# Security Monitoring for Virtual Space Industries

## Presented by CK Security Solutions

# Table of Contents

This document contains the following resources:

01

**Monitoring Environment**

02

**Attack Analysis**

03

**Project Summary & Future Mitigations**

# Monitoring Environment

# Scenario

VSI faced cyber attacks from competitor JobeCorp, targeting our Apache web server and Windows operating system. We utilised Splunk for monitoring and received new logs covering the attack period. Our analysis aims to evaluate the effectiveness of our monitoring solutions and identify areas for improvement.

# Website Monitoring App

# Summary of Website Monitoring App Chosen

## Add-On App: Website Monitoring App

**Purpose:**

Provides real-time visibility into the health and performance of web services.

**Key Features:**

Monitors metrics like response times, HTTP errors, and unusual traffic patterns.

Integrates insights into VSI’s SIEM for proactive detection of security threats.

**Benefits:**

Identifies suspicious activity (e.g., spikes in malicious HTTP methods).

Empowers security teams with dashboards and alerts for rapid response to incidents

# Scenario that Illustrates Benefit of Add-On App

**Real-Time Monitoring:**
Detects anomalies such as a spike in HTTP POST requests (e.g., surge to 1,296 requests).

**Proactive Alerts & Response:**
Alerts the security team to suspicious activity, enabling immediate actions like blocking malicious IPs.

**Threat Mitigation:**
Prevents DDoS attacks and protects VSI's digital assets, ensuring the integrity of customer interactions.

# Website Monitoring App Image

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Executive Summary
Status Overview
Status History
Change History
Create Inputs
Health
Search
Configuration
What's new in 2.9?
App
Website Monitoring
Edit
Export
...
Submit
Hide Filters

Status Overview

Last 24 hours

Include all inputs

| title | url | response | last_checked | response_time | status | average | range | sparkline_response_time |
|---|---|---|---|---|---|---|---|---|
| VSI | https://vsi-corporation.azurewebsites.net/ | Connection failed | 8 minutes ago | | Failed | | | |

Modify the definition of a failure

# Logs Analysed

## 1 Windows Logs

**Log Analysis Overview**

Analysed Windows Server logs for security insights.

**Purpose**

Detect security threats and unauthorised access.
Evaluate security measure effectiveness.

**Findings**

Identified trends in user activity.
Highlighted high-severity events.
Provided recommendations for security improvements.

**Conclusion**

Emphasised the need for ongoing log monitoring.

## 2 Apache Logs

**Method**

Indicates the type of HTTP request
Helps identify primary user actions on the site.

**Referer Domain**

Captures the domain from which requests originated.
Assesses effectiveness of marketing campaigns and traffic sources.

**Status**

Represents HTTP response status codes
Identifies success or failure of requests,
Records the IP address of the client.
Aids in tracking unique users and detecting malicious activity.

**User Agent**

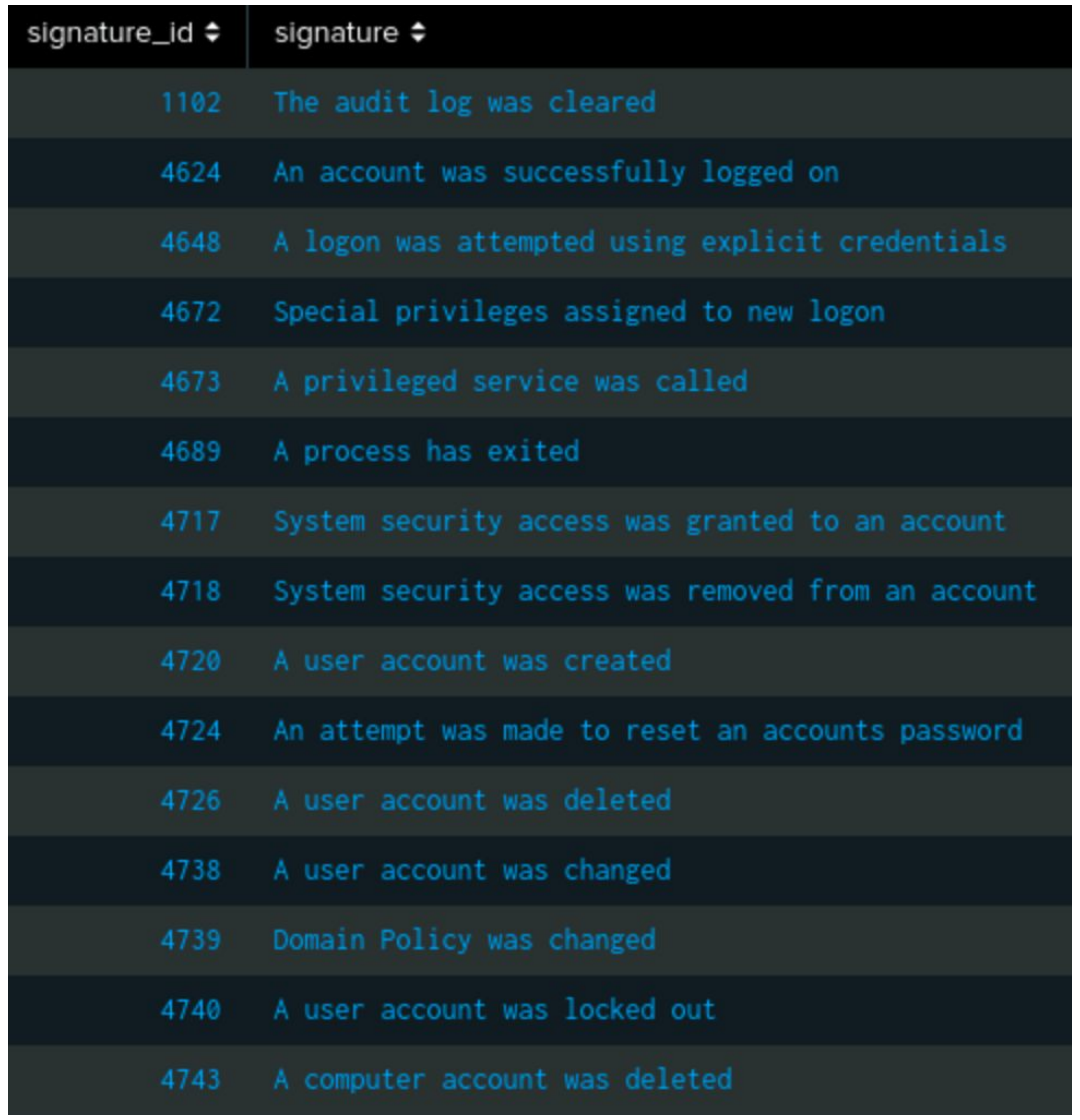
Contains information about the client's browser and operating system.
Informs decisions on website optimisation and compatibility.

# Windows Logs

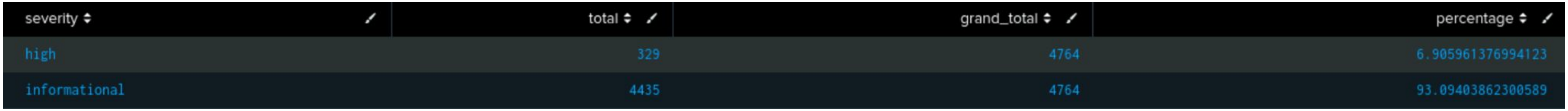
# Reports—Windows

| Report Name | Report Description |
|---|---|
| Signature ID Overview for Windows Activity | This report provides a table of unique signatures and their IDs, facilitating quick identification of Windows activity signatures for VSI. Duplicates are removed for clarity. |
| Severity Levels Overview for Windows Logs | This report displays the count and percentage of each severity level in the Windows logs, enabling VSI to quickly assess the overall security posture. |
| Success vs. Failure Analysis of Windows Activities | This report compares the success and failure rates of Windows activities, allowing VSI to identify any suspicious levels of failed activities on their server. |

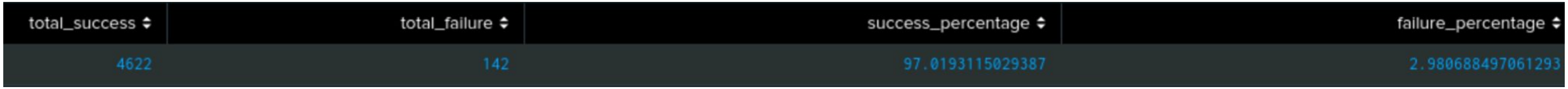
# Images of Reports—Windows



| signature_id | signature |
|---|---|
| 1102 | The audit log was cleared |
| 4624 | An account was successfully logged on |
| 4648 | A logon was attempted using explicit credentials |
| 4672 | Special privileges assigned to new logon |
| 4673 | A privileged service was called |
| 4689 | A process has exited |
| 4717 | System security access was granted to an account |
| 4718 | System security access was removed from an account |
| 4720 | A user account was created |
| 4724 | An attempt was made to reset an accounts password |
| 4726 | A user account was deleted |
| 4738 | A user account was changed |
| 4739 | Domain Policy was changed |
| 4740 | A user account was locked out |
| 4743 | A computer account was deleted |



| severity | total | grand_total | percentage |
|---|---|---|---|
| high | 329 | 4764 | 6.905961376994123 |
| informational | 4435 | 4764 | 93.09403862300589 |



| total_success | total_failure | success_percentage | failure_percentage |
|---|---|---|---|
| 4622 | 142 | 97.0193115029387 | 2.980688497061293 |

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Failed Windows Activity | Monitors hourly failed Windows activity and triggers when the threshold is exceeded, indicating potential suspicious behavior. | 6 | 9 |

**JUSTIFICATION:** This alert helps detect potential brute-force attacks, allowing the SOC to respond quickly to suspicious activities and enhance VSI's security.

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| User Successfully Logged In (4624) | Triggers when successful login events exceed the threshold, indicating potential unusual activity. | 13 | 20 |

**JUSTIFICATION:** A threshold of 20 indicates a significant increase in logins, suggesting potential security risks like brute-force attacks.

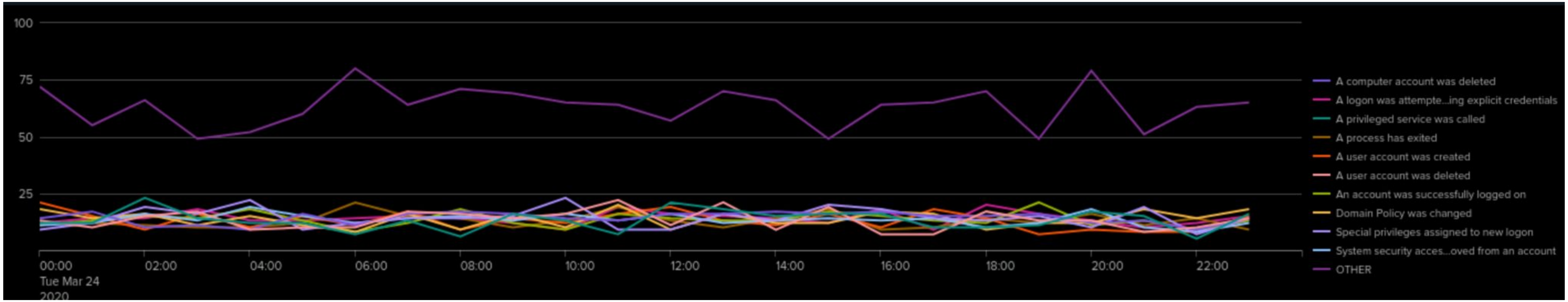
# Alerts—Windows

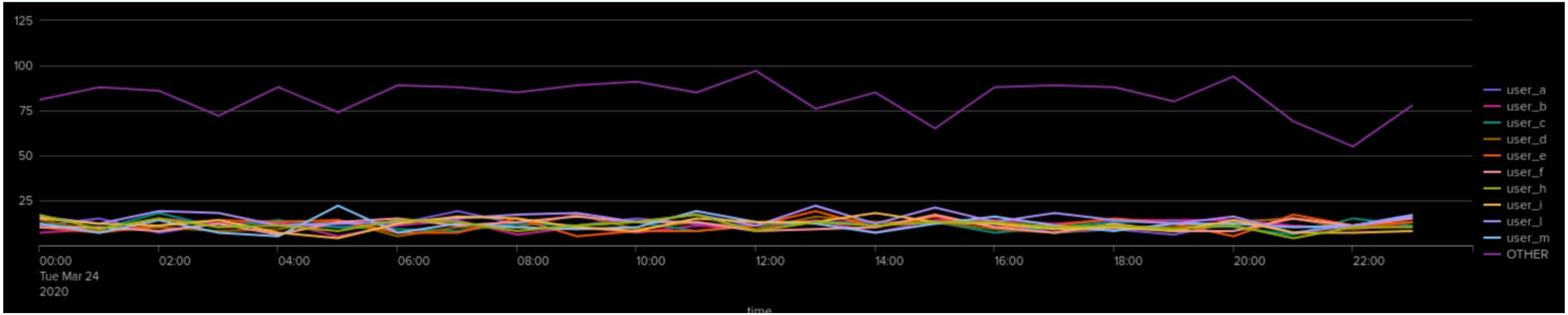
Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Alert - Deleted User | Triggers when the hourly count of user account deletions exceeds the threshold, indicating potential unauthorised account deletions. | 13 | 20 |

**JUSTIFICATION:** A threshold of 20 signifies a notable increase in account deletions, which may indicate malicious activity or policy violations.

