# Defensive Security Project
# by: The Night’s Watch
# (Dylan, Ryan, & Benji)

# Table of Contents

This document contains the following resources:

01

**Monitoring Environment**

02

**Attack Analysis**

03

**Project Summary & Future Mitigations**

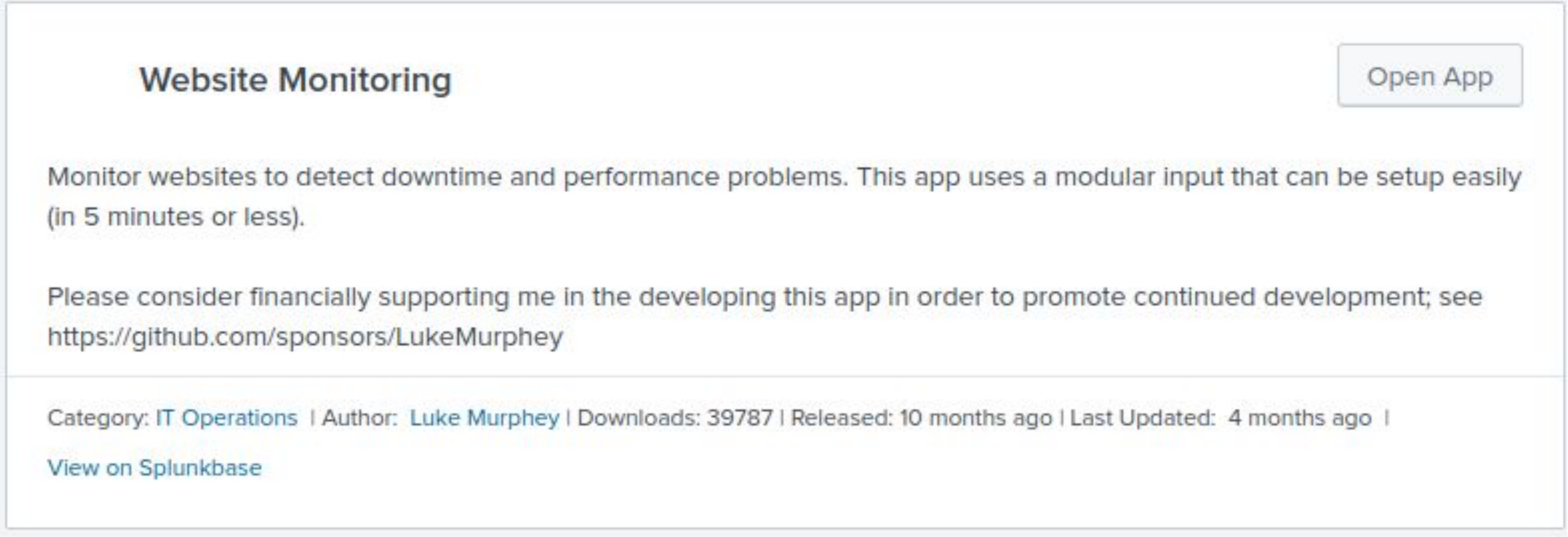
# Monitoring Environment

# Scenario

- Assume the role of a SOC analyst for VSI Corporation to monitor and analyze their Windows and Apache systems before and after an attack
- Analyze events by:
    - Creating reports to assist in monitoring for attacks.
    - Create alerts based on ideal thresholds from baselines.
    - Design visualizations and incorporate into a dashboard for quick access to important data.
    - Adding additional apps for monitoring specific information.

# Website Monitoring Add-on

# Website Monitoring



## Website Monitoring

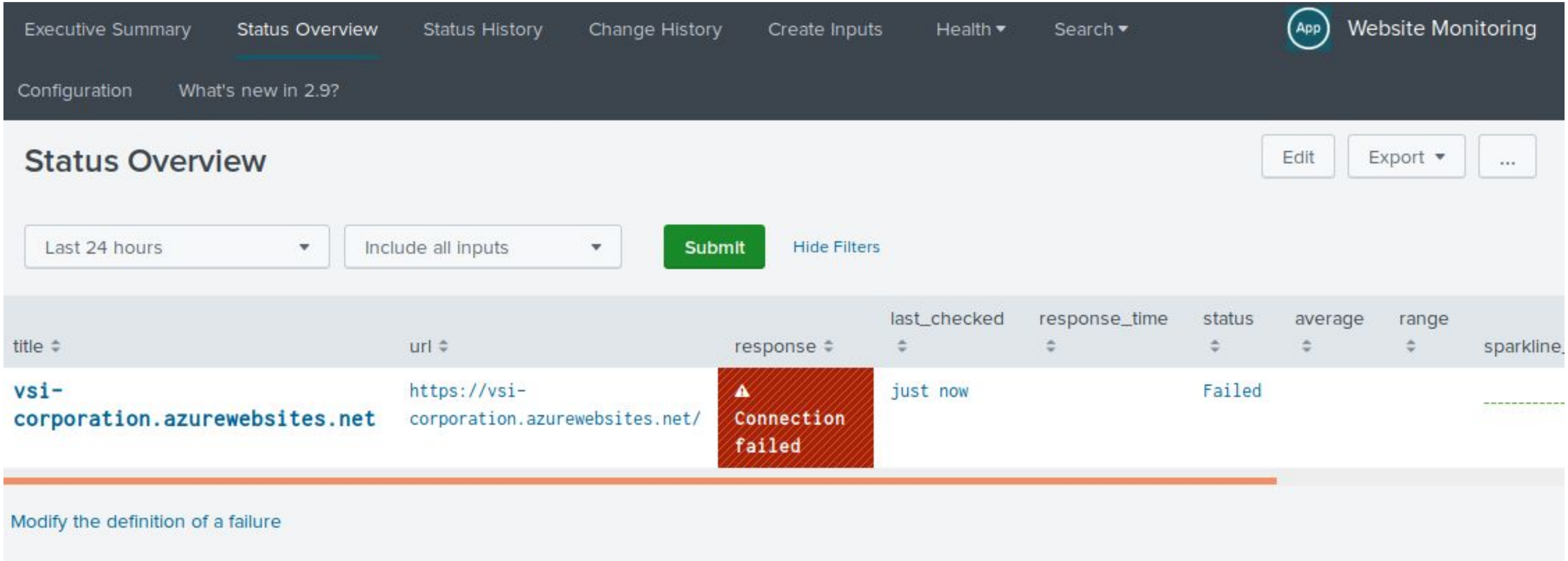
Monitor websites to detect downtime and performance problems. This app uses a modular input that can be setup easily (in 5 minutes or less).

Please consider financially supporting me in the developing this app in order to promote continued development; see https://github.com/sponsors/LukeMurphey

Category: IT Operations | Author: Luke Murphey | Downloads: 39787 | Released: 10 months ago | Last Updated: 4 months ago |

View on Splunkbase

# Website Monitoring (In Use)



Status Overview

Last 24 hours

Include all inputs

| title | url | response | last_checked | response_time | status | average | range | sparkline_ |
|---|---|---|---|---|---|---|---|---|
| vsi-corporation.azurewebsites.net | https://vsi-corporation.azurewebsites.net/ | ⚠ Connection failed | just now | | Failed | | | |

Modify the definition of a failure

# Logs Analyzed

## 1 Windows Logs

- Important information on Windows Machine events
  - User IDs / Account Names
  - Security Privileges
  - Date / Time
  - Event Statuses / Codes

## 2 Apache Logs

- Web Application Server
  - URIs
  - Date / Time
  - Geographic location of source IPs
  - HTTP Statuses
    - GET/HEAD/POST/OPTION
    - 404 etc.

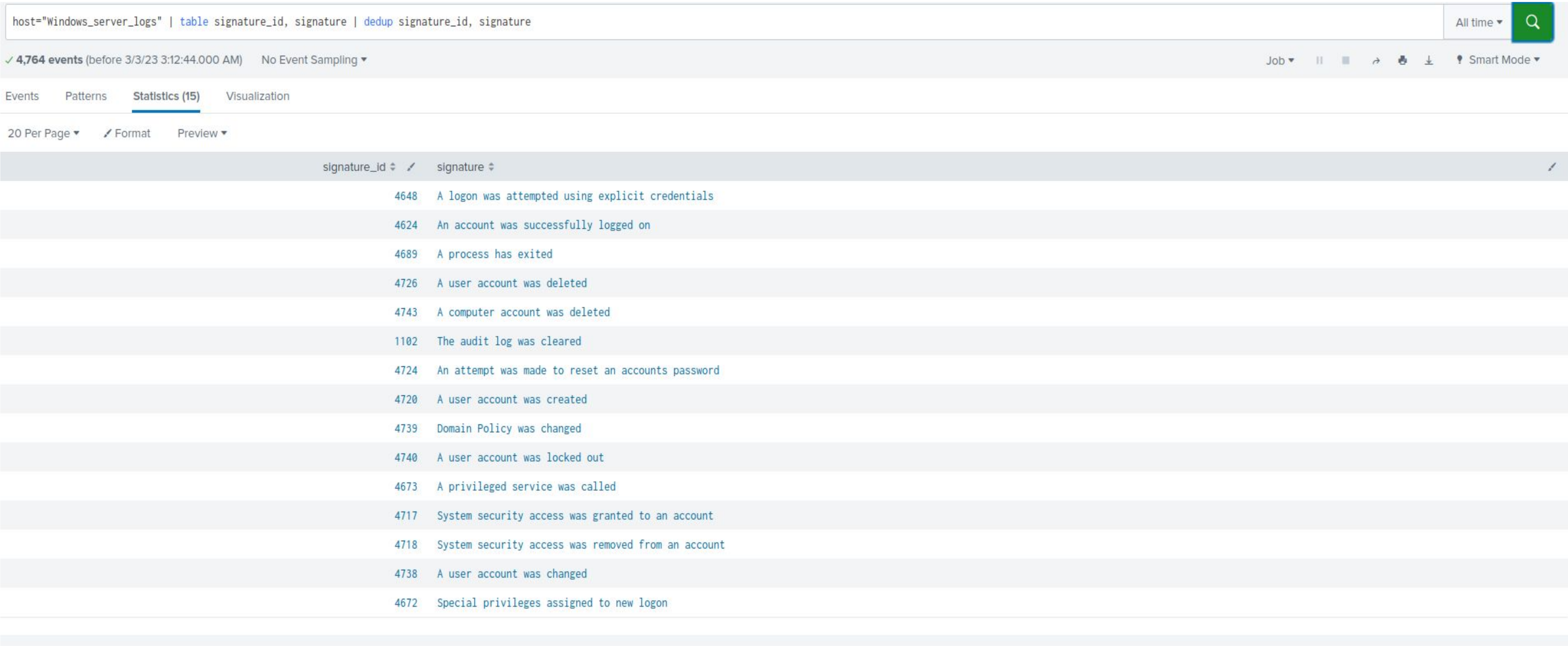
# Windows Logs

# Reports—Windows

| Report Name | Report Description |
|---|---|
| ID Number Associated with Specific Signature | A report for Windows activities that displays the ID number connected to the particular signature. |
| Severity | A report that outlines the severity levels and count of the Windows logs that are being examined. |
| Success and Failure | A report indicating whether the number of unsuccessful operations on their server is suspiciously high. |

# Report 1—Windows

## ID Number Associated with Specific Signature



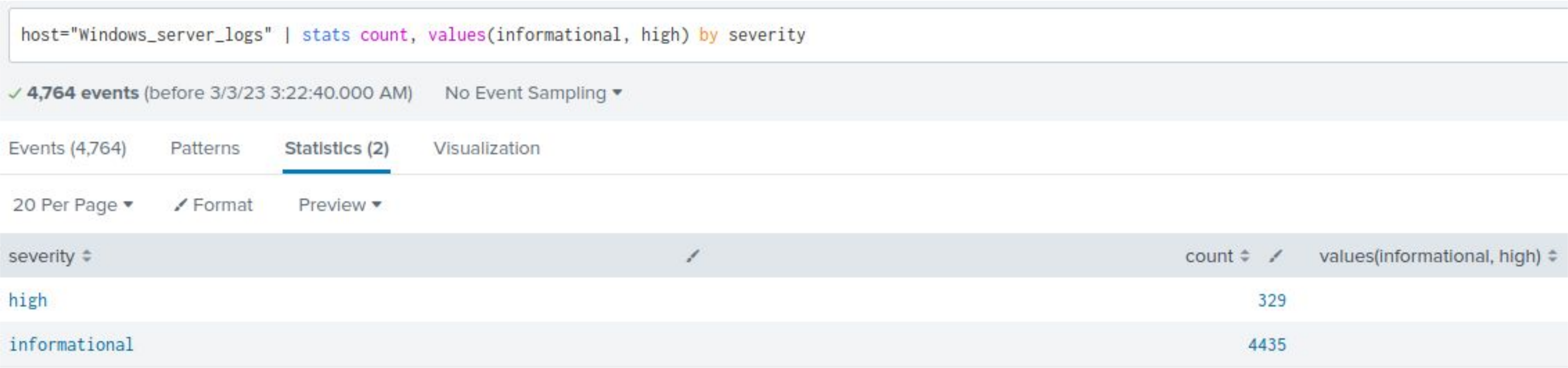
```
host="Windows_server_logs" | table signature_id, signature | dedup signature_id, signature
```

✓ **4,764 events** (before 3/3/23 3:12:44.000 AM) No Event Sampling ▾

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

# Report 2—Windows

## Severity Count



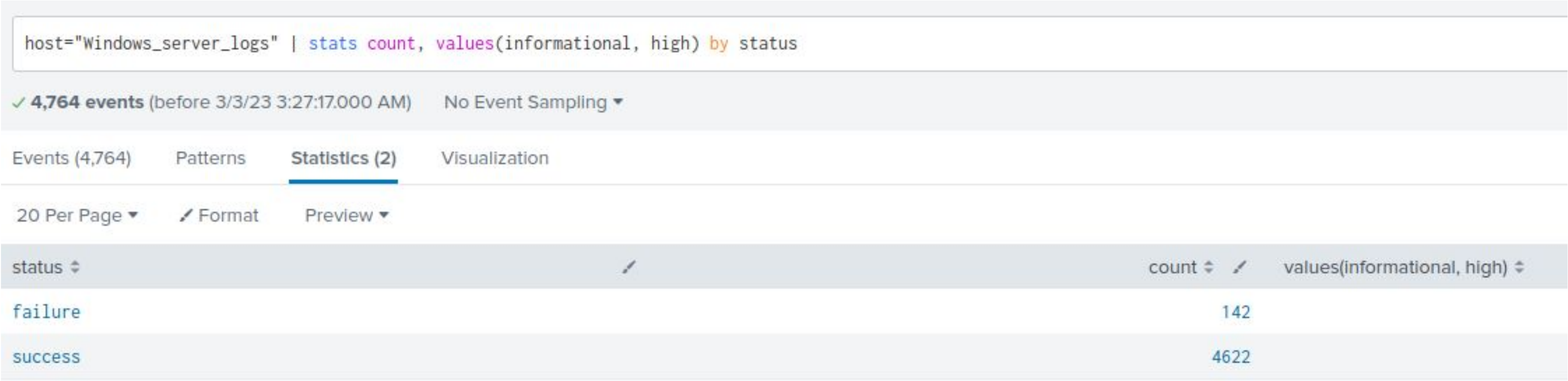
```
host="Windows_server_logs" | stats count, values(informational, high) by severity
```

