—Windows

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

- There were notable shifts in the activity of users A, J, and K, as indicated by the Dashboard items that tracked users by time and total.
  - User K had 1256 events between 9 a.m. and 10 a.m.
  - User A had 984 events between 1a.m. and 2 a.m.
  - User J had 196 events at 11 a.m.

Screenshots of Attack Logs

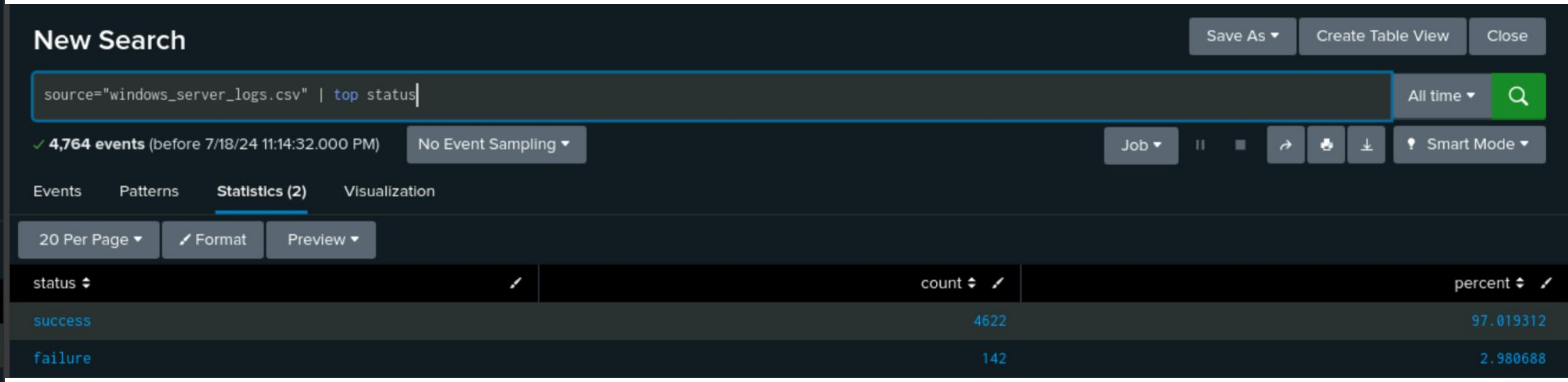


Windows Server Attack Logs

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

✓ **5,949 events** (before 7/22/24 10:53:17.000 PM)