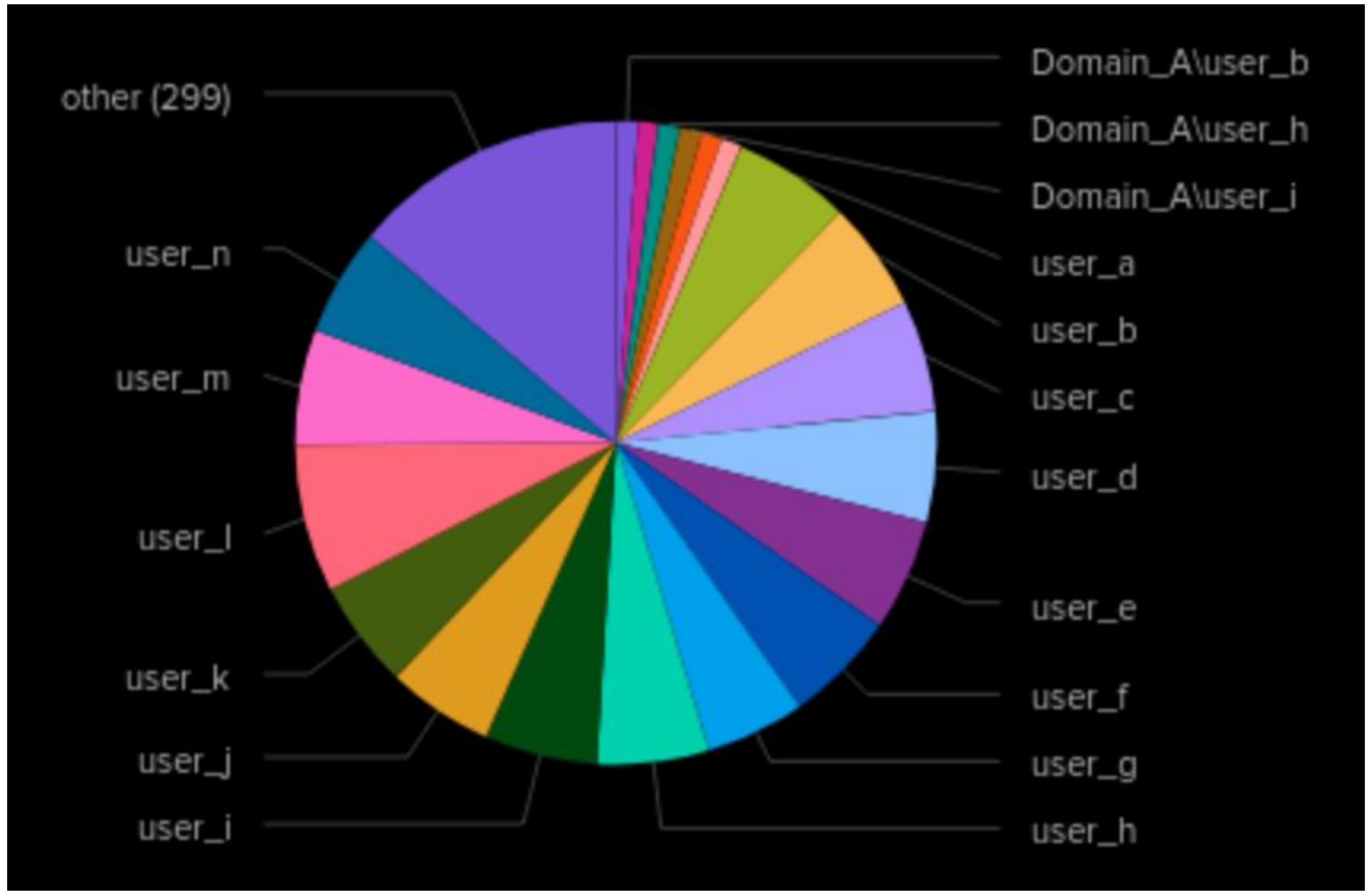
# Dashboards—Windows

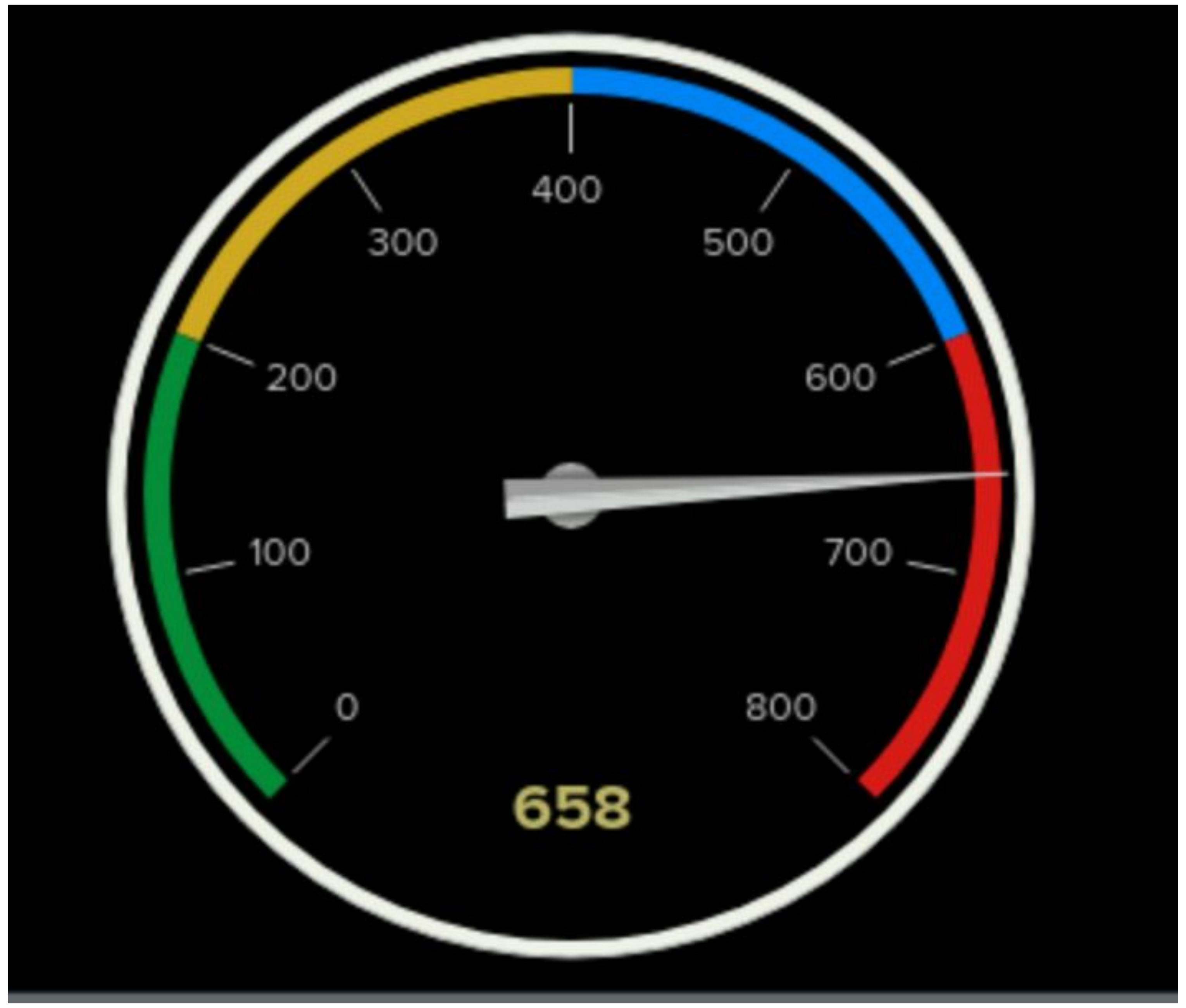




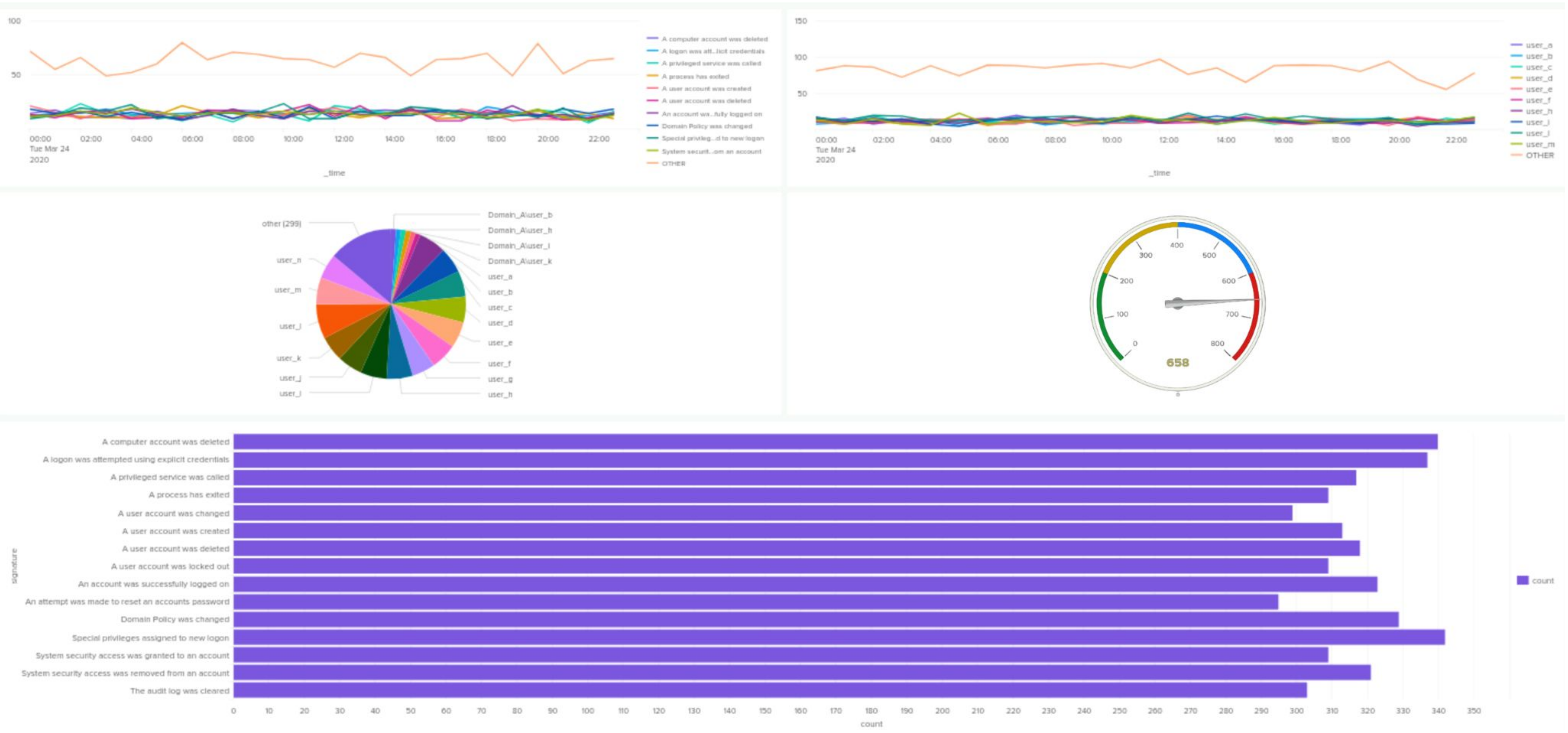
# Dashboards—Windows

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
25
50
75
100
125
150
175
200
225
250
275
300
325
350
count
count





