

# **Defensive Security Project**

## **by: FATMA KAYGISIZ**

# Table of Contents

---

This document contains the following resources:

01

**Monitoring  
Environment**

02

**Attack Analysis**

03

**Project Summary  
& Future  
Mitigations**

# Monitoring Environment

# Scenario

---

- We played the role of and SOC analyst 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 businesses.
- As an SOC analyst, we are tasked with using Splunk to monitor against potential attacks on your systems and applications.
- The VSI products that we have been tasks with monitoring include:
  - \* An administrative webpage: <https://vsi-corporation.azurewebsites.net/>
  - \* An Apache web server, which hosts this webpage
  - \* A Windows operating system, which runs many of VSI, back-end operations.

# Logs Analyzed

---

1

## Windows Logs

This server houses the intellectual property related to VSI's next-generation virtual reality programs.

- Signature
- User
- Severity
- Success and Failure activity

2

## Apache Logs

Logs for VSI's main public-facing website, [vsi-company.com](http://vsi-company.com).

- HTTP Methods
- Referrer Domains
- HTTP Response Codes
- International Activity

# Windows Logs

# Reports—Windows

---

Designed the following reports:

Report Name	Report Description
Signature ID's Report	This will allow VSI to view reports that show the ID number associated with the specific signature for Windows activity.
Severity Levels Report	This will allow VSI to quickly understand the severity levels of the Windows being viewed.
Windows Activity Success and Failure	This will show VSI if there is a suspicious level of failed activities on their server.



# Images of Reports—Windows





# Images of Reports—Windows

## Windows Activity Success and Failure

Edit ▼

More Info ▼

Add to Dashboard ▼

This will show VSI if there is a suspicious level of failed activities on their server.

All time ▼

✓ 4,764 events (before 10/28/24 7:40:57.000 PM)

Job ▼

||

■

↺

↻

↗

⬇

2 results    20 per page ▼

status ↕	total ↕	percentage ↕
failure	142	2.98
success	4622	97.02

# Images of Reports–Windows

Signature ID's Report

Edit

More Info

Add to Dashboard

This report will allow VSI to view reports that show the ID number associated with the specific signature for Windows activity.

All time

✓ 15 events (before 10/28/24 7:38:16.000 PM)

Job

||

■

↺

↻

↷

⌵

15 results

20 per page

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
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718

# Alerts—Windows

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Login Alert	Threshold of failed Windows Activity Reach	Lower:2 Upper: 10	15

**JUSTIFICATION:** The average amount of failed Windows activity is among 2-10 and our baseline yet never got close to 15.Failures exceeding 15 would certainly indicate suspicious activity.

# Alerts—Windows

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Login Alert	Threshold of Successful Logged on by Account Was Successfully Logged On	Lower: 8 Upper: 21	18

**JUSTIFICATION:** The number of Successful Logins is among 8-21 and our baseline yet never got close to 32. Successful exceeding 18 would certainly indicate suspicious activity.



# Alerts—Windows

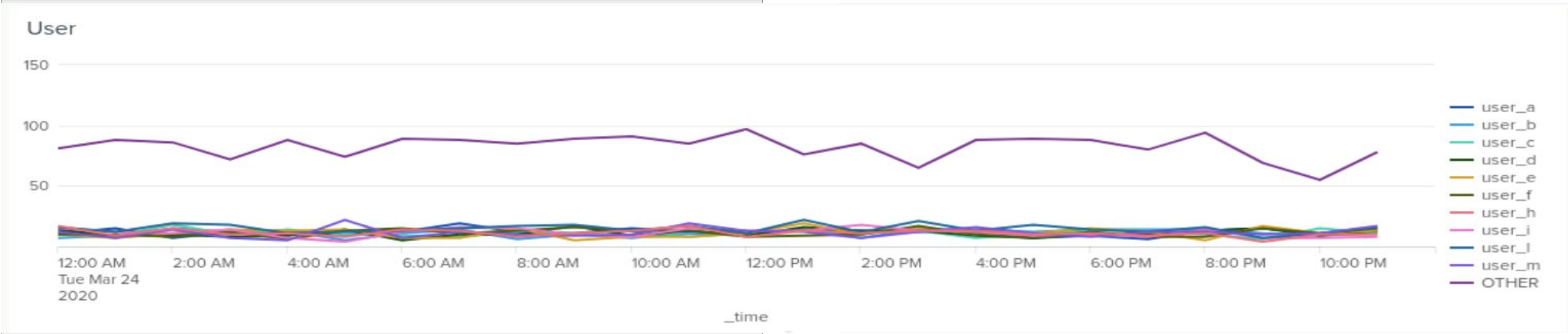
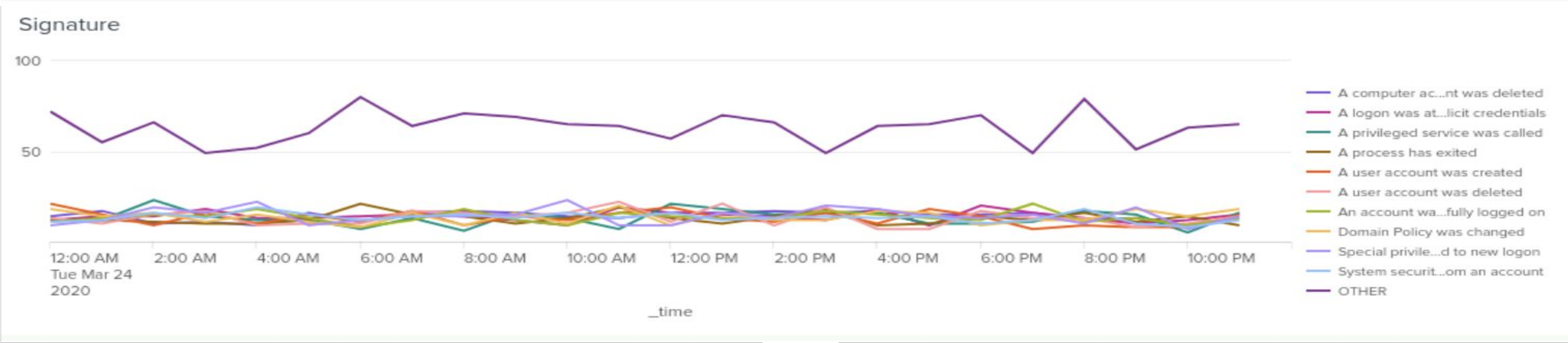
---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deleted Alert	Threshold of Deleted User Accounts	Lower: 7 Upper: 22	33

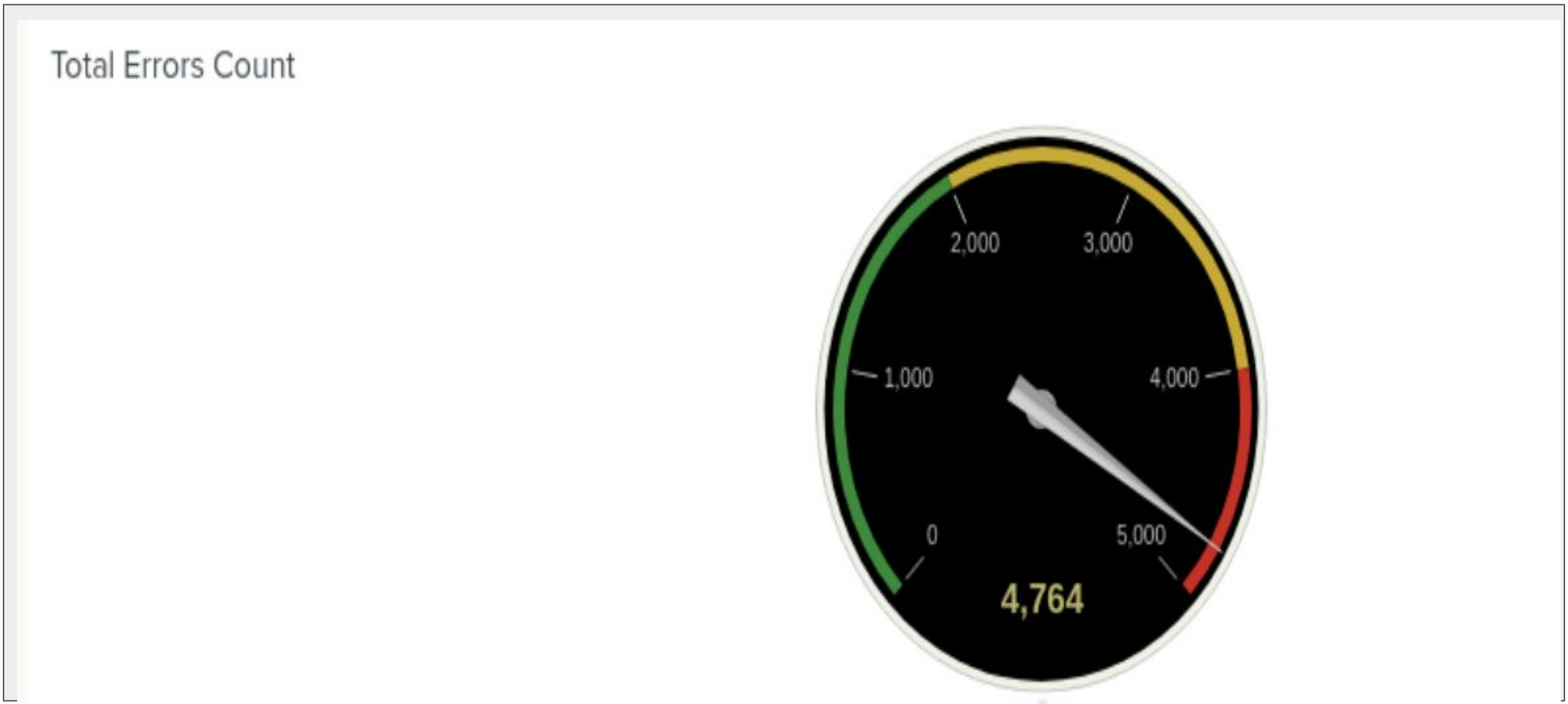
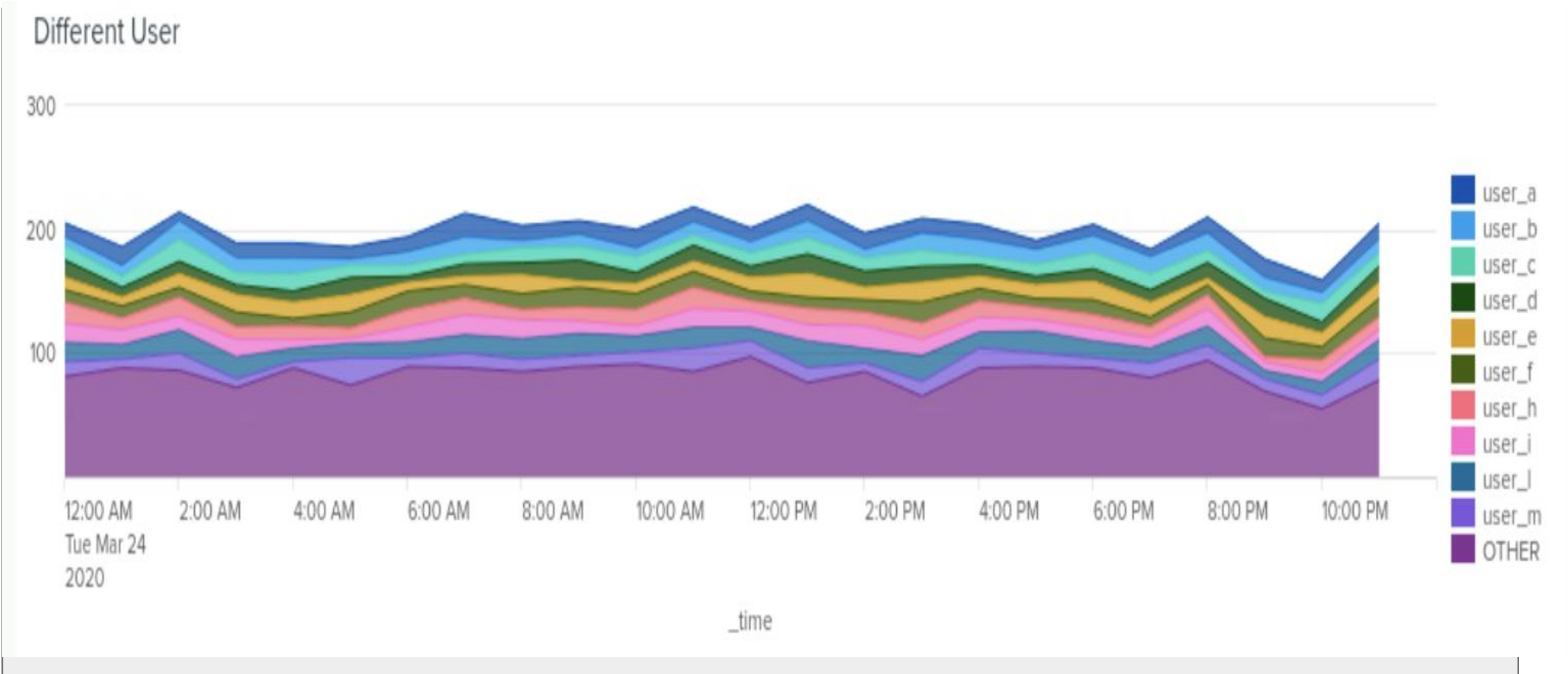
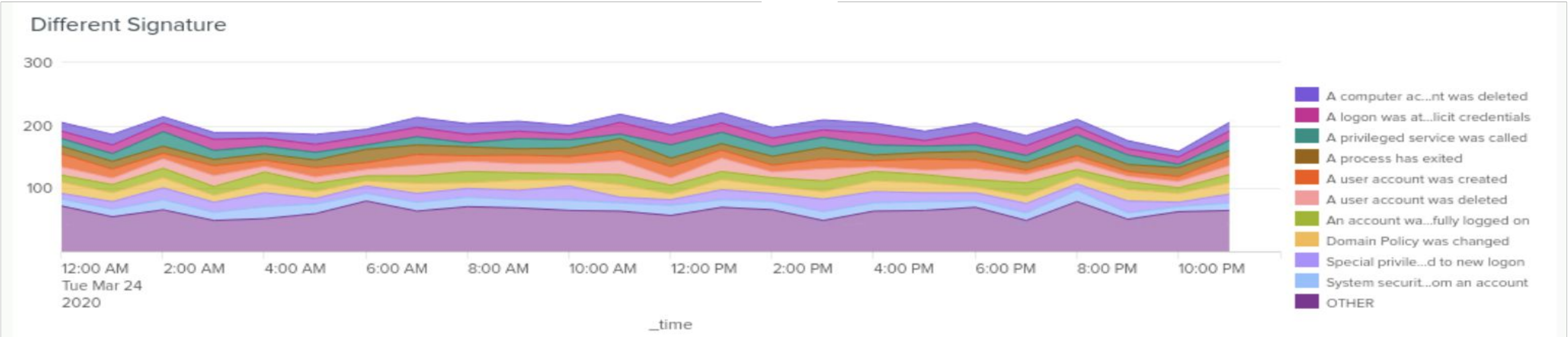
**JUSTIFICATION:** A baseline of 7-22 seemed on par with a "normal" hour. Exceeding 33 would raise suspicion levels and indicate a problem.

