Defensive Security Project
by: SOC Analysts (VSI)

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- We are SOC analysts at a small company called **Virtual Space Industries (VSI)**, which designs virtual-reality programs for businesses.
- VSI has heard rumors that a competitor, **JobeCorp**, may launch cyberattacks to disrupt VSI’s business.
- As SOC analysts, we are tasked with using Splunk to monitor potential attacks on our systems and applications.
- The VSI products that we have been tasked with monitoring include:
    - An Apache web server, which hosts the administrative webpage
    - A Windows operating system, which runs many of VSI’s back-end operations
- Our networking team has provided us with past logs to help us develop baselines and create reports, alerts, dashboards, and more.

“WHOIS” App

WHOIS - Summary

This app implements investigative actions that query the whois database

Supported Actions

- Test connectivity: Validate the configuration for connectivity
- Whois domain: Execute a whois lookup on the given domain
- Whois ip: Execute a whois lookup on the given IP

WHOIS – Scenario Illustrating Benefits

Suspicious Activity Detected

SIEM alerts us to a series of failed login attempts targeting VSI's internal developer portal. The attempts originate from multiple IP addresses that are unfamiliar to us. Concerned, we pivot to Splunk to investigate further.

Using the WHOIS Add-on for Threat Attribution

To quickly determine if these IPs are linked to a known adversary, we utilize the WHOIS Splunk add-on to enrich our logs with domain registration details. Within seconds, we discover:

- Several of the flagged IPs are registered under a hosting provider frequently used for malicious activity.
- One domain, jobe-securedev.com, was registered just days ago using privacy masking. The name is suspiciously similar to our competitor JobeCorp.
- The WHOIS information reveals that the registrar is the same one JobeCorp has used in the past for legitimate domains.

Escalation & Defensive Action

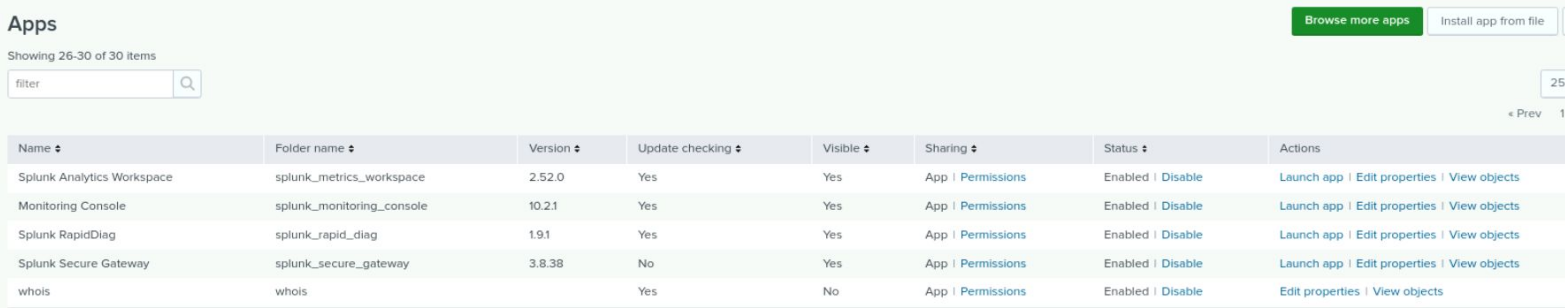
With this intelligence, our SOC team correlates the failed logins with previously observed phishing attempts impersonating VSI's internal services. We escalate the case to leadership, who notify legal and IT security.

- IT blocks all traffic from the suspicious IPs to prevent further login attempts.
- We update firewall rules and SIEM alerts to monitor for future activity from similar IP ranges.
- SOC initiates proactive threat hunting, using WHOIS lookups to identify other potentially related domains.

Outcome: Attack Disrupted, Security Strengthened

Thanks to the WHOIS add-on in Splunk, we quickly linked the attack attempts to our competitor and took preventive measures before an actual breach could occur. Moving forward, we integrate automated WHOIS lookups into our SIEM workflows to enhance our threat detection capabilities.

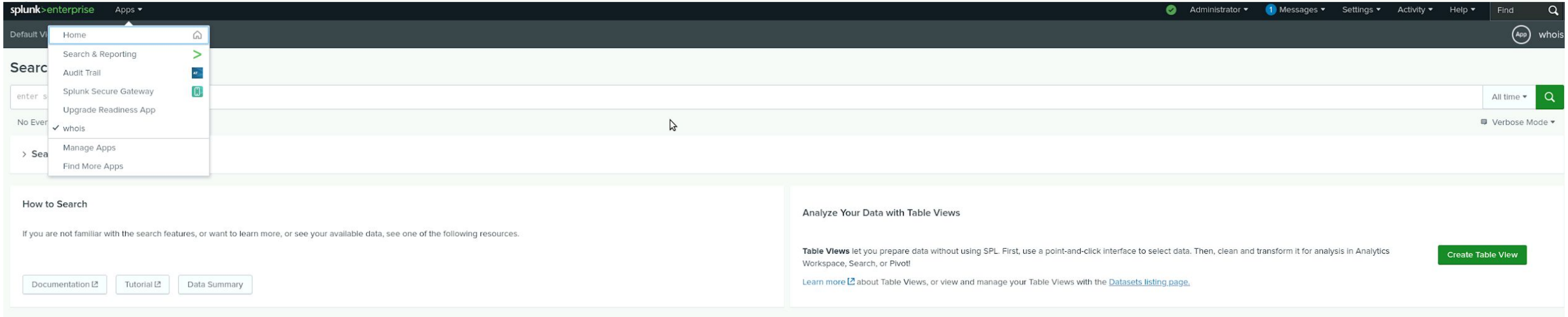
WHOIS - Images



Apps

Showing 26-30 of 30 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Analytics Workspace	splunk_metrics_workspace	2.52.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Monitoring Console	splunk_monitoring_console	10.2.1	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Splunk RapidDiag	splunk_rapid_diag	1.9.1	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Splunk Secure Gateway	splunk_secure_gateway	3.8.38	No	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
whois	whois		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects



How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Logs Analyzed

1 **Windows Logs**

This Server contains the properties of VSI's next generation virtual-reality programs

2 **Apache Logs**

Logs for VSI's Main Public website

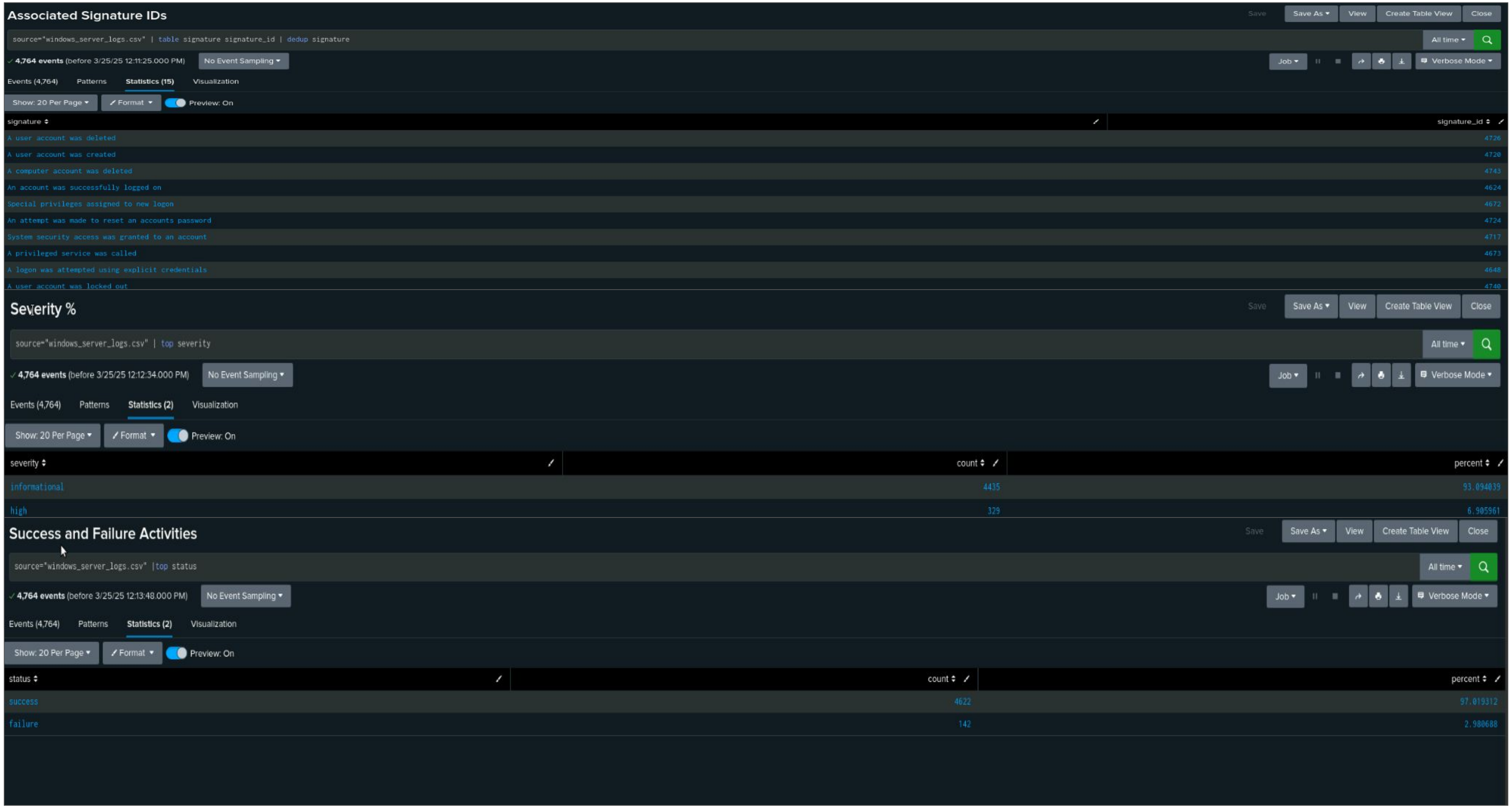
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Associated Signature IDs	A report of IDs associated with Windows activities that are attached with specific signature
Severity %	A quick report of Informational and High Percentages showcasing the severity level of the Logs being viewed
Success and Failure Activities	A report that showcases if there are any suspicious activity of failure or success on the server

Images of Reports—Windows



Associated Signature IDs

```
source="windows_server_logs.csv" | table signature signature_id | dedup signature
```

✓ **4,764 events** (before 3/25/25 12:11:25.000 PM)

signature	signature_id
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740

Severity %

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

✓ **4,764 events** (before 3/25/25 12:12:34.000 PM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Success and Failure Activities

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

✓ **4,764 events** (before 3/25/25 12:13:48.000 PM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Failure Alert	Threshold of Failed Windows Activity being reached	6	10

JUSTIFICATION: Looking through the data we noticed that with the average number of failed activity being around 6 it can be determined that this would be the baseline. After looking at the data again we came to the decision that since none of the data hit an activity count of 10 we choose that to be the threshold for alerts.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Successful Log In	Threshold of Successful Logged on	12	30

JUSTIFICATION: With the data presenting an average of about 12 to make the baseline for use we noticed that it as well never came close to our threshold of 30 but if it were to reach 30 then that would trigger our suspicious activity alert.