✓ **4,764 events** (before 3/3/23 3:22:40.000 AM)

| severity | count | values(informational, high) |
|---|---|---|
| high | 329 | |
| informational | 4435 | |

# Report 3—Windows

## Success and Failure Rate



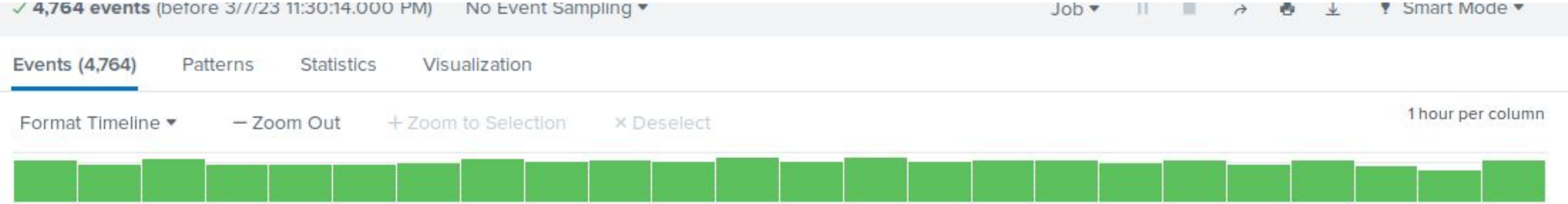
```
host="Windows_server_logs" | stats count, values(informational, high) by status
```

✓ 4,764 events (before 3/3/23 3:27:17.000 AM)

| status | count | values(informational, high) |
|---|---|---|
| failure | 142 | |
| success | 4622 | |

# Alert 1 — Windows

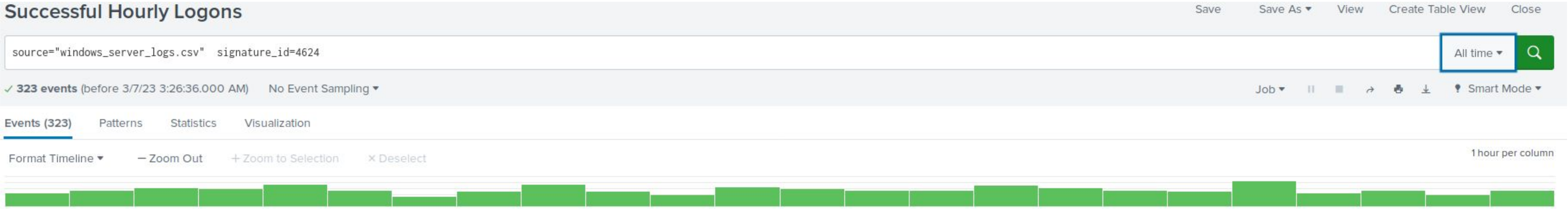
| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Suspicious Activity | Threshold of failed Windows Activity | 199 | 199 |



✓ 4,764 events (before 3/7/23 11:30:14.000 PM)

# Alert 2 — Windows

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Successful Logins | Hourly successful logon rate | 15 | 15 |



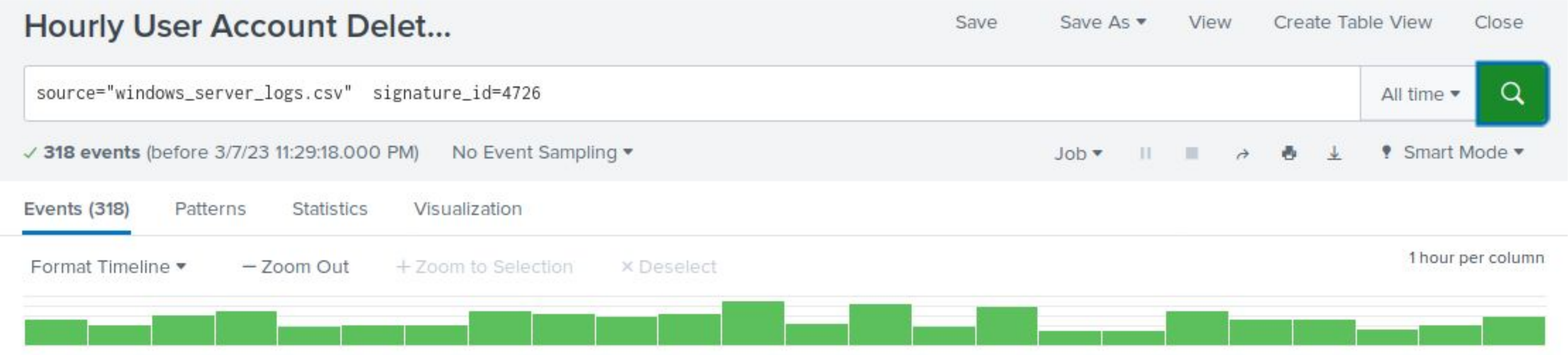
Successful Hourly Logons

```
source="windows_server_logs.csv"  signature_id=4624
```

✓ 323 events (before 3/7/23 3:26:36.000 AM)   No Event Sampling ▾

# Alert 3— Windows

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Deleted User Accounts | Threshold of Deleted User Accounts | 17 | 17 |



Hourly User Account Delet...

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

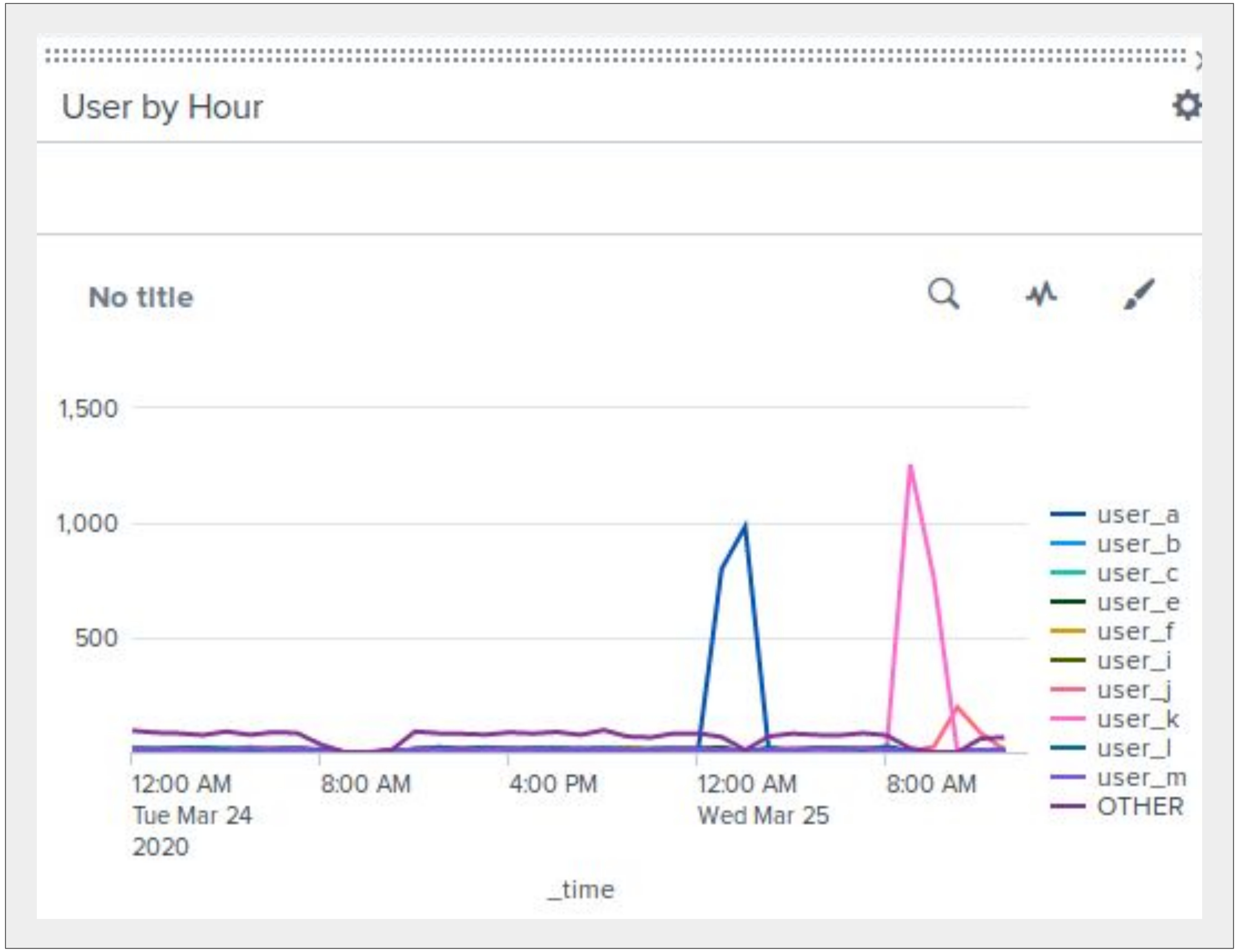
All time

✓ 318 events (before 3/7/23 11:29:18.000 PM)

No Event Sampling

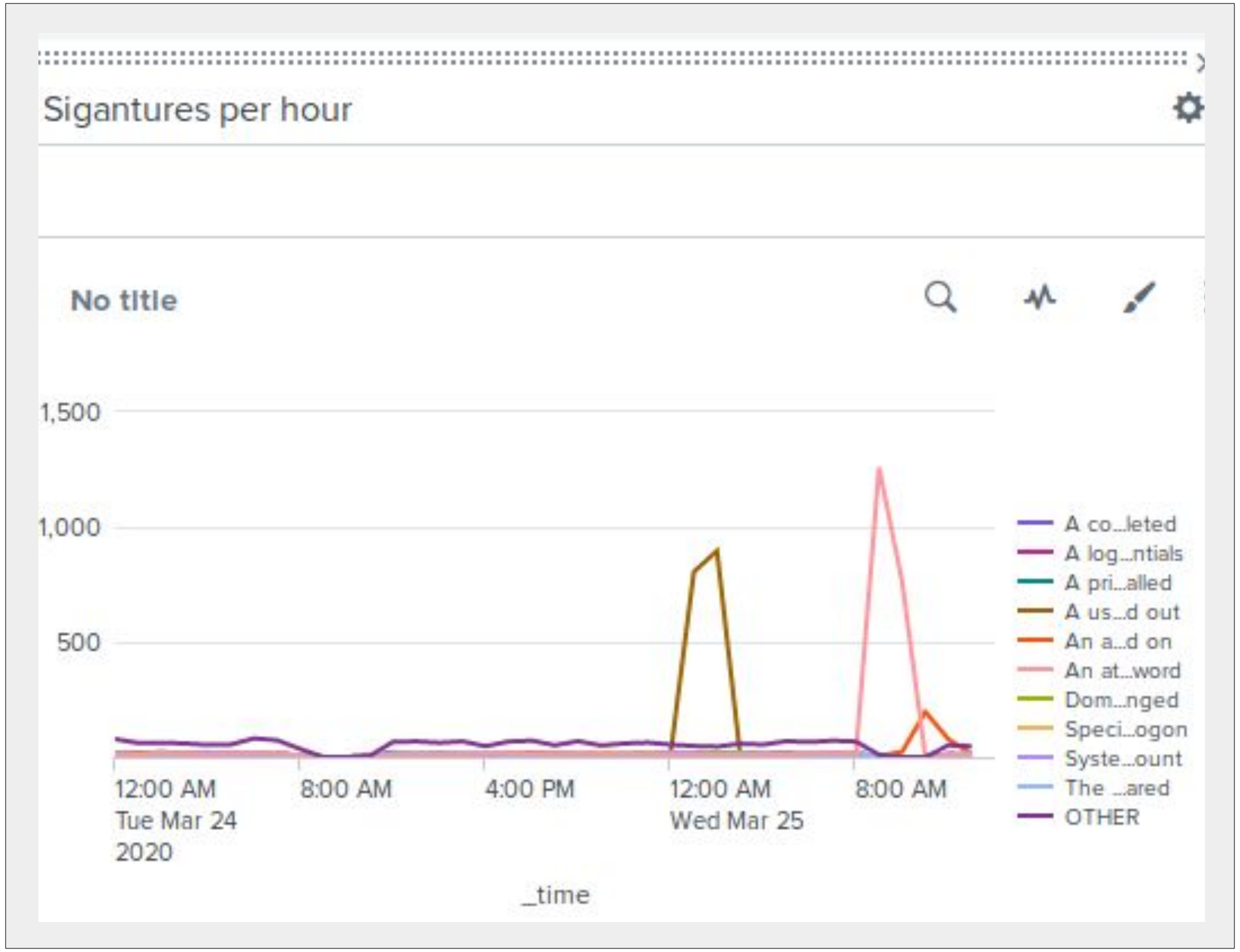
Smart Mode

# Dashboards—Windows



User by Hour

No title



Sigantures per hour

No title

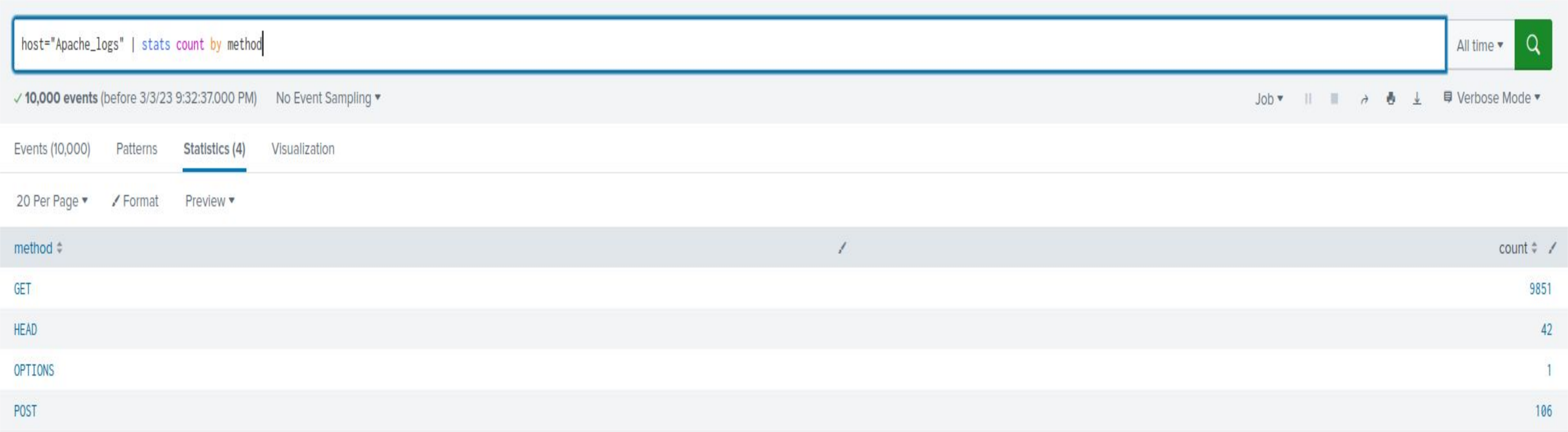
# Apache Logs

# Reports—Apache

| Report Name | Report Description |
|---|---|
| HTTP Methods | Displays list of HTTP method and their count |
| Top 10 Referrer Domains | Lists the top 10 referrer Domains and count |
| Count of each HTTP Response Code | HTTP code and their count |