# Dashboards—Windows


100
50
00:00
Tue Mar 24
2020
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
_time
A computer account was deleted
A logon was att...licit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account wa...fully logged on
Domain Policy was changed
Special privileg...d to new logon
System securit...om an account
OTHER
150
100
50
00:00
Tue Mar 24
2020
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
_time
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_l
user_m
OTHER
other (299)
user_n
user_m
user_l
user_k
user_j
user_i
Domain_A\user_b
Domain_A\user_h
Domain_A\user_i
Domain_A\user_k
user_a
user_b
user_c
user_d
user_e
user_f
user_g
user_h
0
100
200
300
400
500
600
700
800
658
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
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350
count
count

# Apache Logs

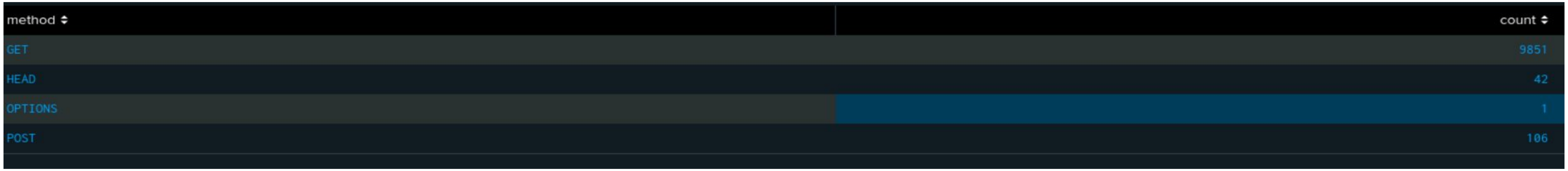
# Reports—Apache

Designed the following reports:

| Report Name | Report Description |
|---|---|
| HTTP Methods Activity Overview | This report presents a table of various HTTP methods (GET, POST, HEAD, etc.), offering insights into the types of HTTP requests being made to VSI's web server. |
| Top Referring Domains Analysis | This report lists the top 10 domains referring traffic to VSI's website, helping to identify any potentially suspicious referrers. |
| HTTP Response Codes Summary | This report displays the count of each HTTP response code, providing insights into the overall health of HTTP responses and highlighting any suspicious patterns. |

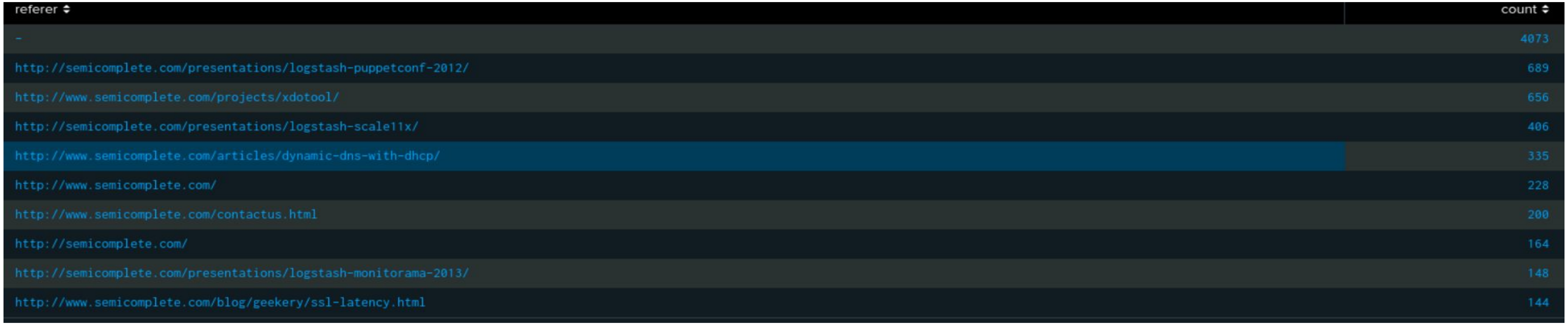
# Apache Logs

HTTP Methods



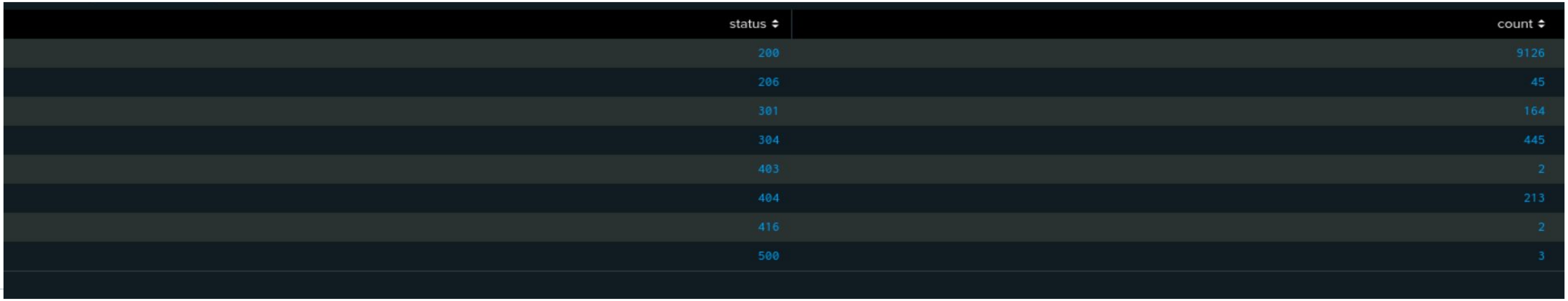
| method ⬍ | count ⬍ |
|---|---|
| GET | 9851 |
| HEAD | 42 |
| OPTIONS | 1 |
| POST | 106 |

Top 10 Domains by Refer



| referer ⬍ | count ⬍ |
|---|---|
| - | 4073 |
| http://semicomplete.com/presentations/logstash-puppetconf-2012/ | 689 |
| http://www.semicomplete.com/projects/xdotool/ | 656 |
| http://semicomplete.com/presentations/logstash-scale11x/ | 406 |
| http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/ | 335 |
| http://www.semicomplete.com/ | 228 |
| http://www.semicomplete.com/contactus.html | 200 |
| http://semicomplete.com/ | 164 |
| http://semicomplete.com/presentations/logstash-monitorama-2013/ | 148 |
| http://www.semicomplete.com/blog/geekery/ssl-latency.html | 144 |

HTTP Response Codes



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

# Alerts—Apache

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Apache - Hourly Activity from Any Country Besides the United States | Triggered when the hourly activity from any non-U.S. country exceeds the threshold, indicating potential unusual traffic patterns that may warrant investigation. | 120 | 130 |

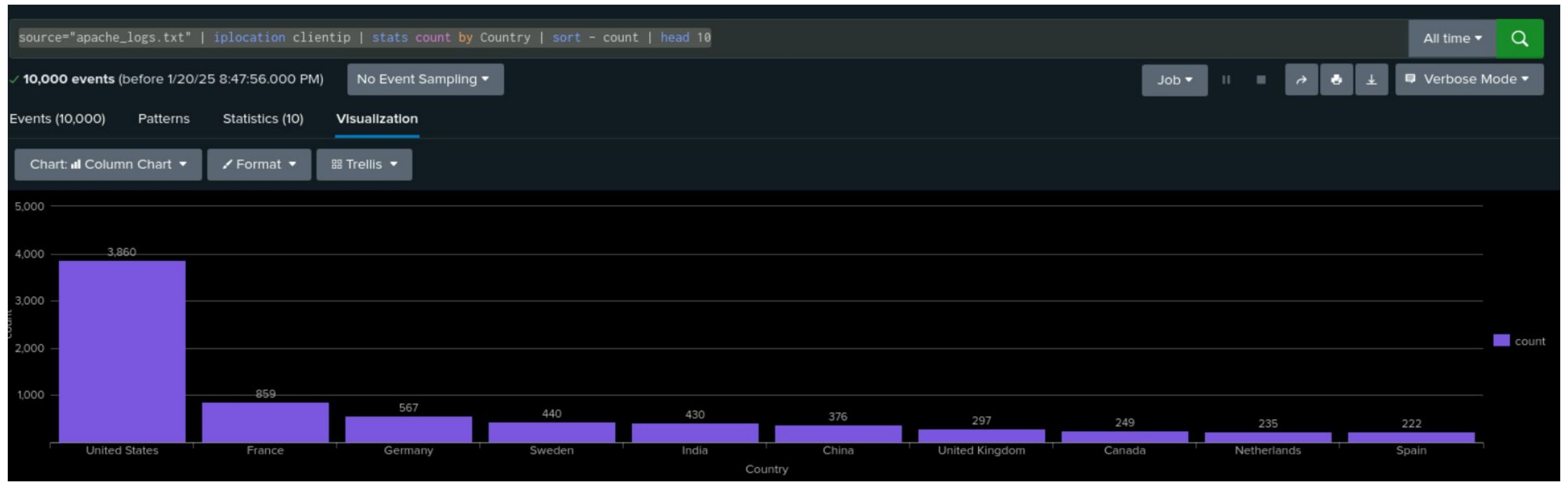
**JUSTIFICATION:**A threshold of 130 is important for identifying spikes in international traffic, which could suggest potential security threats or unauthorised access attempts. Monitoring this alert enables the SOC to respond promptly to any suspicious activity.

# Alerts—Apache

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Apache - Hourly Count of the HTTP POST Method | Triggered when the hourly count of HTTP POST requests exceeds the threshold, indicating potential abnormal activity that may require further analysis. | 7 | 10 |

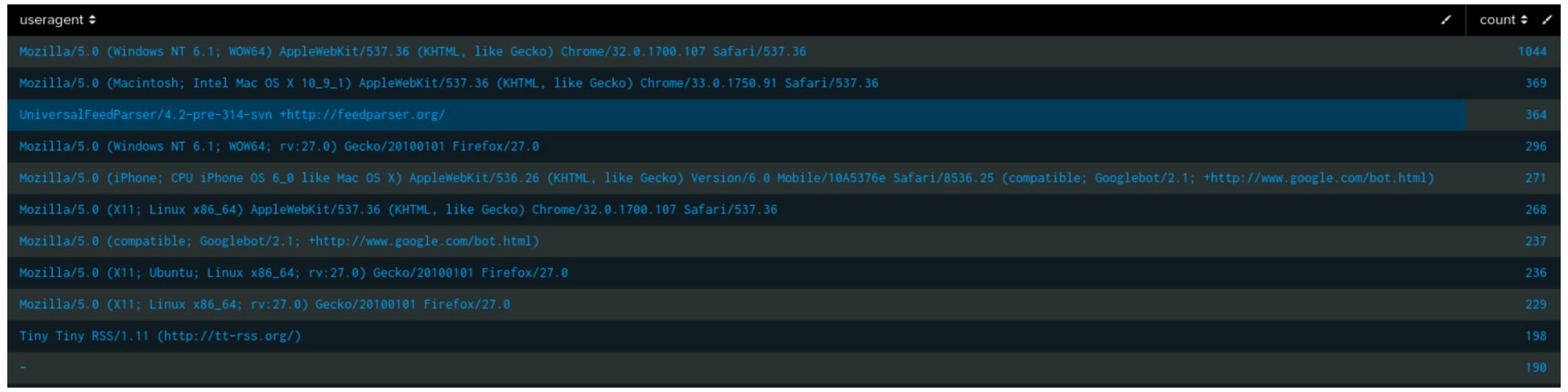
**JUSTIFICATION:** A threshold of 10 is critical for detecting potential security incidents, such as data exfiltration or web application attacks. By monitoring this alert, the SOC can quickly investigate any spikes in POST activity.