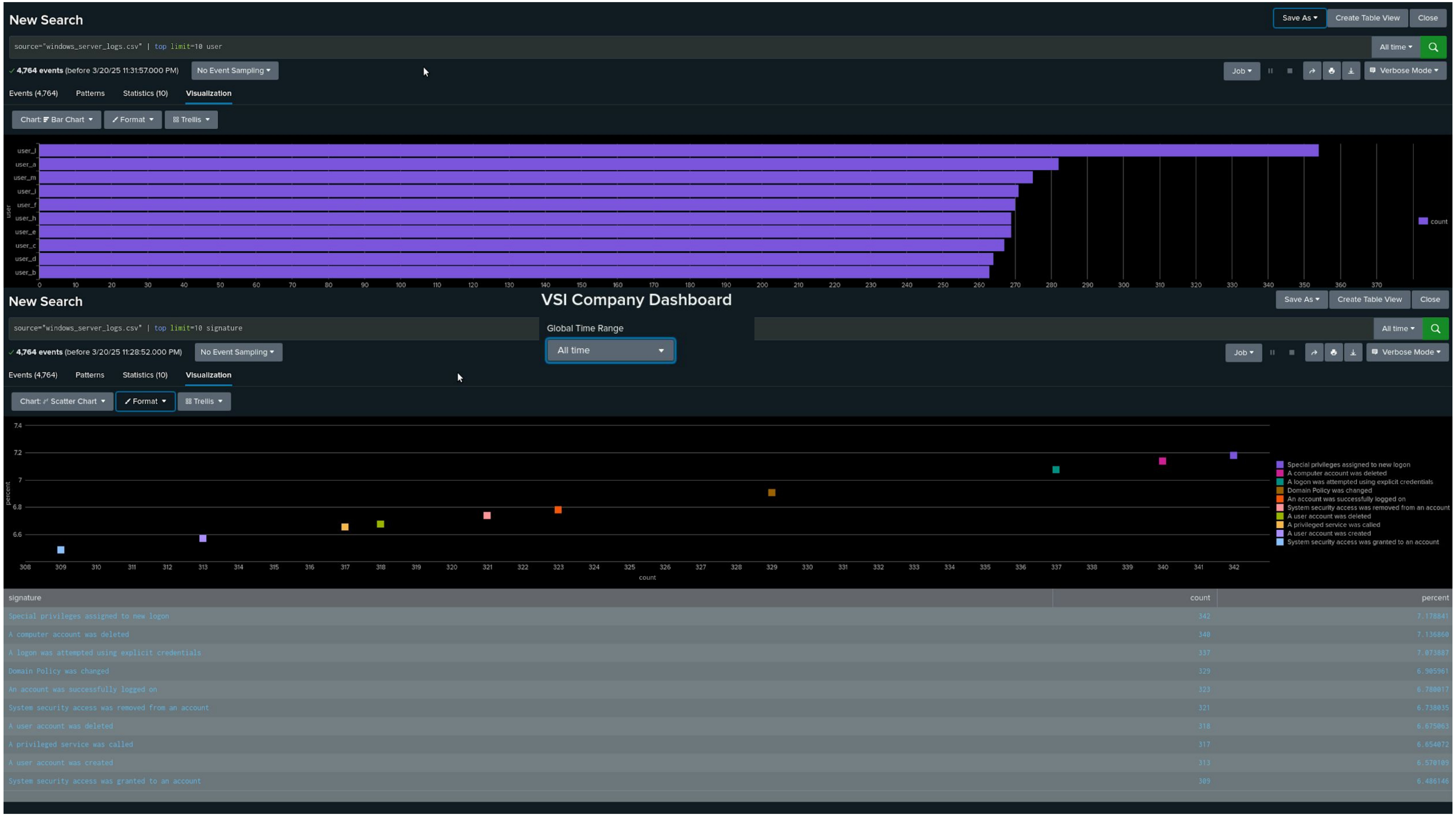
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Account Deleted	Threshold for Deleted User Accounts	13	40

JUSTIFICATION: Through the data an average of 13 determined our baseline and after looking at the data more having a threshold of 40 would trigger a suspicious alert.

Dashboards—Windows



New Search

```
source="windows_server_logs.csv" | top limit=10 user
```

✓ 4,764 events (before 3/20/25 11:31:57.000 PM)

Events (4,764) Patterns Statistics (10) Visualization

Chart: Bar Chart

VSI Company Dashboard

Global Time Range: All time

New Search

```
source="windows_server_logs.csv" | top limit=10 signature
```

✓ 4,764 events (before 3/20/25 11:28:52.000 PM)

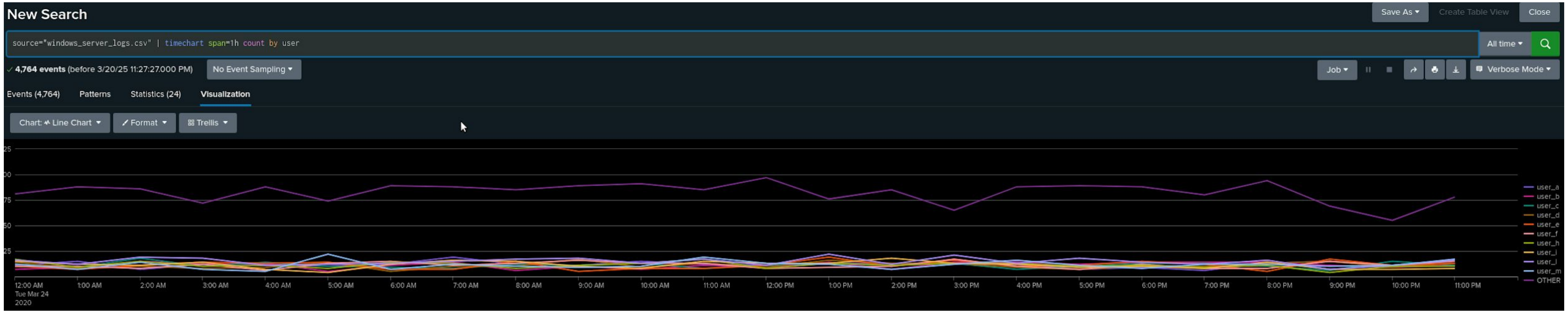
Events (4,764) Patterns Statistics (10) Visualization

Chart: Scatter Chart

Save As
Create Table View
Close
All time
No Event Sampling
Job
Verbose Mode
Format
Trellis
7.4
7.2
7
6.8
6.6
percent
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
count
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
System security access was removed from an account
A user account was deleted
A privileged service was called
A user account was created
System security access was granted to an account

signature	count	percent
Special privileges assigned to new logon	342	7.178841
A computer account was deleted	340	7.136860
A logon was attempted using explicit credentials	337	7.073887
Domain Policy was changed	329	6.905961
An account was successfully logged on	323	6.780017
System security access was removed from an account	321	6.738035
A user account was deleted	318	6.675063
A privileged service was called	317	6.654072
A user account was created	313	6.570109
System security access was granted to an account	309	6.486146

Dashboards—Windows

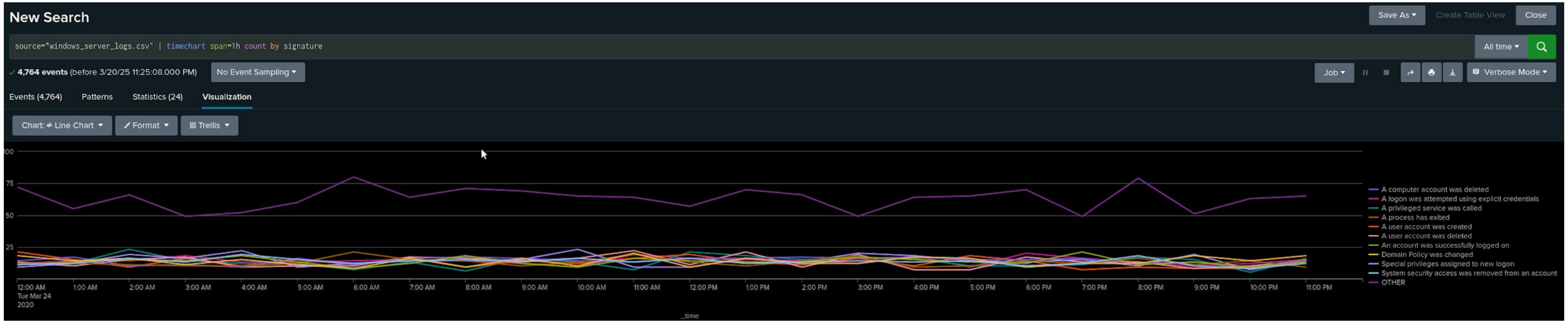


New Search

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

✓ **4,764 events** (before 3/20/25 11:27:27.000 PM)

Events (4,764) Patterns Statistics (24) **Visualization**



New Search

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

✓ **4,764 events** (before 3/20/25 11:25:08.000 PM)

Events (4,764) Patterns Statistics (24) **Visualization**

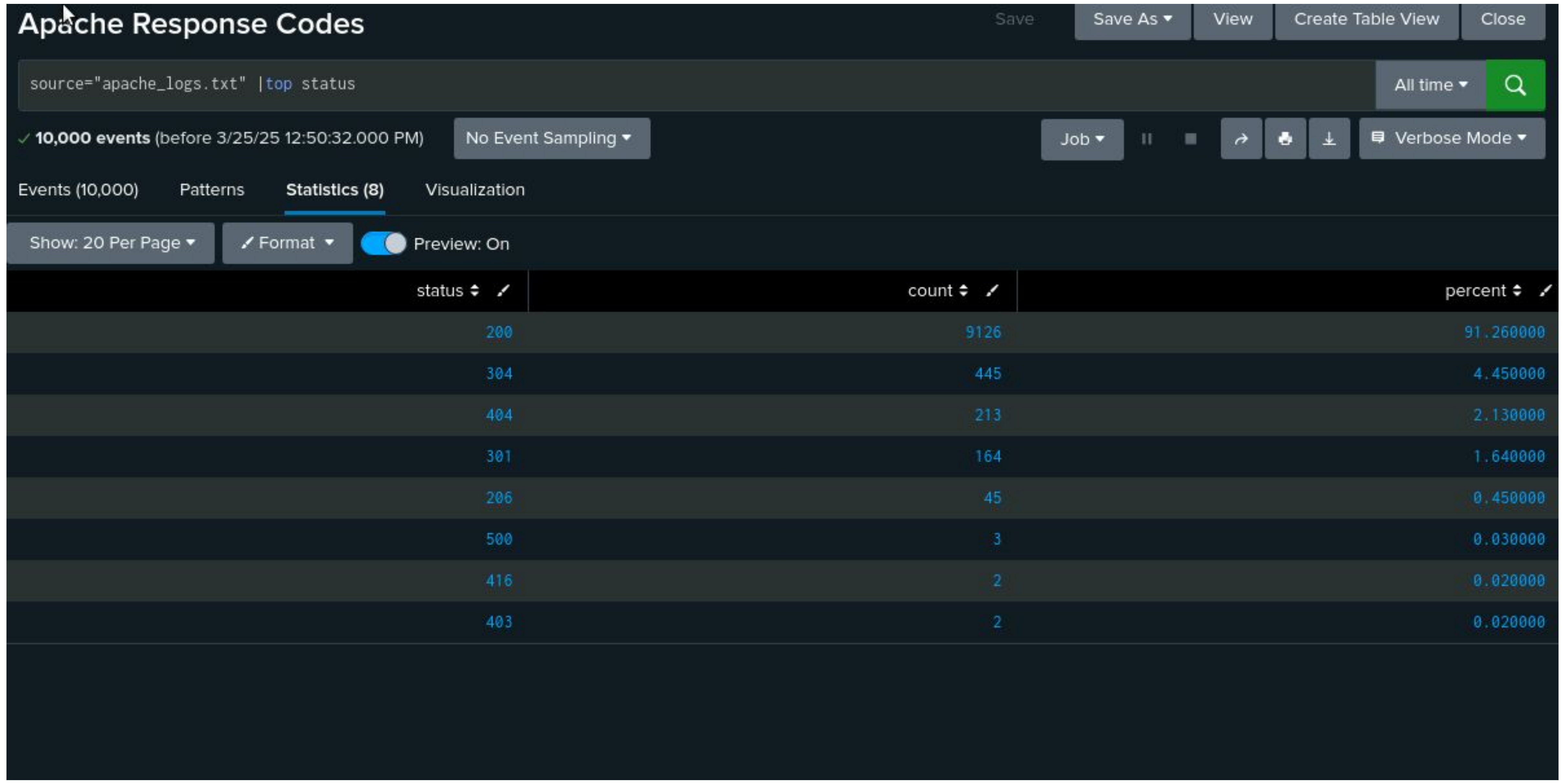
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
Apache Methods	Shows which HTTP Methods are being requested the most
Apache Top Domains	Shows the top domains that are associated to VSI's website
Apache Response Codes	Shows the HTTP codes and the count of how frequent is it being used