# Report 1—Apache

## HTTP Methods



```
host="Apache_logs" | stats count by method
```

✓ **10,000 events** (before 3/3/23 9:32:37.000 PM)

No Event Sampling ▾

All time ▾

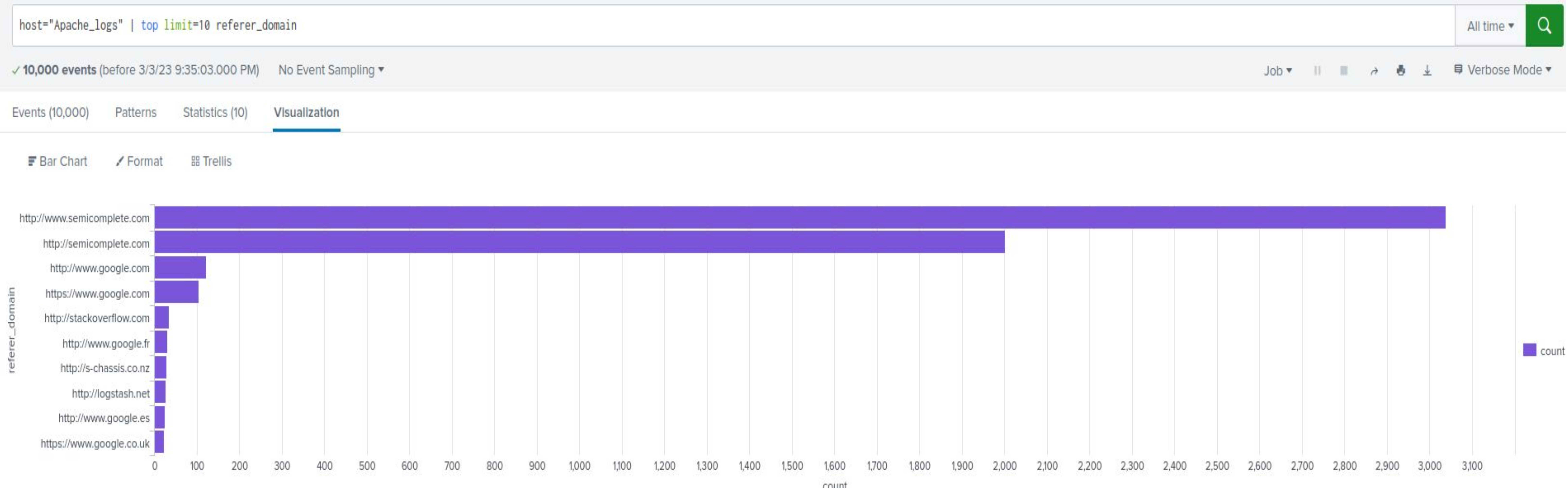
Verbose Mode ▾

20 Per Page ▾

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

# Report 2—Apache

## Top 10 Referrer Domains

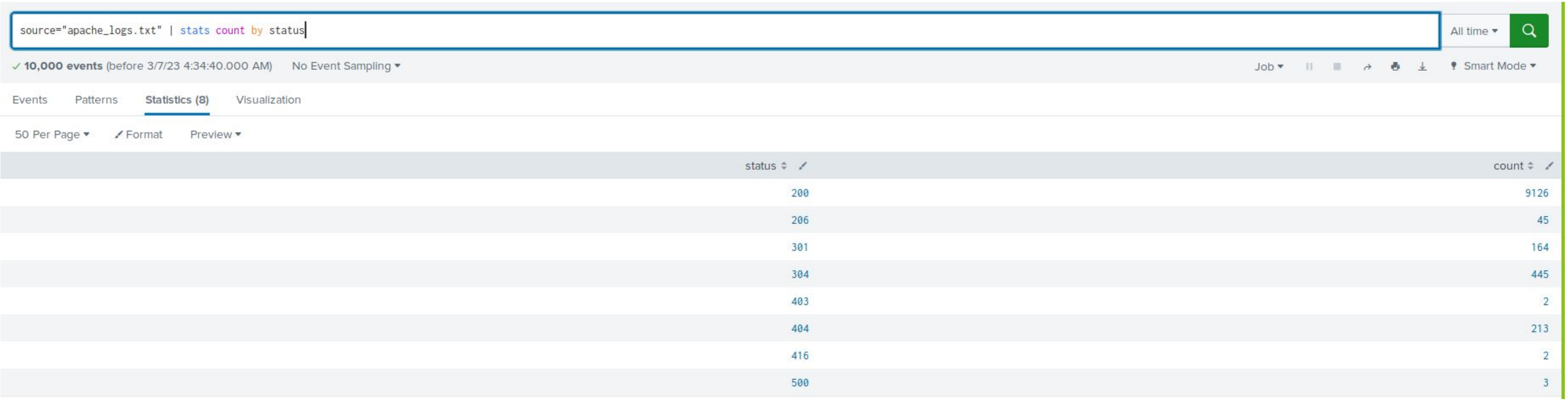


```
host="Apache_logs" | top limit=10 referer_domain
```

✓ 10,000 events (before 3/3/23 9:35:03.000 PM) No Event Sampling ▾

# Report 3—Apache

## Count of each HTTP Response Code



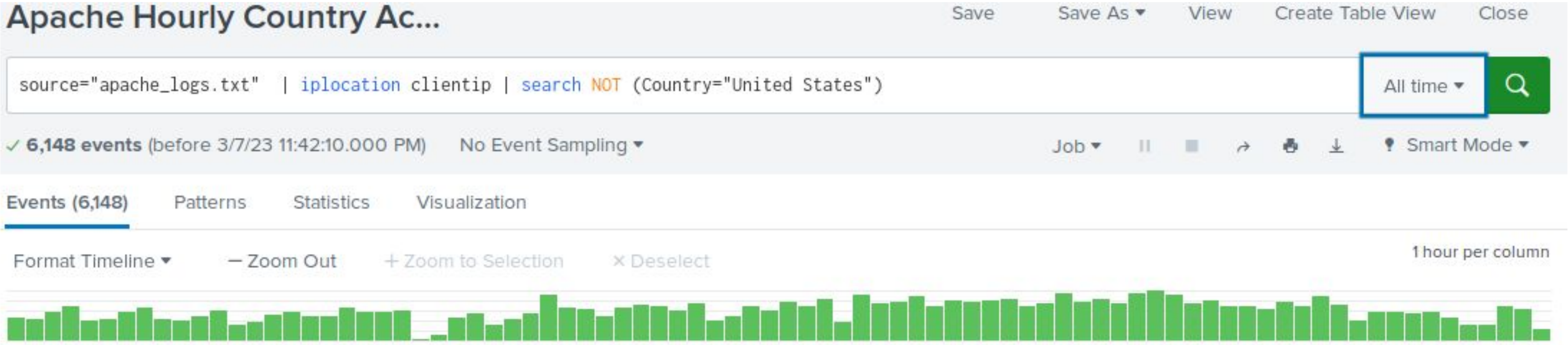
```
source="apache_logs.txt" | stats count by status
```

✓ 10,000 events (before 3/7/23 4:34:40.000 AM)

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

# Alert 1 — Apache

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Non-USA Activity | If the hourly activity from any nation other than the United States surpasses the cutoff, send out an alert. | 99 | 99 |



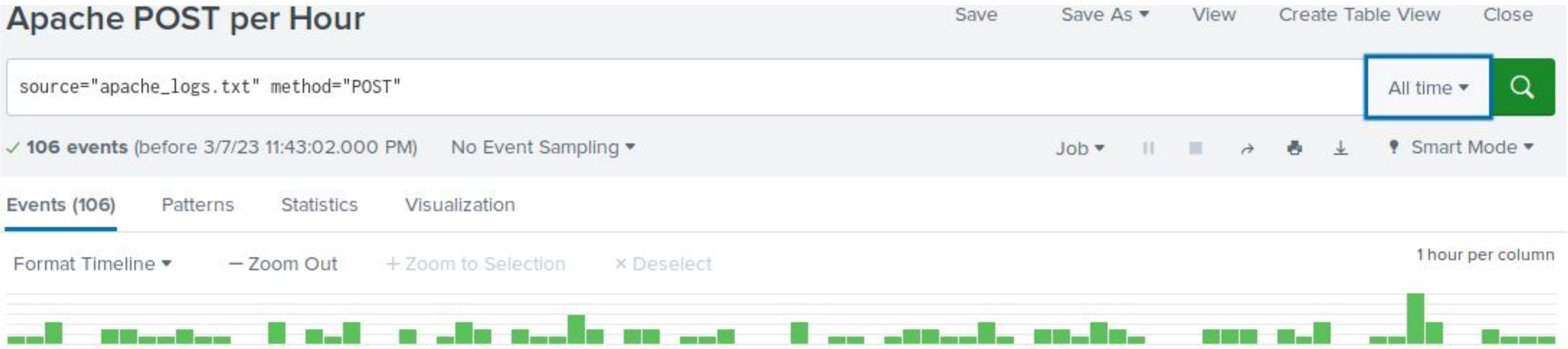
Apache Hourly Country Ac...

```
source="apache_logs.txt"  | iplocation clientip | search NOT (Country="United States")
```

✓ 6,148 events (before 3/7/23 11:42:10.000 PM)

# Alert 2 — Apache

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| HTTP POST Count | If the HTTP POST method hourly count goes over the limit, an alert is sent. | 4 | 4 |