# Visualisations—Apache

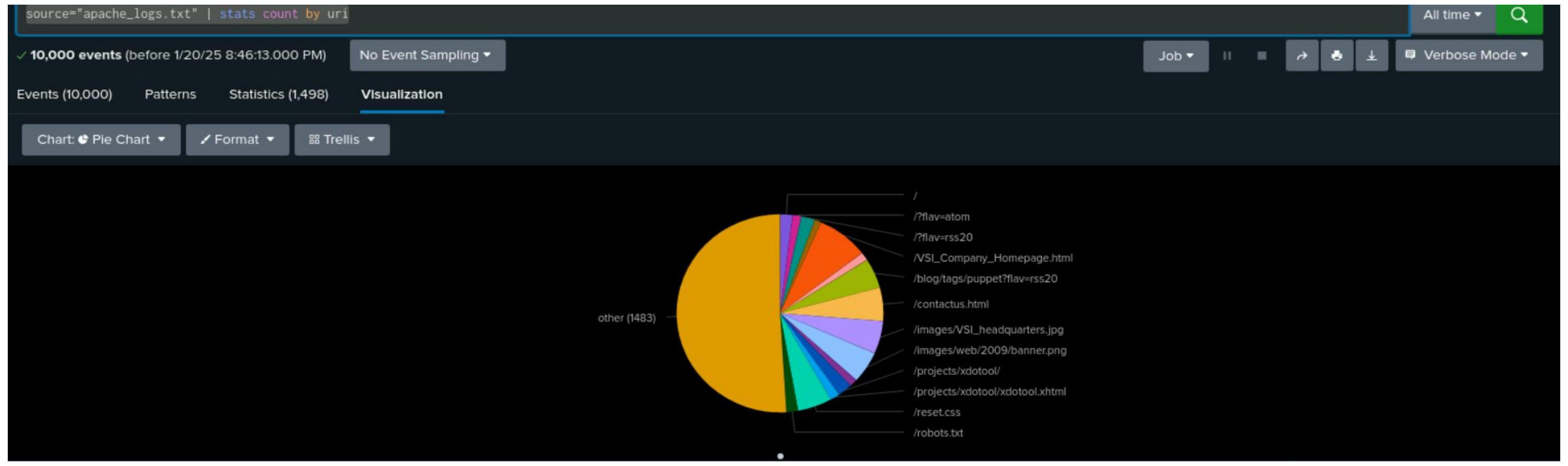


```
source="apache_logs.txt" | iplocation clientip | stats count by Country | sort - count | head 10
```

✓ 10,000 events (before 1/20/25 8:47:56.000 PM)

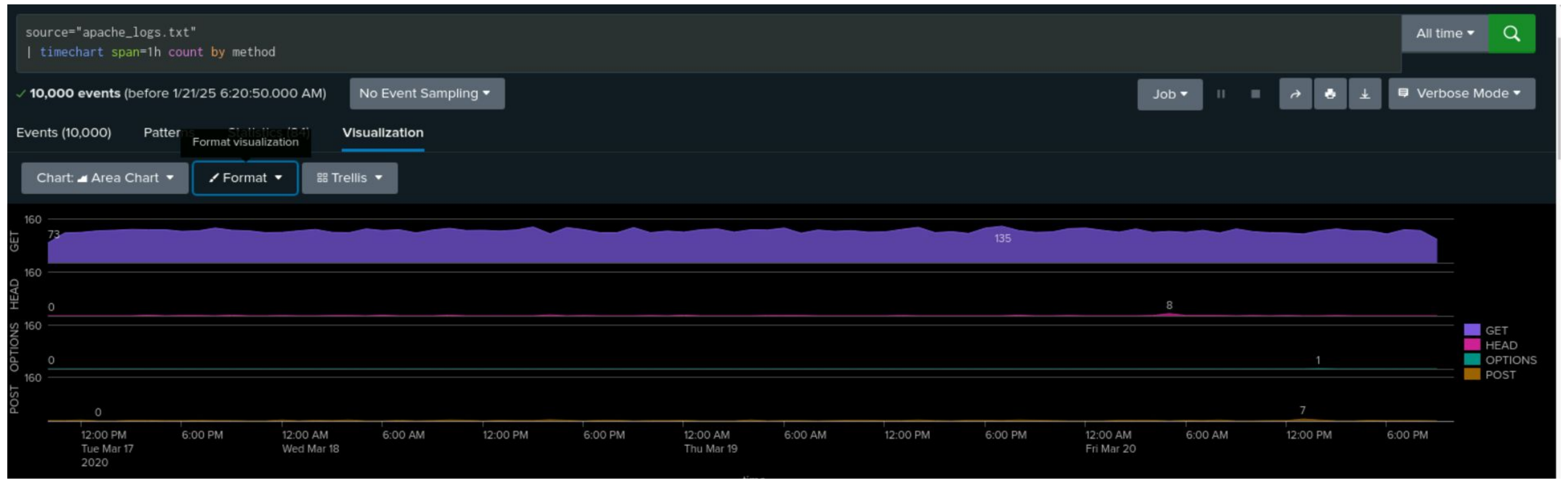


| useragent | count |
|---|---|
| Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 1044 |
| Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36 | 369 |
| UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/ | 364 |
| Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0 | 296 |
| 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 |
| Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 268 |
| Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 237 |
| Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0 | 236 |
| Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0 | 229 |
| Tiny Tiny RSS/1.11 (http://tt-rss.org/) | 198 |
| - | 190 |



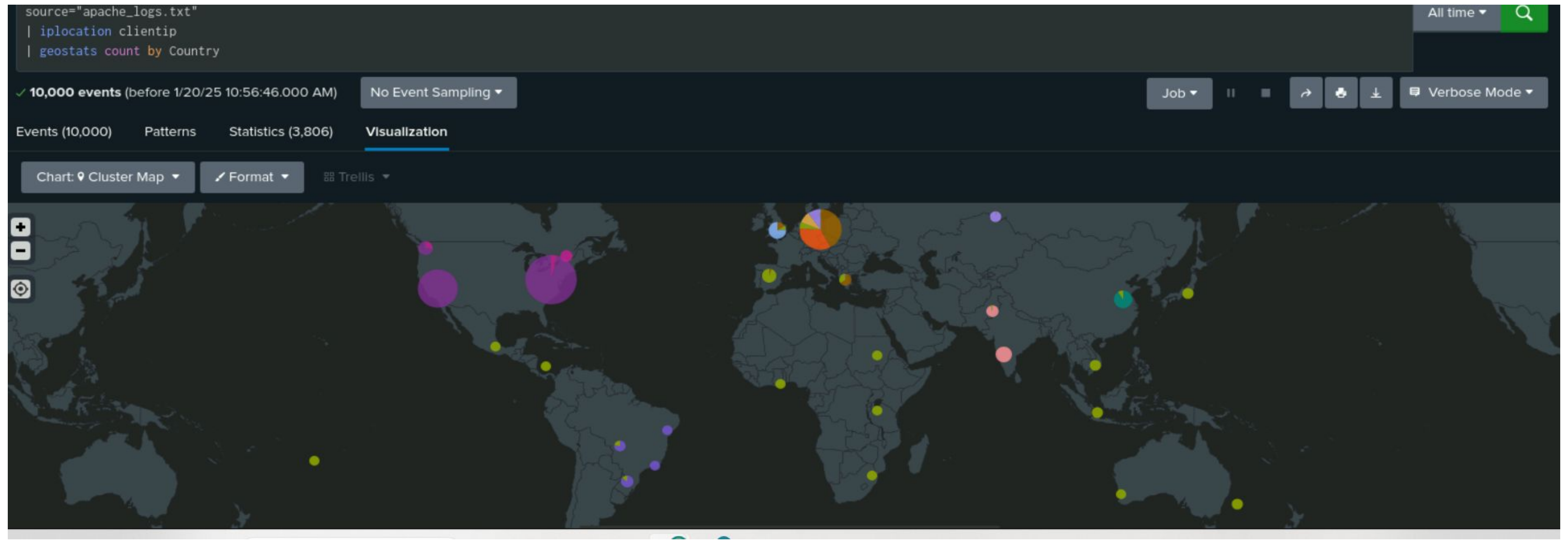
```
source="apache_logs.txt" | stats count by uri
```

✓ 10,000 events (before 1/20/25 8:46:13.000 PM)



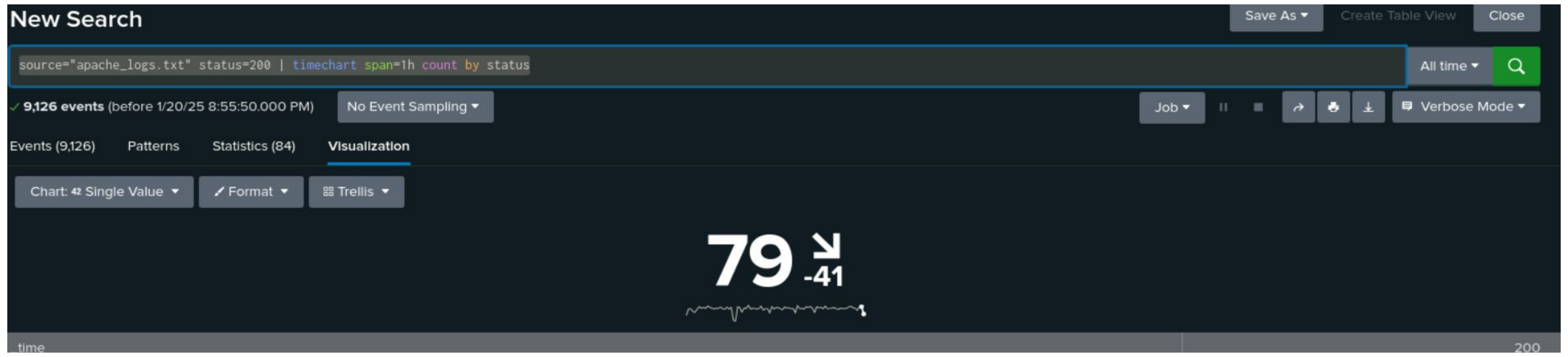
```
source="apache_logs.txt"
| timechart span=1h count by method
```

✓ 10,000 events (before 1/21/25 6:20:50.000 AM)



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

✓ 10,000 events (before 1/20/25 10:56:46.000 AM)