Images of Reports—Apache

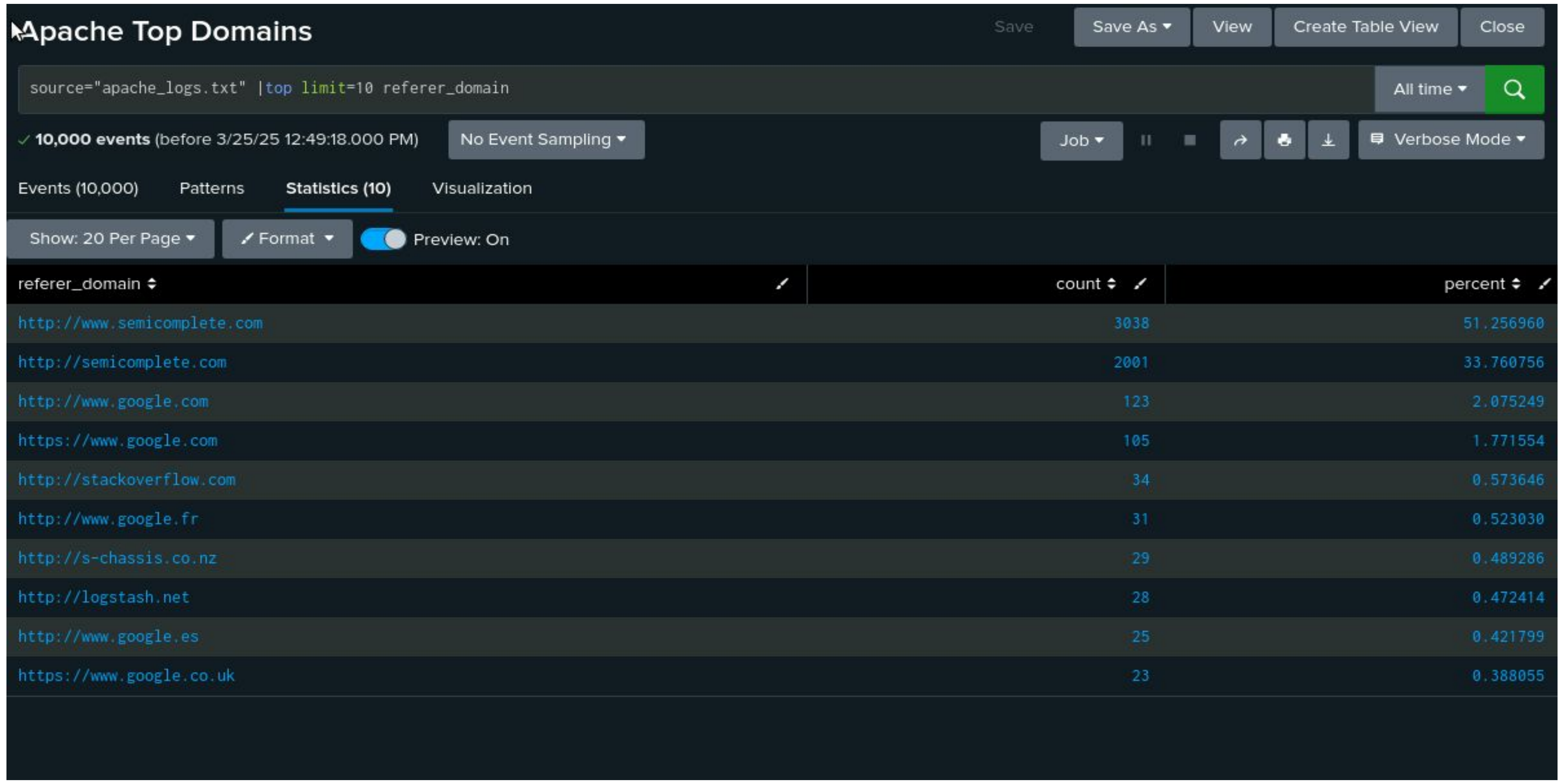


Apache Response Codes

```
source="apache_logs.txt" |top status
```

✓ **10,000 events** (before 3/25/25 12:50:32.000 PM)

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

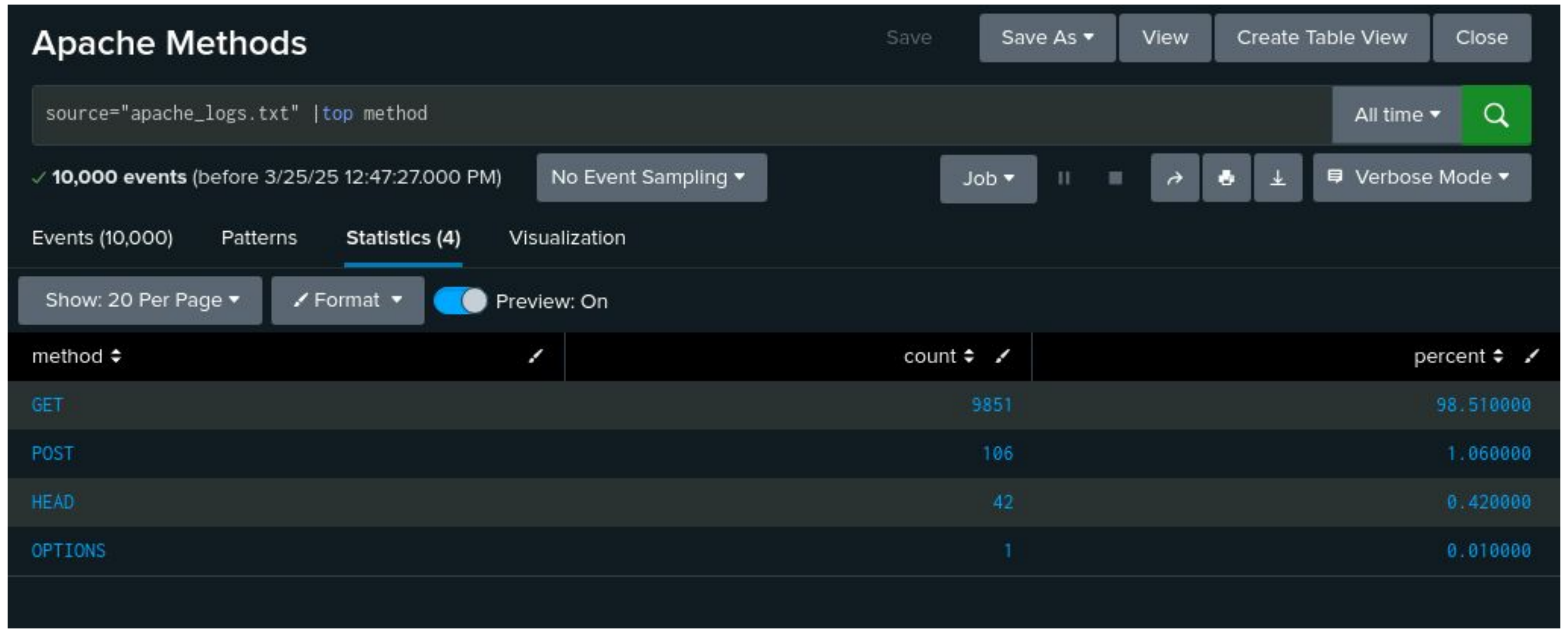


Apache Top Domains

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

✓ **10,000 events** (before 3/25/25 12:49:18.000 PM)

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



Apache Methods

```
source="apache_logs.txt" |top method
```

✓ **10,000 events** (before 3/25/25 12:47:27.000 PM)

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Outside USA Activity	Creates an Alert if the Threshold is triggered by increased Activity outside of the USA	85	160

JUSTIFICATION: After reviewing the data and noticing an average of 85 events being standards in the logs but with some events being in the 100s as well creating a threshold of 160 would create a large suspicious radar as none of the data came close to that data number.

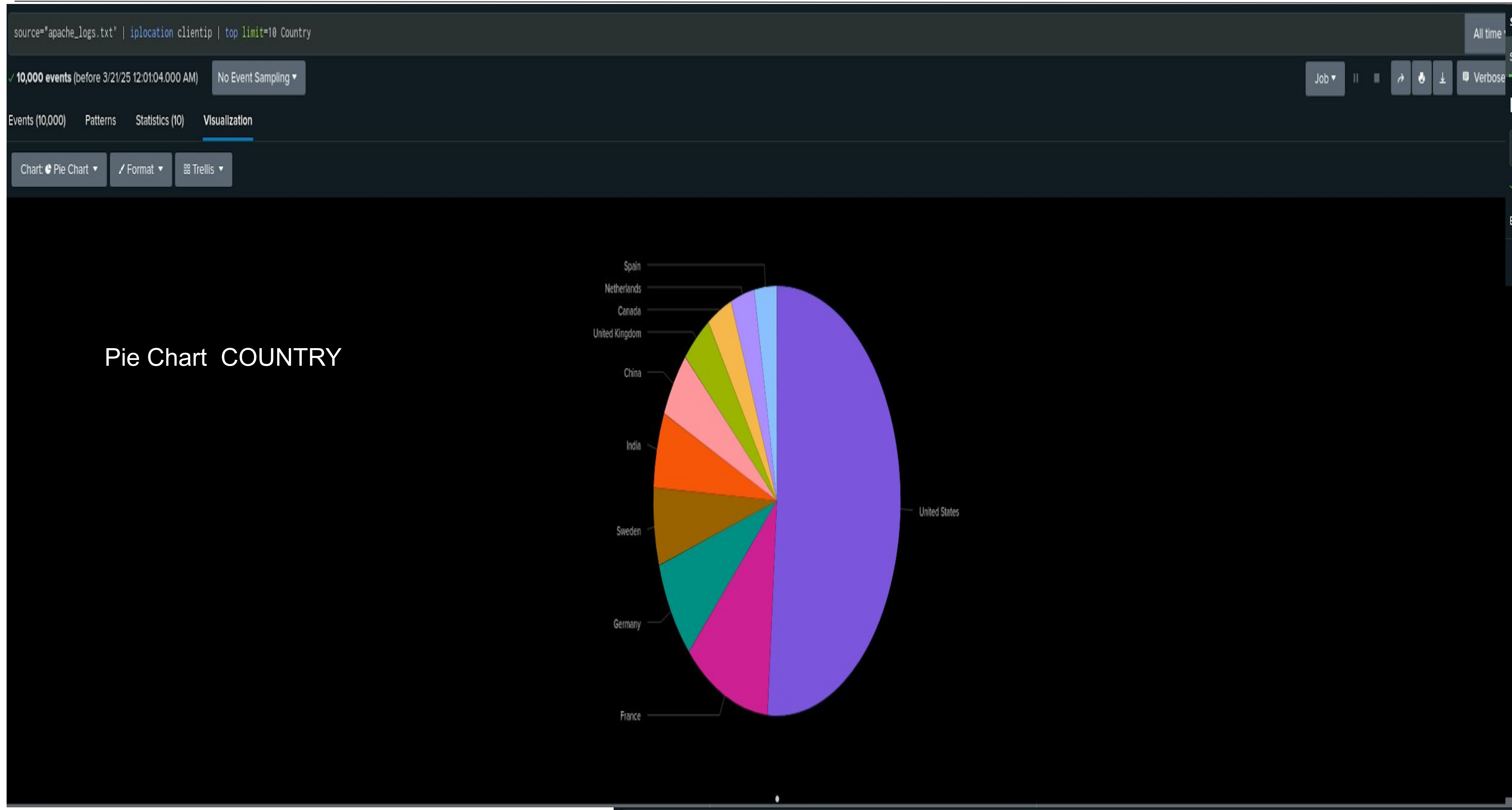
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST Count	Triggers when the threshold count is reached during its hourly check of POST method for HTTP	3	10

JUSTIFICATION: The average through the data was between the low numbers of 1 and 4 and by creating a threshold that doubles the amount from the average would trigger suspicious.