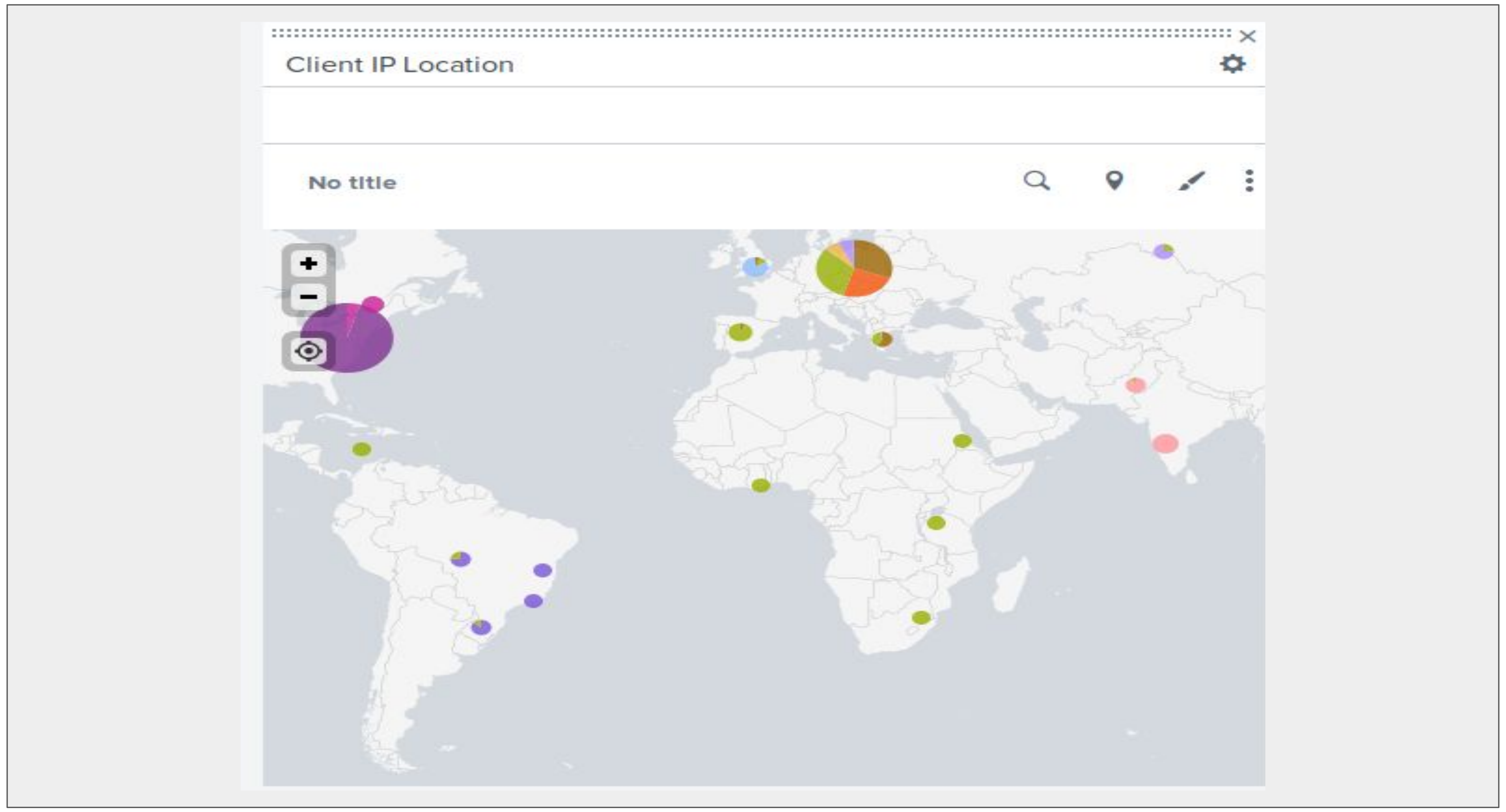


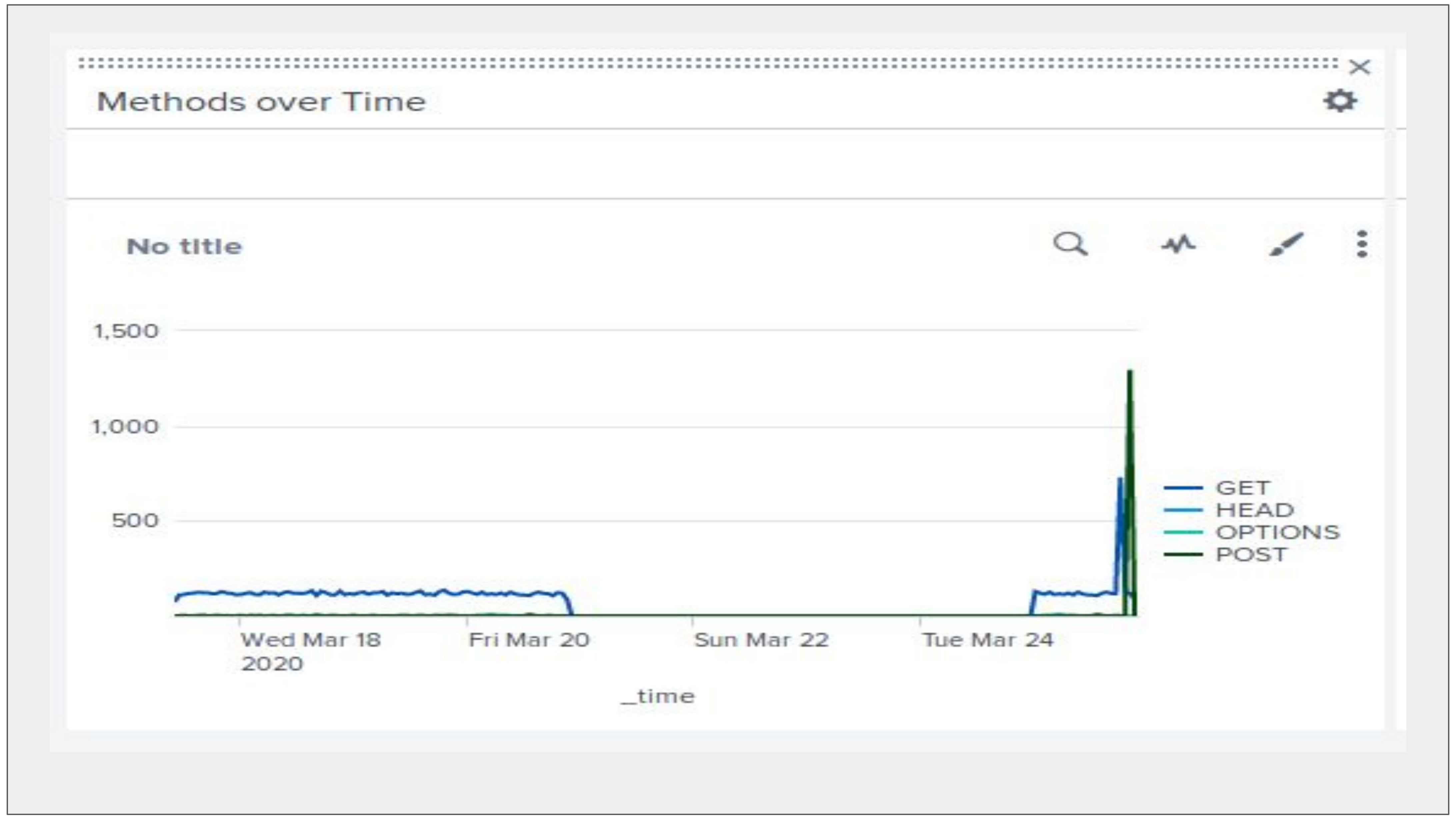
Apache POST per Hour

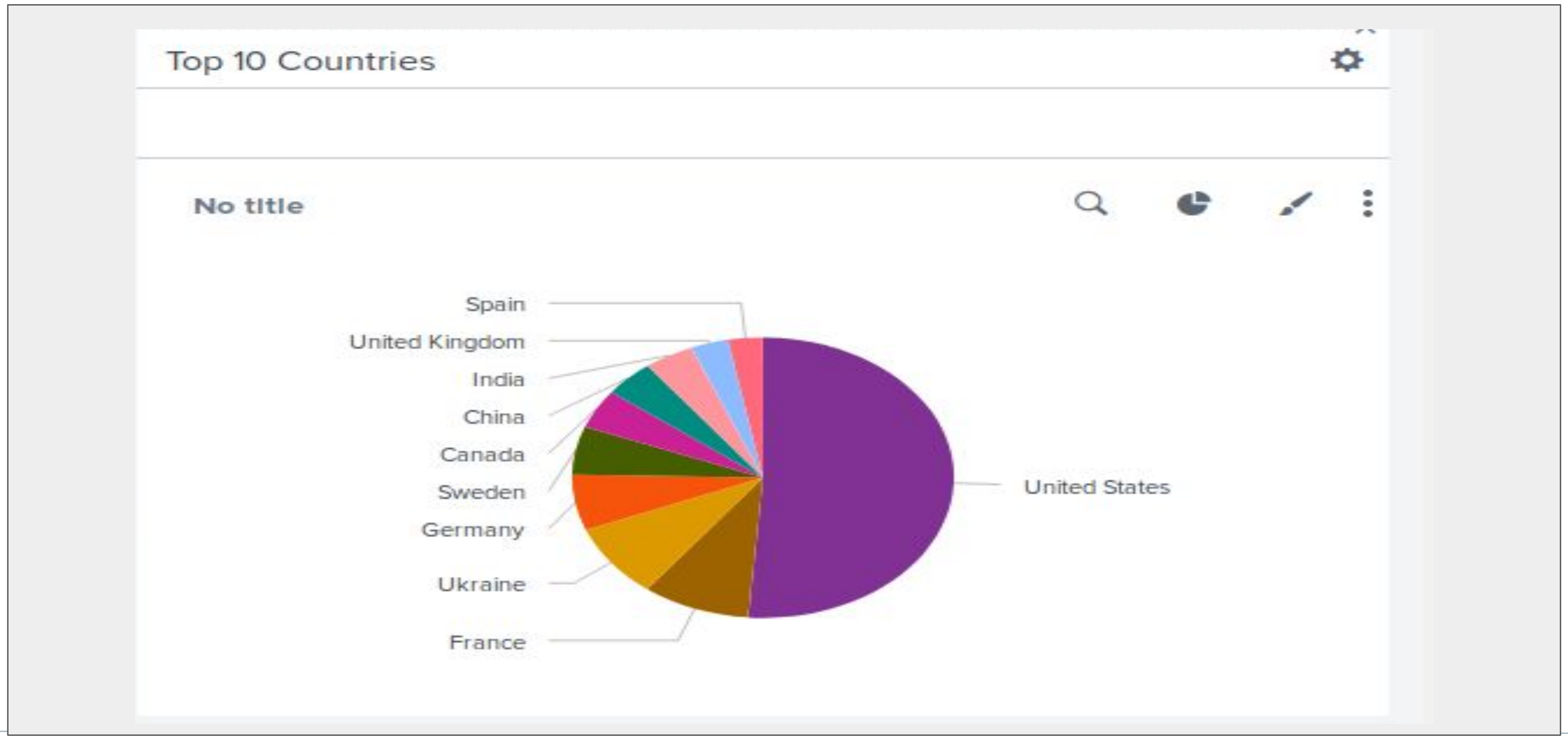
```
source="apache_logs.txt" method="POST"
```

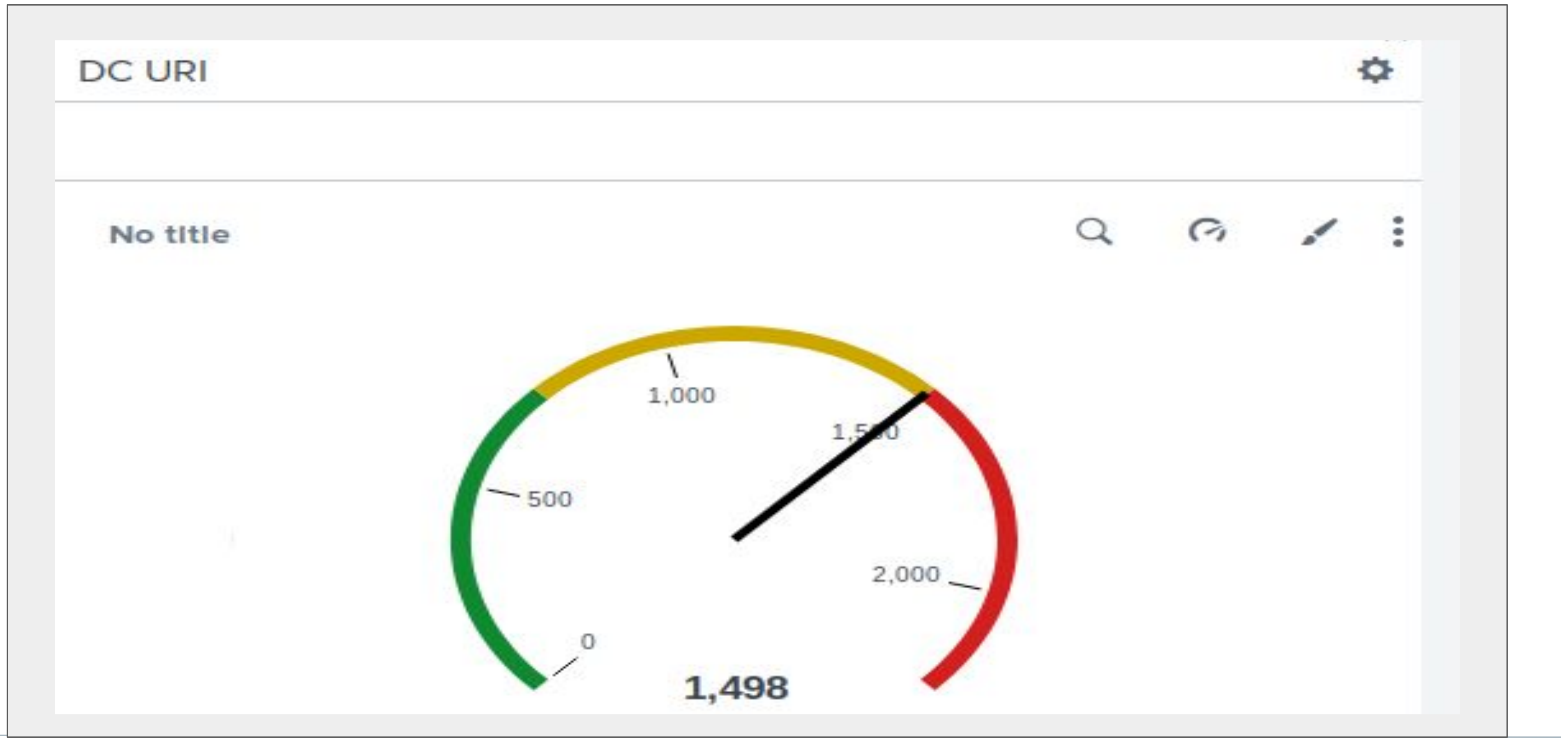
✓ 106 events (before 3/7/23 11:43:02.000 PM)

# Dashboards—Apache







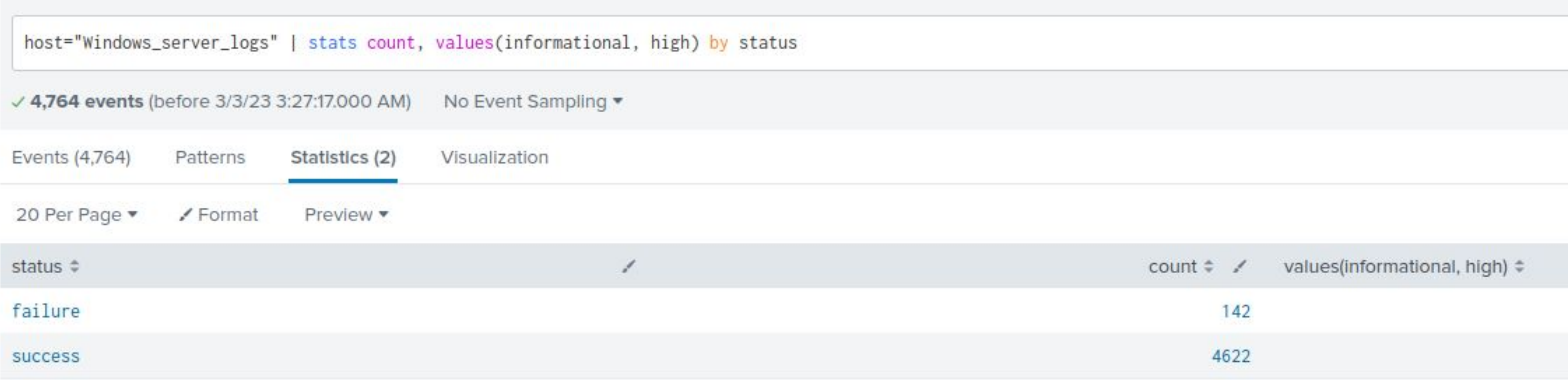


# Attack Analysis

# Attack Report Summary—Windows

- During the investigation of the log files, account deletions were noted along with the creation of accounts. Some accounts were also given special privileges, with data confirming successful logins.