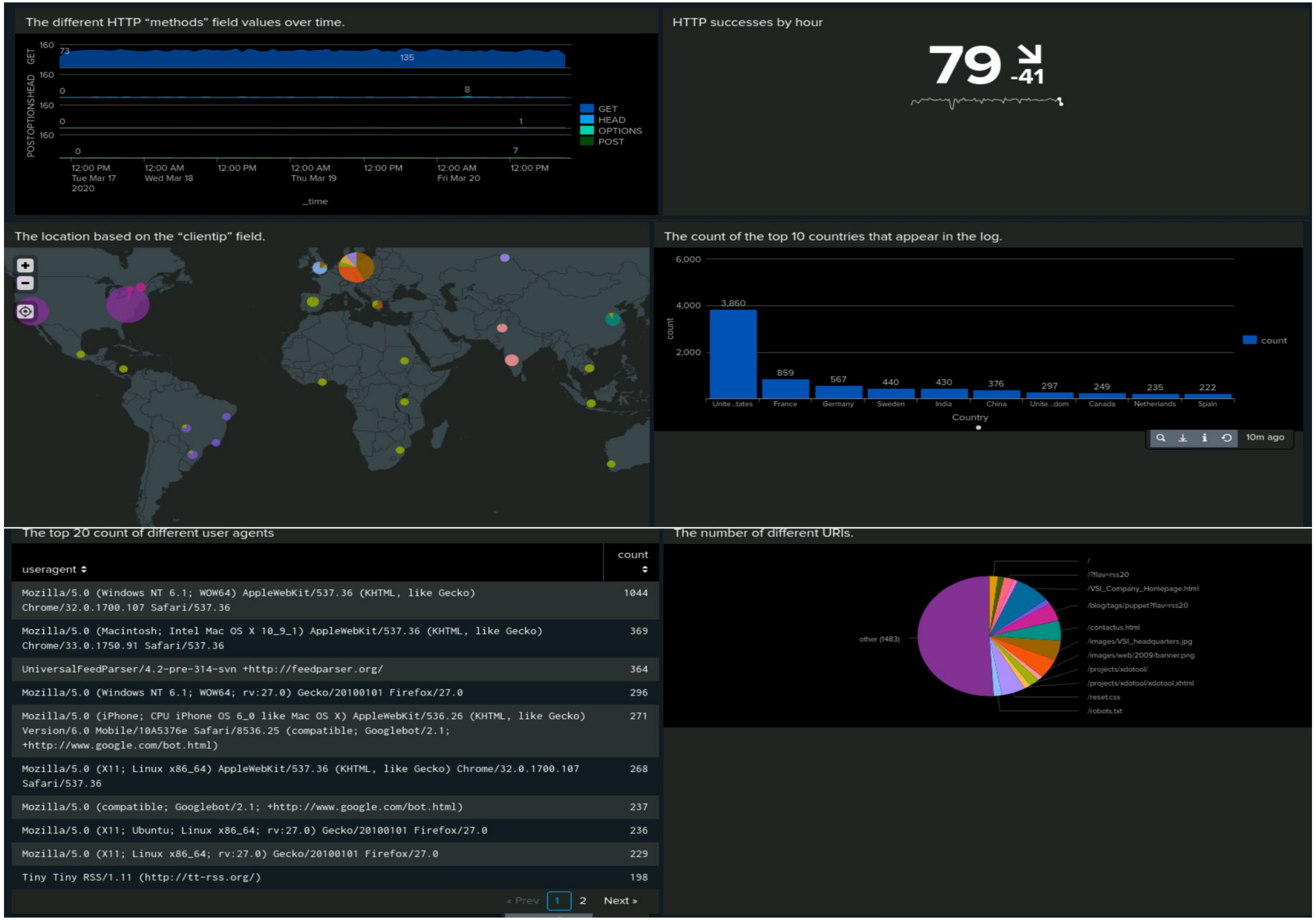


New Search

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

✓ 9,126 events (before 1/20/25 8:55:50.000 PM)

# Dashboard—Apache



The different HTTP "methods" field values over time.

HTTP successes by hour

The location based on the "clientip" field.

The count of the top 10 countries that appear in the log.

The top 20 count of different user agents

| useragent ⬍ | count ⬍ |
|---|---|
| Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 1044 |
| 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 |
| UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/ | 364 |
| Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0 | 296 |
| 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 |
| Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 268 |
| Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 237 |
| Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0 | 236 |
| Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0 | 229 |
| Tiny Tiny RSS/1.11 (http://tt-rss.org/) | 198 |

The number of different URIs.

/
/?flav=rss20
/VSI_Company_Homepage.html
/blog/tags/puppet?flav=rss20
/contactus.html
/images/VSI_headquarters.jpg
/images/web/2009/banner.png
/projects/xdotool/
/projects/xdotool/xdotool.xhtml
/reset.css
/robots.txt
other (1483)

# Attack Analysis

# Attack Summary—Windows

**Report Analysis for Severity:**

**Suspicious Changes Detected:**

Analysed Windows server logs and attack logs.

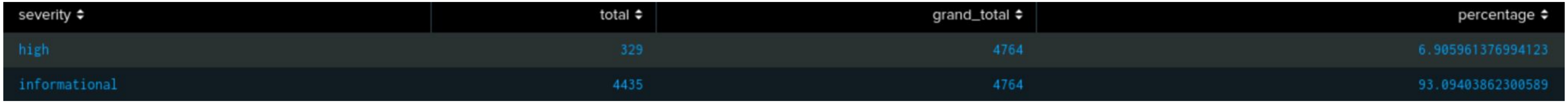
**Query Executed:** Aggregated severity levels to identify trends.

**Findings:**

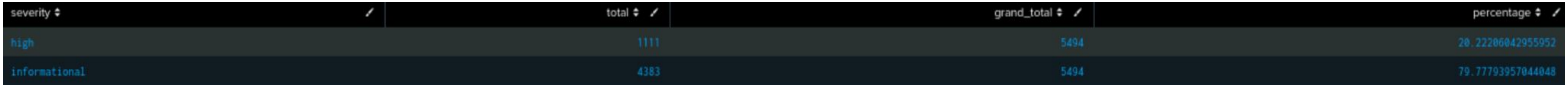
14% increase in high-severity alerts.

14% decrease in informational alerts.

**Implication:** Indicates a shift in event nature, warranting further investigation.



| severity | total | grand_total | percentage |
|---|---|---|---|
| high | 329 | 4764 | 6.905961376994123 |
| informational | 4435 | 4764 | 93.09403862300589 |



| severity | total | grand_total | percentage |
|---|---|---|---|
| high | 1111 | 5494 | 20.22206042955952 |
| informational | 4383 | 5494 | 79.77793957044048 |

# Attack Summary—Windows

## Report Analysis for Failed Activities:

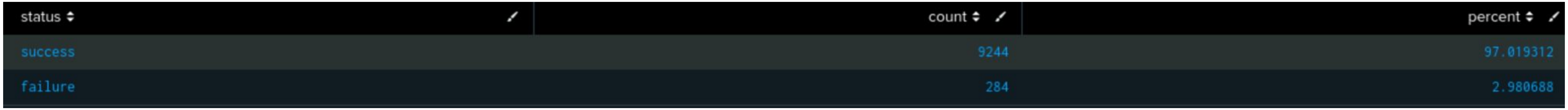
### Suspicious Changes Detected:

Reviewed Windows server and attack server logs.

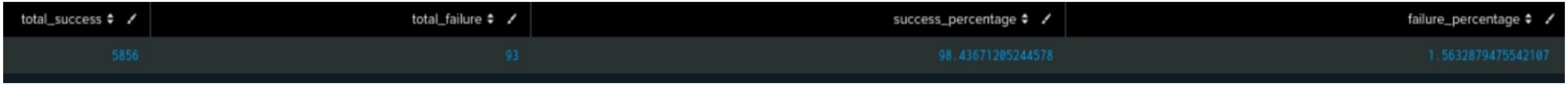
### Findings:

1% increase in successful activities.

1% decrease in failed activities.



| status | count | percent |
|---|---|---|
| success | 9244 | 97.019312 |
| failure | 284 | 2.980688 |



| total_success | total_failure | success_percentage | failure_percentage |
|---|---|---|---|
| 5856 | 93 | 98.43671205244578 | 1.5632879475542107 |

# Alert Attack Summary—Windows

## Failed Windows Activity:

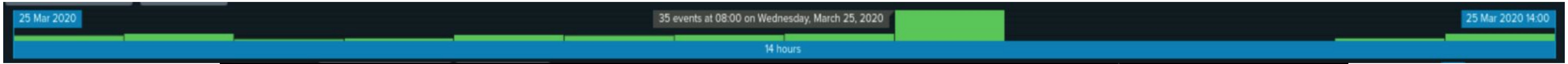
**Suspicious Volume Detected:** Yes, a peak of 25 failed activities was recorded, indicating a potential attack.

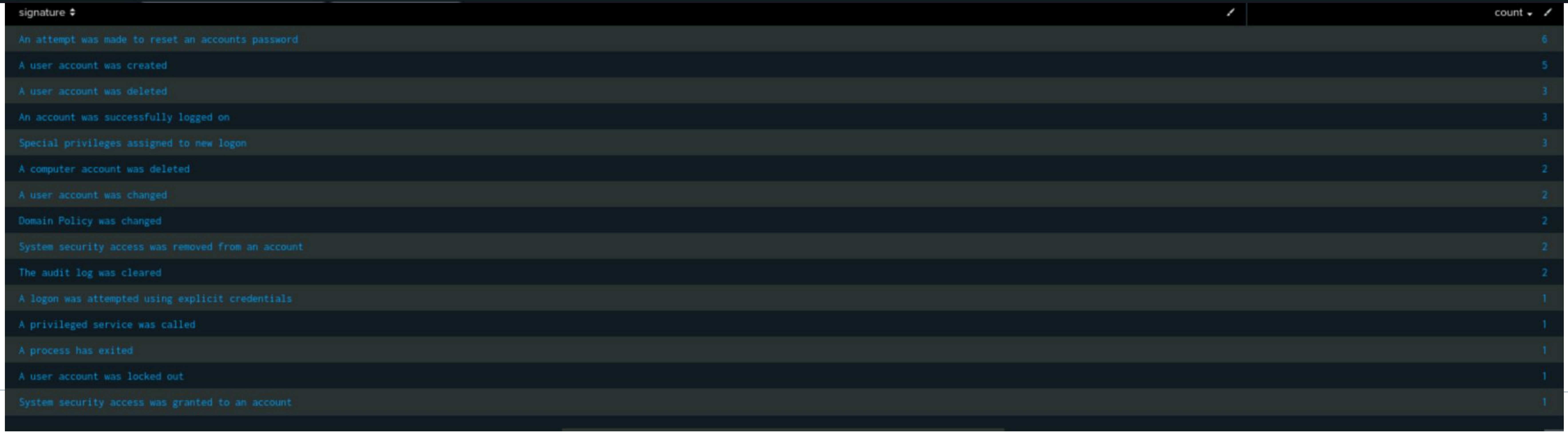
**Count of Events:** The highest count was 6 events related to password reset attempts.

**Time of Occurrence:** March 25, 2020, between 08:00 - 09:00.

**Alert Trigger:** Yes

**Threshold Review:** No changes needed





| signature | count |
|---|---|
| An attempt was made to reset an accounts password | 6 |
| A user account was created | 5 |
| A user account was deleted | 3 |
| An account was successfully logged on | 3 |
| Special privileges assigned to new logon | 3 |
| A computer account was deleted | 2 |
| A user account was changed | 2 |
| Domain Policy was changed | 2 |
| System security access was removed from an account | 2 |
| The audit log was cleared | 2 |
| A logon was attempted using explicit credentials | 1 |
| A privileged service was called | 1 |
| A process has exited | 1 |
| A user account was locked out | 1 |
| System security access was granted to an account | 1 |

# Alert Attack Summary—Windows

**Successful Logins:**

**Suspicious Volume Detected:** Yes, a peak of 1970 successful logins occurred between 01:00 - 03:00.

**Primary User:** User A was the main user logging in during this period.

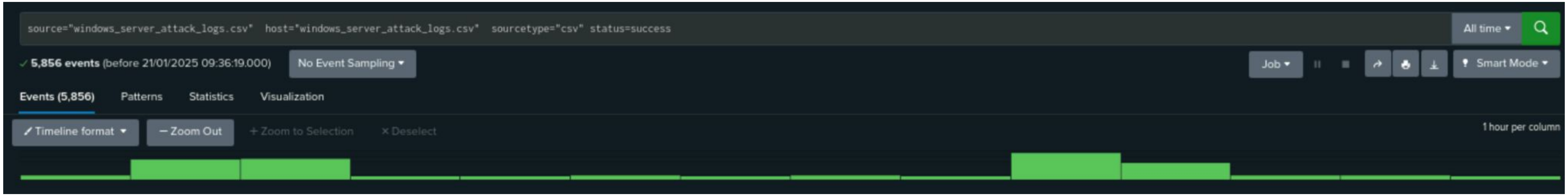
**Time of Peak Activity:** The peak was also observed between 09:00 - 11:00, attributed to normal work-related logins.