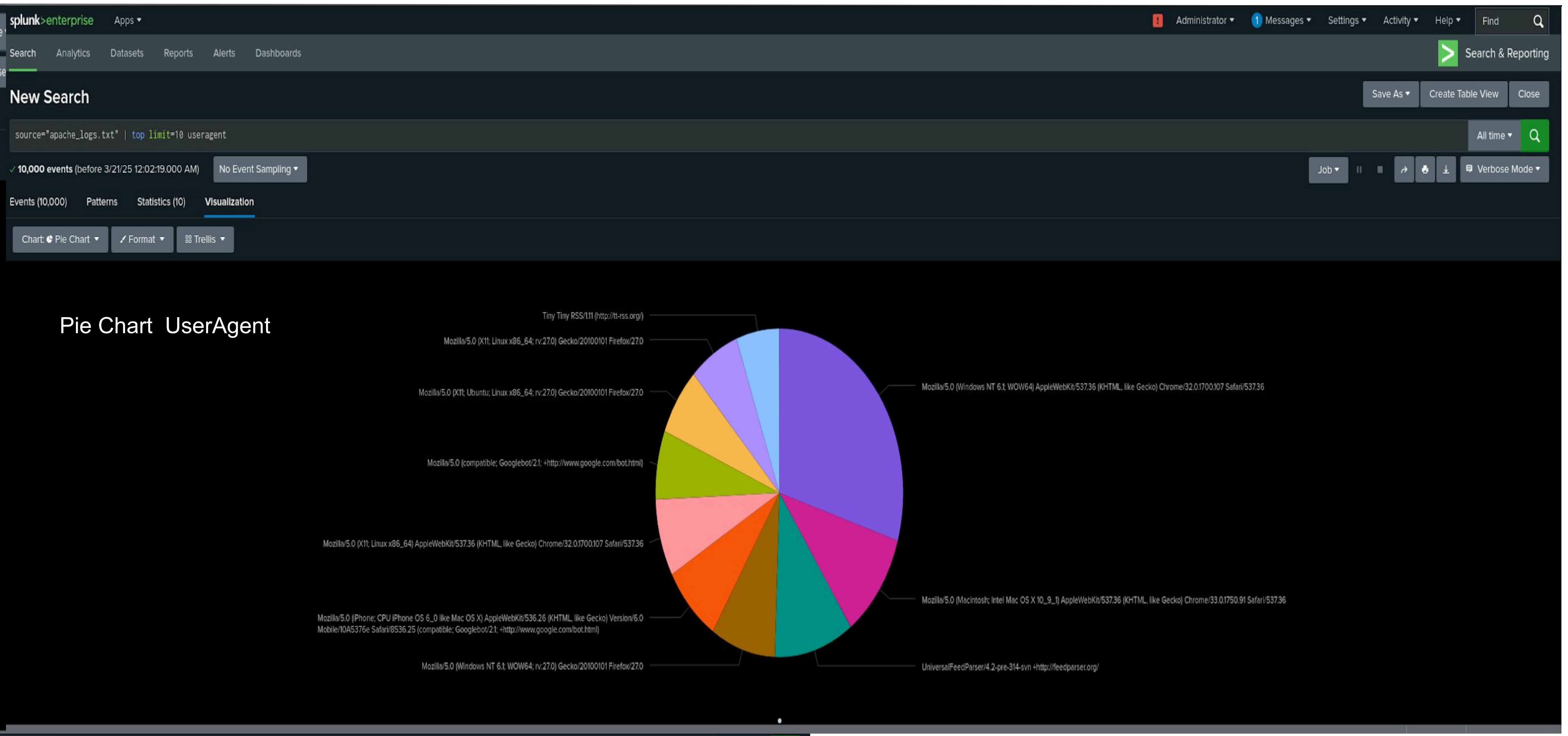
Dashboards—Apache



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

✓ 10,000 events (before 3/21/25 12:01:04.000 AM)

Pie Chart COUNTRY



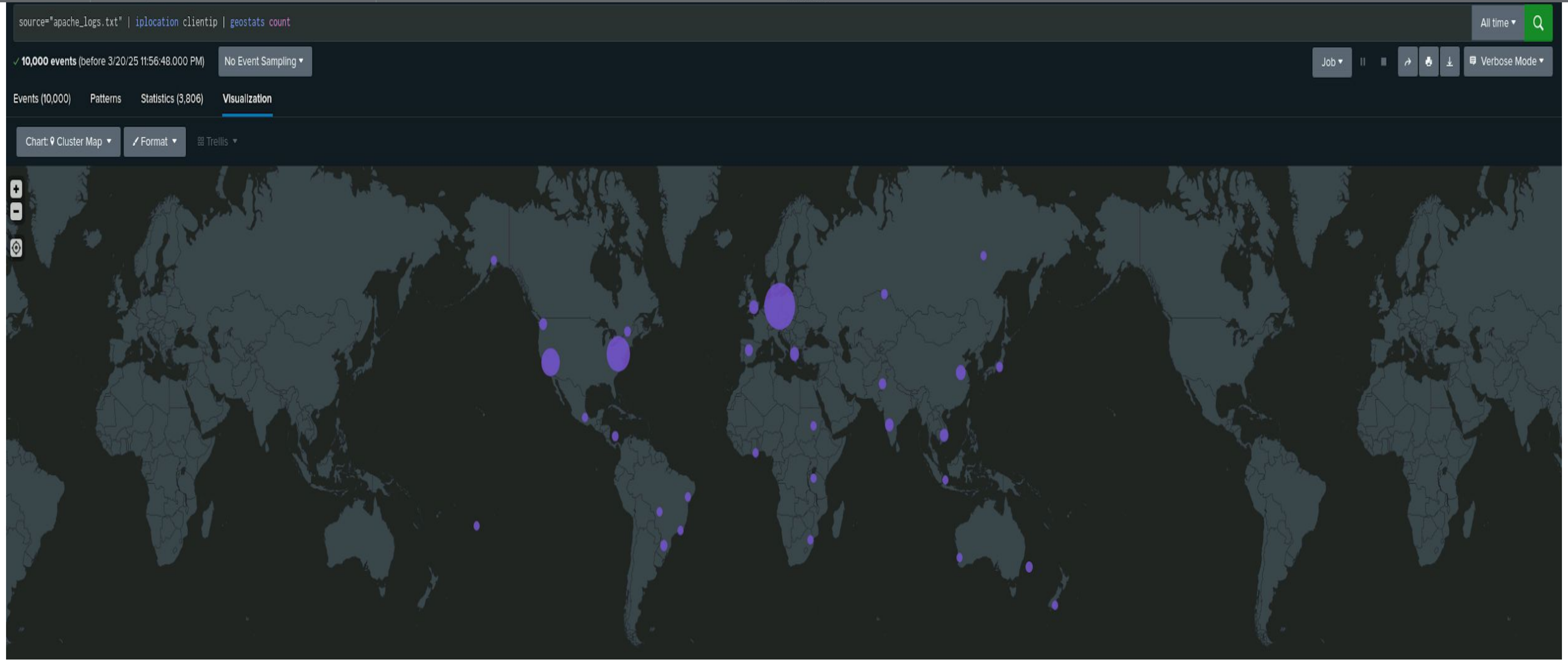
New Search

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

✓ 10,000 events (before 3/21/25 12:02:19.000 AM)

Pie Chart UserAgent

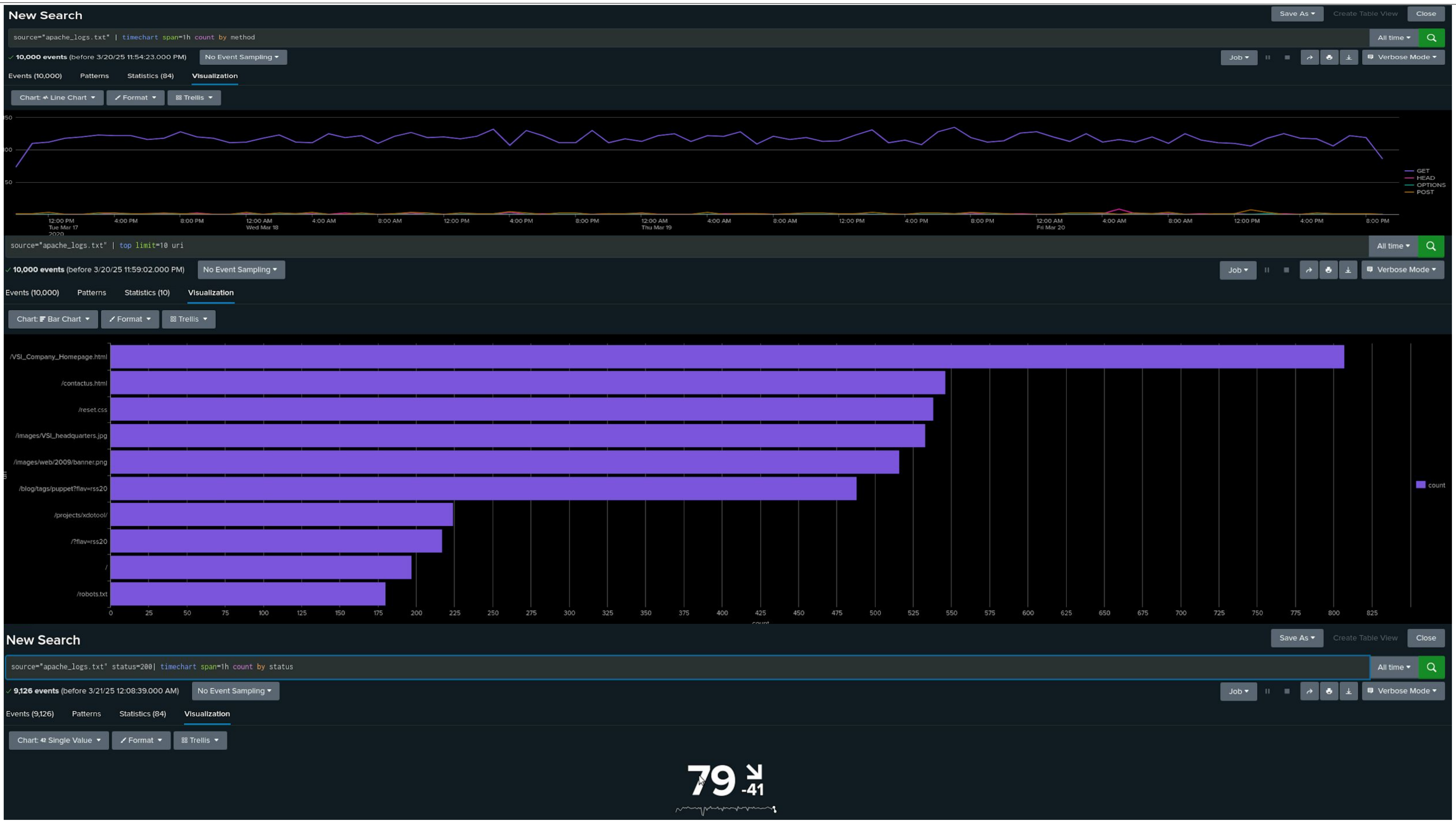
splunk>enterprise
Apps ▾
Administrator ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Save As ▾
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Verbose Mode ▾
Events (10,000)
Patterns
Statistics (10)
Visualization
Chart: Pie Chart ▾
Format ▾
Trellis ▾
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
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)
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
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)
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
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 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/



```
source="apache_logs.txt" | iplocation clientip | geostats count
```