**Windows Status Count (Initial)**

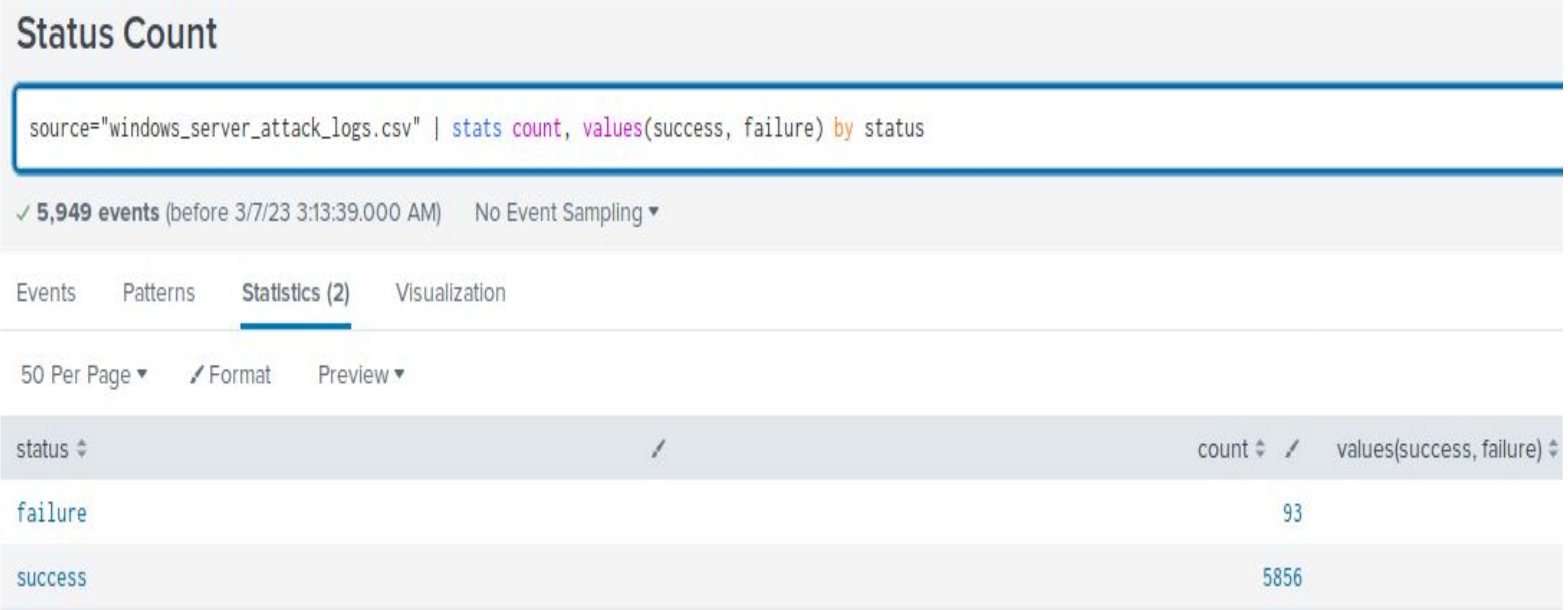


```
host="Windows_server_logs" | stats count, values(informational, high) by status
```

✓ **4,764 events** (before 3/3/23 3:27:17.000 AM) No Event Sampling ▾

| status | count | values(informational, high) |
|---|---|---|
| failure | 142 | |
| success | 4622 | |

**Windows Status Count (Attack)**



Status Count

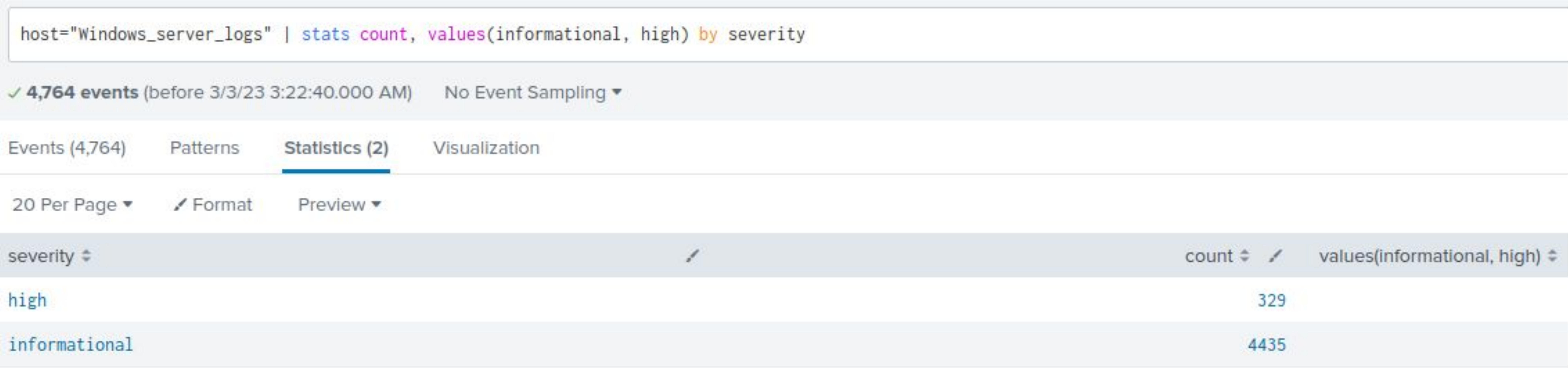
```
source="windows_server_attack_logs.csv" | stats count, values(success, failure) by status
```

✓ **5,949 events** (before 3/7/23 3:13:39.000 AM) No Event Sampling ▾

| status | count | values(success, failure) |
|---|---|---|
| failure | 93 | |
| success | 5856 | |

# Attack Report Summary—Windows

## Windows Severity Count (Initial)

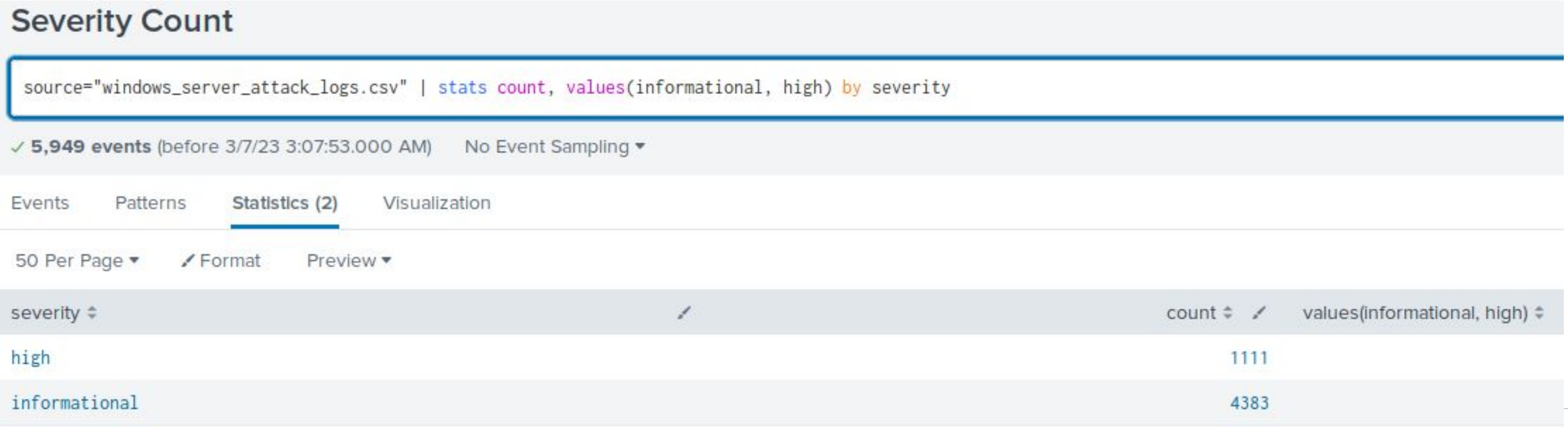


```
host="Windows_server_logs" | stats count, values(informational, high) by severity
```

✓ **4,764 events** (before 3/3/23 3:22:40.000 AM)

| severity | count | values(informational, high) |
|---|---|---|
| high | 329 | |
| informational | 4435 | |

## Windows Severity Count (Attack)



### Severity Count

```
source="windows_server_attack_logs.csv" | stats count, values(informational, high) by severity
```

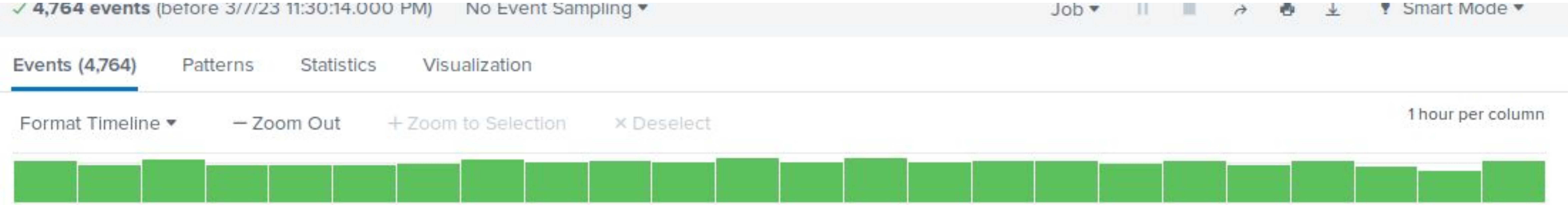
✓ **5,949 events** (before 3/7/23 3:07:53.000 AM)

| severity | count | values(informational, high) |
|---|---|---|
| high | 1111 | |
| informational | 4383 | |

# Attack Alert Summary—Windows

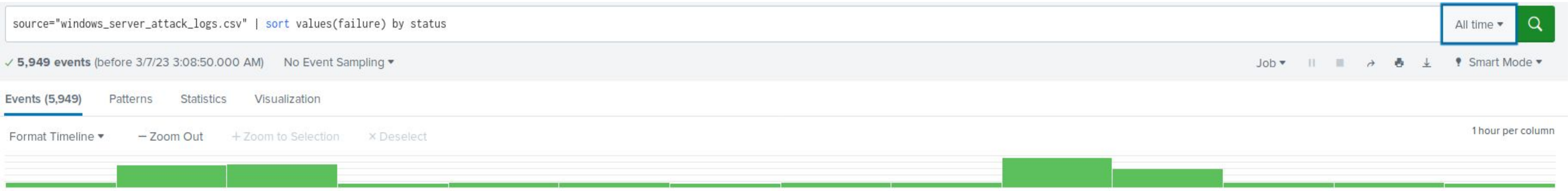
- During the attack, the team was alerted to suspicious activities on the network. This activity was in the form of failed login attempts. When the threshold was set at 199 failed activities per hour, there was an unusually high volume of failed activity. Four reports of suspicious activity far exceeded the threshold. They occured at 1am: 973, 2am: 1007, 9am: 1293, and at 10am: 784.

**Failed Windows Activity (Initial)**



✓ 4,764 events (before 3/7/23 11:30:14.000 PM)

**Failed Windows Activity (Attack)**

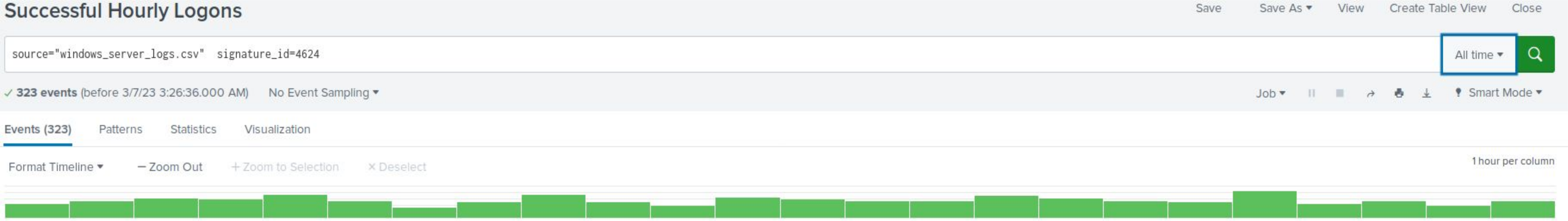


```
source="windows_server_attack_logs.csv" | sort values(failure) by status
```

✓ 5,949 events (before 3/7/23 3:08:50.000 AM)

# Attack Alert Summary—Windows

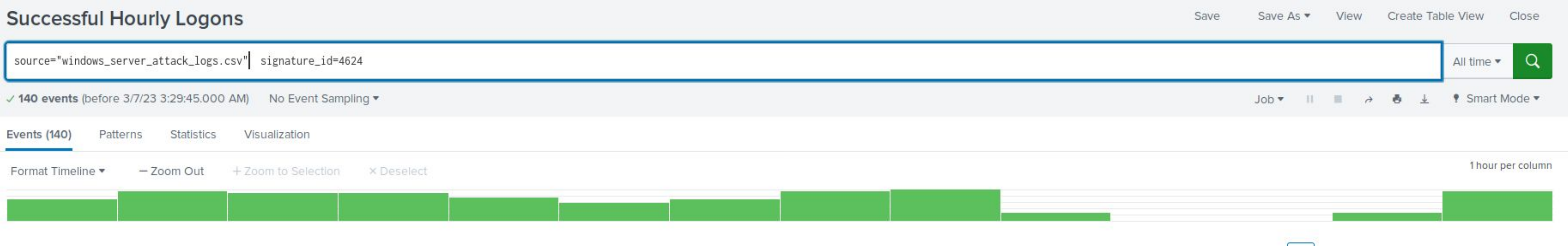
## Successful Hourly Logons (Initial)



```
source="windows_server_logs.csv"  signature_id=4624
```

✓ 323 events (before 3/7/23 3:26:36.000 AM)

## Successful Hourly Logons (Attack)



```
source="windows_server_attack_logs.csv"  signature_id=4624
```

✓ 140 events (before 3/7/23 3:29:45.000 AM)