**Alert Trigger:** Yes

**Threshold Review:** No changes needed

**Deleted Accounts:**

**Suspicious Volume Detected:** No significant attacks or outliers were found in the volume of deleted accounts.



```
source="windows_server_attack_logs.csv" host="windows_server_attack_logs.csv" sourcetype="csv" status=success
```

✓ 5,856 events (before 21/01/2025 09:36:19.000)

# Dashboard Attack Summary—Windows

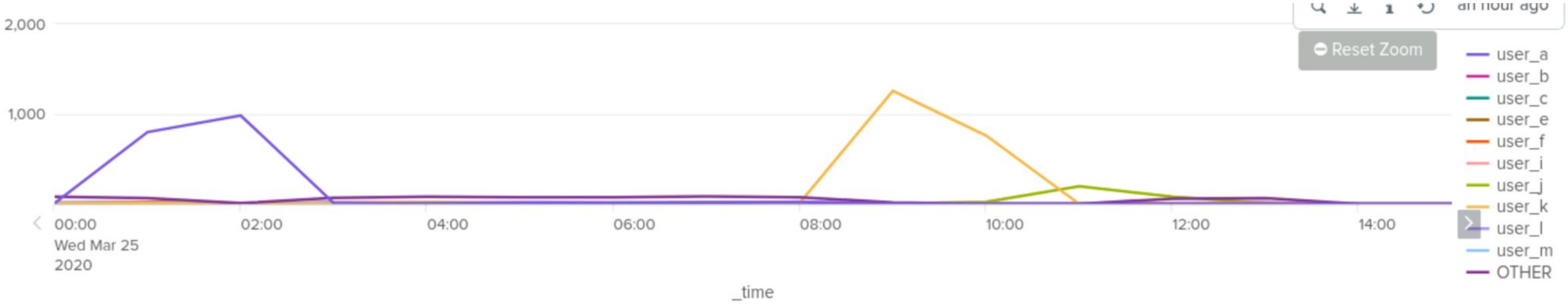
**Dashboard Analysis for Users:**

**Suspicious Activity Detected:** Yes, two peaks correspond with those observed in the signature reports, indicating potential areas of concern.

**Notable Users:**

User A: Activity from March 25, 2020, 00:00 - 03:00 with a peak count of 984 events.

User K: Activity from March 25, 2020, 08:00 - 11:00 with a peak count of 1256 events.

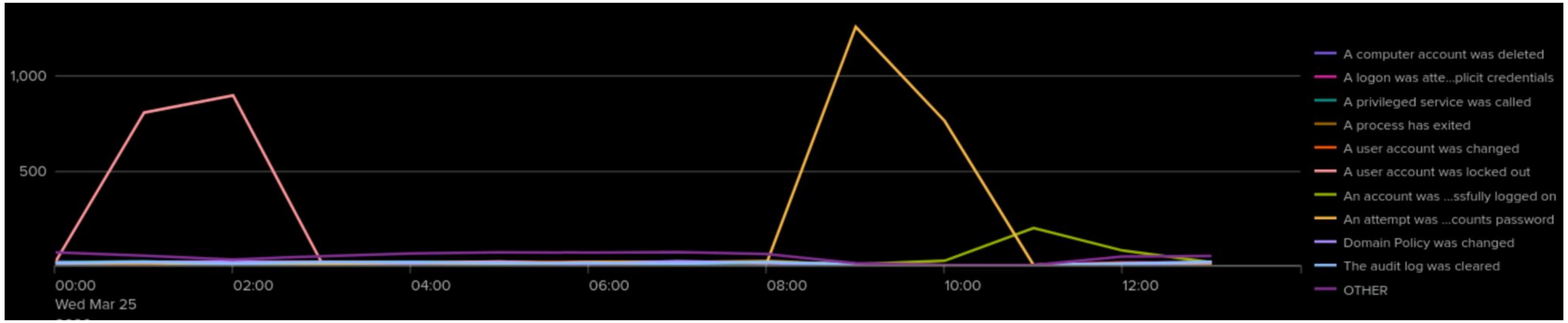


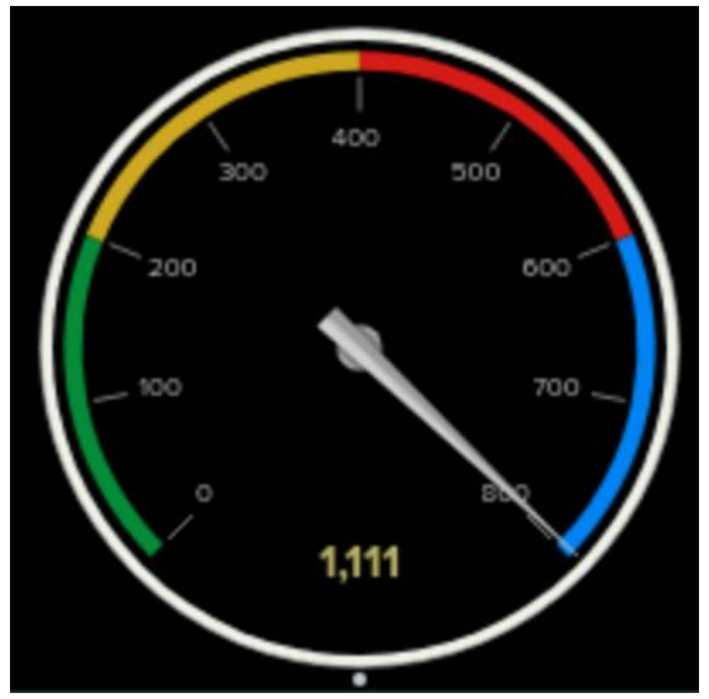
# Dashboard Attack Summary—Windows

## Dashboard Analysis for Signatures (Bar, Graph, and Pie Charts):

**Suspicious Activity:** The bar graph shows a significant number of attacks, while the radial chart indicates exceptionally high volumes of high-severity events.

**Results Confirmation:** Findings match previous analyses, confirming elevated risks.





## Dashboard Analysis for Users (Bar, Graph, and Pie Charts):

**Suspicious Activity:** The pie chart highlights distinct activity for Users A and K, contrasting with more dispersed user activity.

**Results Confirmation:** Data reinforces the prominence of Users A and K in overall metrics.

# Attack Summary—Report Analysis for HTTP Methods

**Suspicious Changes Detected:**

**March 25:**

6:00 PM: GET requests surged from 117 to 729.

5:00 AM: HEAD requests increased from 0 to 8 (possible reconnaissance).

2:00 PM: Notable 1 OPTIONS request (unusual activity).

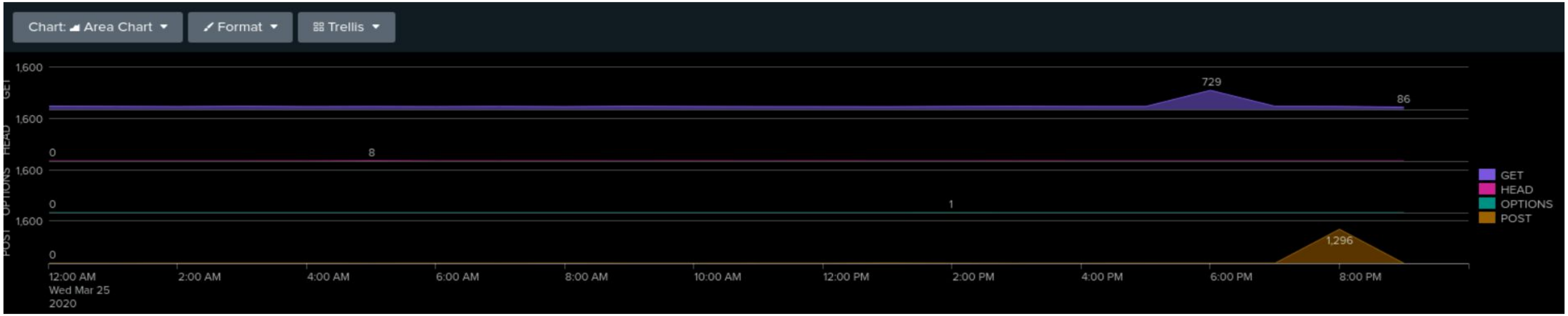
8:00 PM: POST requests spiked to 1,296.

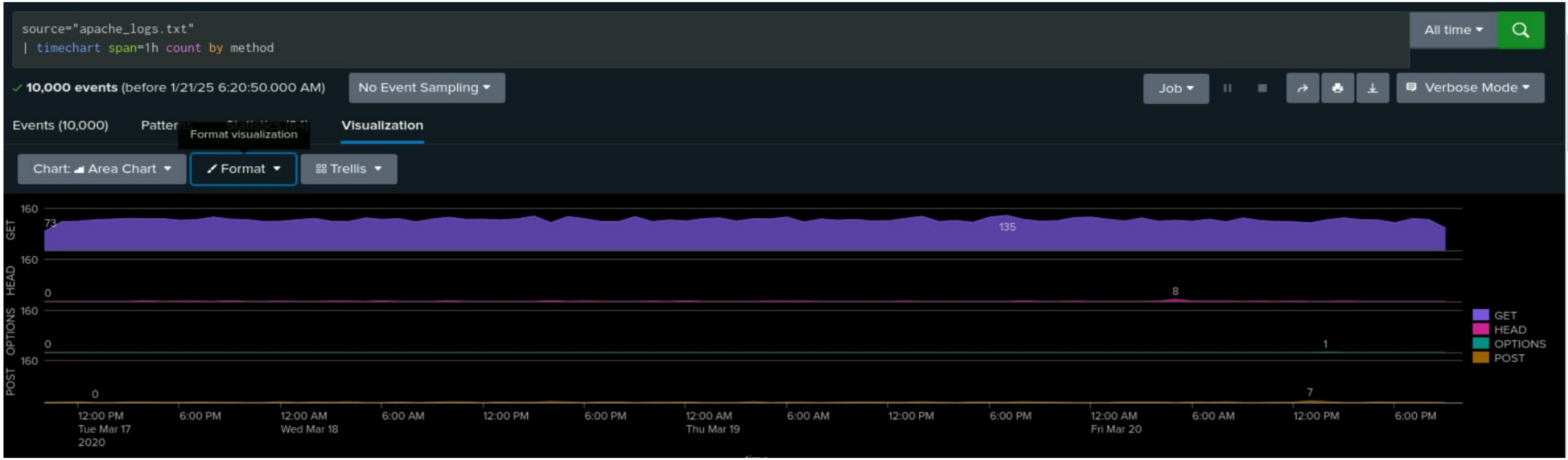
**Implications:**

Anomalies suggest potential reconnaissance or exploitation attempts.

Further investigation into the source and intent of these requests is recommended.

# Attack Summary—Report Analysis for HTTP Methods





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

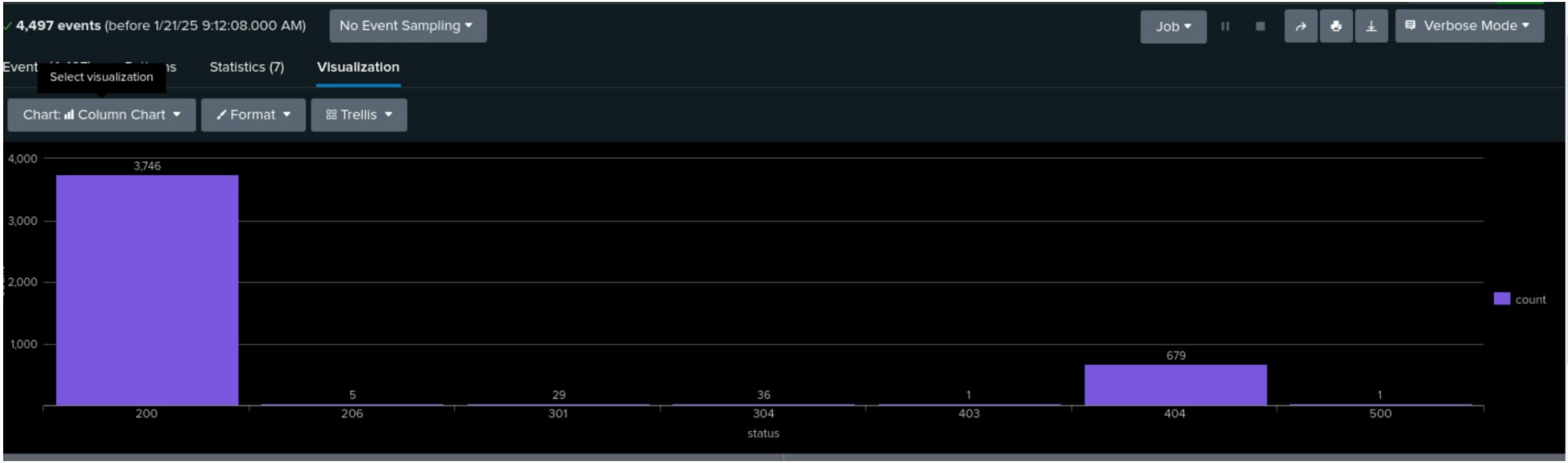
✓ **10,000 events** (before 1/21/25 6:20:50.000 AM)