✓ 10,000 events (before 3/20/25 11:56:48.000 PM)

Dashboards—Apache



New Search

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

✓ 10,000 events (before 3/20/25 11:54:23.000 PM)

Chart: Line Chart · Format · Trellis

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

✓ 10,000 events (before 3/20/25 11:59:02.000 PM)

Chart: Bar Chart · Format · Trellis

New Search

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

✓ 9,126 events (before 3/21/25 12:08:39.000 AM)

Chart: Single Value · Format · Trellis

Attack Analysis

Attack Summary—Windows

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

- Upon analyzing the attack logs, we observed notable shifts in severity levels that suggest potential suspicious activity. The percentage of informational severity incidents decreased from 93% to 80%, marking a 13% decline, while high-severity incidents rose from 7% to 20%, reflecting a corresponding 13% increase. This significant change indicates a possible escalation in threat levels, warranting further investigation into the nature of these high-severity events. However, when examining failed window activities, we found no major fluctuations that would suggest unusual behavior. Successful activities increased slightly from 97% to 98%, while failed attempts decreased from 3% to 2%, indicating a minor shift but nothing indicative of a widespread attack or significant breach attempt. While the failed activity report does not raise immediate concerns, the increase in high-severity incidents suggests a potential emerging threat that requires closer monitoring to determine the root cause and mitigate any risks.

Attack Summary—Windows

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

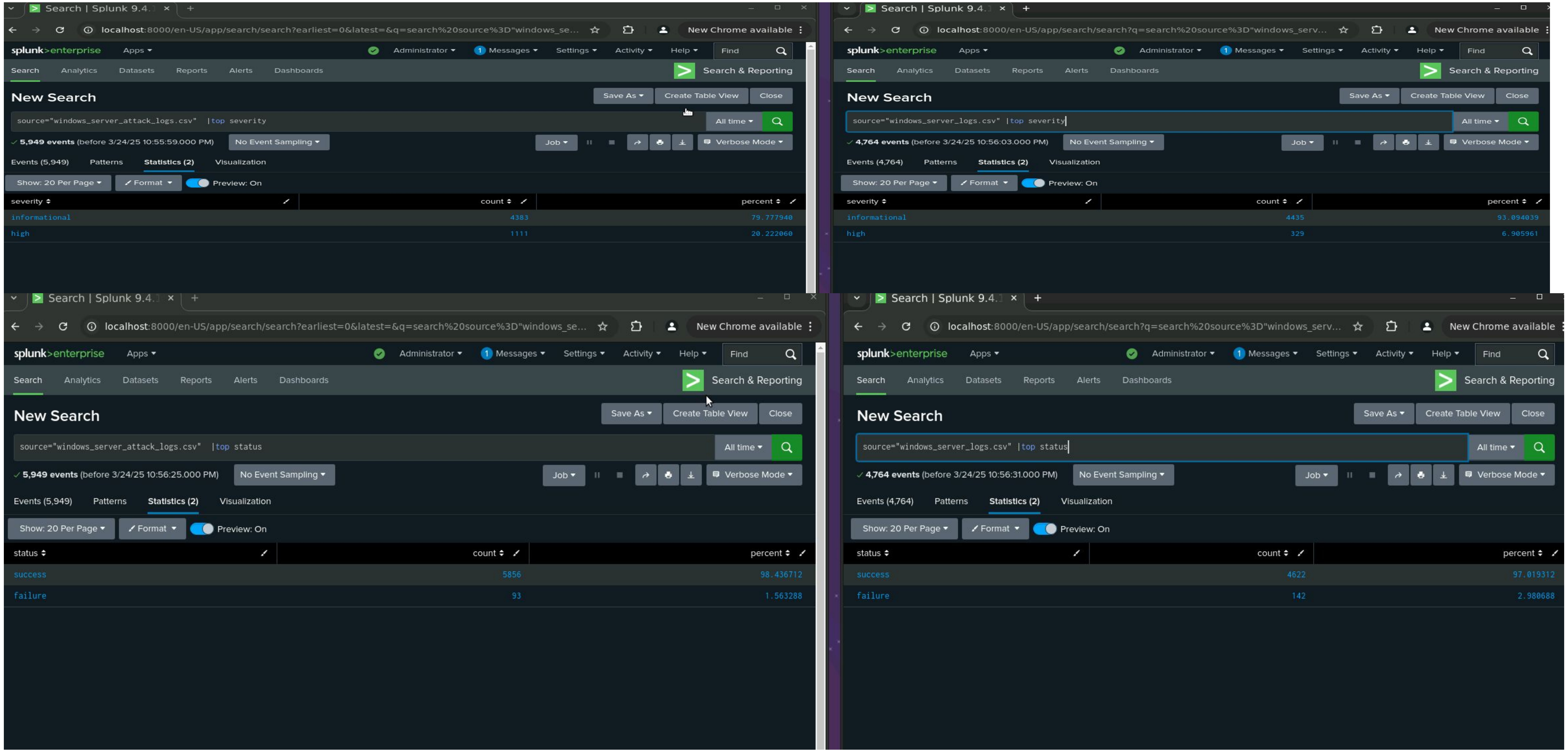
- When analyzing the attack logs, we detected a suspicious volume of both failed Windows activity and successful logins, both of which triggered our alert thresholds. The failed Windows activity spiked to 35 events at 8 AM on March 25, surpassing our threshold of greater than 10, confirming that the alert system functioned as expected. Similarly, we observed an unusual volume of successful logins, with 94 events occurring at 2 AM, primarily associated with User_A. This activity also triggered our alert, reinforcing the reliability of our threshold settings. Upon review, we determined that our predefined thresholds were appropriate and did not require adjustment, as they effectively captured these anomalies. Additionally, we found no suspicious volume of deleted accounts, indicating no immediate concerns in that area. Overall, our alert system correctly identified and flagged potentially concerning activities, supporting its effectiveness in monitoring and responding to security threats.

Attack Summary—Windows

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

- Upon analyzing the attack logs through our dashboards, we identified several suspicious activities that were consistently reflected across multiple data visualizations. In the time chart of signatures, the "Other" category was the most prominent, indicating an anomaly that warranted further scrutiny. The most notable signatures included a locked-out user account and an attempt to reset an account password, occurring between 12 AM and 3 AM and 8 AM and 11 AM, respectively. The peak count for account lockouts reached 856, while password reset attempts peaked at 1,258, suggesting a potentially targeted attack or unauthorized access attempt. Additionally, user activity data revealed two specific users, User_A and User_K, who exhibited unusually high activity during these same timeframes, with peak counts of 984 and 1,256, respectively. The consistency of these findings was reinforced through bar, graph, and pie chart visualizations, which further highlighted the same two suspicious periods. Our analysis of user activity with statistical charts confirmed these trends, reinforcing our concerns while also providing a broader perspective on user behavior. Overall, our dashboard analysis effectively identified and validated unusual activity, confirming the need for closer monitoring and potential security measures to mitigate any risks associated with these anomalies.

Screenshots of Attack Logs



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

✓ **5,949 events** (before 3/24/25 10:55:59.000 PM)

Events (5,949) Patterns **Statistics (2)** Visualization

severity	count	percent
informational	4383	79.777940
high	1111	20.222060

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

✓ **4,764 events** (before 3/24/25 10:56:03.000 PM)

Events (4,764) Patterns **Statistics (2)** Visualization

severity	count	percent
informational	4435	93.094039
high	329	6.905961

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

✓ **5,949 events** (before 3/24/25 10:56:25.000 PM)

Events (5,949) Patterns **Statistics (2)** Visualization

status	count	percent
success	5856	98.436712
failure	93	1.563288

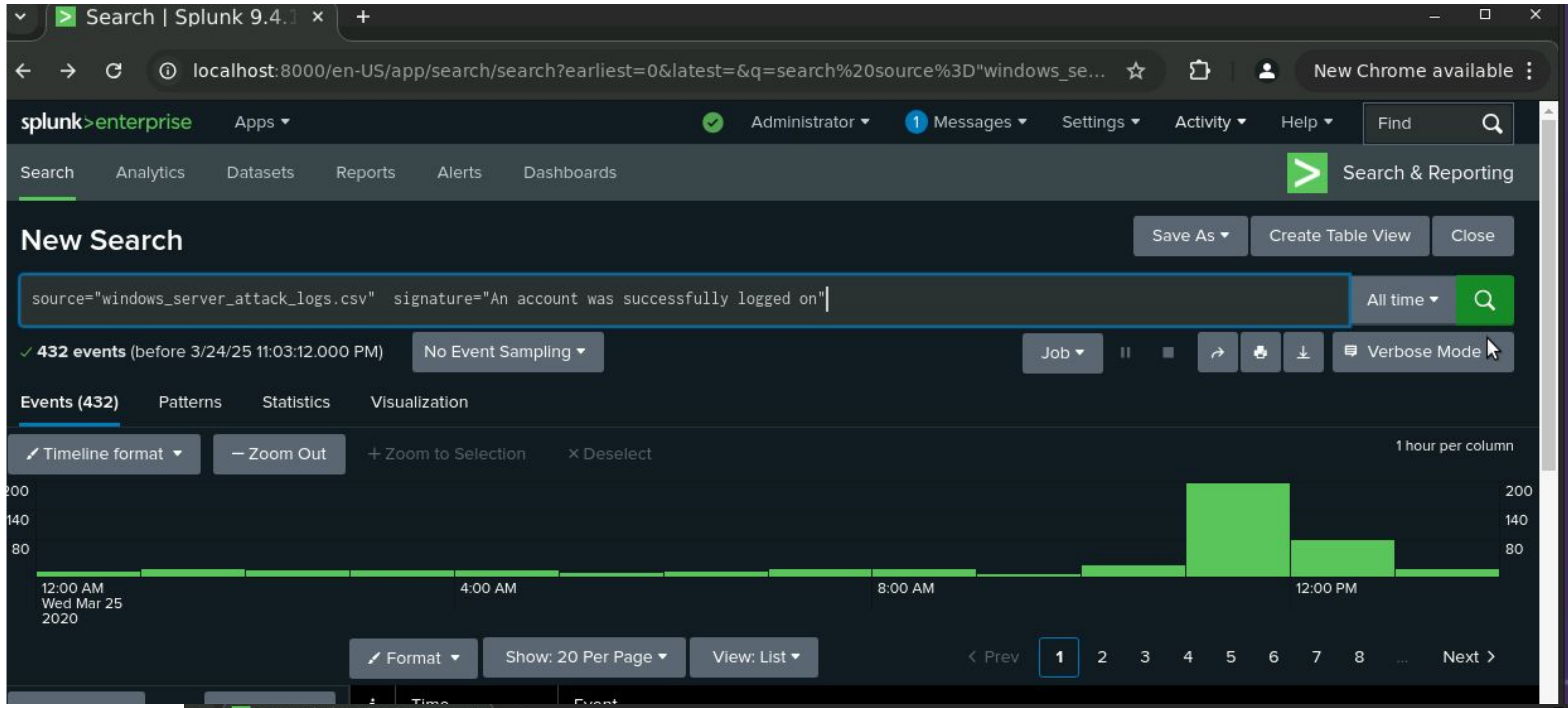
```
source="windows_server_logs.csv"  |top status
```