# Dashboards—Windows





# Dashboards—Windows



# Apache Logs

# Reports—Apache

---

Designed the following reports:

Report Name	Report Description
HTTP Methods Activity Report	This report will provide insight into the type of HTTP activity being requested against VSI's web server.
Top Referring Domain Report	This report that shows the top 10 domains that refer to VSI's website.
HTTP Response Codes Reports	This report that shows the count of each HTTP response code.



# Images of Reports—Apache

## HTTP Methods Activity Report

Edit

More Info

Add to Dashboard

All time

✓ 10,000 events (1/28/20 1:00:48.000 PM to 10/28/24 8:20:25.000 PM)

Job

||

■

↺

↻

↗

🖨

⬇

4 results

20 per page

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

# Images of Reports–Apache

HTTP Response Codes Report

All time ▼

✓ 10,000 events (before 10/28/24 8:25:23.000 PM)

Edit ▼

More Info ▼

Add to Dashboard ▼

Job ▼

||

■

↺

↻

↗

🖨

⬇

8 results

20 per page ▼

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

# Images of Reports–Apache

Top Referring Domains Report			Edit ▾	More Info ▾	Add to Dashboard ▾
All time ▾					
✓ 10,000 events (before 10/28/24 8:22:38.000 PM)			Job ▾    ■ ↺ ↻ ⏏ ⬇		
20 results    20 per page ▾					
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			
http://www.s-chassis.co.nz	22	0.371183			
http://www.google.de	18	0.303695			
https://www.google.fr	15	0.253079			
http://www.google.co.uk	14	0.236207			
https://www.google.de	13	0.219335			
https://www.google.co.in	13	0.219335			
http://www.google.co.in	12	0.202463			
http://tuxradar.com	12	0.202463			
http://r.duckduckgo.com	11	0.185591			
http://kufli.blogspot.com	10	0.168719			



# Alerts—Apache

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Outside US IP Activity	Alert if the hourly activity from any country besides the United States exceeds the threshold.	Lower: 1 Upper: 120	150

**JUSTIFICATION:** 120 events in a hour seemed standard in the logs, yet exceeding 150 seemed unlikely on a normal day. Seeing any number of events greater than the threshold would indicate issues.