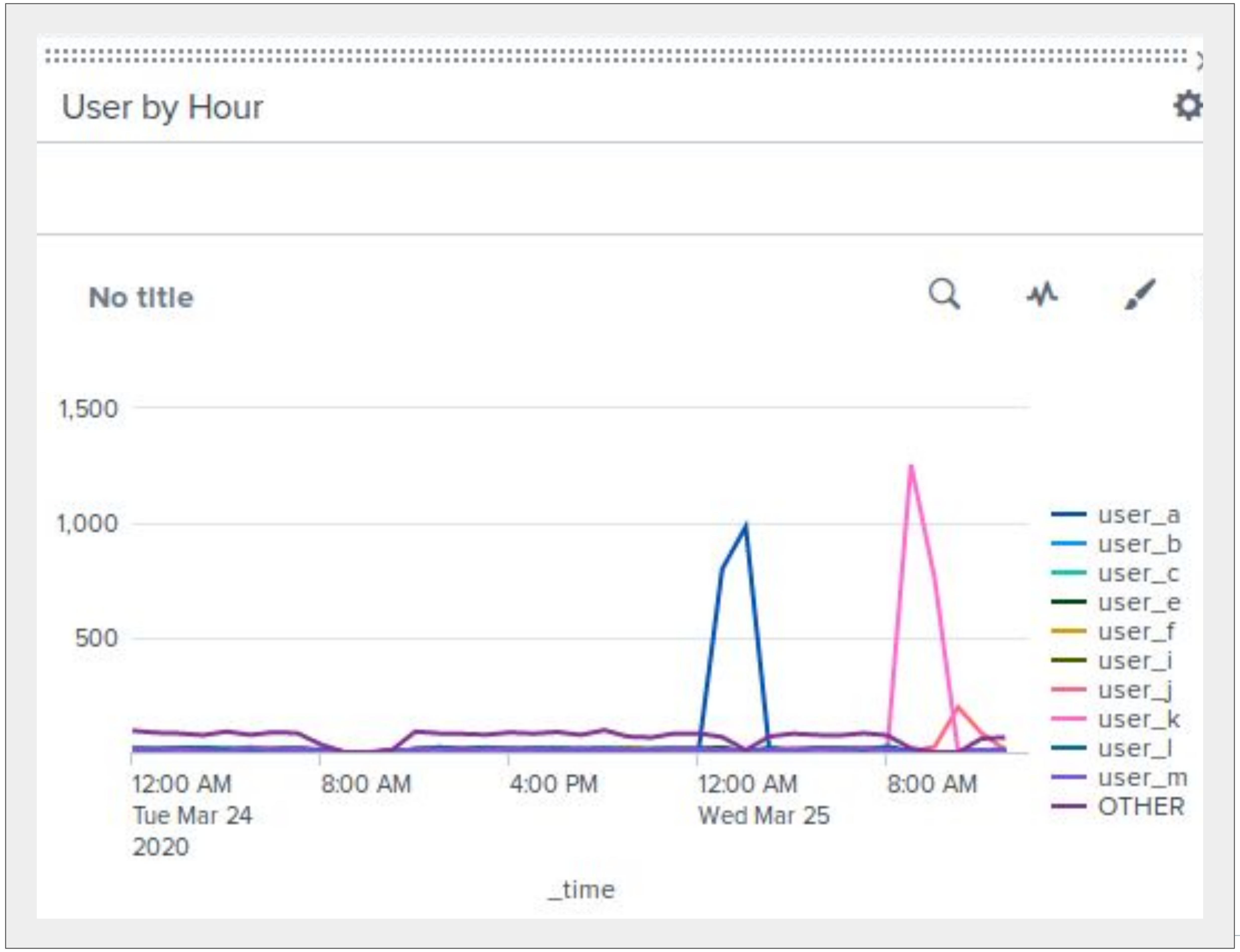
# Attack Alert Summary—Windows

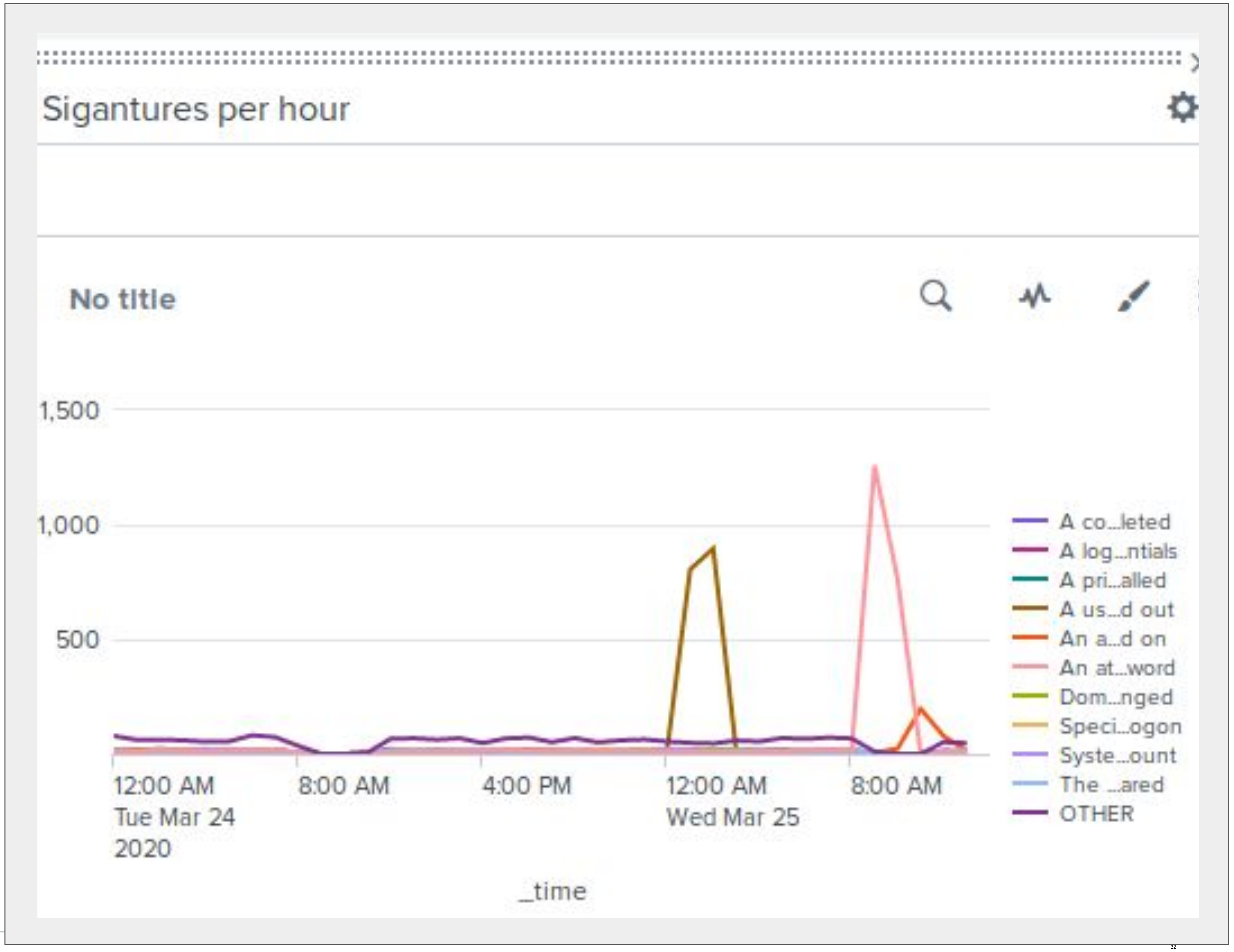
## User Accounts Deleted

Sigantures per hour
1,500
1,000
500
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
12:00 AM Wed Mar 25
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
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 removed from an account
The audit log was cleared
OTHER

# Attack Dashboard Summary—Windows

- The dashboards provided a wealth of information. On Wednesday, March 25th, there were two significant spikes. User accounts were locked out, password reset attempts were made, and successful logins were made. We were able to identify the time and date of the attack(March 15th between 01:00 am and 02:00 am)

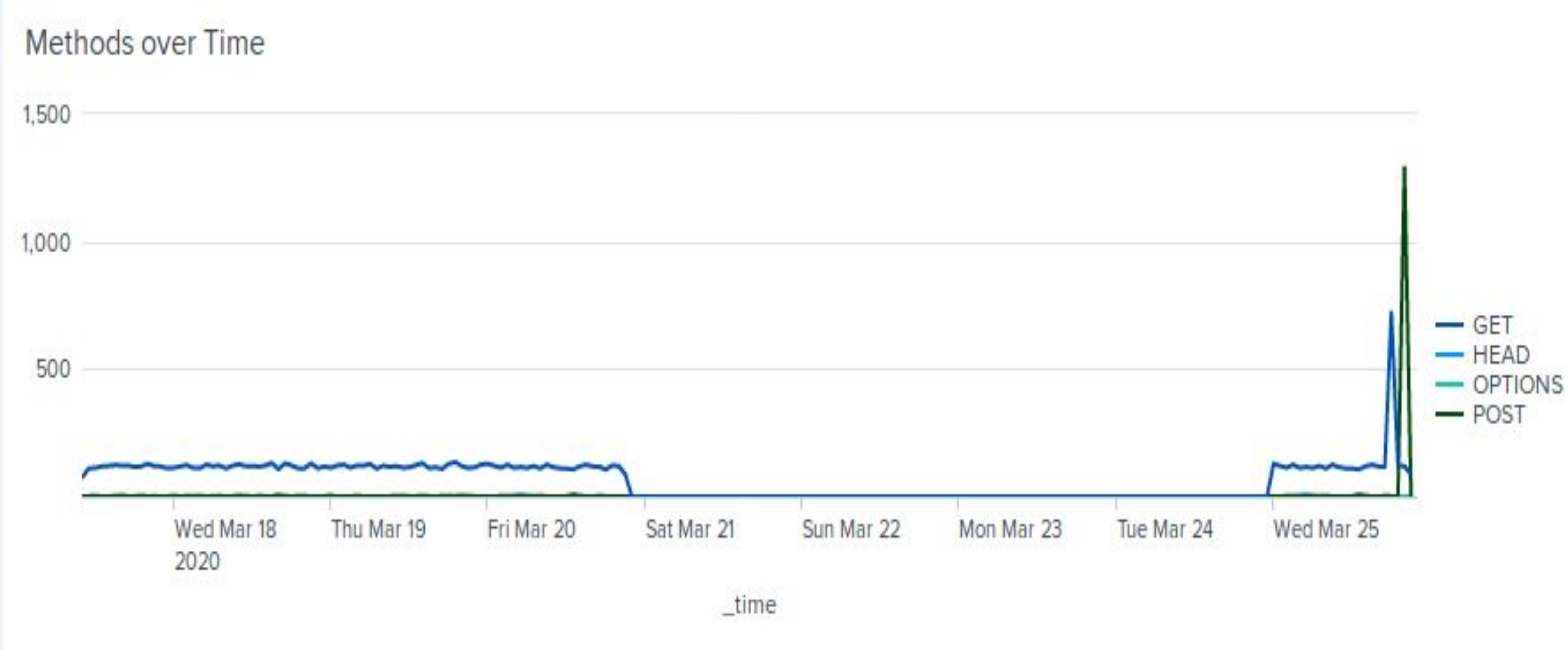




# Attack Report Summary—Apache

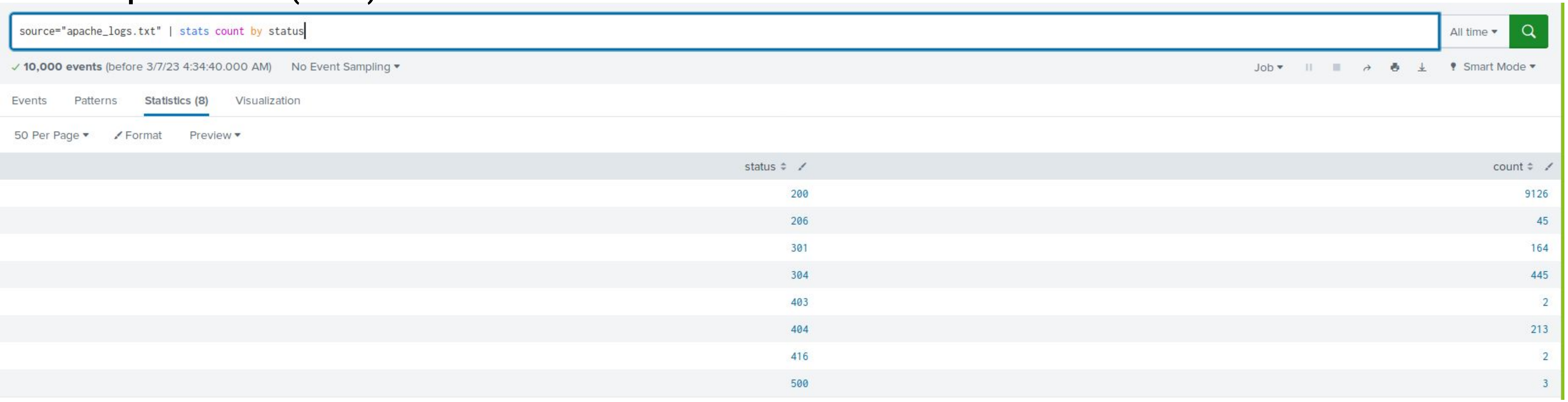
- We noticed a change in the HTTP methods GET and POST during the first attack. Both requests had high spike counts.The amount of response code 200 decreased, while the amount of response code 404 increased. The number of referrer domains is lower than in the original Apache log file.

**HTTP Methods During Attack**



# Attack Report Summary—Apache

## HTTP Response Codes (Initial)

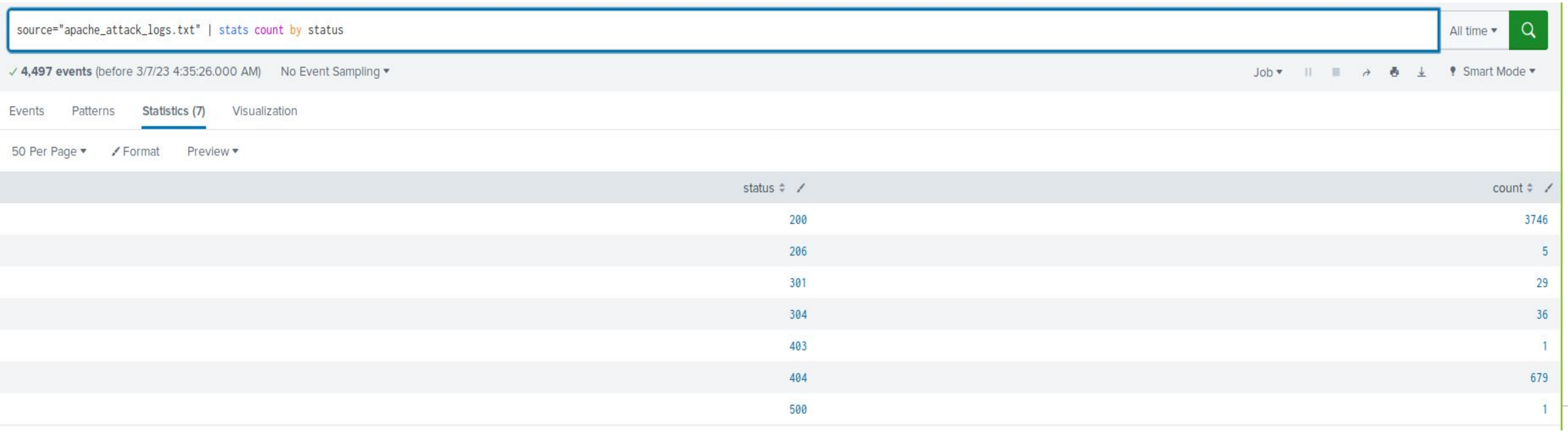


```
source="apache_logs.txt" | stats count by status
```