✓ **4,764 events** (before 3/24/25 10:56:31.000 PM)

Events (4,764) Patterns **Statistics (2)** Visualization

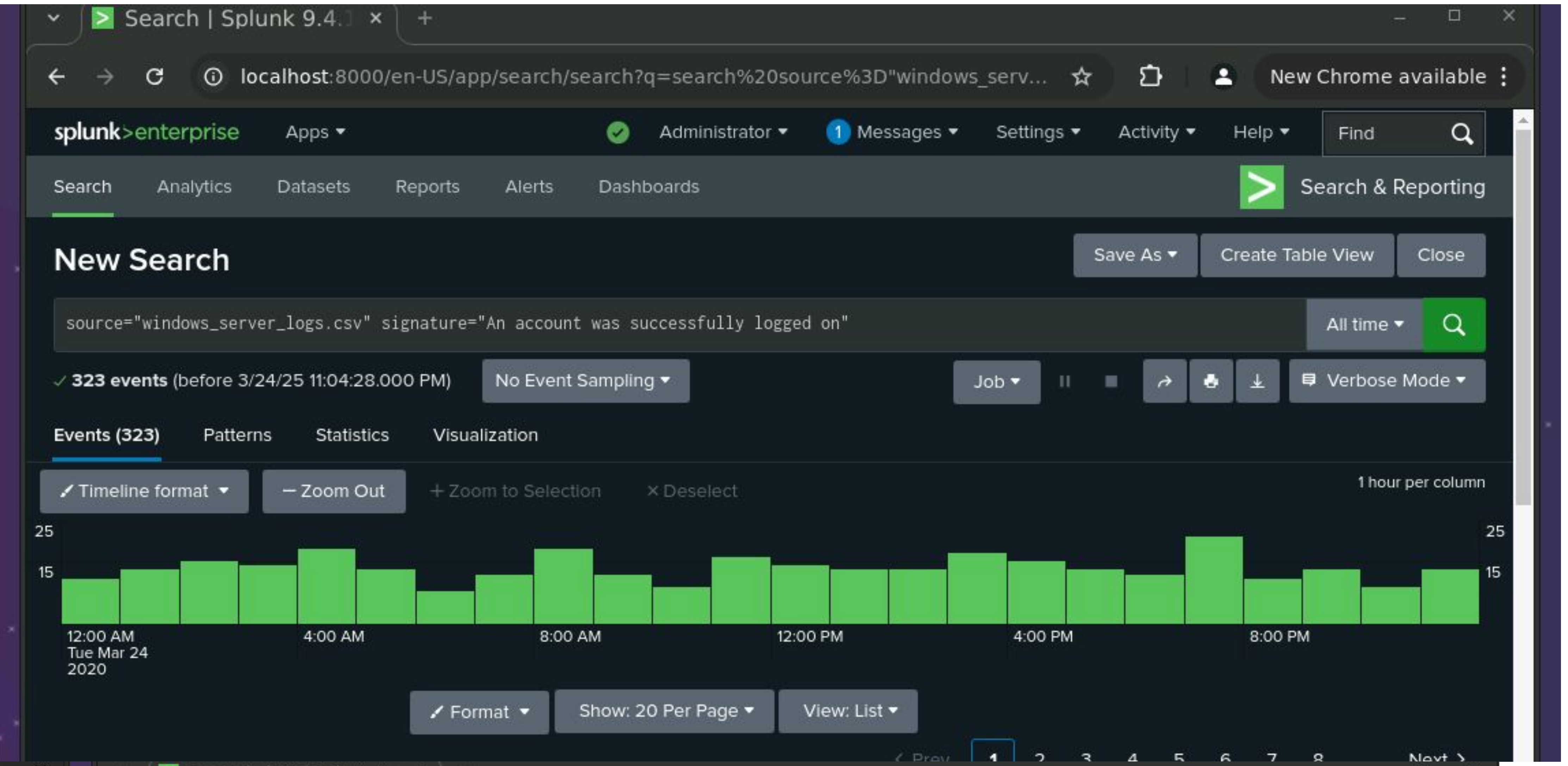
status	count	percent
success	4622	97.019312
failure	142	2.980688

Screenshots of Attack Logs



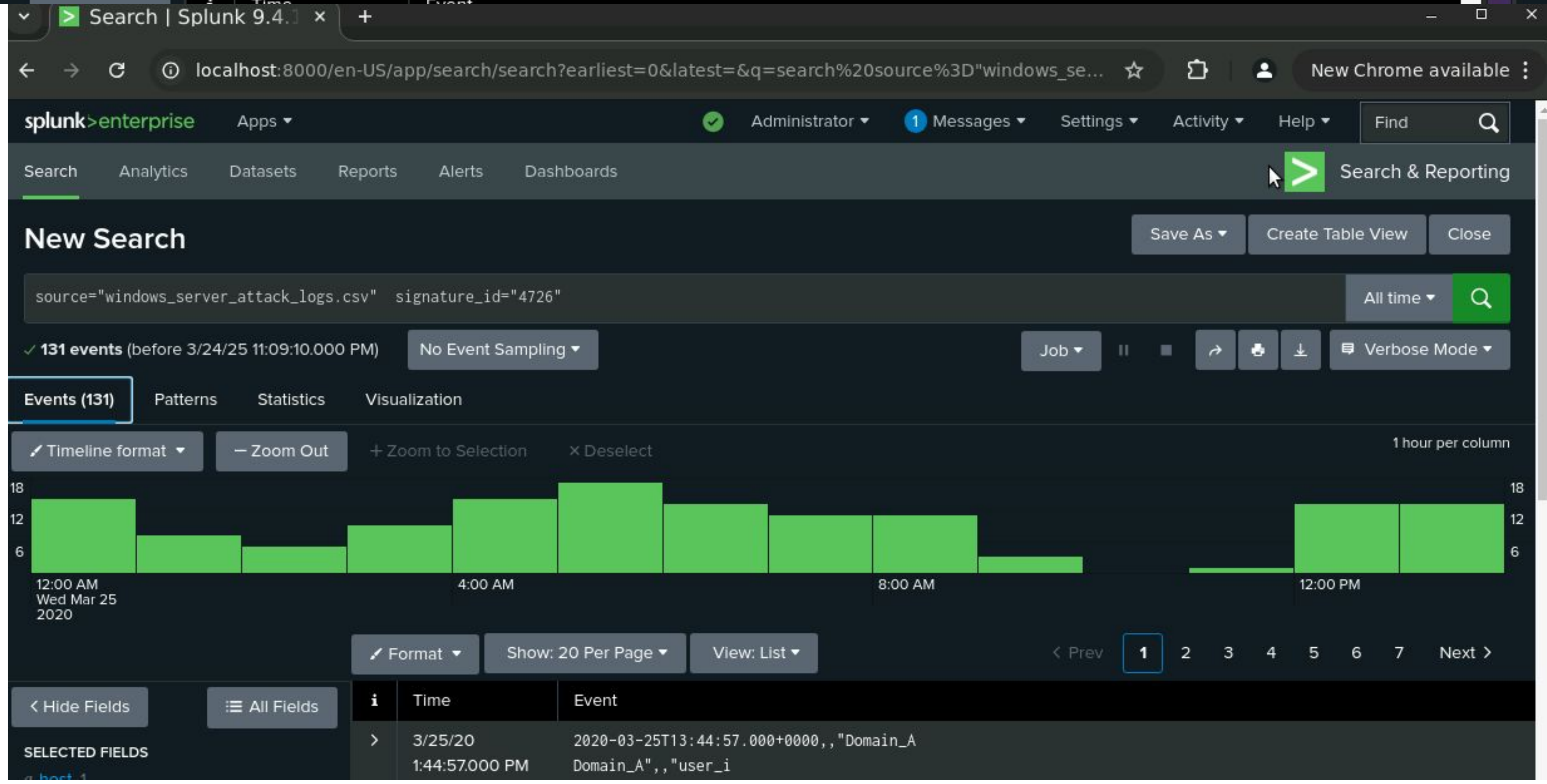
```
source="windows_server_attack_logs.csv"  signature="An account was successfully logged on"
```

✓ **432 events** (before 3/24/25 11:03:12.000 PM)



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

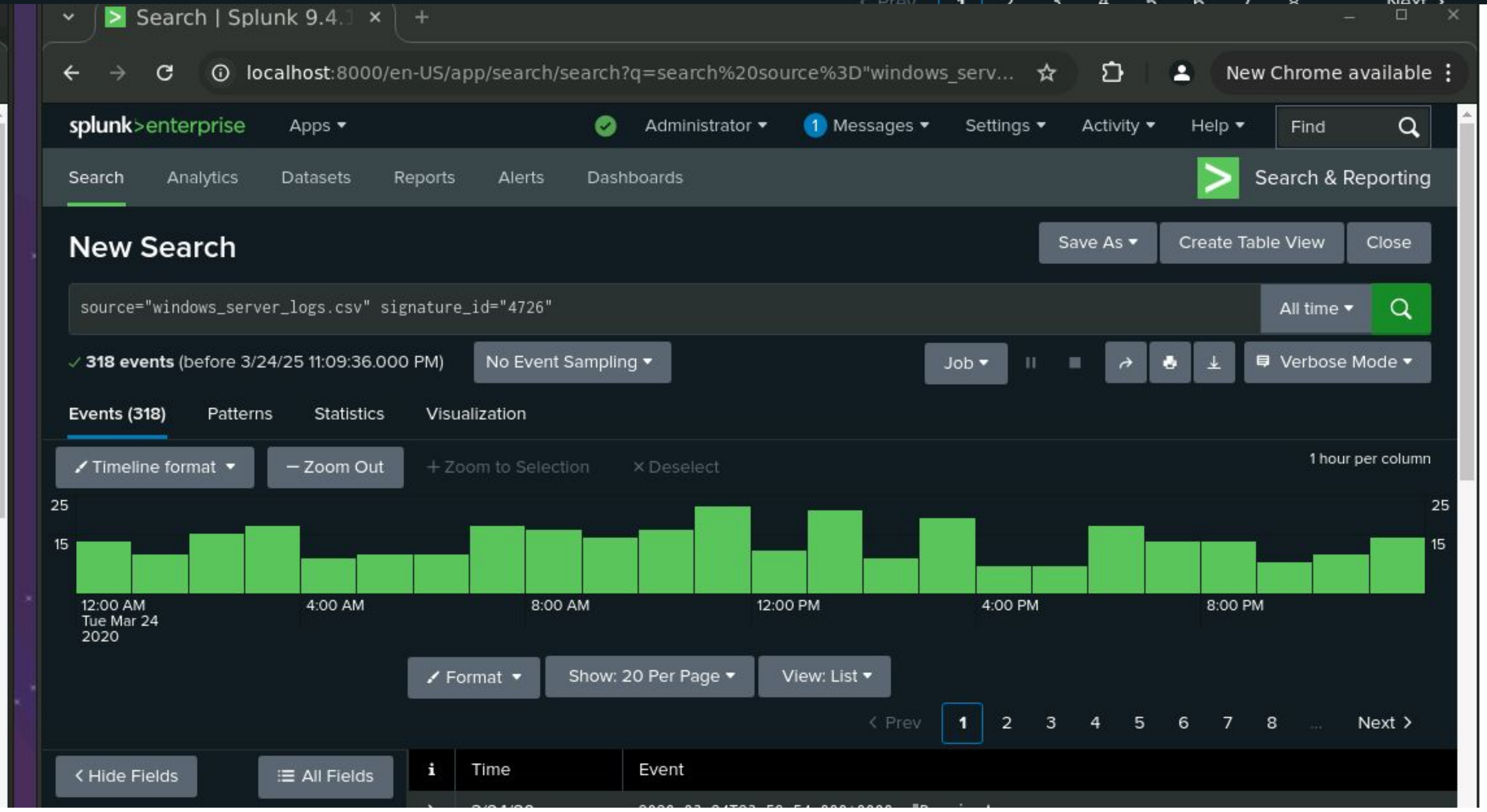
✓ **323 events** (before 3/24/25 11:04:28.000 PM)



```
source="windows_server_attack_logs.csv"  signature_id="4726"
```