# Alerts—Apache

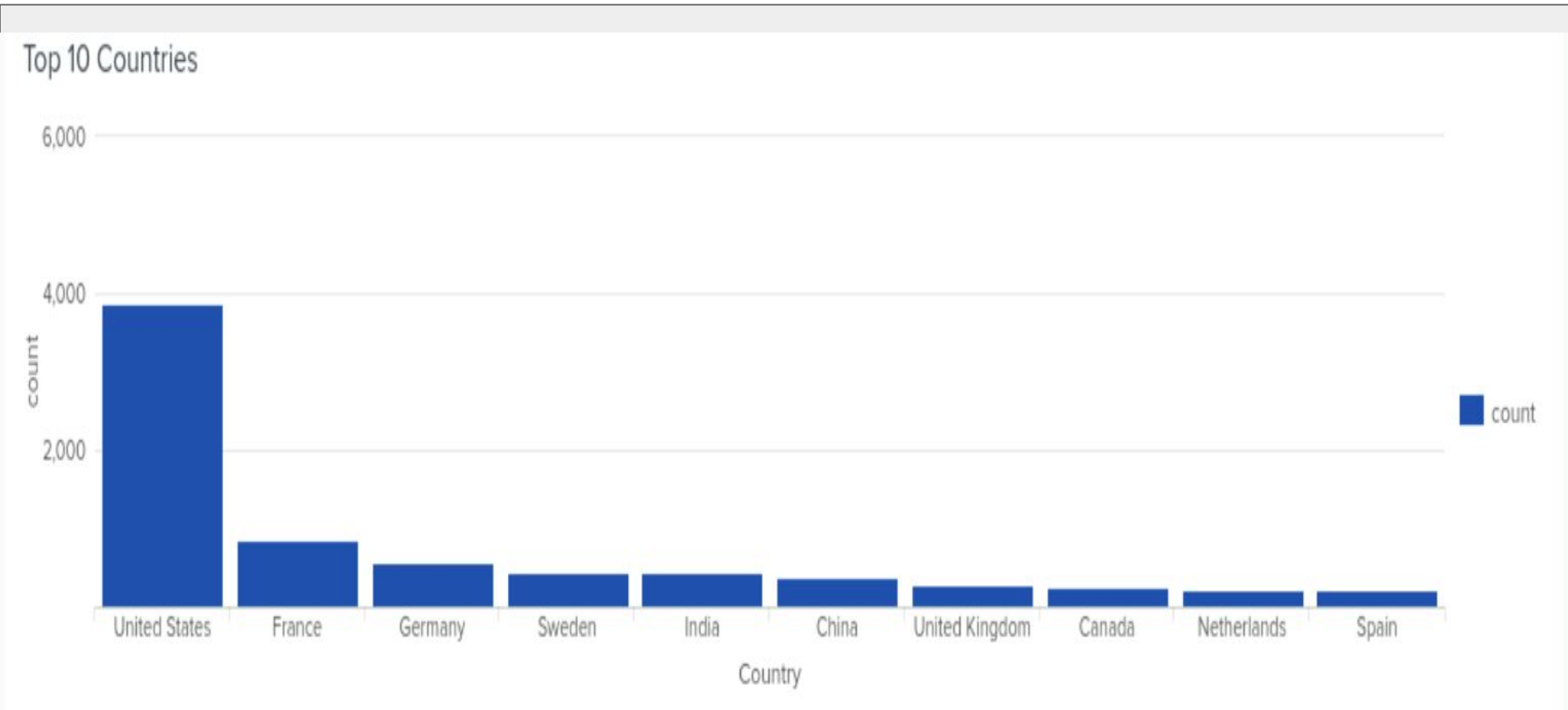
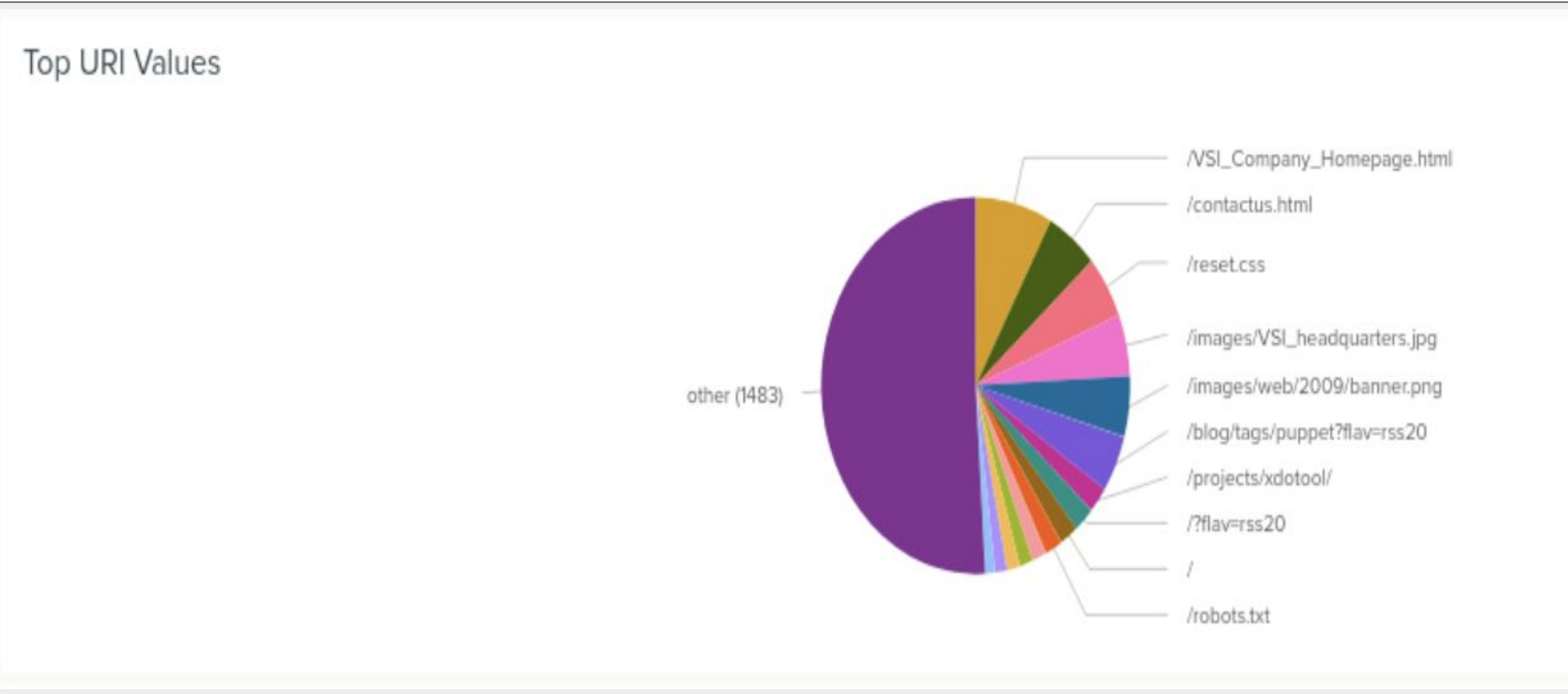
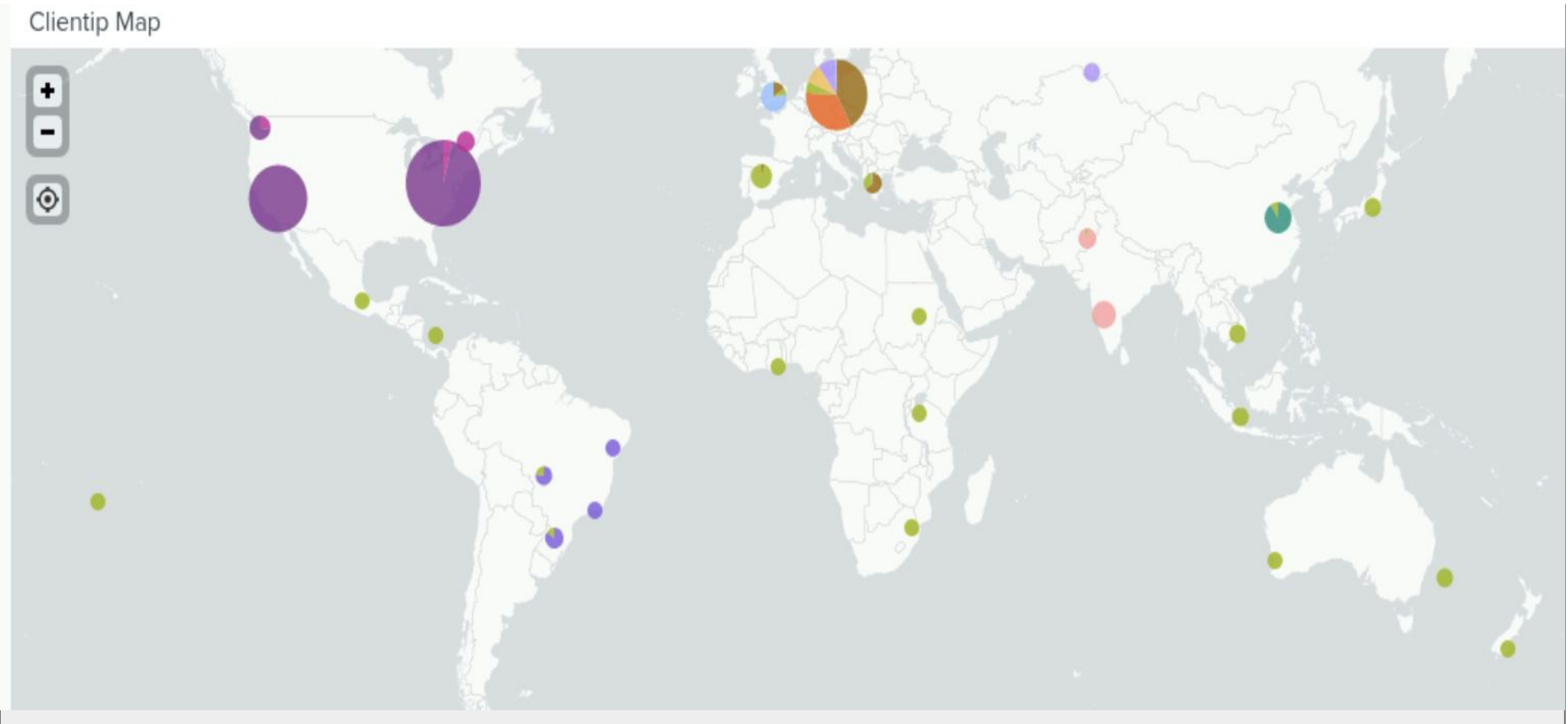
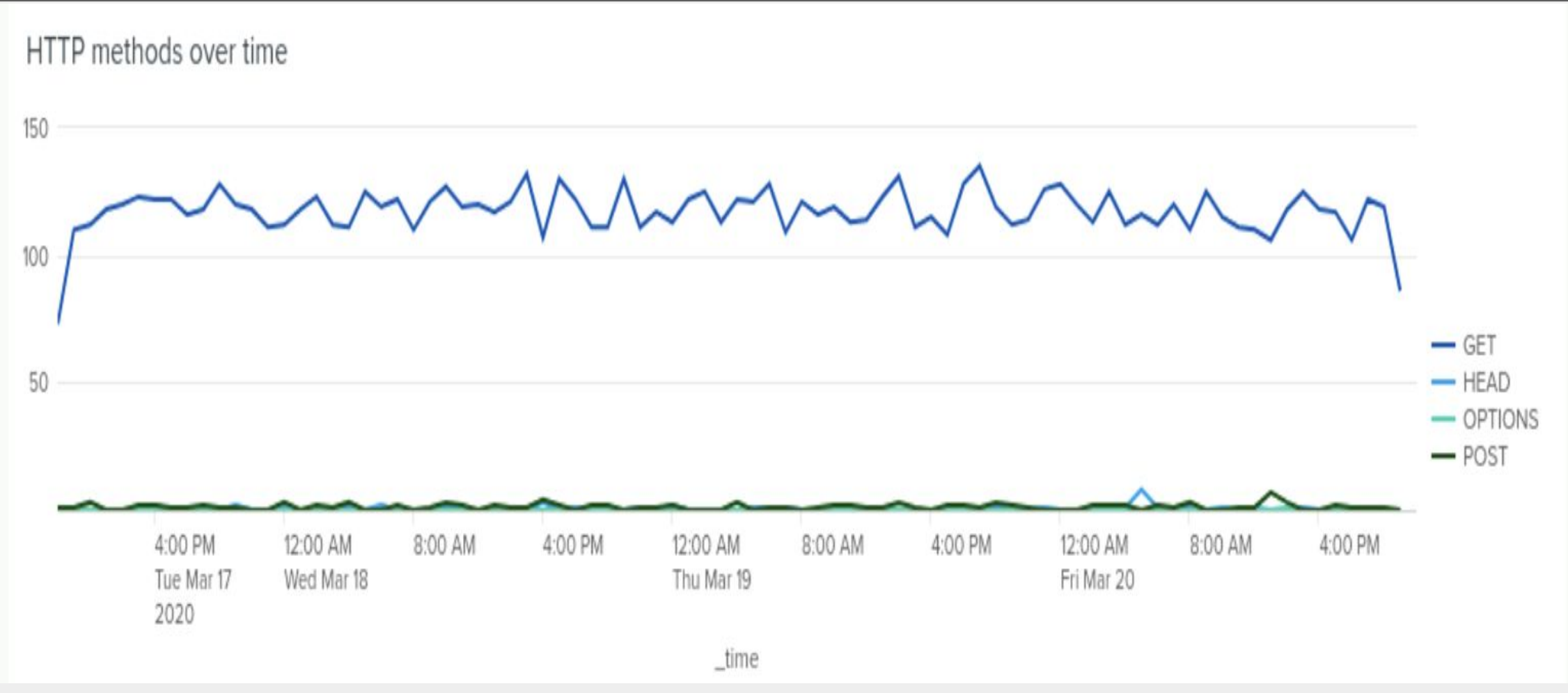
---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Method Alert	Alert if the hourly count of the HTTP POST method exceeds the threshold.	Lower: 0 Upper: 7	10

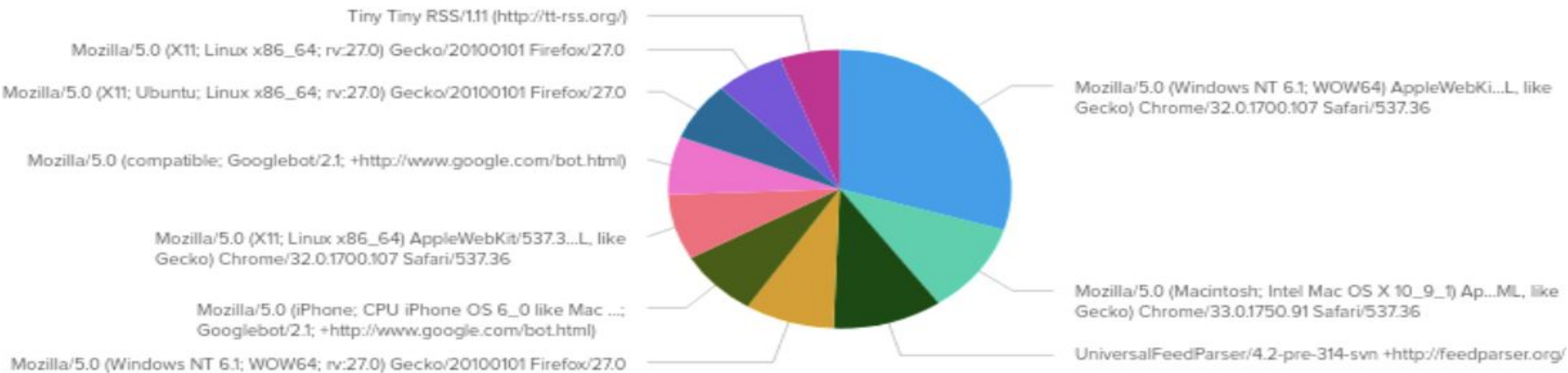
**JUSTIFICATION:** Most events per hour hovered between 1 and 4 and never surpassed 7. A threshold of 10 seemed like a number that would be out of reach of "normal" hourly events but small enough to catch malicious activity.