# Attack Summary— Report Analysis for HTTP Response Codes

## Notable Changes Detected:

404 Response Codes: Increased by 190%; suggests probing for hidden files or vulnerabilities.

200 Response Codes: Decreased by 58%; may reflect disruptions due to invalid requests or server issues.

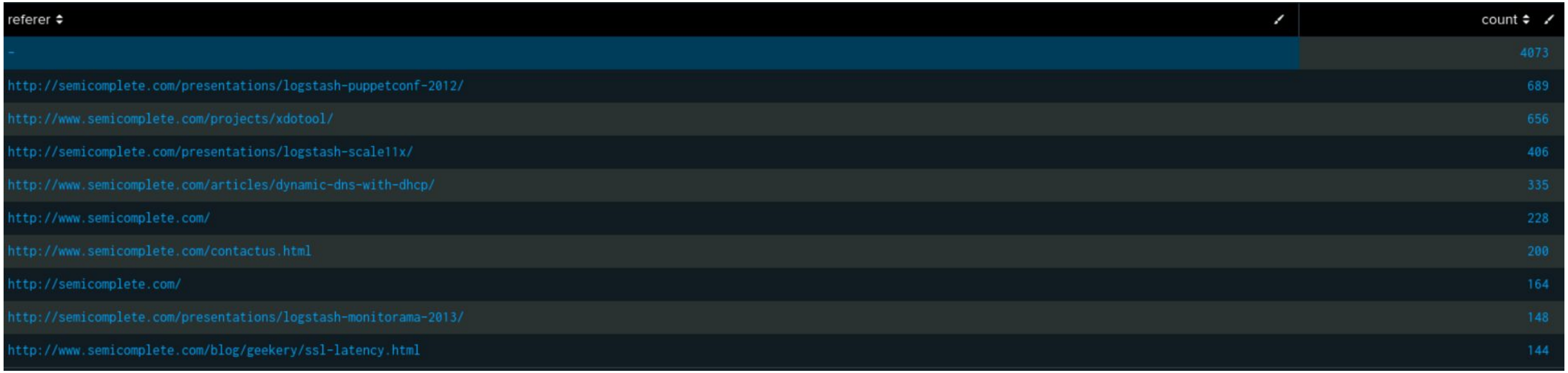


✓ 4,497 events (before 1/21/25 9:12:08.000 AM)

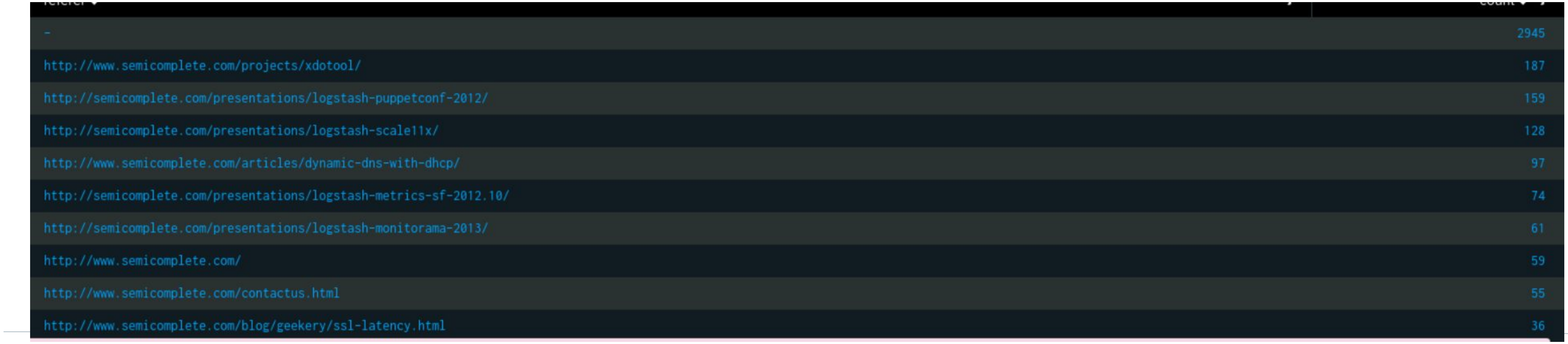
Chart: Column Chart

# Report Analysis for Referrer Domains

**Suspicious Changes:** No suspicious referrer domains detected during the attack.



| referer | count |
|---|---|
| - | 4073 |
| http://semicomplete.com/presentations/logstash-puppetconf-2012/ | 689 |
| http://www.semicomplete.com/projects/xdotool/ | 656 |
| http://semicomplete.com/presentations/logstash-scale11x/ | 406 |
| http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/ | 335 |
| http://www.semicomplete.com/ | 228 |
| http://www.semicomplete.com/contactus.html | 200 |
| http://semicomplete.com/ | 164 |
| http://semicomplete.com/presentations/logstash-monitorama-2013/ | 148 |
| http://www.semicomplete.com/blog/geekery/ssl-latency.html | 144 |



| referer | count |
|---|---|
| - | 2945 |
| http://www.semicomplete.com/projects/xdotool/ | 187 |
| http://semicomplete.com/presentations/logstash-puppetconf-2012/ | 159 |
| http://semicomplete.com/presentations/logstash-scale11x/ | 128 |
| http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/ | 97 |
| http://semicomplete.com/presentations/logstash-metrics-sf-2012.10/ | 74 |
| http://semicomplete.com/presentations/logstash-monitorama-2013/ | 61 |
| http://www.semicomplete.com/ | 59 |
| http://www.semicomplete.com/contactus.html | 55 |
| http://www.semicomplete.com/blog/geekery/ssl-latency.html | 36 |

# Attack Summary — Alert Analysis for International Activity

**Suspicious Activity Detected:**

Date & Time: March 25, 8:00 PM

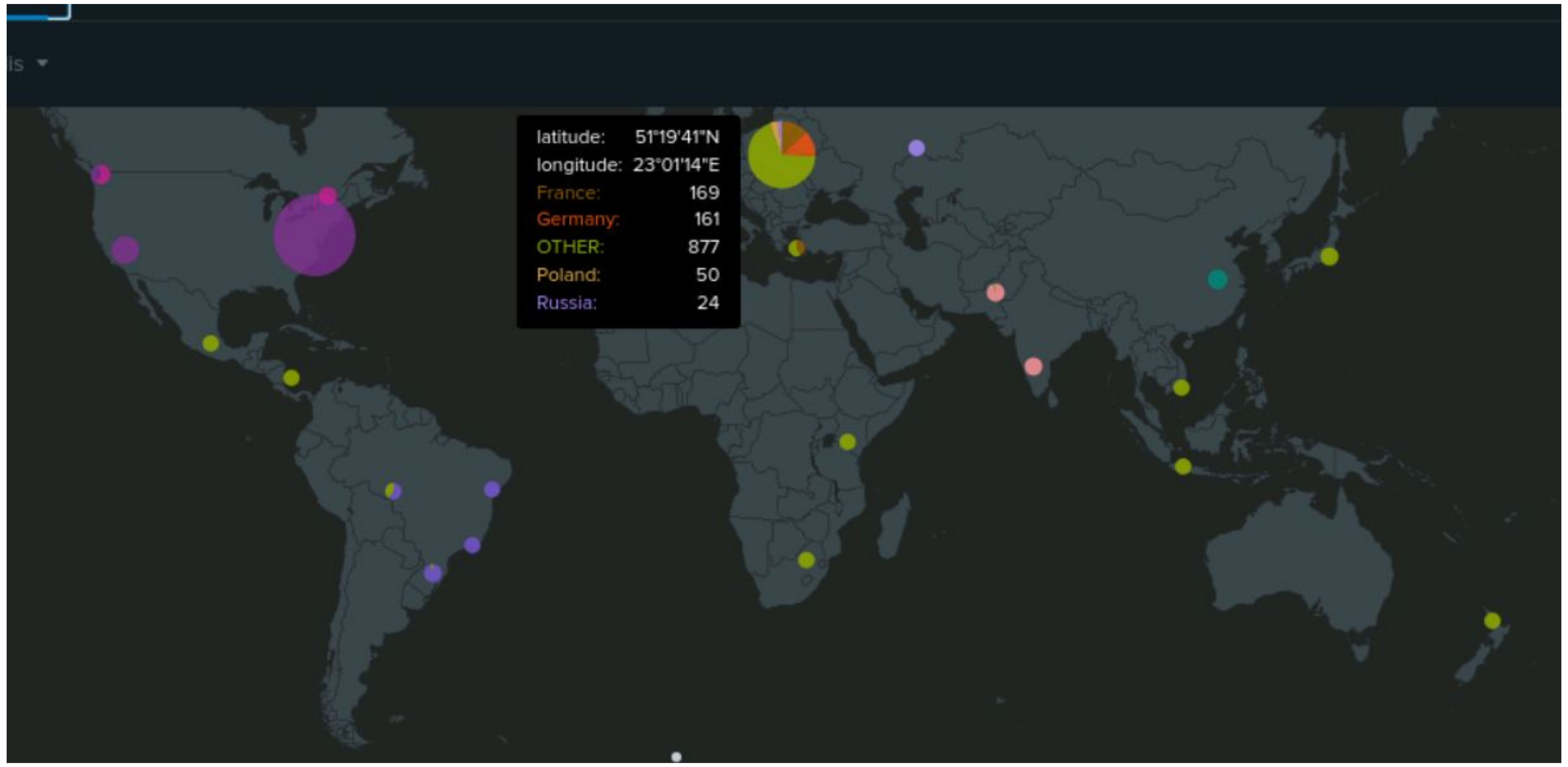
Count: 937 requests from Ukraine.

**Threshold Trigger:**

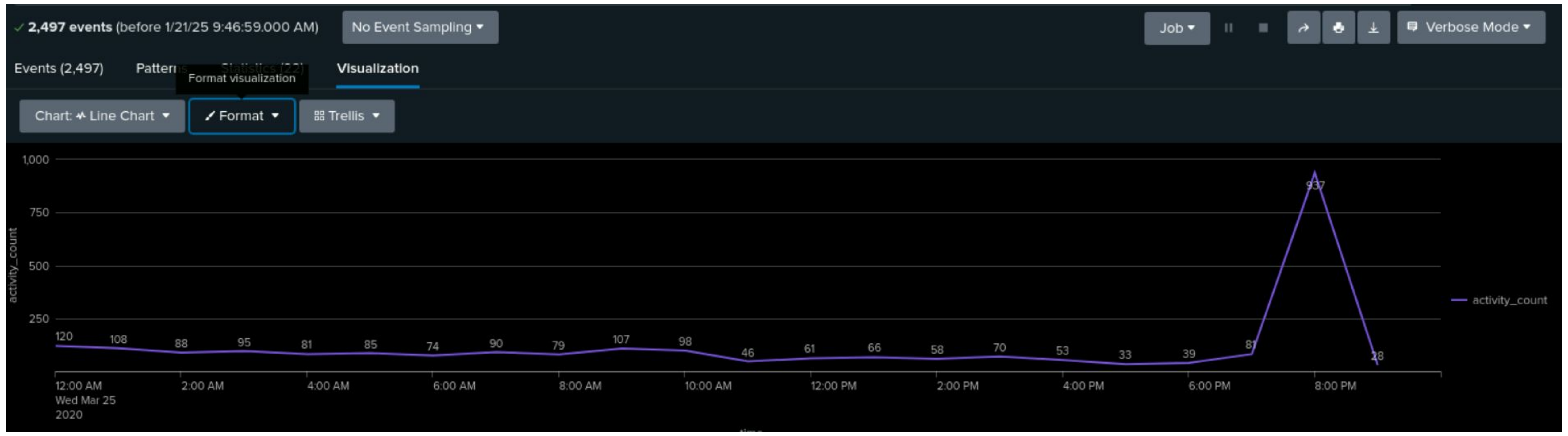
Alert Triggered: Yes, threshold set at 130 requests.