status	count	percent
success	5856	98.436712
failure	93	1.563288

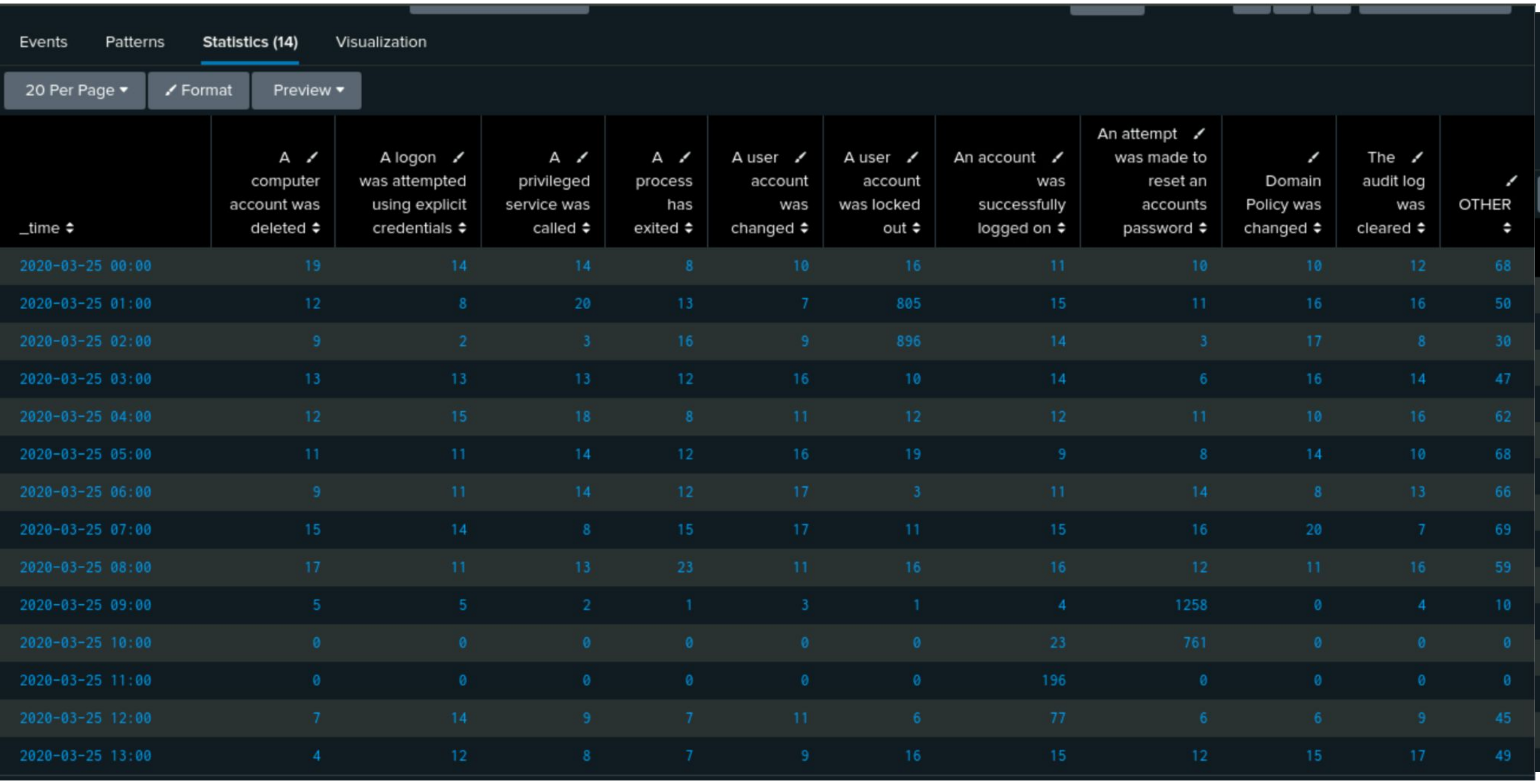


New Search

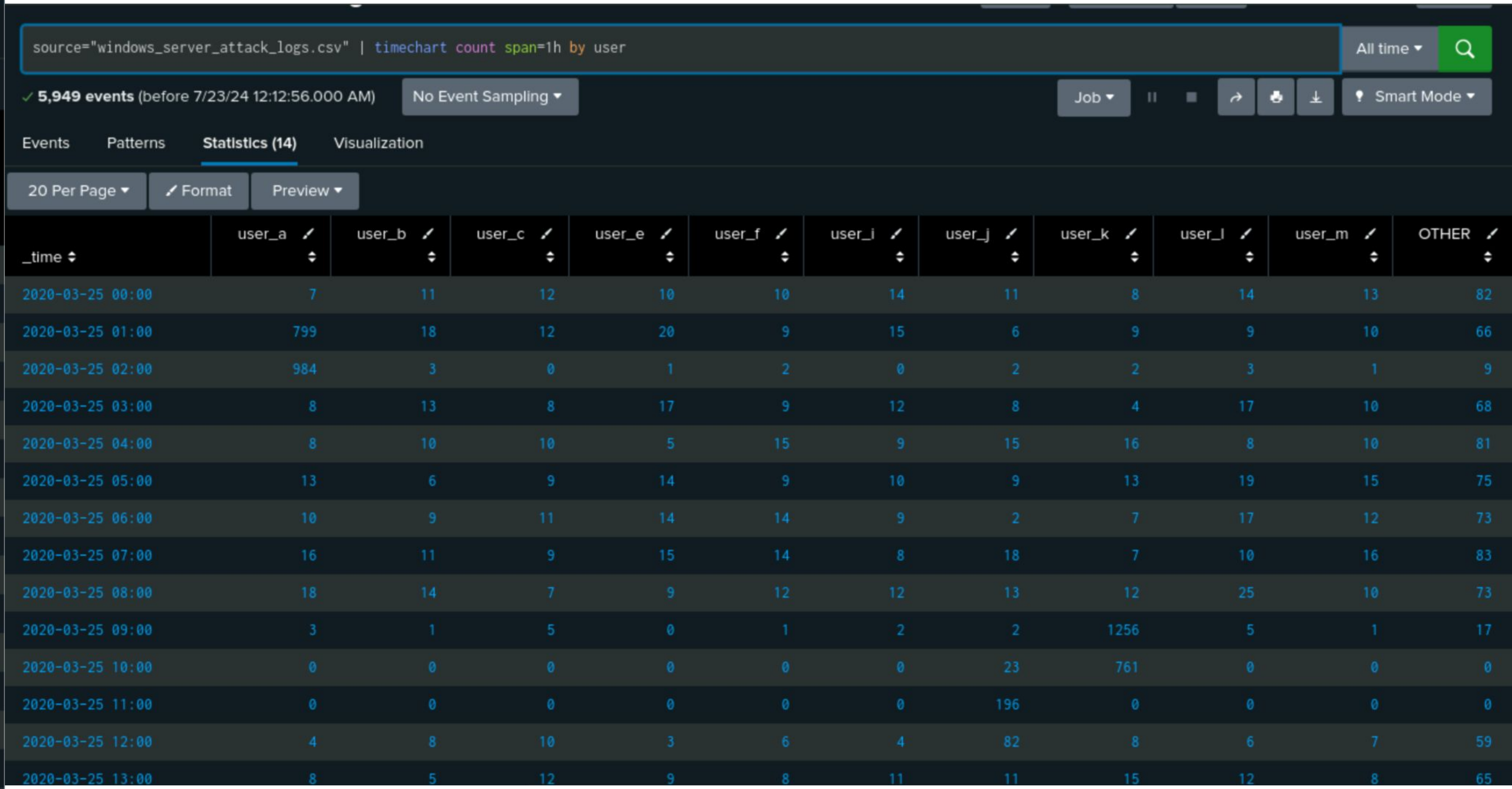
```
source="windows_server_logs.csv" | top status
```

✓ **4,764 events** (before 7/18/24 11:14:32.000 PM)

status	count	percent
success	4622	97.019312
failure	142	2.980688



_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 locked out	An account was successfully logged on	An attempt was made to reset an accounts password	Domain Policy was changed	The audit log was cleared	OTHER
2020-03-25 00:00	19	14	14	8	10	16	11	10	10	12	68
2020-03-25 01:00	12	8	20	13	7	805	15	11	16	16	50
2020-03-25 02:00	9	2	3	16	9	896	14	3	17	8	30
2020-03-25 03:00	13	13	13	12	16	10	14	6	16	14	47
2020-03-25 04:00	12	15	18	8	11	12	12	11	10	16	62
2020-03-25 05:00	11	11	14	12	16	19	9	8	14	10	68
2020-03-25 06:00	9	11	14	12	17	3	11	14	8	13	66
2020-03-25 07:00	15	14	8	15	17	11	15	16	20	7	69
2020-03-25 08:00	17	11	13	23	11	16	16	12	11	16	59
2020-03-25 09:00	5	5	2	1	3	1	4	1258	0	4	10
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	7	14	9	7	11	6	77	6	6	9	45
2020-03-25 13:00	4	12	8	7	9	16	15	12	15	17	49