# Dashboards—Apache



# Dashboards–Apache

Top 10 User Agents



Total Request





# Attack Analysis

# Attack Summary—Windows

---

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

- 1- The Windows attack system exhibited significantly more severity levels categorized as "high" than the nearly 95% classified as "informational" prior to the attack.
- 2- Also, noted significant changes between the normal and attack logs for failed activities. There was an increase in successful logins and decrease in failed logins as a result.
- 3-The signature ID's for "An attempt was made to reset a password" and "A successful account login" increased dramatically in the attack report.



# Attack Summary—Windows

---

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

3- Alert analysis indicated suspicious volume of failed activity:

- Failed logins “35” events occurred at 08:00 AM on 03/25/2020. Threshold (15) was exceeded and no changes are recommended.

4- Alert analysis indicated suspicious volume of successful logins:

- “196” events detected in an hour. Primary user logging in “user-j” occurred on 03/25/2020 at 11:00 AM. Threshold (18) was exceeded and no changes are recommended.

5- Alert analysis indicated suspicious volume of deleted account:

- Between 09:00 AM and 11:00 AM, we noticed a suspicious decrease in account deletions. There were 11 deletions at 08:00 AM, dropping to 3 at 09:00 AM, then 0 at both 10:00 AM and 11:00 AM. The number returned to normal at 12:00 PM with 13 deletions. Threshold (33) was exceeded and no changes are recommended.

# Attack Summary—Windows

---

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

6- Dashboard analysis for time chart of signatures:

- The time chart for the "attack logs" showed unusual events compared to regular Windows activity logs.
  - "An attempt was made to reset an account password" occurred between 09:00 AM and 11:00 AM, peaked at 896.
  - "A user account was locked out" occurred between 01:00 AM and 02:30 AM, peaked at 1258.

7- Dashboard analysis for users:

- There were two users "user\_a and user\_k" who have significant increase in activity.
  - User\_a had increased activity between 01:00 AM and 02:00 AM, peaked at 984.
  - User\_k had increased activity between 09:00 AM and 10:00 AM, peaked at 1256.

# Attack Summary—Windows

---

8- Dashboard analysis for signatures with pie charts:

- There was a significant increase in two signature types.
  - An attempt was made to reset an account password.
  - A user account was locked out.

9- Dashboard analysis for users with pie charts:

- There was increased activity for user\_a and user\_k.

# Screenshots of Attack Logs

splunk>enterprise

Apps ▾

⚠ Administrator ▾

1 Messages ▾

Settings ▾

Activity ▾

Help ▾

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

>

Severity Levels Report

Save Save As ▾ View Create Table View Close

source="windows\_server\_attack\_logs.csv" | stats count as total\_count by severity

| eventstats sum(total\_count) as overall\_count

| eval percentage = round((total\_count / overall\_count) \* 100, 2)

| table severity, total\_count, percentage

All time ▾

✓ 5,949 events (before 10/26/24 1:12:14.000 AM) No Event Sampling ▾

Job ▾

||

■

↶

🖨

⬇

💡 Smart Mode ▾

Events

Patterns

Statistics (2)

Visualization

20 Per Page ▾

✍ Format

Preview ▾

severity ⬆ ⬆	total_count ⬆ ⬆	percentage ⬆ ⬆
high	1111	20.22
informational	4383	79.78



splunk>enterprise

Apps

Administrator

1 Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Windows Activity Success and Failure

SaveSave AsViewCreate Table ViewClose

source="windows\_server\_attack\_logs.csv" | stats count as total by status | eventstats sum(total) as overall\_count | eval percentage = round((total / overall\_count) \* 100, 2) | table status, total, percentage

All time

✓ 5,949 events (before 10/26/24 1:42:26.000 AM) No Event SamplingJobPauseRefreshPrintDownloadSmart Mode

Events

Patterns

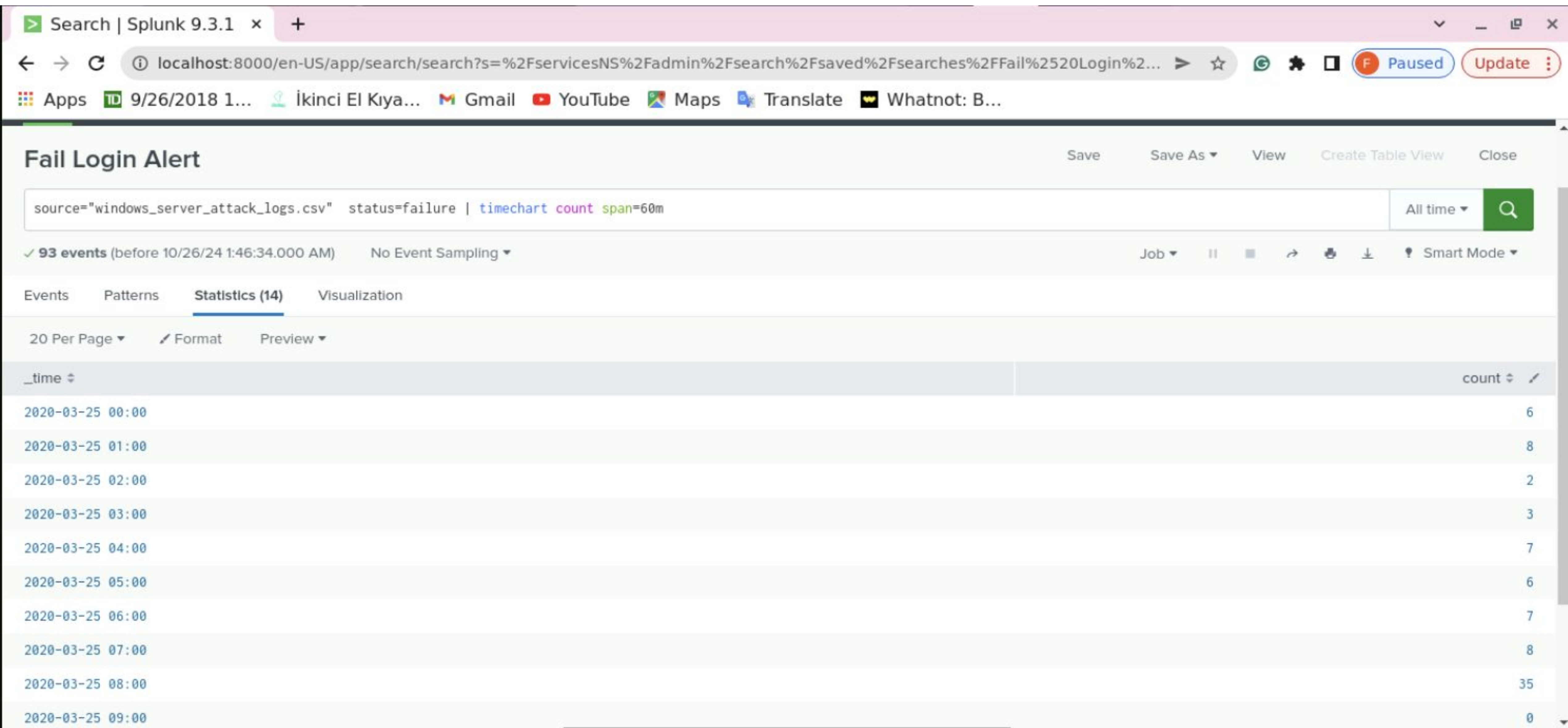
Statistics (2)

Visualization

20 Per PageFormatPreview

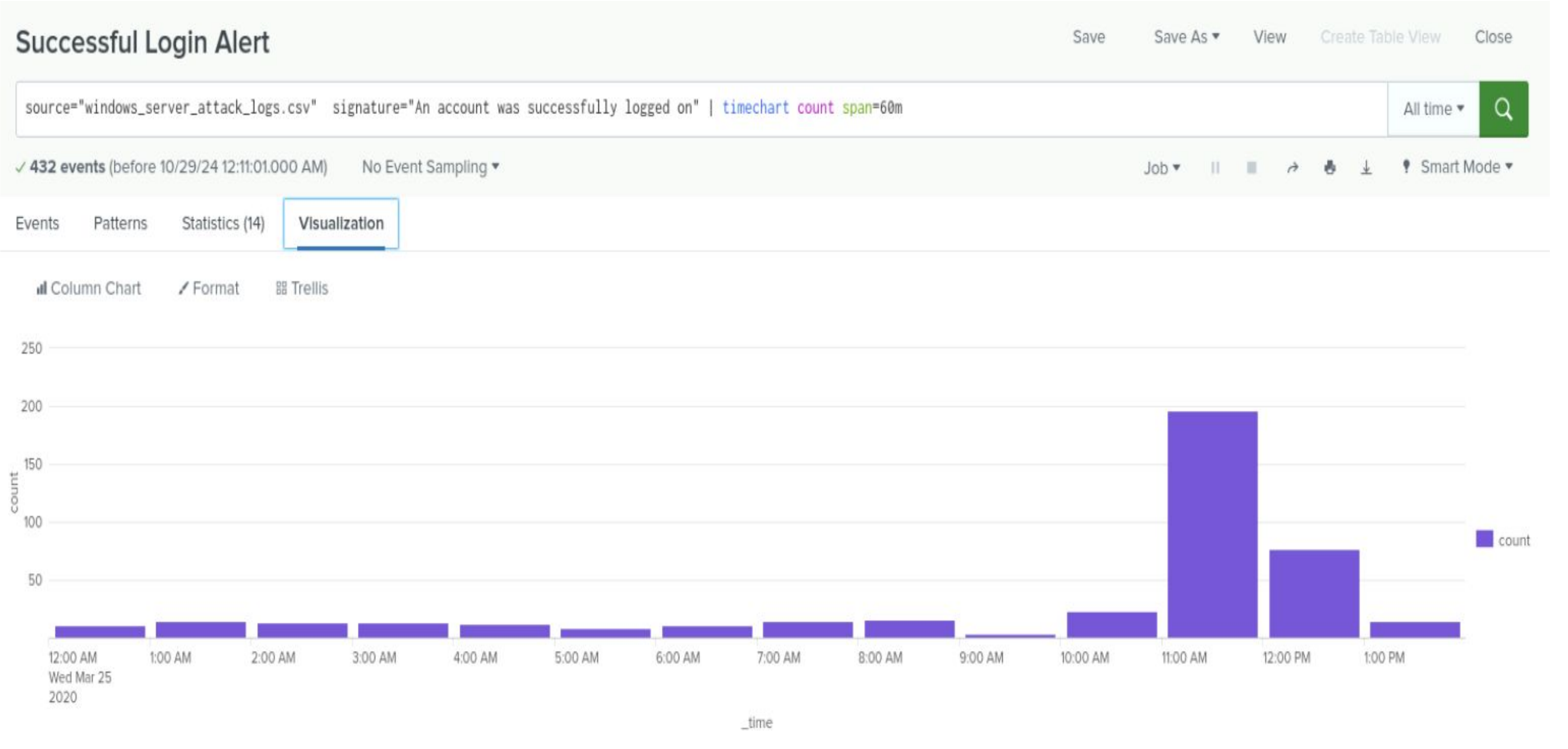
status	total	percentage
failure	93	1.56
success	5856	98.44