✓ 10,000 events (before 3/7/23 4:34:40.000 AM)

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

## Increase in HTTP 404 Response Codes



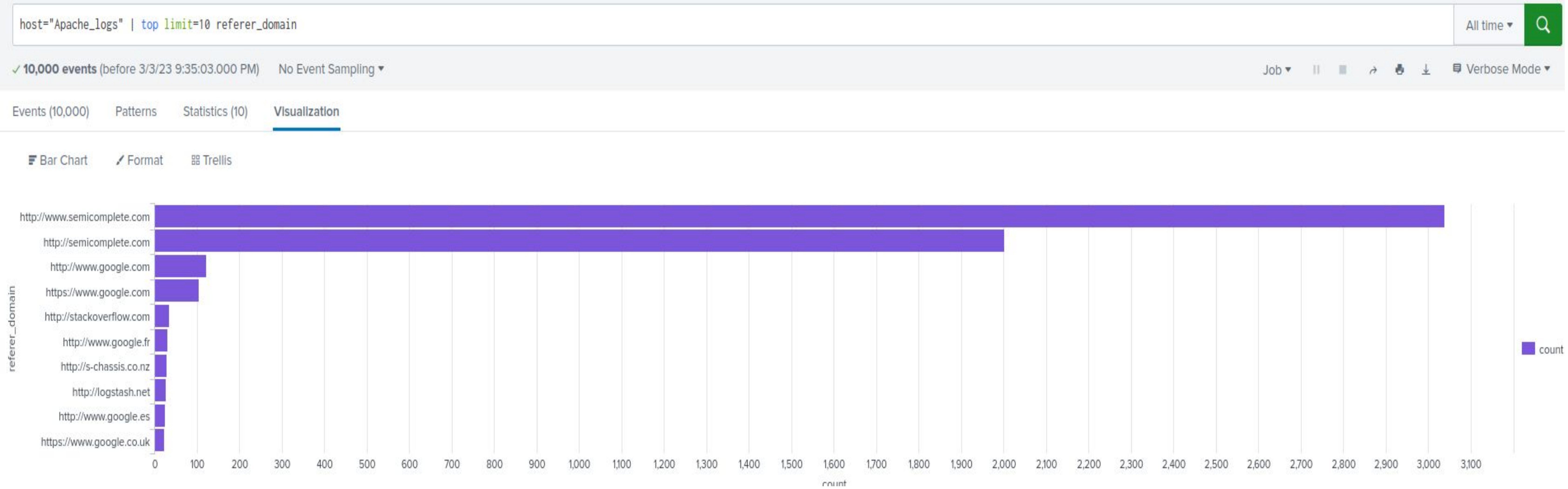
```
source="apache_attack_logs.txt" | stats count by status
```

✓ 4,497 events (before 3/7/23 4:35:26.000 AM)

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

# Attack Report Summary—Apache

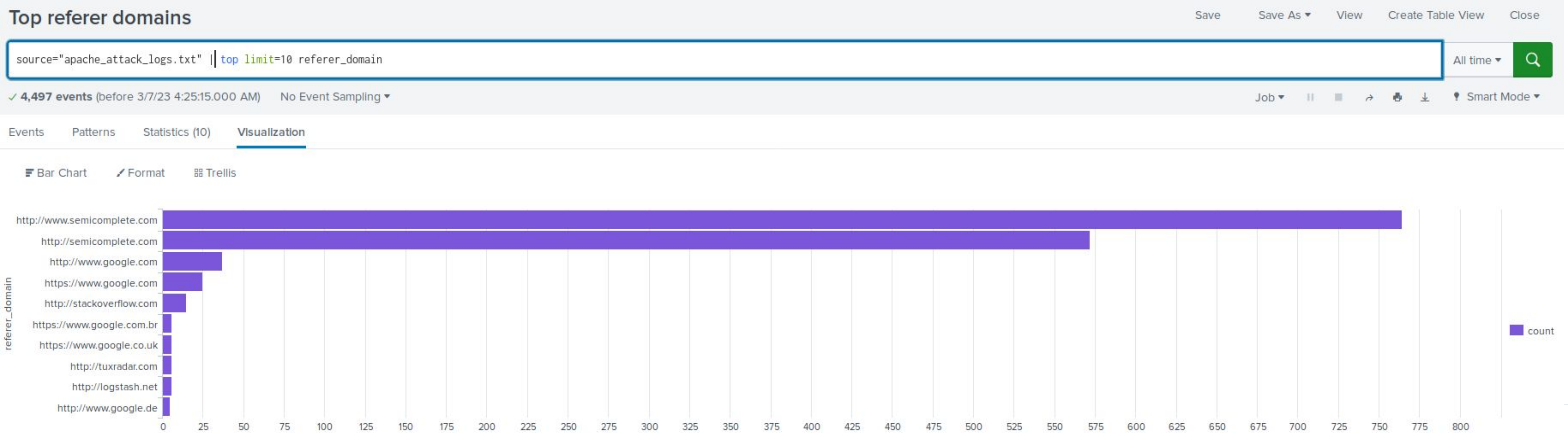
## Referrer Domains (Initial)



```
host="Apache_logs" | top limit=10 referer_domain
```

✓ 10,000 events (before 3/3/23 9:35:03.000 PM) No Event Sampling ▾

## Decrease in Referrer Domains



Top referer domains

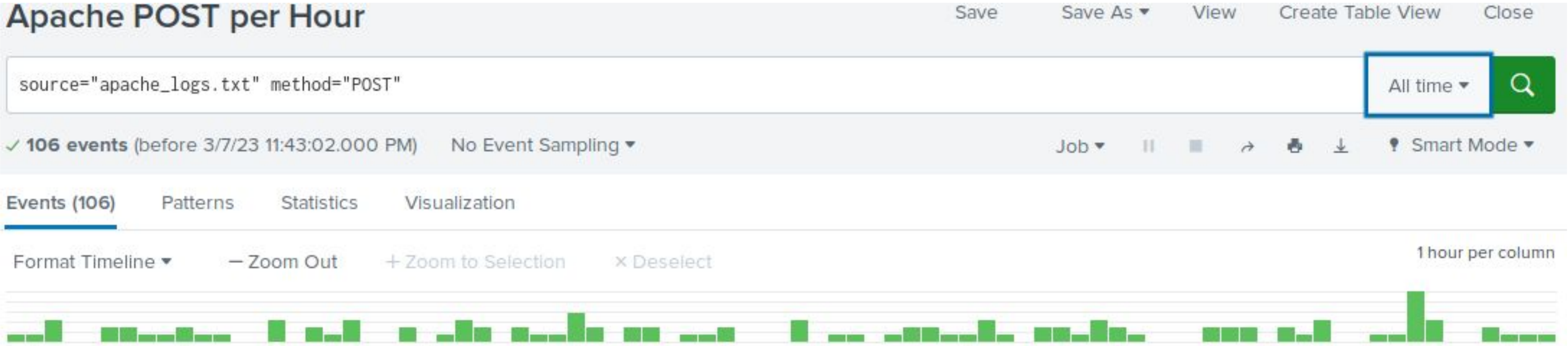
```
source="apache_attack_logs.txt" | top limit=10 referer_domain
```

✓ 4,497 events (before 3/7/23 4:25:15.000 AM) No Event Sampling ▾

# Attack Alert Summary—Apache

- On Wednesday, March 25th, between 08:00 pm and 09:00 pm, 939 international events were observed. A large number of HTTP POST requests were made to the Apache server and it peaked at 1,296. After review, we would adjust our threshold  between 7 and 10.

**POST Count (Initial)**

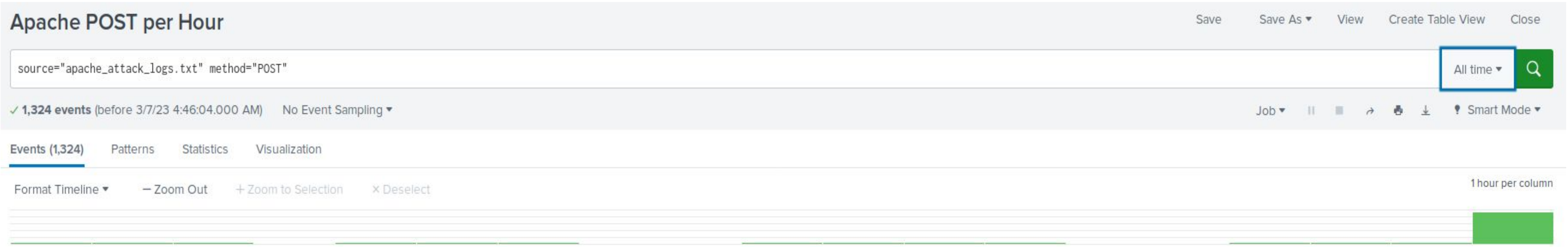


Apache POST per Hour

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

✓ 106 events (before 3/7/23 11:43:02.000 PM) No Event Sampling

**POST During Attack**



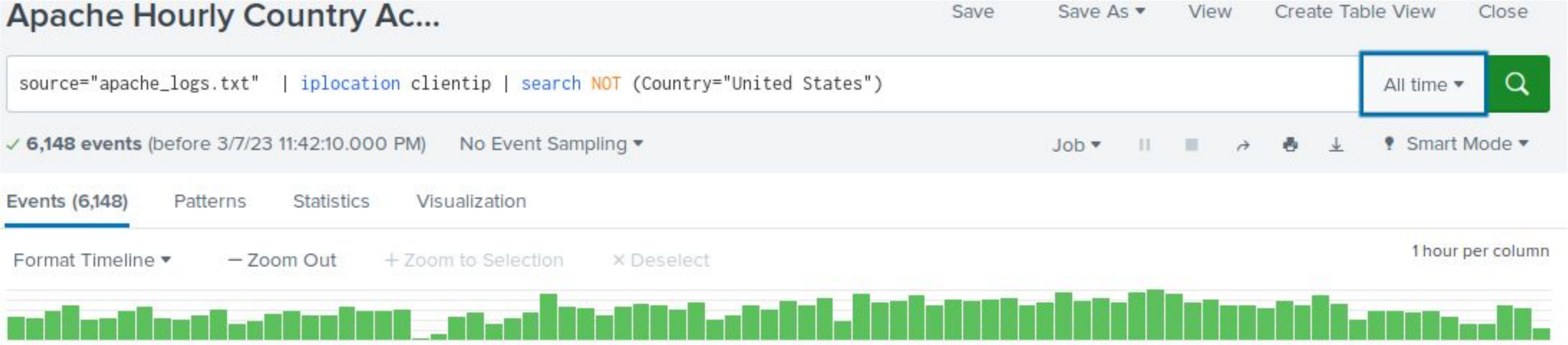
Apache POST per Hour

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

✓ 1,324 events (before 3/7/23 4:46:04.000 AM) No Event Sampling

# Attack Alert Summary—Apache

## International Activity (Initial)

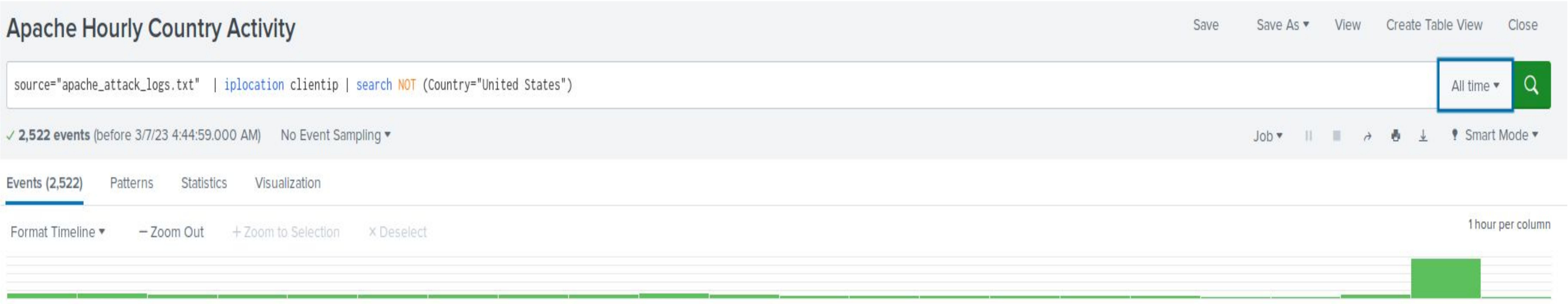


Apache Hourly Country Ac...

```
source="apache_logs.txt"  | iplocation clientip | search NOT (Country="United States")
```

✓ 6,148 events (before 3/7/23 11:42:10.000 PM)