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

✓ **5,949 events** (before 7/23/24 12:12:56.000 AM)

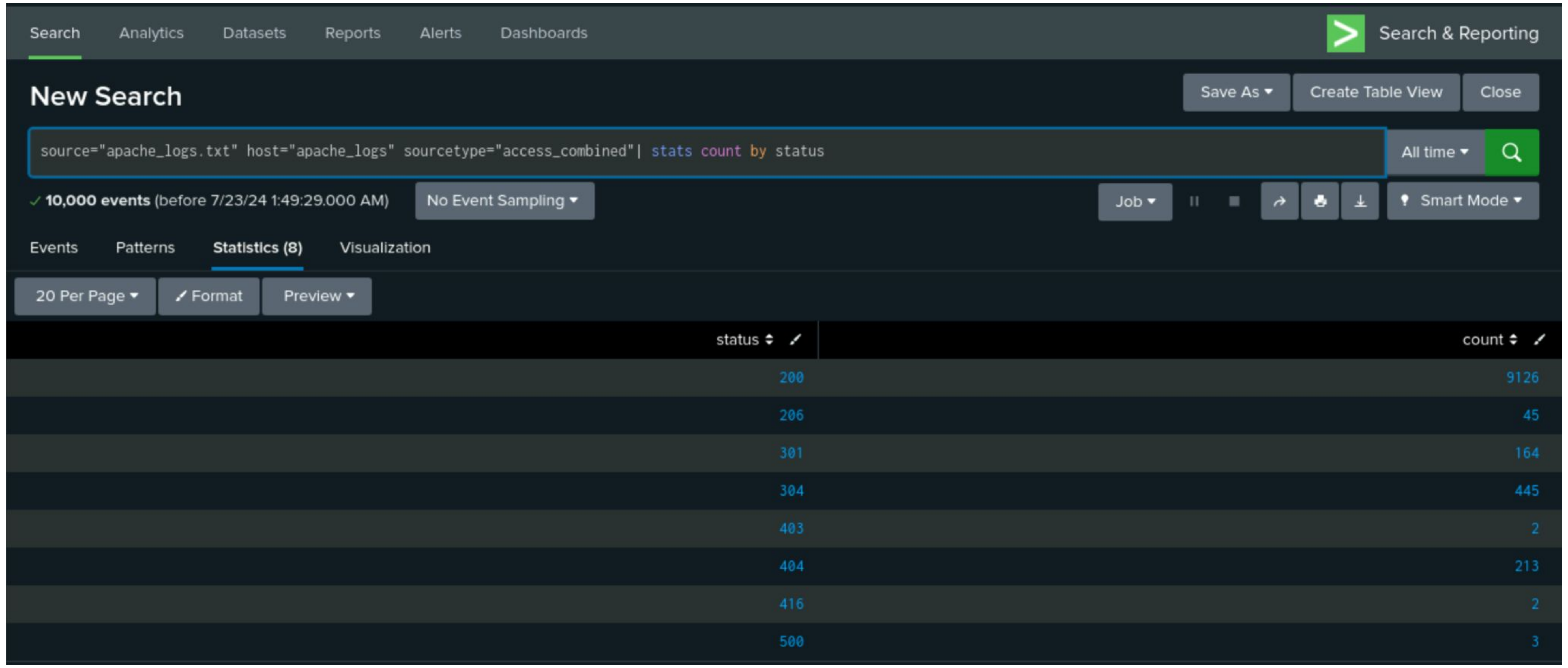
_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	16	83
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	4	8	10	3	6	4	82	8	6	7	59
2020-03-25 13:00	8	5	12	9	8	11	11	15	12	8	65

Attack Summary—Apache

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

- The use of POST and HTTP techniques increased significantly.
- Regarding referral domains, we found no indications of questionable activities.
- The research on HTTP Response Codes revealed an increase in "404" responses.