# Screenshots of Attack Logs





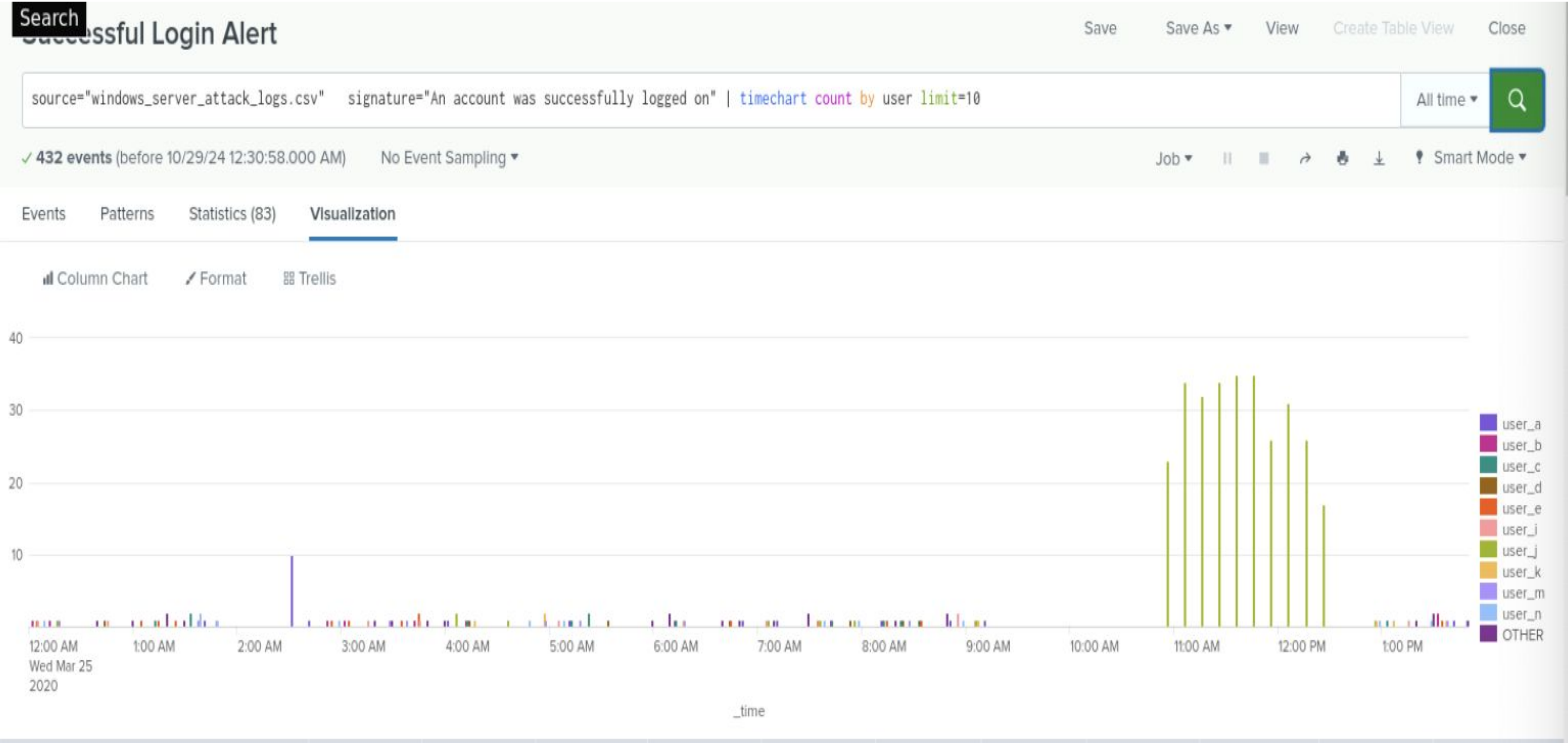
# Screenshots of Attack Logs



# Screenshots of Attack Logs

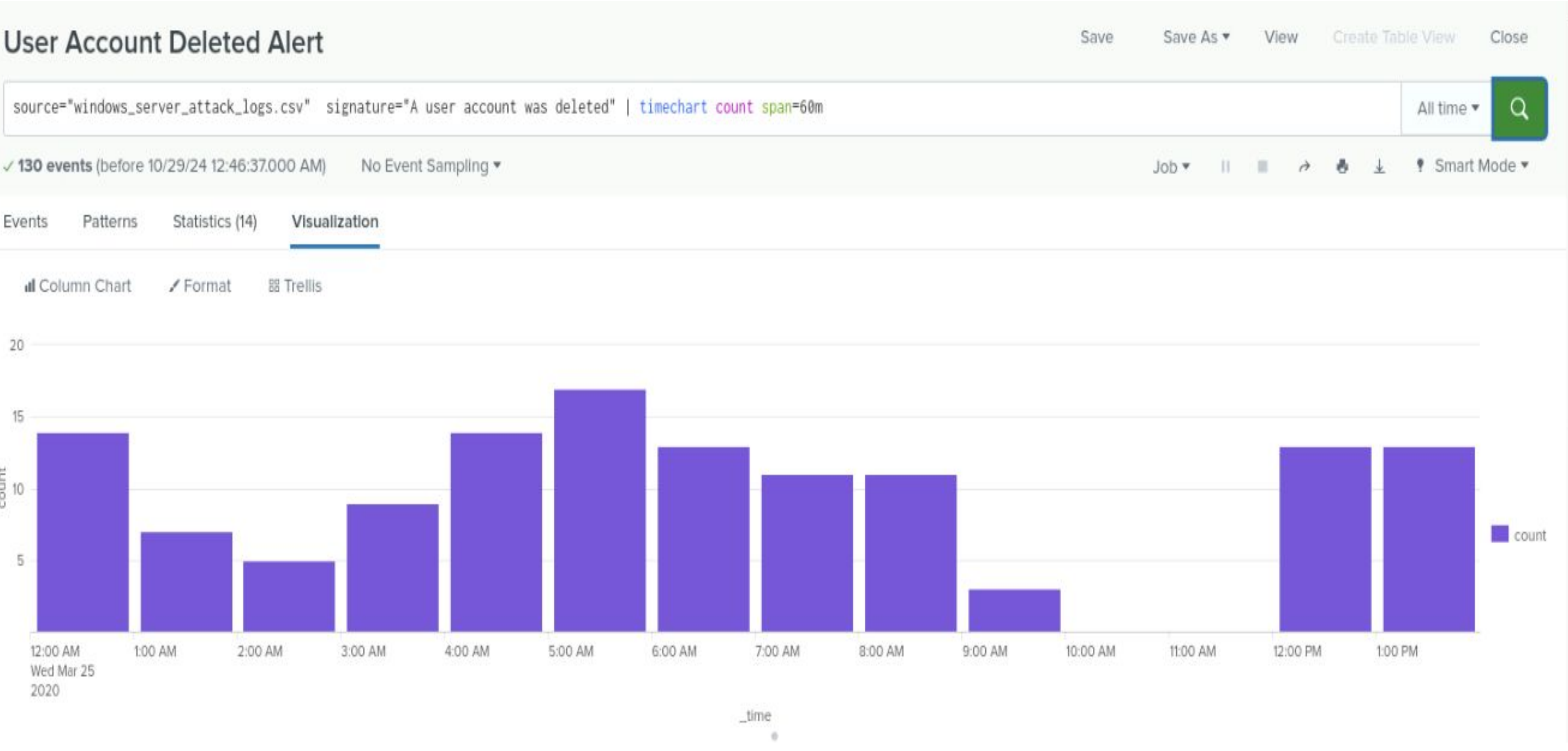
Events	Patterns	Statistics (14)	Visualization
20 Per Page ▾	Format	Preview ▾	
_time ↕	count ↕		
2020-03-25 00:00	11		
2020-03-25 01:00	15		
2020-03-25 02:00	14		
2020-03-25 03:00	14		
2020-03-25 04:00	12		
2020-03-25 05:00	9		
2020-03-25 06:00	11		
2020-03-25 07:00	15		
2020-03-25 08:00	16		
2020-03-25 09:00	4		
2020-03-25 10:00	23		
2020-03-25 11:00	196		
2020-03-25 12:00	77		
2020-03-25 13:00	15		

# Screenshots of Attack Logs



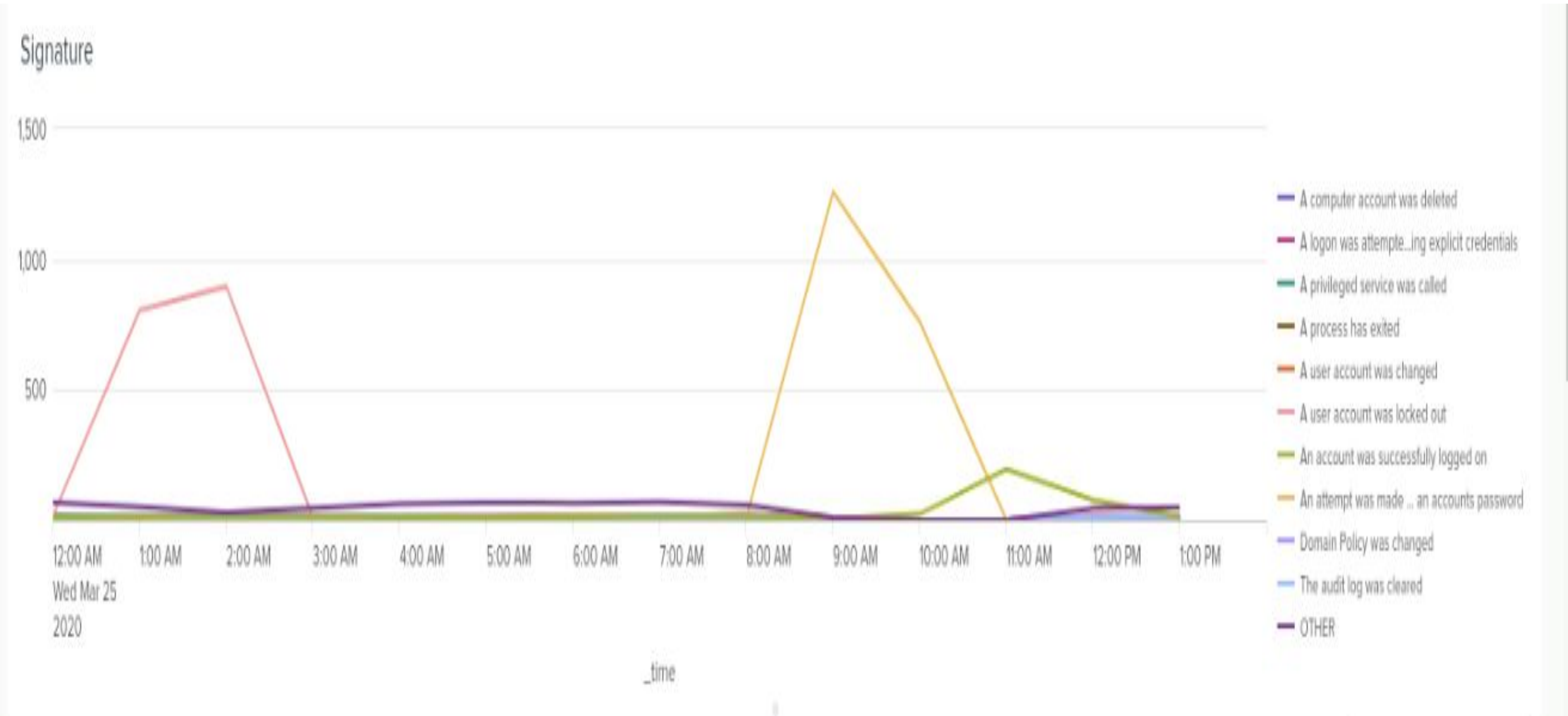


# Screenshots of Attack Logs





# Screenshots of Attack Logs



# Screenshots of Attack Logs

source="windows\_server\_attack\_logs.csv" | timechart span=1h count by signature