✓ **131 events** (before 3/24/25 11:09:10.000 PM)

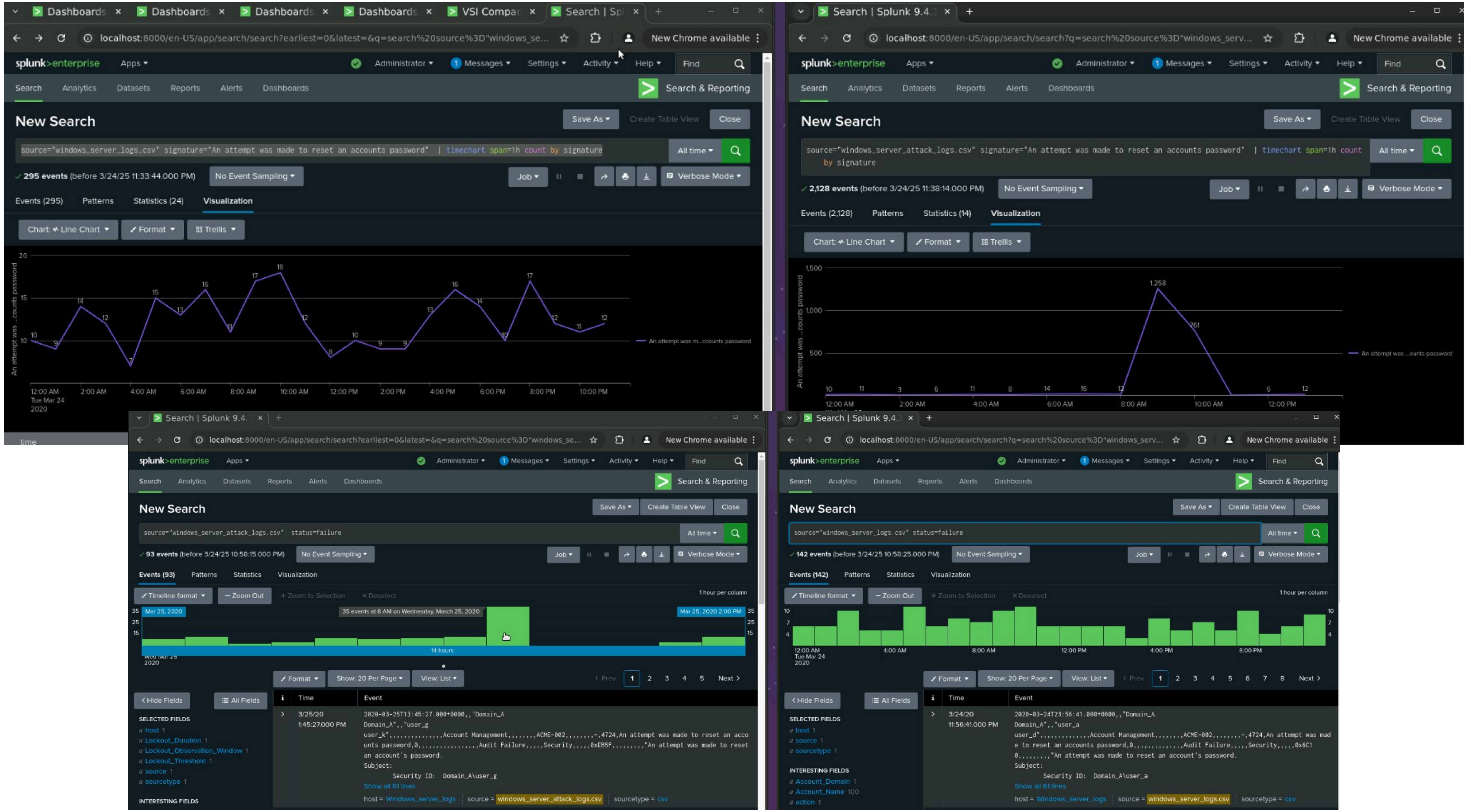
Time	Event
3/25/20 1:44:57.000 PM	2020-03-25T13:44:57.000+0000,,"Domain_A Domain_A",,"user_i



```
source="windows_server_logs.csv" signature_id="4726"
```

✓ **318 events** (before 3/24/25 11:09:36.000 PM)

Screenshots of Attack Logs



```
source="windows_server_logs.csv" signature="An attempt was made to reset an accounts password"  | timechart span=1h count by signature
```

✓ 295 events (before 3/24/25 11:33:44.000 PM)

```
source="windows_server_attack_logs.csv" signature="An attempt was made to reset an accounts password"  | timechart span=1h count
    by signature
```

✓ 2,128 events (before 3/24/25 11:38:14.000 PM)

```
source="windows_server_attack_logs.csv"  status=failure
```

✓ 93 events (before 3/24/25 10:58:15.000 PM)

35 events at 8 AM on Wednesday, March 25, 2020

Time	Event
3/25/20 1:45:27.000 PM	2020-03-25T13:45:27.000+0000,,"Domain_A Domain_A",,"user_g user_k",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0xEB5F,,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_g Show all 61 lines host = Windows_server_logs | source = windows_server_attack_logs.csv | sourcetype = csv

```
source="windows_server_logs.csv"  status=failure
```

✓ 142 events (before 3/24/25 10:58:25.000 PM)

Time	Event
3/24/20 11:56:41.000 PM	2020-03-24T23:56:41.000+0000,,"Domain_A Domain_A",,"user_a user_d",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x6C10,,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_a Show all 61 lines host = Windows_server_logs | source = windows_server_logs.csv | sourcetype = csv

Attack Summary—Apache

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

- Upon analyzing the attack logs through our reports, we identified suspicious changes in HTTP methods, specifically in the POST and GET requests. However, when reviewing referrer domains, we did not detect any significant changes that would raise security concerns. Additionally, our analysis of HTTP response codes revealed a minor fluctuation in the number of 404 errors, but this change was not substantial enough to be considered suspicious. While the HTTP methods anomaly warrants further investigation to determine if it is linked to any malicious activity, the overall findings from the referrer domains and response codes suggest no immediate widespread security threat.

Attack Summary—Apache

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

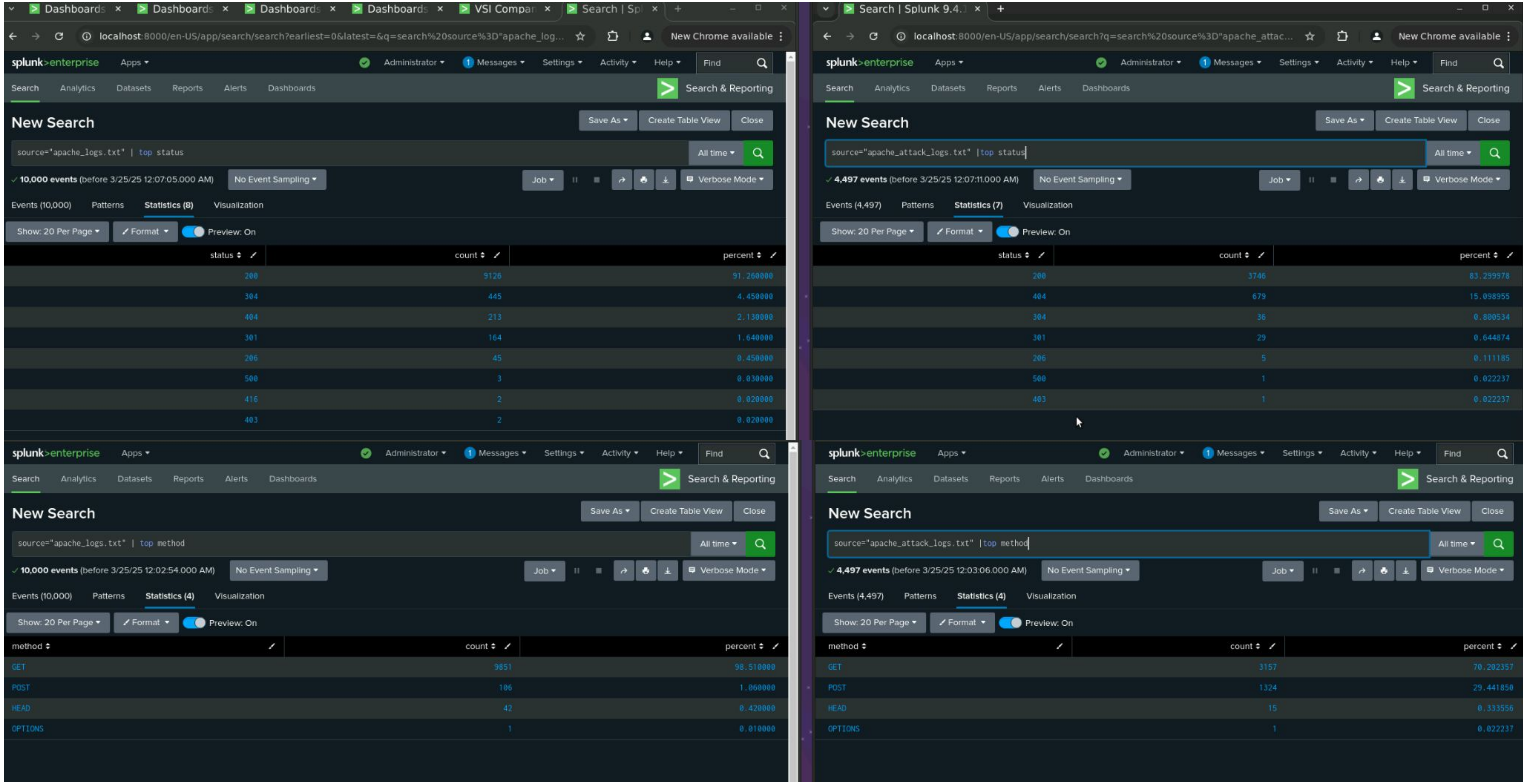
- Upon analyzing the attack logs through our alerts, we identified a significant spike in both international activity and HTTP POST requests, both occurring at 8 PM on March 25th. The international activity primarily originated from Ukraine, with a total count of 1,369 during the spike, which was substantial enough to trigger our alert system. Similarly, we observed an unusually high volume of HTTP POST requests, reaching 1,269 within the same timeframe. However, after reviewing the established thresholds, we determined that no changes were necessary, as they effectively detected and highlighted the anomalies. The consistency in detection across both international activity and HTTP POST logs further validated the accuracy of our threshold settings.

Attack Summary—Apache

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

- Upon analyzing the attack logs through our dashboards, we identified multiple suspicious activities across different metrics, indicating a potential security threat. The time chart of HTTP methods revealed a significant spike in GET request activity between 5:00 PM and 7:00 PM, with a peak count of 729, suggesting a targeted attempt to access specific resources. The cluster map analysis further reinforced this concern, showing an unusual surge in activity from Kiev and Kharkiv, Ukraine, with respective counts of 439 and 432. This unexpected international activity aligns with the suspicious HTTP request patterns, indicating that the source of the attack may be originating from these regions. Additionally, the URI data analysis identified two specific endpoints—/VSI_Account_logon.php and files/logstash/logstash-1.3.2-monolithic.jar—as the most frequently accessed during the attack window. Given that one of these URIs is related to account logins, it suggests that the attacker may be attempting credential stuffing, brute-force login attempts, or unauthorized access to user accounts. The repeated access to the Logstash JAR file could also indicate an attempt to exploit vulnerabilities within the system's logging infrastructure. These findings, combined with the geographical anomalies and method-specific attack patterns, highlight a coordinated attack effort that warrants immediate investigation and enhanced security measures to prevent further exploitation.