Screenshots of Attack Logs

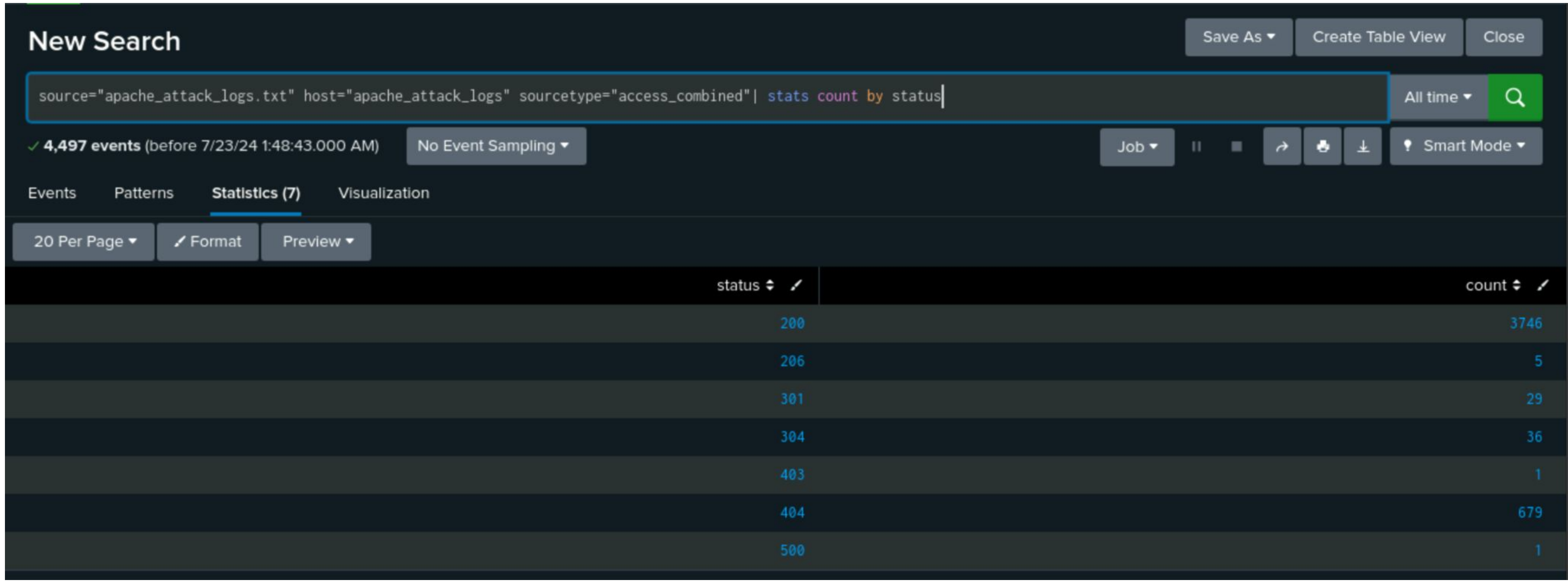


New Search

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

✓ 10,000 events (before 7/23/24 1:49:29.000 AM)

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



New Search

```
source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined"| stats count by status
```

✓ 4,497 events (before 7/23/24 1:48:43.000 AM)

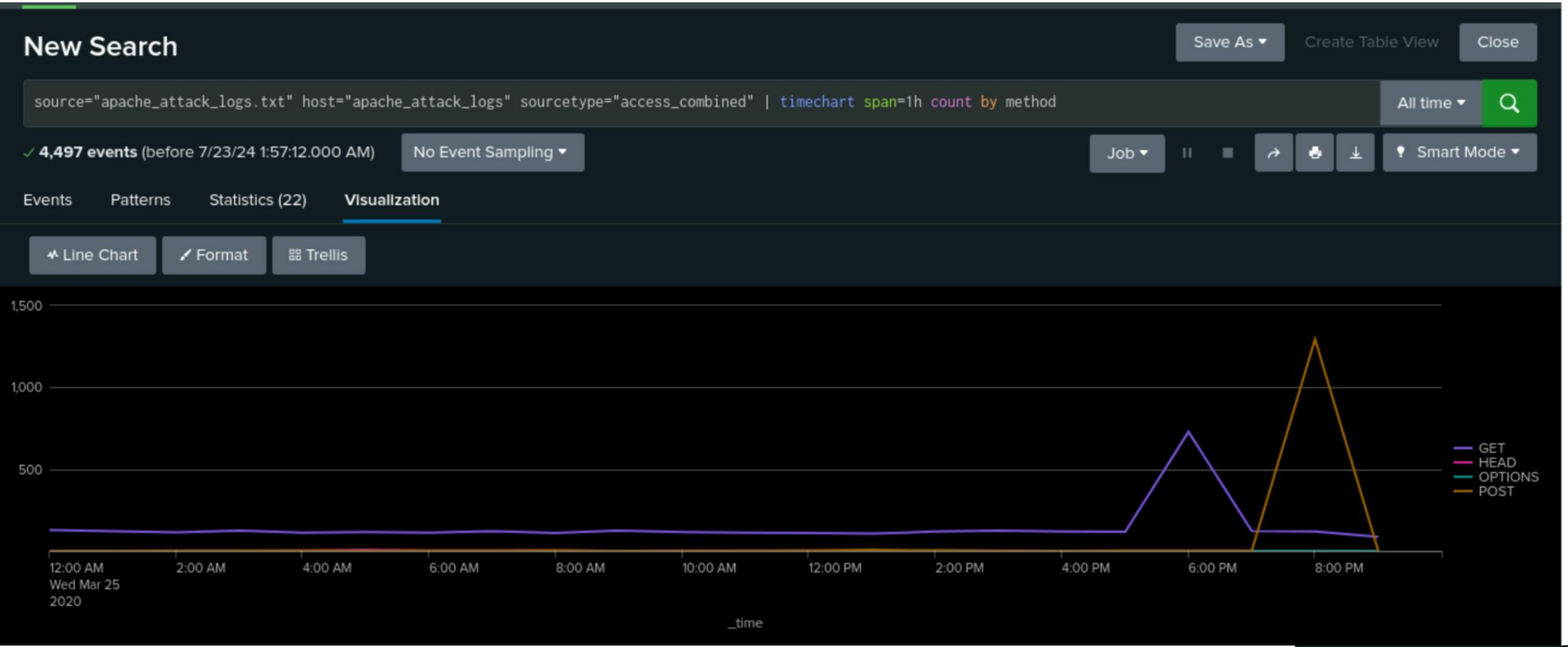
status	count
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

Attack Summary—Apache

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

- Unusual GET and POST method volumes were shown in our HTTP methods Time Chart.
  - Between 5 and 7 o'clock in the evening, the GET attack peaked with a count of 729.
  - The POST attack peaked with a total of 1,296 and ran from 7 to 9 p.m.
- "/VSI_Account_logon.php" was identified by our URI Data as having an unusually high volume.