All time

5,949 events (before 10/26/24 3:39:16.000 PM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (14)

Visualization

20 Per Page

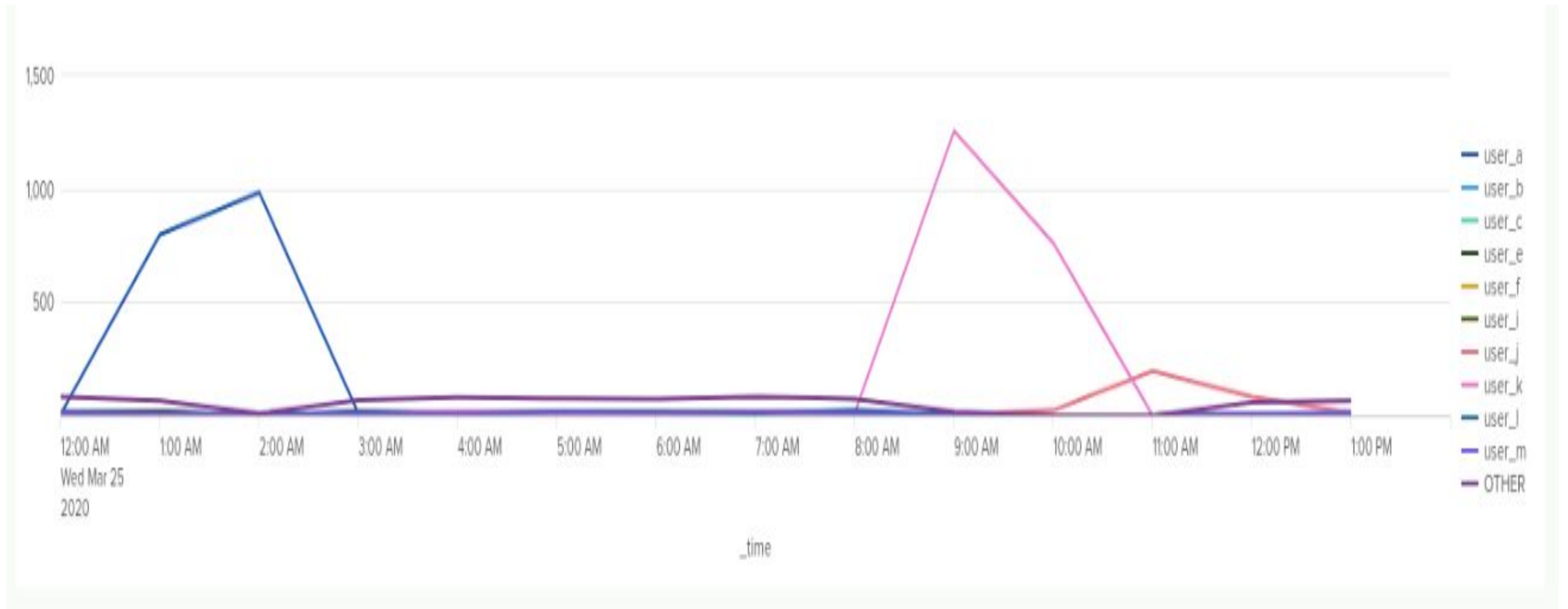
Format

Preview

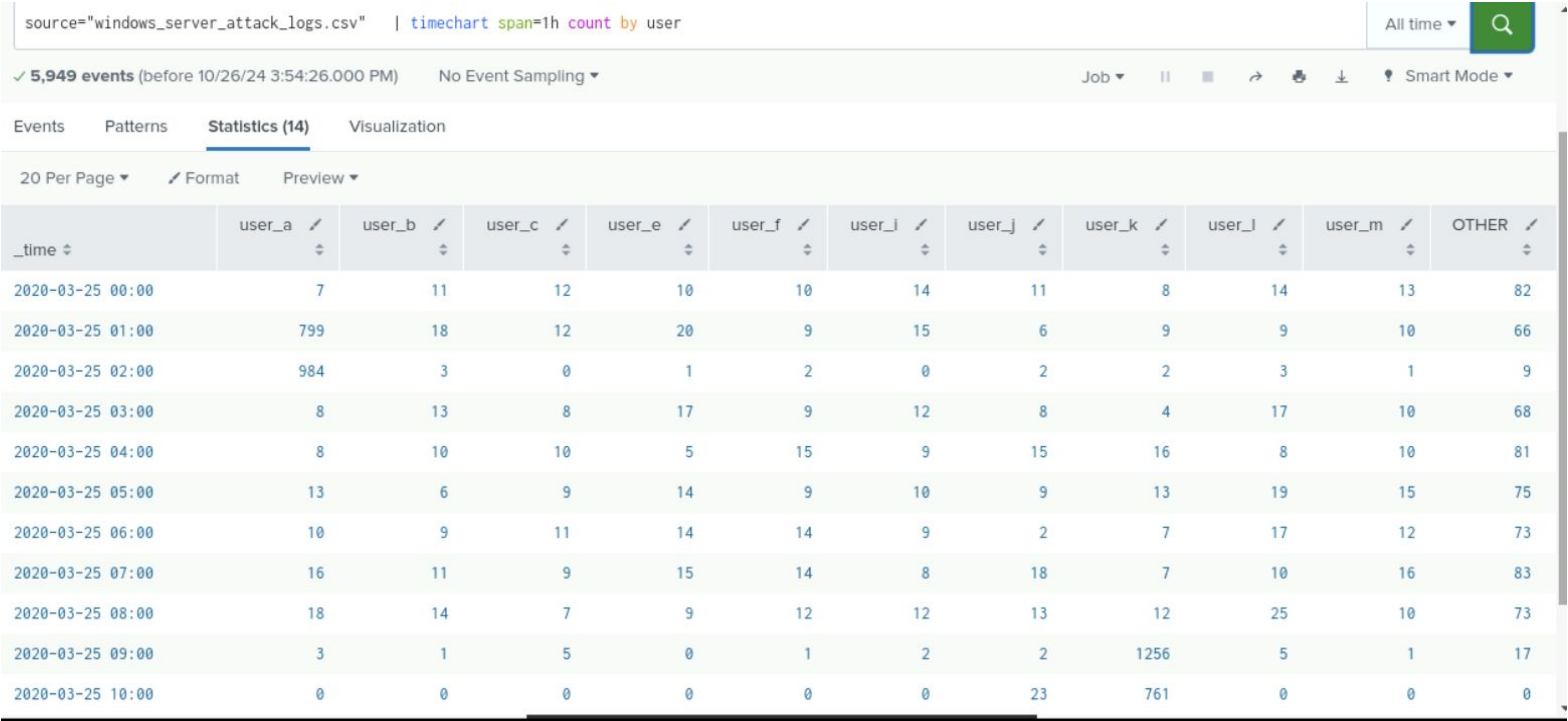
_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was changed	A user account was locked out	An account was successfully logged on	An attempt was made to reset an accounts password	Domain Policy was 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