Screenshots of Attack Logs



```
source="apache_logs.txt" | top status
```

✓ 10,000 events (before 3/25/25 12:07:05.000 AM)

Events (10,000) | Statistics (8)

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

```
source="apache_attack_logs.txt" |top status
```

✓ 4,497 events (before 3/25/25 12:07:11.000 AM)

Events (4,497) | Statistics (7)

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

```
source="apache_logs.txt" | top method
```

✓ 10,000 events (before 3/25/25 12:02:54.000 AM)

Events (10,000) | Statistics (4)

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

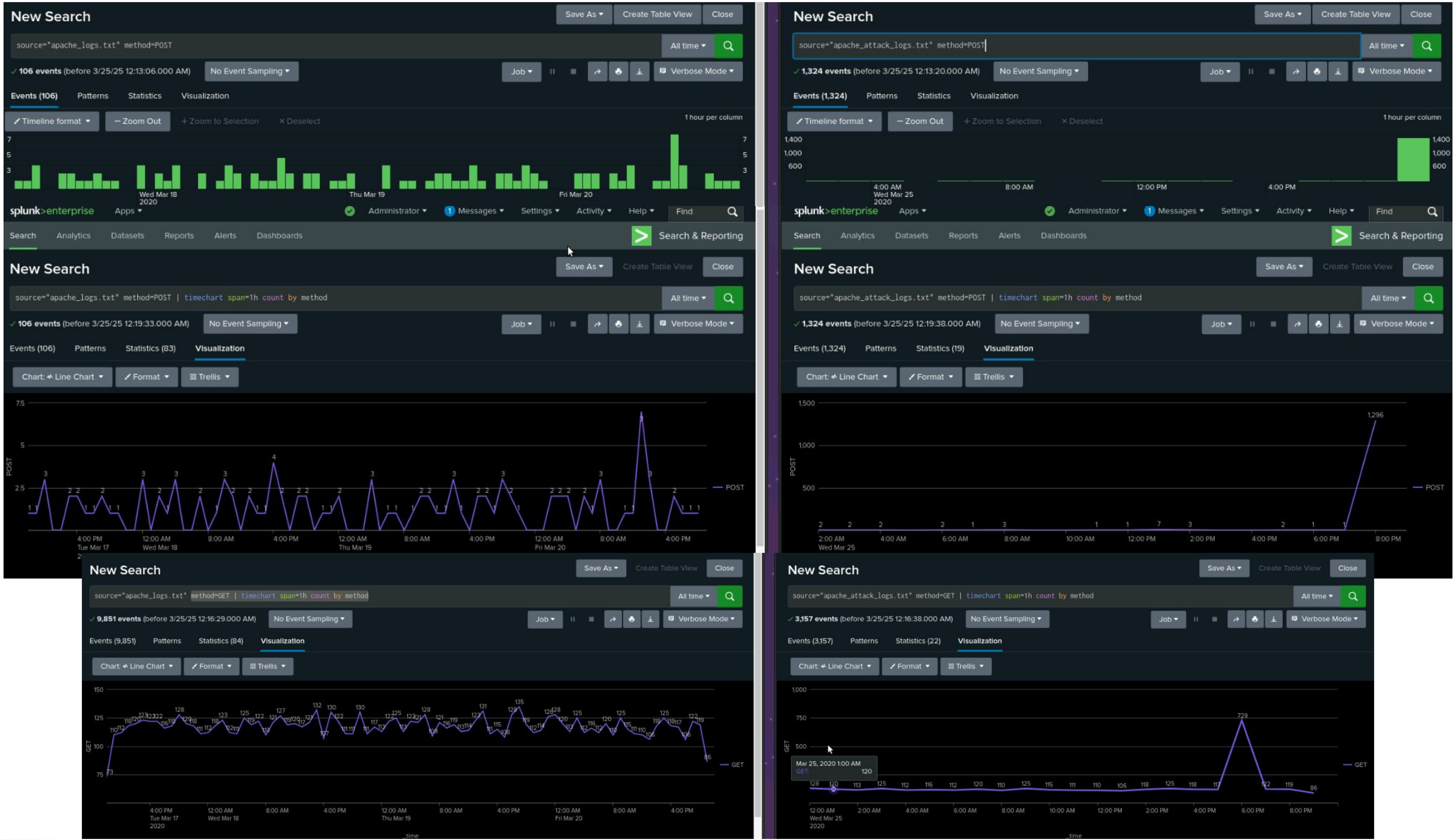
```
source="apache_attack_logs.txt" |top method
```

✓ 4,497 events (before 3/25/25 12:03:06.000 AM)

Events (4,497) | Statistics (4)

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

Screenshots of Attack Logs



New Search

```
source="apache_logs.txt" method=POST
```

✓ 106 events (before 3/25/25 12:13:06.000 AM)

New Search

```
source="apache_attack_logs.txt" method=POST
```

✓ 1,324 events (before 3/25/25 12:13:20.000 AM)

New Search

```
source="apache_logs.txt" method=POST | timechart span=1h count by method
```

✓ 106 events (before 3/25/25 12:19:33.000 AM)

New Search

```
source="apache_attack_logs.txt" method=POST | timechart span=1h count by method
```

✓ 1,324 events (before 3/25/25 12:19:38.000 AM)

New Search

```
source="apache_logs.txt" method=GET | timechart span=1h count by method
```

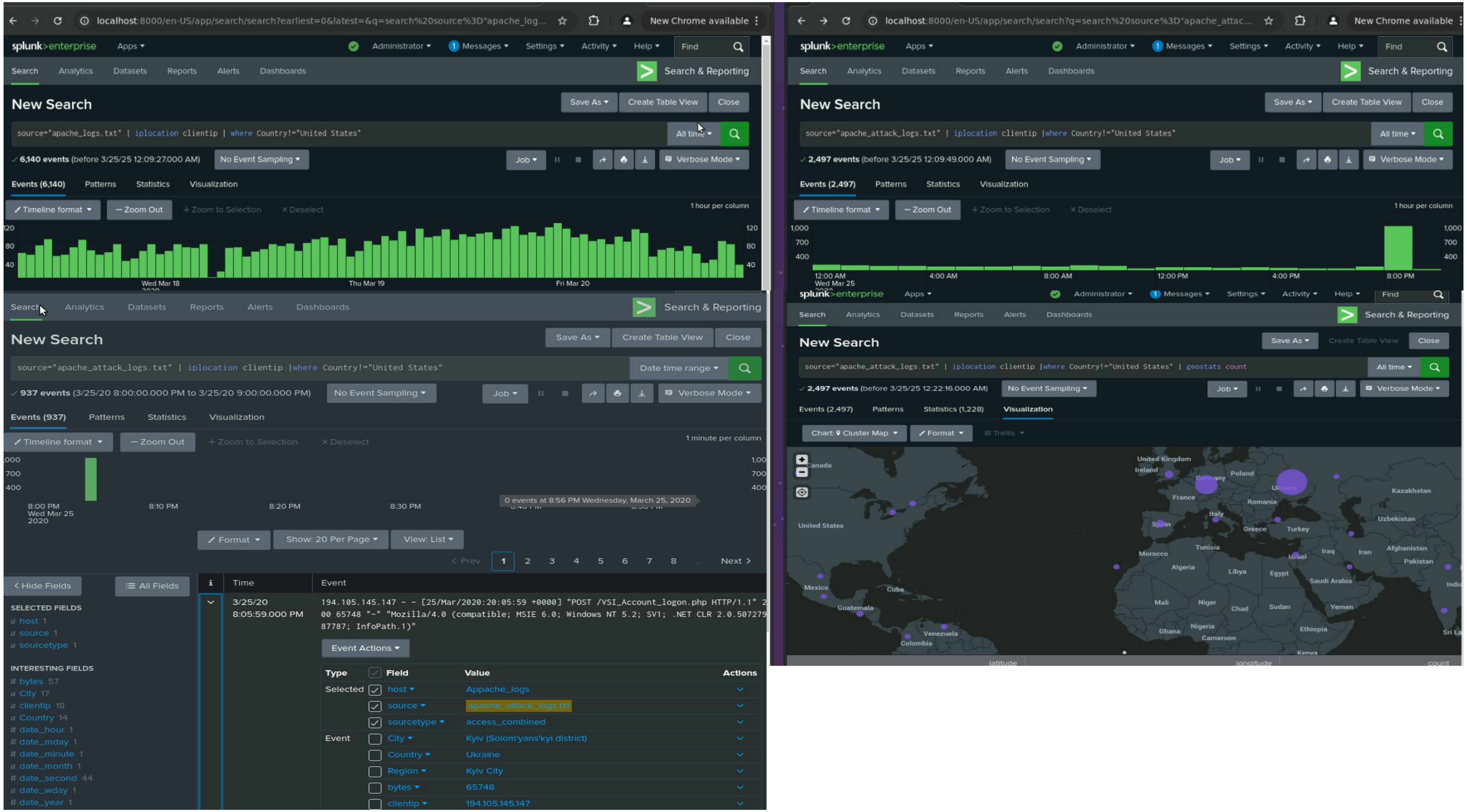
✓ 9,851 events (before 3/25/25 12:16:29.000 AM)

New Search

```
source="apache_attack_logs.txt" method=GET | timechart span=1h count by method
```

✓ 3,157 events (before 3/25/25 12:16:38.000 AM)

Screenshots of Attack Logs



```
source="apache_logs.txt" | iplocation clientip | where Country!="United States"
```

✓ 6,140 events (before 3/25/25 12:09:27.000 AM) No Event Sampling

Events (6,140) Patterns Statistics Visualization

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

✓ 2,497 events (before 3/25/25 12:09:49.000 AM) No Event Sampling

Events (2,497) Patterns Statistics Visualization

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

✓ 937 events (3/25/20 8:00:00.000 PM to 3/25/20 9:00:00.000 PM) No Event Sampling

Events (937) Patterns Statistics Visualization

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- bytes 57
- City 17
- clientip 18
- Country 14
- date_hour 1
- date_mday 1
- date_minute 1
- date_month 1
- date_second 44
- date_wday 1
- date_year 1

Time: 3/25/20 8:05:59.000 PM

```
194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 2
00 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.507279
87787; InfoPath.1)"
```

Type		Field	Value
Selected	☑	host	Appache_logs
	☑	source	apache_attack_logs.txt
	☑	sourcetype	access_combined
Event	□	City	Kyiv (Solom'yans'kyi district)
	□	Country	Ukraine
	□	Region	Kyiv City
	□	bytes	65748
	□	clientip	194.105.145.147

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

✓ 2,497 events (before 3/25/25 12:22:16.000 AM) No Event Sampling

Events (2,497) Patterns Statistics (1,228) Visualization

Summary and Future Mitigations

Project 3 Summary

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

  Our overall findings revealed a coordinated attack involving credential-based attempts (brute force password spamming), international activity spikes, and suspicious HTTP methods on March 25. VSI experienced different attacks that varied on both servers (Windows and Apache) from all different regions of the globe.

- To protect VSI from future attacks, what future mitigations would you recommend?
  - A strong Two factor authentications which will work as creating stronger password policies to ensure safety from brute force attacks
  - We would recommend to lock users after a certain amount of attempts of getting a login incorrect or noticing a login success within a short amount of time from one user