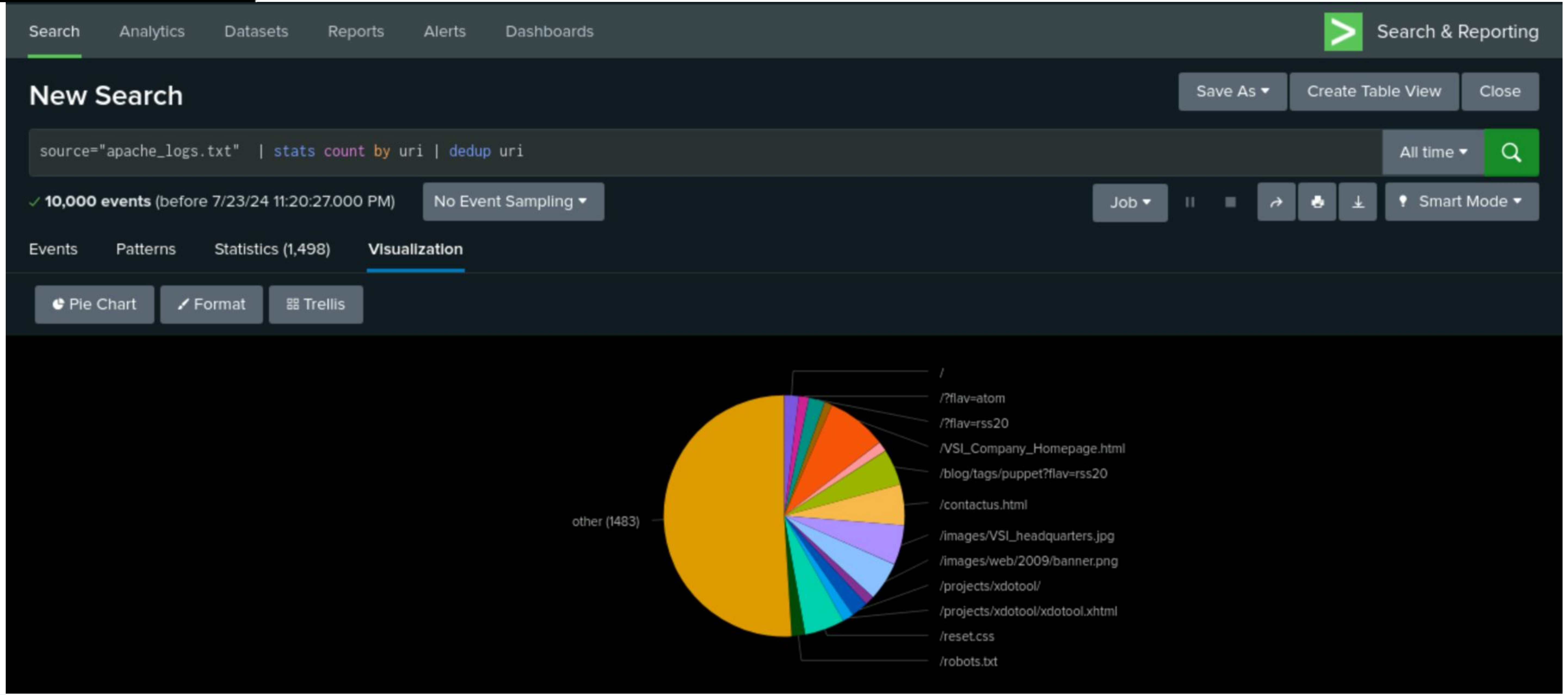
Screenshots of Attack Logs



New Search

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

✓ **4,497 events** (before 7/23/24 1:57:12.000 AM)



New Search

```
source="apache_logs.txt"  | stats count by uri | dedup uri
```

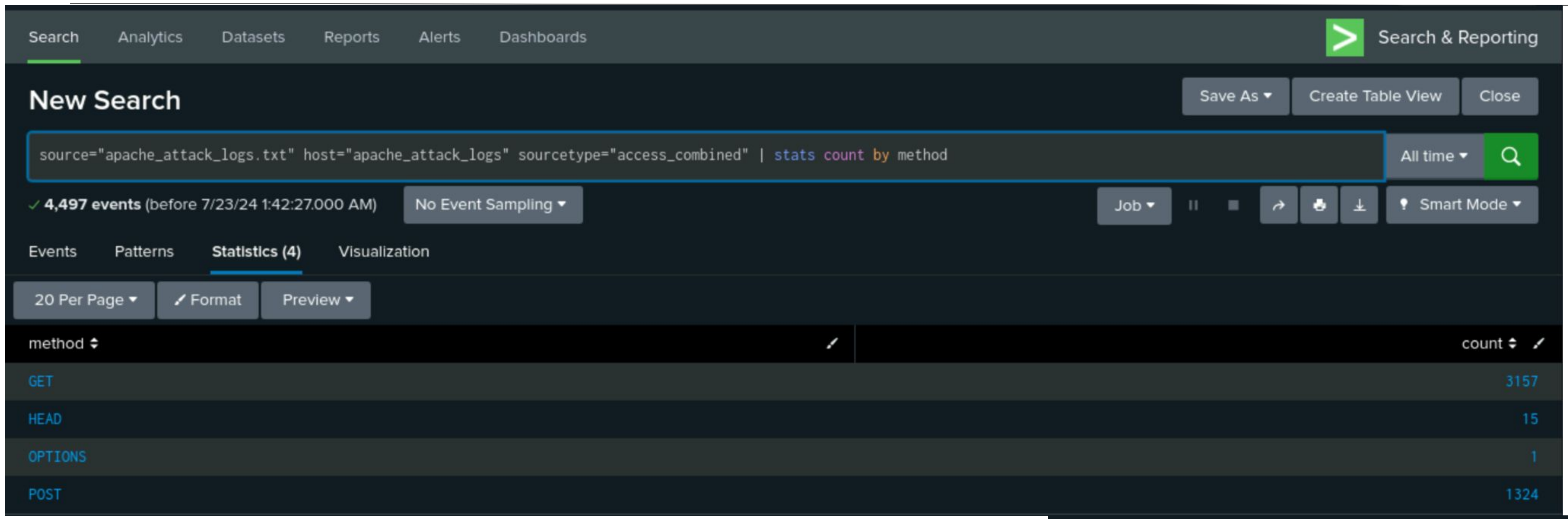
✓ **10,000 events** (before 7/23/24 11:20:27.000 PM)