# Screenshots of Attack Logs

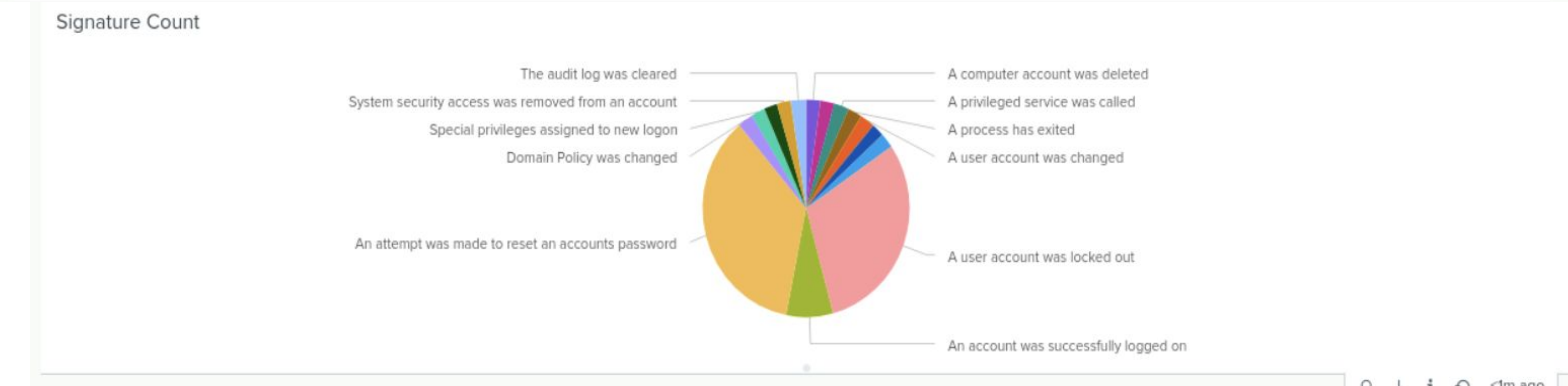


# Screenshots of Attack Logs



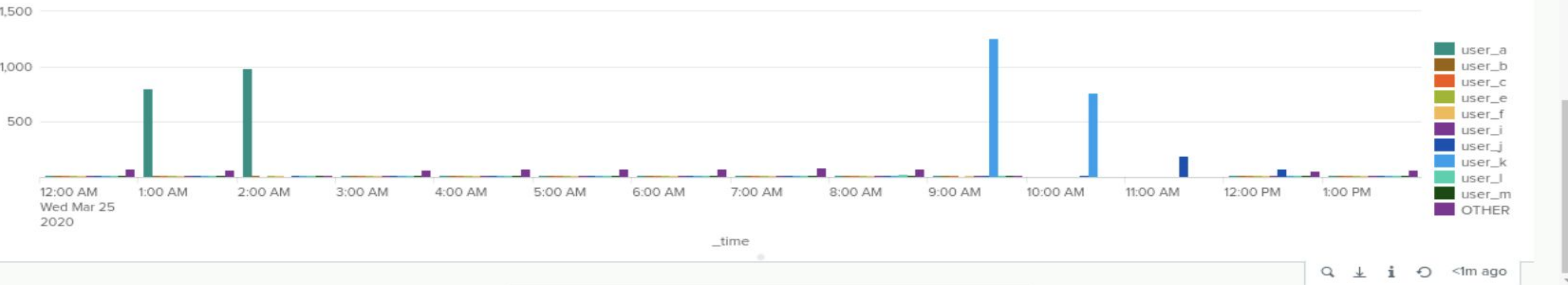


# Screenshots of Attack Logs

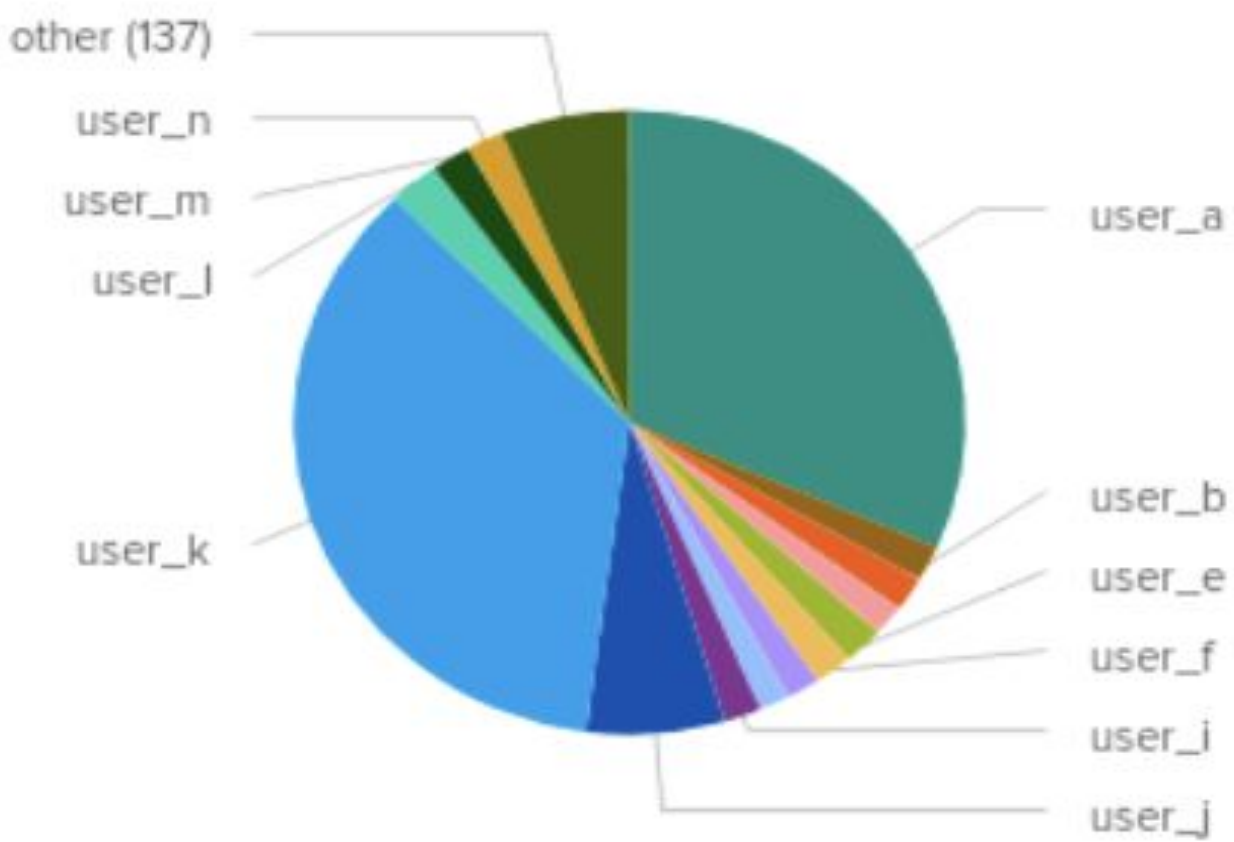


# Screenshots of Attack Logs

Different Users by Hour



User Count



# Attack Summary—Apache

---

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

- 1- There was a significant increase in HTTP methods, specifically with “POST”.
- 2- There was some changes in the results of the top 10 referrer domains, specifically with the last 5 of the list.
- 3- There was a suspicious changes in HTTP response codes, specifically with response code “200” and “404”. Response code 200 saw a decrease in amount and 404 saw an increase.

# Attack Summary—Apache

---

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

4- Alert analysis for international activity:

- There was a suspicious volume of international activity on 2020-03-25 at 08:00 PM, counted 937. And our alert would have been triggered, as we set the threshold to over 150 events per hour, and this activity significantly exceeded that limit. So, the threshold is kept as same we set.

5- Alert analysis for HTTP POST activity:

- There was a suspicious volume of HTTP POST activity on 2020-03-25 at 08:00 PM, counted 1296. The threshold was correct and no changes are recommended.



# Attack Summary—Apache

---

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

6- Dashboard analysis for time chart of HTTP methods:

- There was a significant difference in HTTP method time charts which was “POST”.It occurred between 07:00 PM and 09:00 PM, peaked at 1296.

7- Dashboard analysis for cluster map:

- There was a high volume of activity with Kiev and Kharkiv in Ukraine and both had an increase.The count was 440 for Kiev and 432 for Kharkiv.

8- Dashboard analysis for URI Data:


- Taking out the “other” as it is composed of many URIs too small to chart, the URI hit the most is “VSI\_Account\_logon.php”.The attacker may be performing reconnaissance through a brute force attack or SQL injection, as indicated by numerous 404 errors. This suggests a focus on scanning the network to gather information.

# Screenshots of Attack Logs




HTTP Methods Activity Report

SaveSave As ▾ViewCreate Table ViewClose

source="apache\_attack\_logs.txt" sourcetype=access\_combined | top limit=20 method

All time ▾

✓ 4,497 events (1/28/20 1:00:48.000 PM to 10/29/24 1:25:56.000 AM) No Event Sampling ▾

Job ▾ ||    Smart Mode ▾

EventsPatternsStatistics (4)Visualization

20 Per Page ▾ / Format Preview ▾

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

# Screenshots of Attack Logs

Top Referring Domains Report

SaveSave AsViewCreate Table ViewClose

source="apache\_attack\_logs.txt" | top limit=10 referer\_domainAll time

4,497 events (before 10/26/24 5:32:46.000 PM)No Event SamplingJobSmart Mode

EventsPatternsStatistics (10)Visualization

20 Per PageFormatPreview

referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165



# Screenshots of Attack Logs

HTTP Response Codes Report

SaveSave AsViewCreate Table ViewClose

source="apache\_attack\_logs.txt" | top limit=10 status

All time

✓ 4,497 events (before 10/26/24 5:34:45.000 PM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (7)

Visualization

20 Per Page

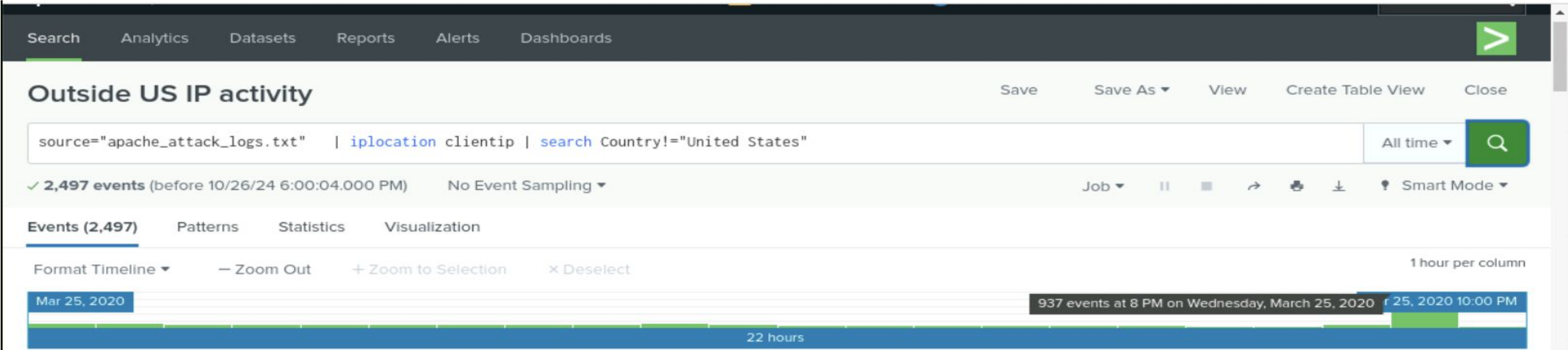
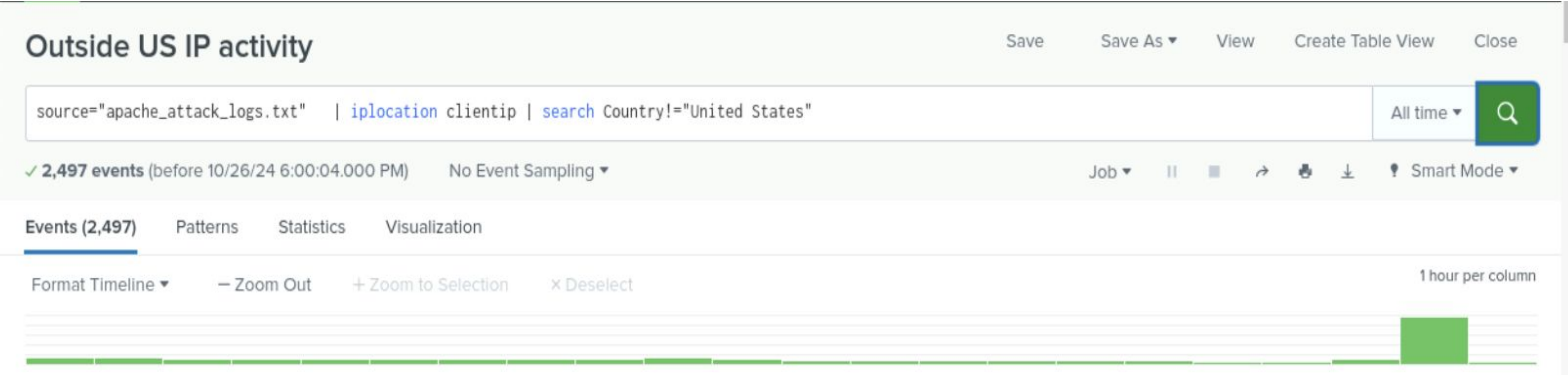
Format