## International Activity During Attack



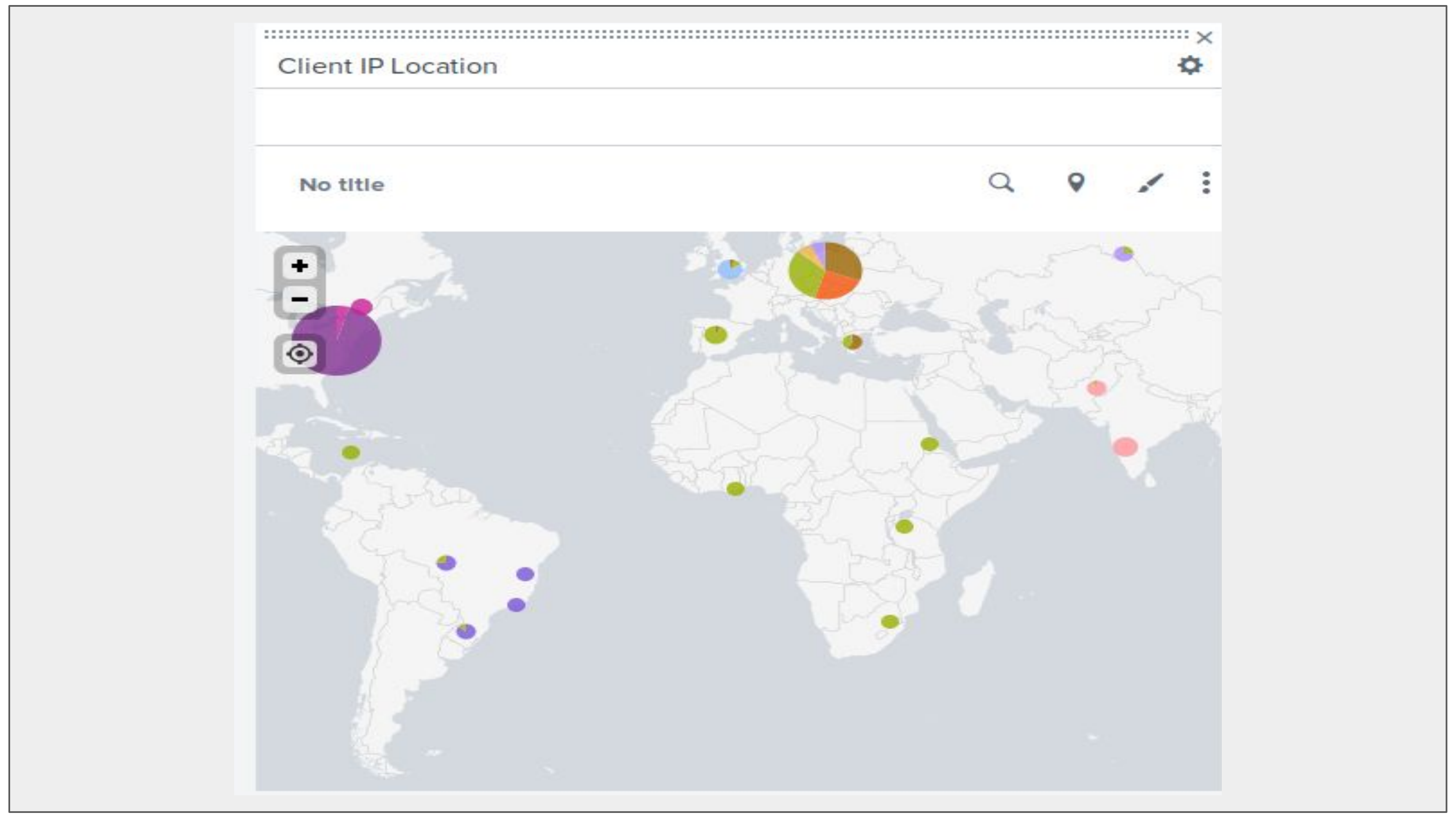
Apache Hourly Country Activity

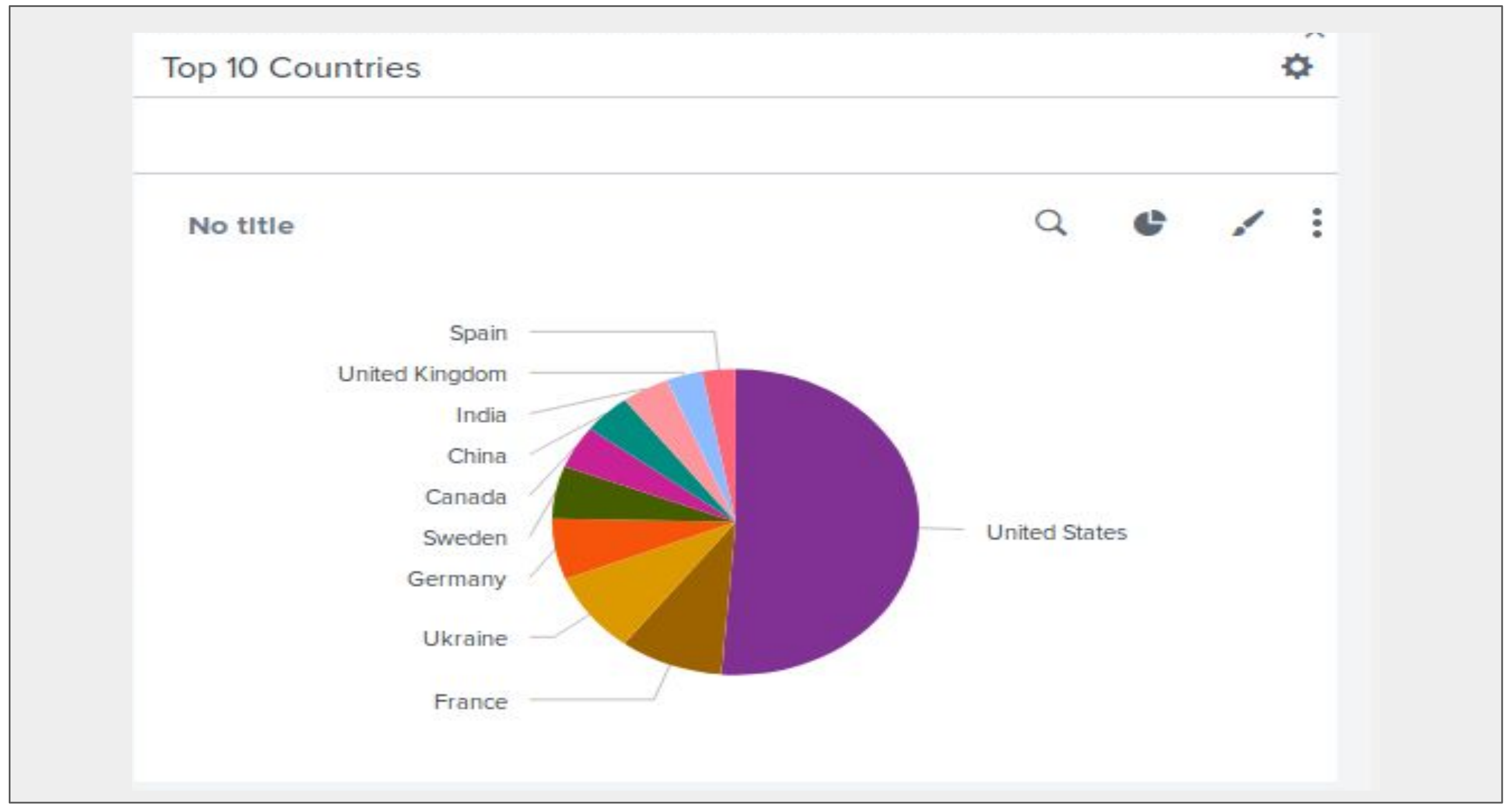
```
source="apache_attack_logs.txt"  | iplocation clientip | search NOT (Country="United States")
```

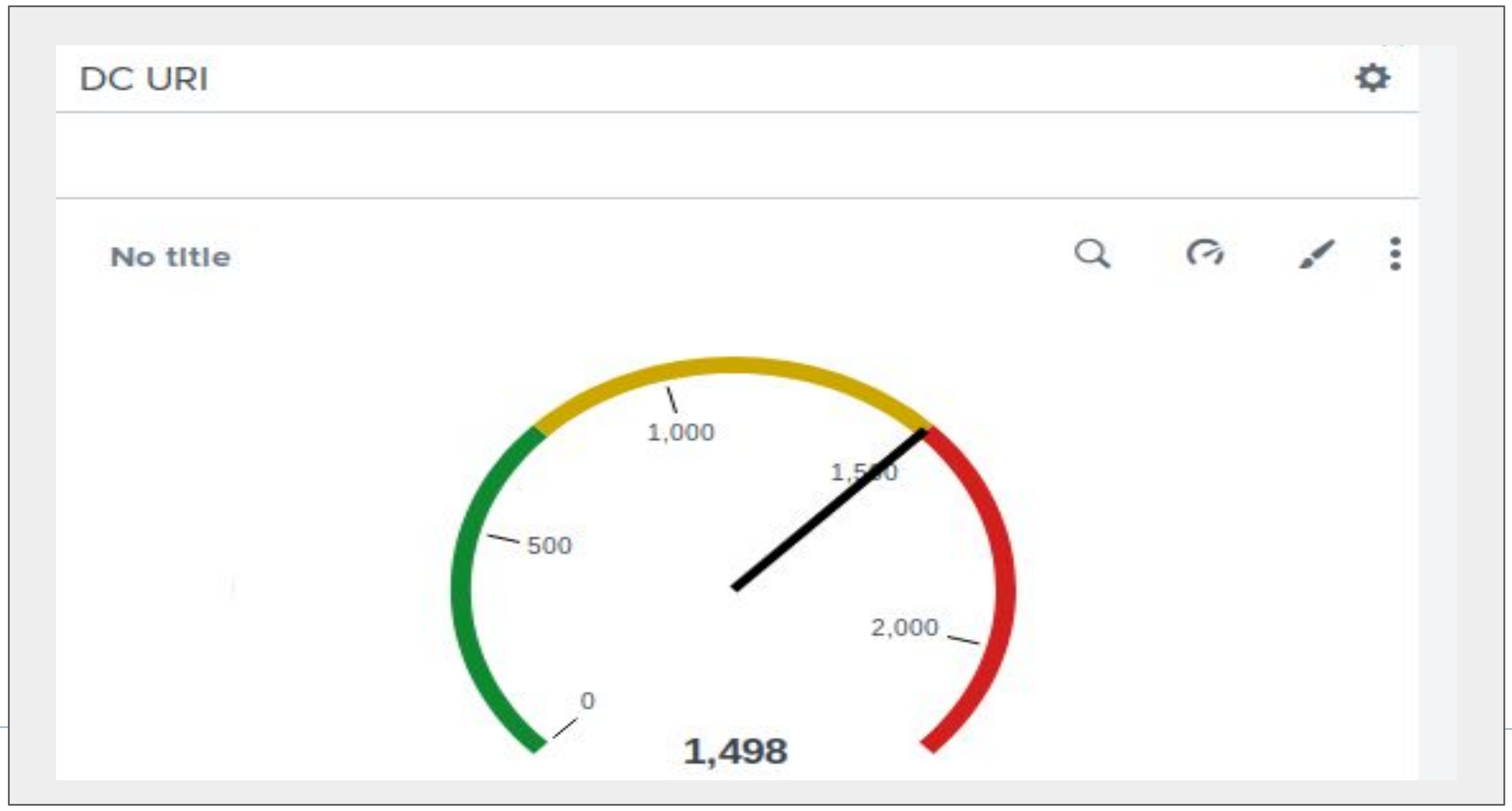
✓ 2,522 events (before 3/7/23 4:44:59.000 AM)

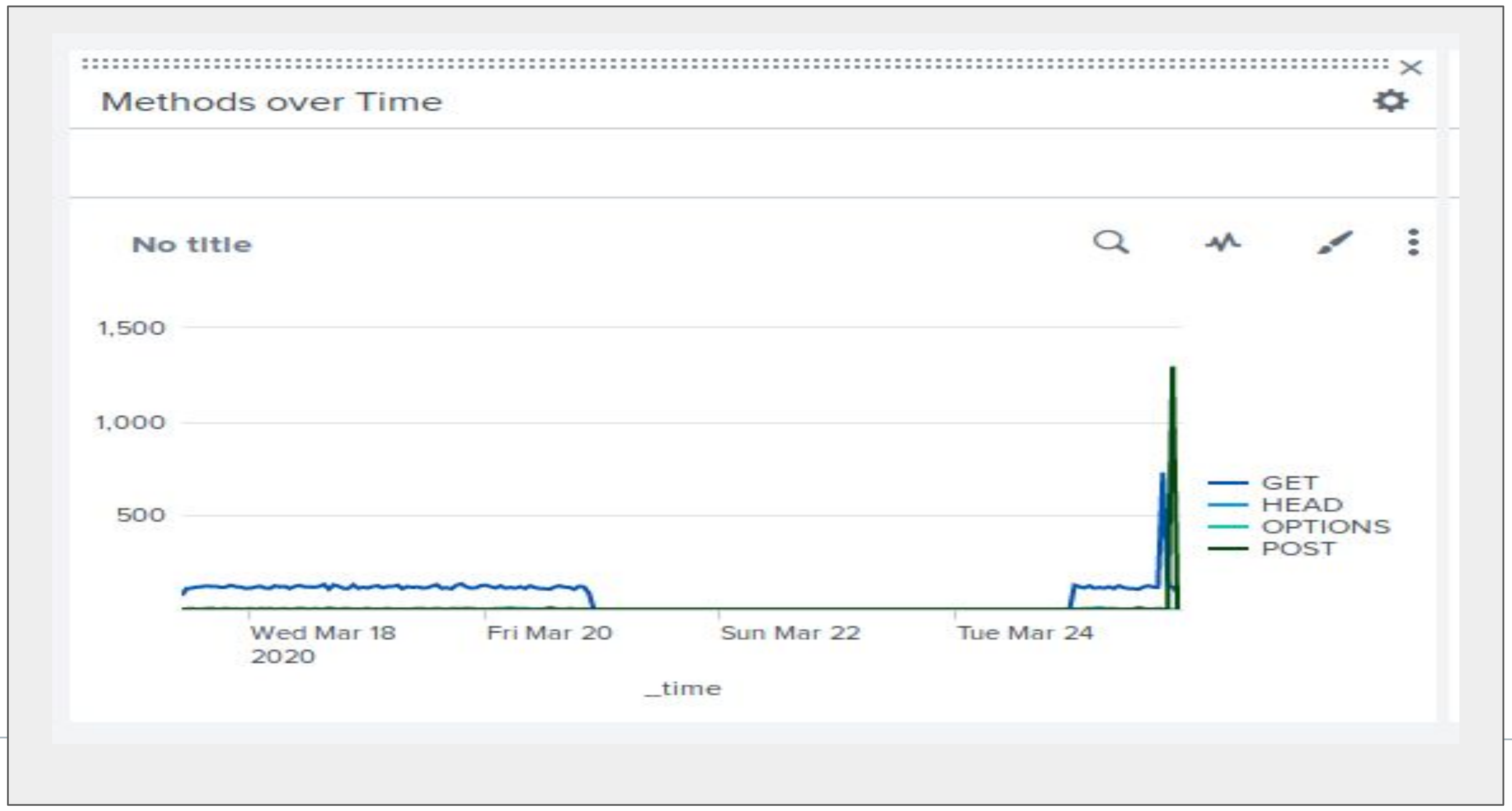
# Attack Dashboard Summary—Apache

- According to our Time Chart of HTTP Methods both GET and POST requests began to spike between 06:00 pm and 08:00 pm. Most of the activity originated in Ukraine, according to the produced Cluster Map. Kharkiv and Kyiv were the specific cities identified in the attack with Kharkiv having an event count of 433 and Kyiv with an event count of 439.









# Summary and Future Mitigations

# Project 3 Summary

- **Overall Findings**
  - Our conclusion was that VSI had numerous attacks on its Windows and Apache servers on March 25th. The majority of these attacks appeared to be a brute force attack against the Windows machine and a DoS attack against the Apache machine.

- **Mitigation Strategies**
  - To stop upcoming attacks, lock users after a particular number of login attempts.
  - Using two-factor authentication as your first line of security will help avoid Brute Force attacks.
  - Create a whitelist for POST requests to prevent unwanted requests.