Attack Summary—Apache

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

- A few cities' unusual activity was shown on our cluster map.
- There was an increase in HTTP POST traffic from Ukraine, which resulted in several attempts to reach the login page.
  - In comparison, Switzerland accounted for the second-highest number of events, with a count of 299, and Ukraine, with a count of 887.

Screenshots of Attack Logs

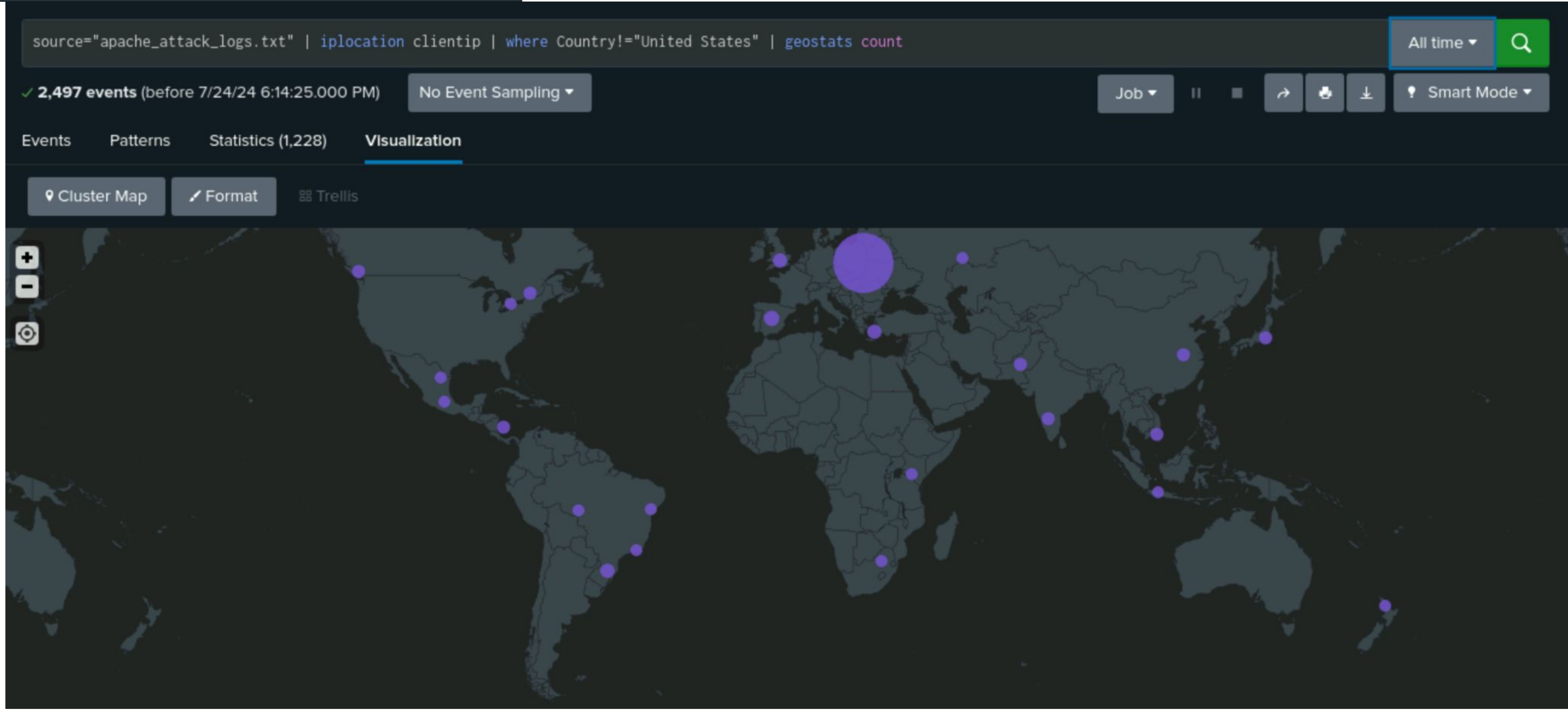


New Search

```
source="apache_attack_logs.txt" host="apache_attack_logs" sourcetype="access_combined" | stats count by method
```

✓ 4,497 events (before 7/23/24 1:42:27.000 AM)