**Threshold Review:**

Change Needed: No



| | |
|---|---|
| latitude: | 51°19'41"N |
| longitude: | 23°01'14"E |
| France: | 169 |
| Germany: | 161 |
| OTHER: | 877 |
| Poland: | 50 |
| Russia: | 24 |



✓ 2,497 events (before 1/21/25 9:46:59.000 AM)

# Attack Summary — Alert Analysis for HTTP POST Activity

**Suspicious Activity Detected:**

Date & Time: March 25, 8:00 PM

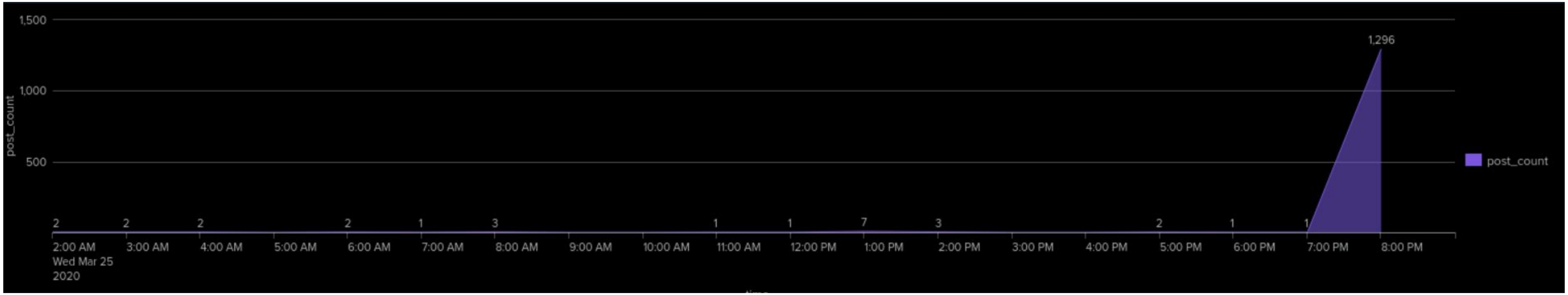
Count: 1,296 POST requests

**Threshold Trigger:**

Alert Triggered: Yes, activity peaked in a single hour.

**Threshold Review:**

Change Needed: No



# Dashboard Analysis for Time Chart of HTTP Methods

**Suspicious Activity Detected:**

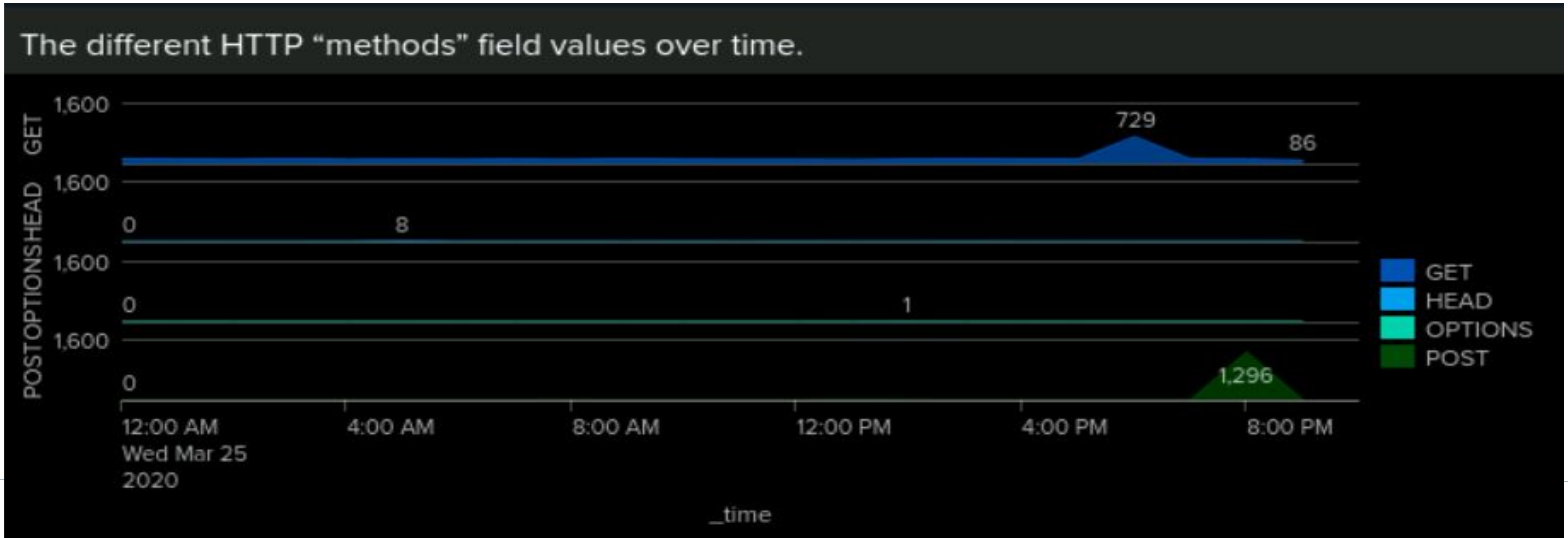
The GET method between 5:00 PM and 7:00 PM on Wednesday, March 25th, and with the POST method between 7:00 PM and 8:00 PM on the same day.

**Method of Attack**

GET and POST

**Peak Count of Method during the attack:**

GET (729) and POST (1,296)



# Attack Summary — Dashboard Analysis for Cluster Map

**Suspicious Activity Detected:**

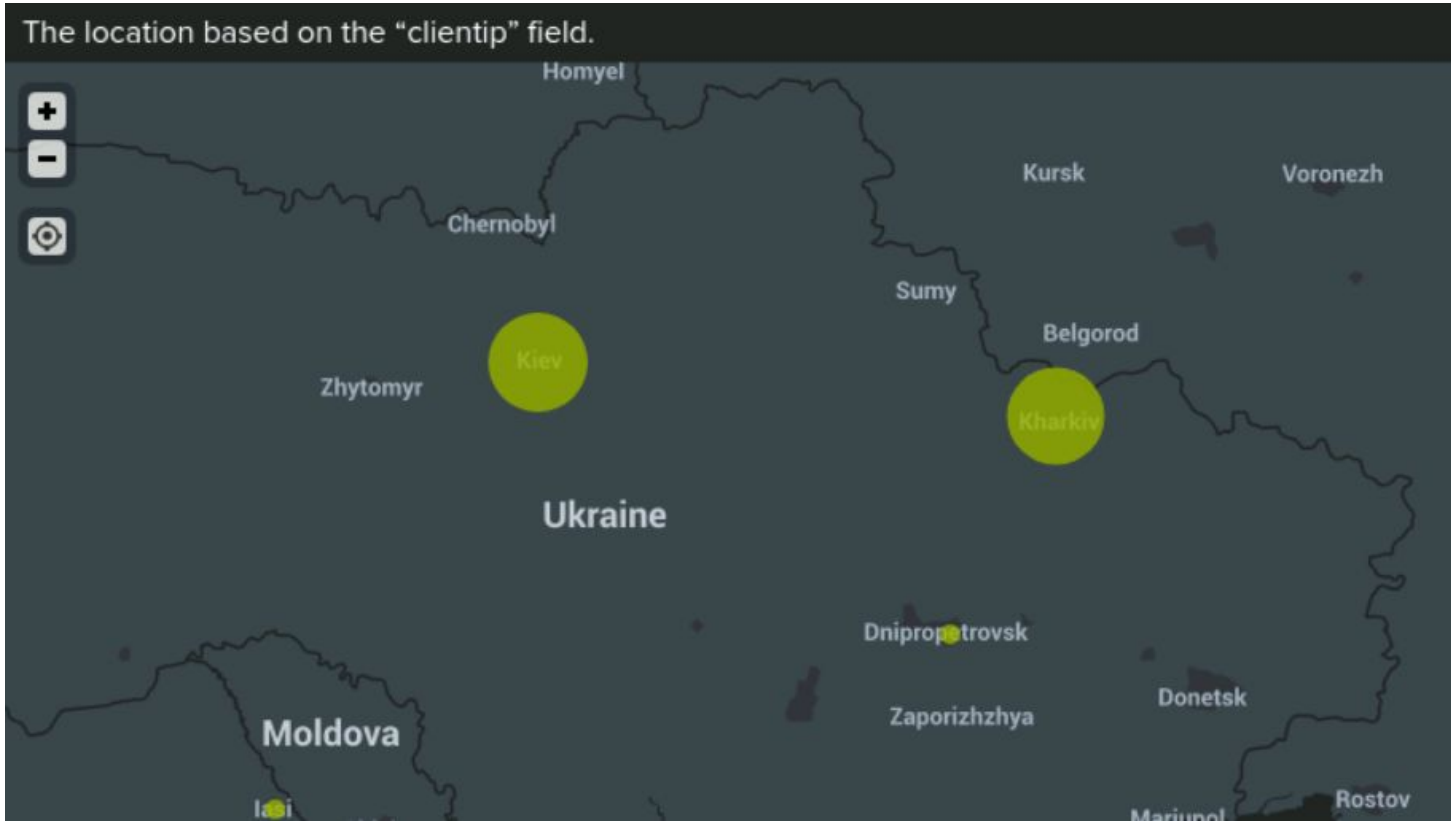
High volume of activity from **Ukraine.**

**Notable cities:** Kiev and Kharkiv.

**Activity Counts:**

**Kiev:** 440 requests

**Kharkiv:** 432 requests



The location based on the “clientip” field.

# Attack Summary — Dashboard Analysis for URI Data

**Suspicious Activity Observed:**

URI *"/files/logstash/logstash-1.3.2-monolithic.jar"* between **6:00 PM and 7:00 PM** on March 25.

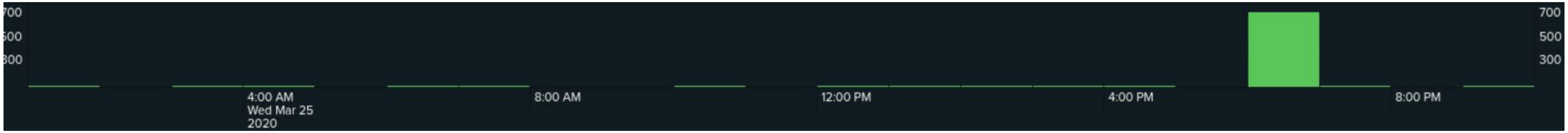
URI *"/VSI_Account_logon.php"* between **8:00 PM and 9:00 PM** on March 25.

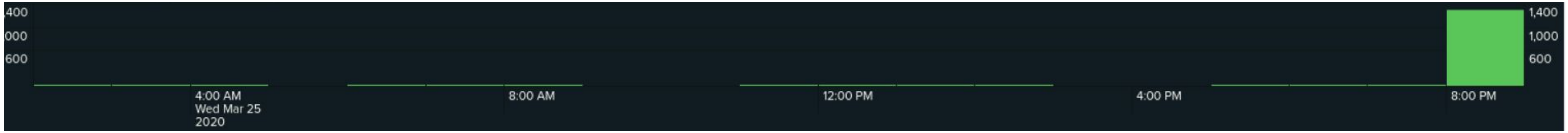
**Most Frequently Accessed URI:**

*"/VSI_Account_logon.php"*

**Potential Attacker Intent:**

Suggests a brute force attack, indicating multiple login attempts for unauthorised access.





# Summary and Future Mitigations

# Overall Findings from the Attack

**Windows Logs:**

User A: Multiple failed login attempts indicate potential brute force attacks.

User K: Unusual access times suggest possible unauthorised access.

Anomalies: Spikes in login attempts during peak hours increase account compromise risk.

**Apache Logs:**

HTTP Methods:

POST requests surged to 1,296; GET requests rose from 117 to 729, indicating reconnaissance and exploitation attempts.

HEAD requests increased from 0 to 8, suggesting probing.

**International Activity:**

High request volumes from Ukraine, especially Kiev (440) and Kharkiv (432), indicate targeted attacks.

# Recommended Future Mitigations

**Windows Logs:**

**Account Lockout Policies:** Lock accounts after multiple failed login attempts, especially for User A.

**Enhanced Monitoring:** Use real-time monitoring for unusual patterns, focusing on User K.

**Apache Logs:**

**Rate Limiting:** Set thresholds to control excessive requests from single sources.

**Web Application Firewall (WAF):** Deploy to filter malicious requests and protect sensitive URIs.

# END OF THE REPORT - Thank you for your attention.