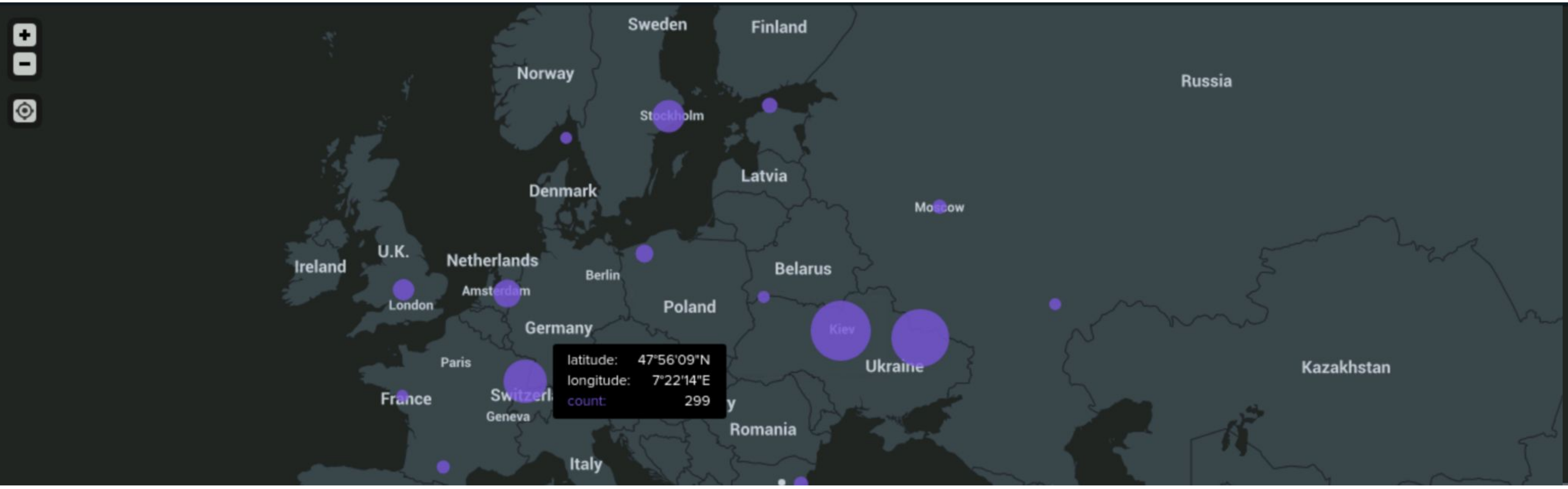
method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324



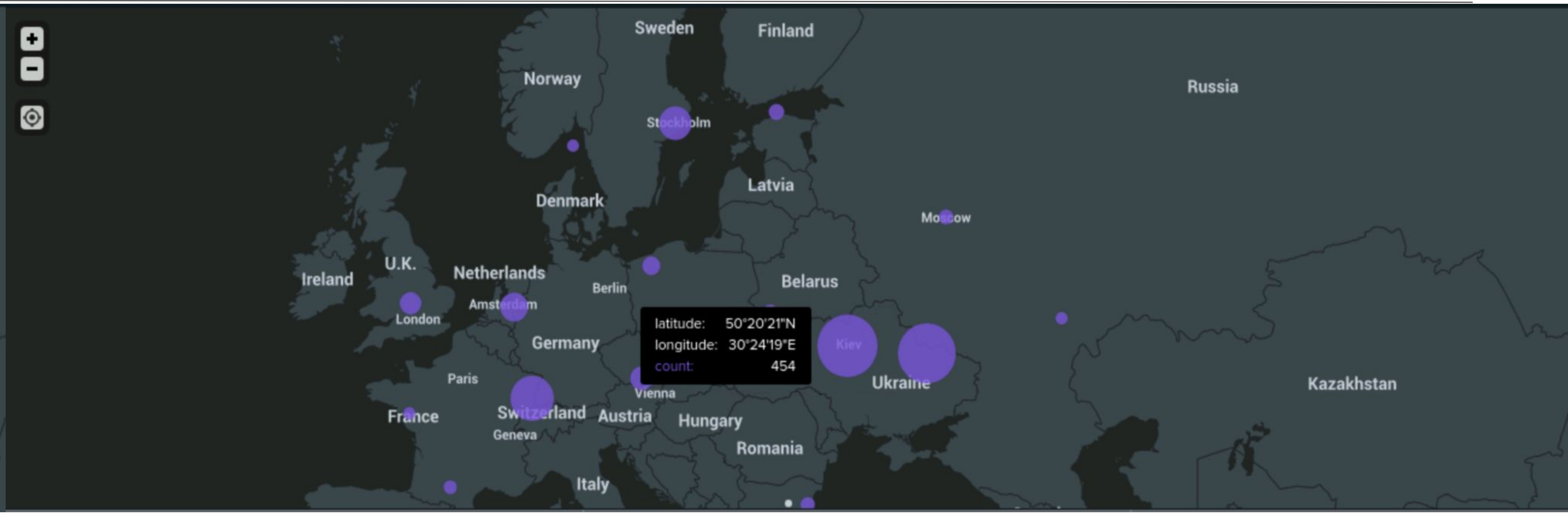
```
source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States" | geostats count
```

✓ 2,497 events (before 7/24/24 6:14:25.000 PM)

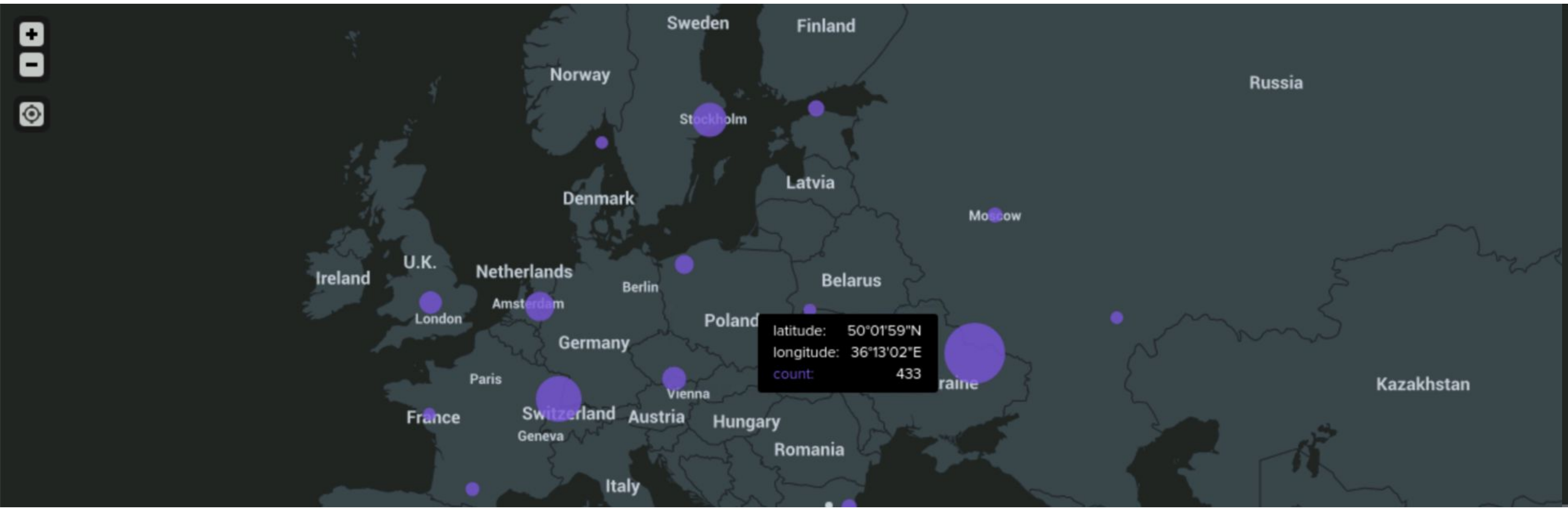
Screenshots of Attack Logs



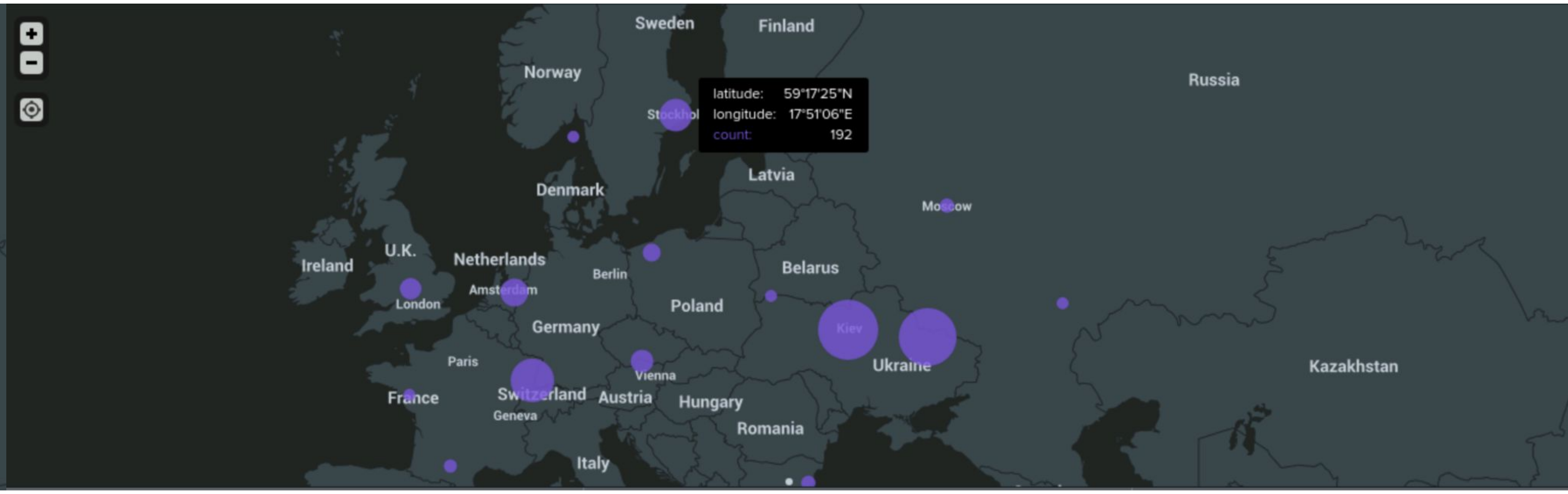
latitude: 47°56'09"N
longitude: 7°22'14"E
count: 299



latitude: 50°20'21"N
longitude: 30°24'19"E
count: 454



latitude: 50°01'59"N
longitude: 36°13'02"E
count: 433



latitude: 59°17'25"N
longitude: 17°51'06"E
count: 192

Summary and Future Mitigations

Project 3 Summary

Summary of the Windows Server Attack and Suggestions: General Results

- On March 25, 2020 a person or people going by the names of K, A, and J were attacked using bruteforce, the Windows server in an attempt to access the system. Resetting account passwords was attempted during the attack, and it seems that some of those attempts were effective in increasing the number of successful logins.

- To protect VSI from future attacks, what future mitigations would you recommend?
  - The first level of protection against brute force assaults is two-factor authentication.
  - To stop such attacks, lock users out after a set number of failed login attempts.