Preview

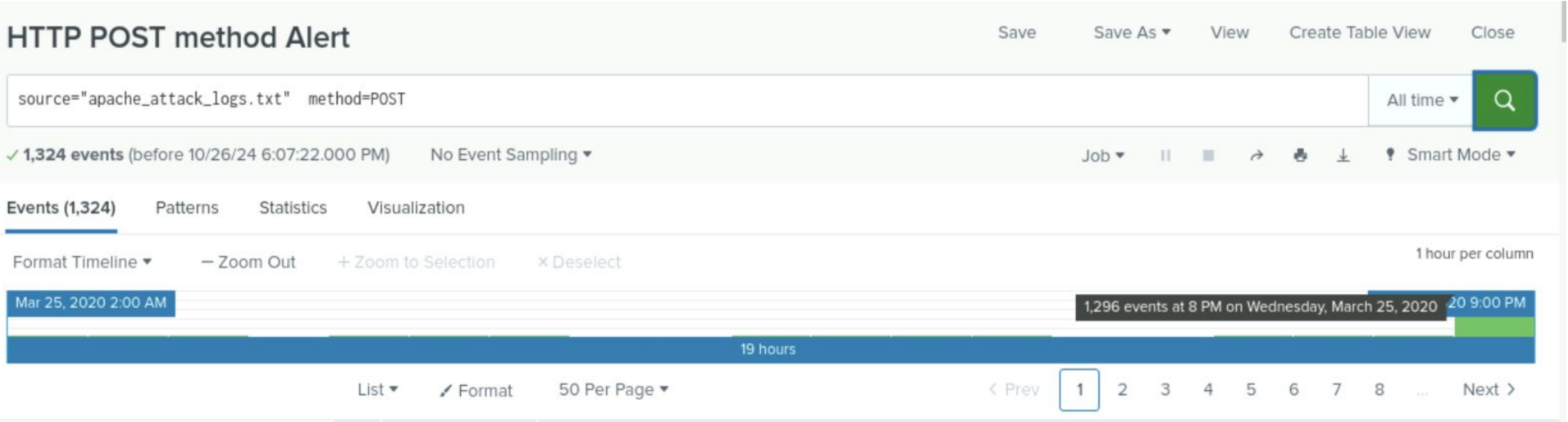
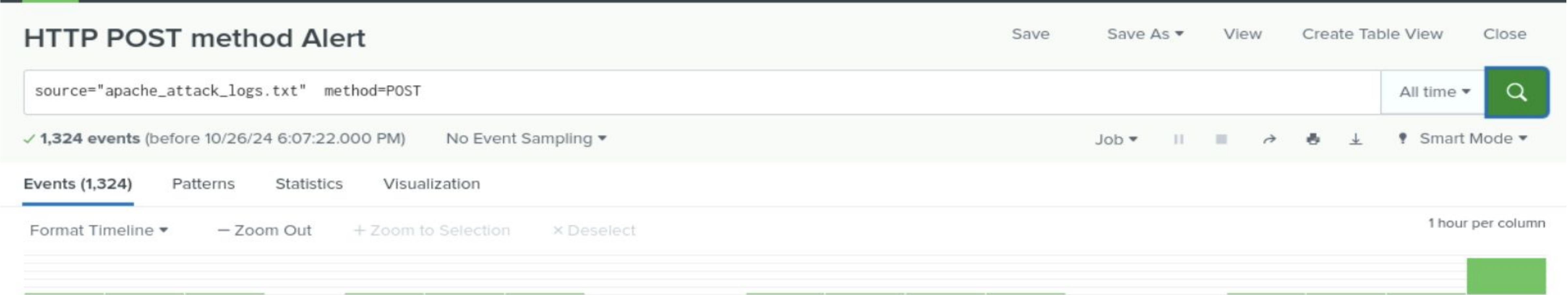
status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237



# Screenshots of Attack Logs

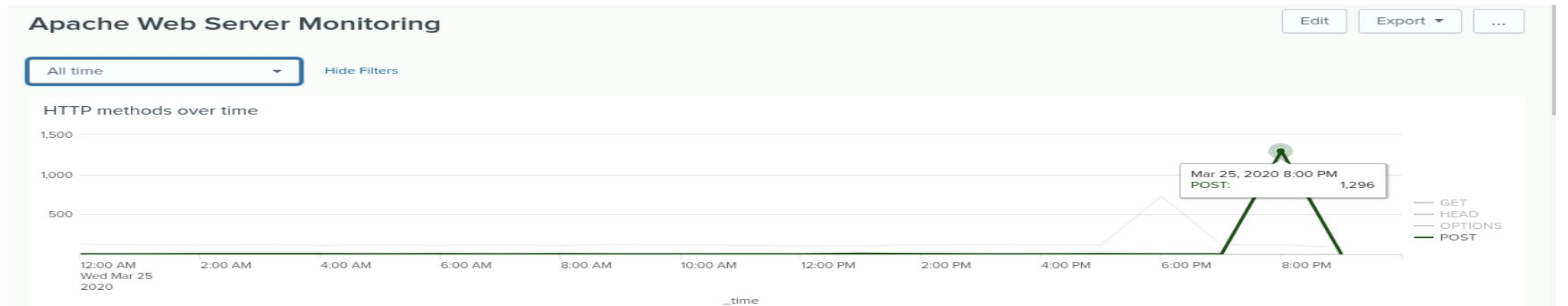
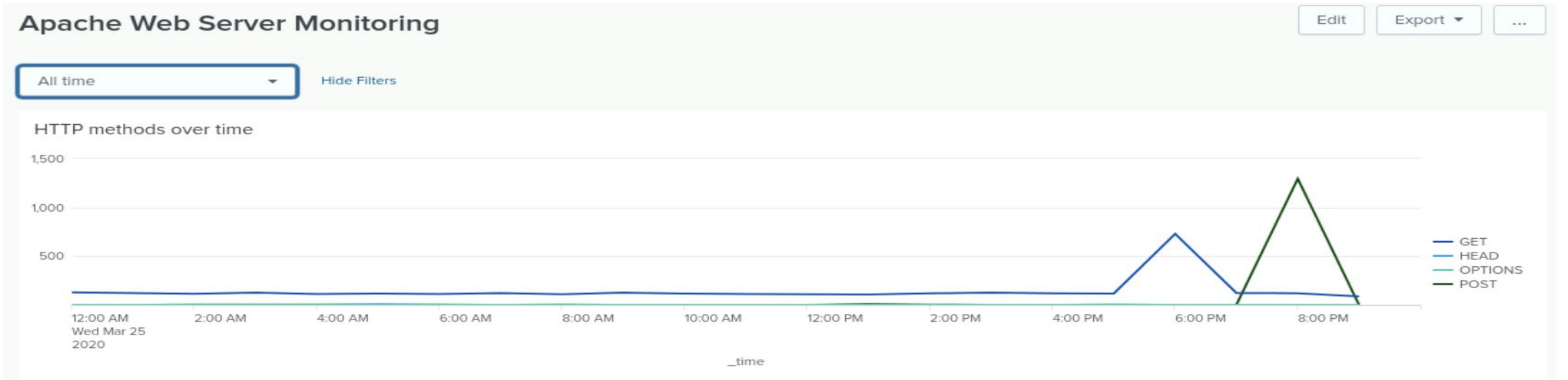


# Screenshots of Attack Logs

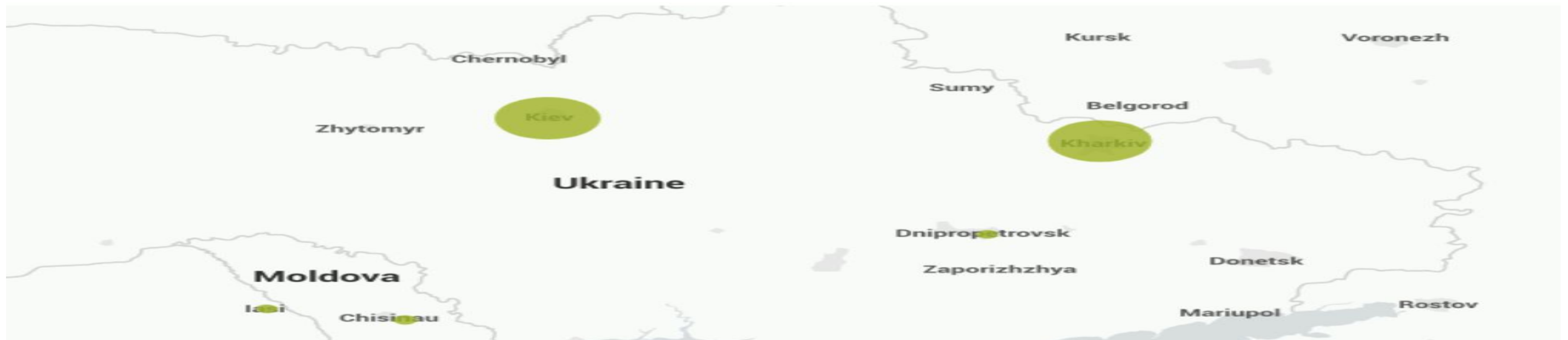
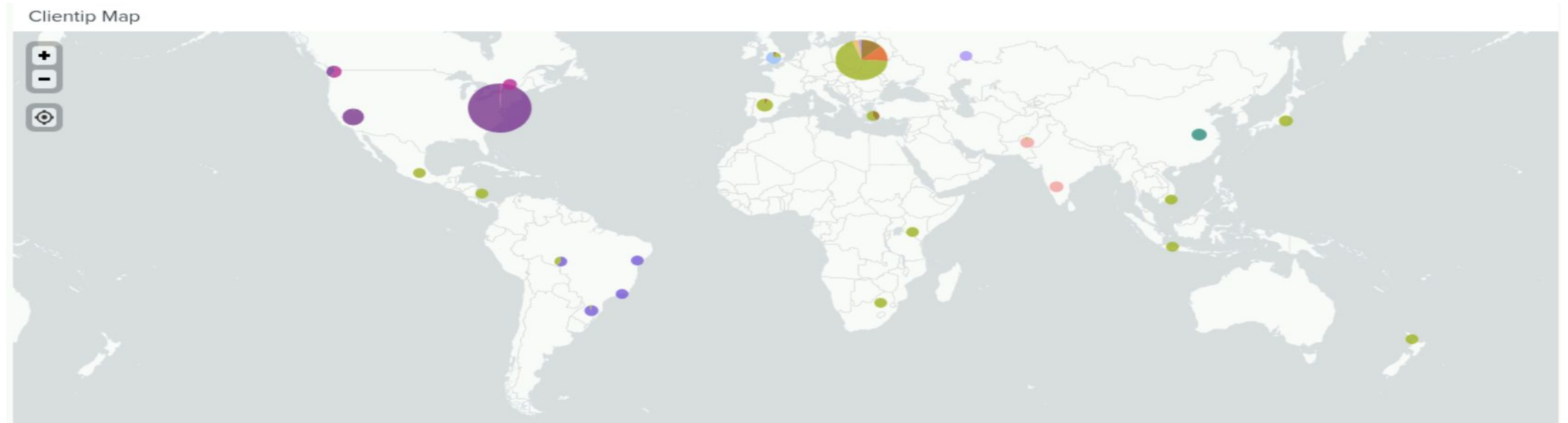




# Screenshots of Attack Logs



# Screenshots of Attack Logs





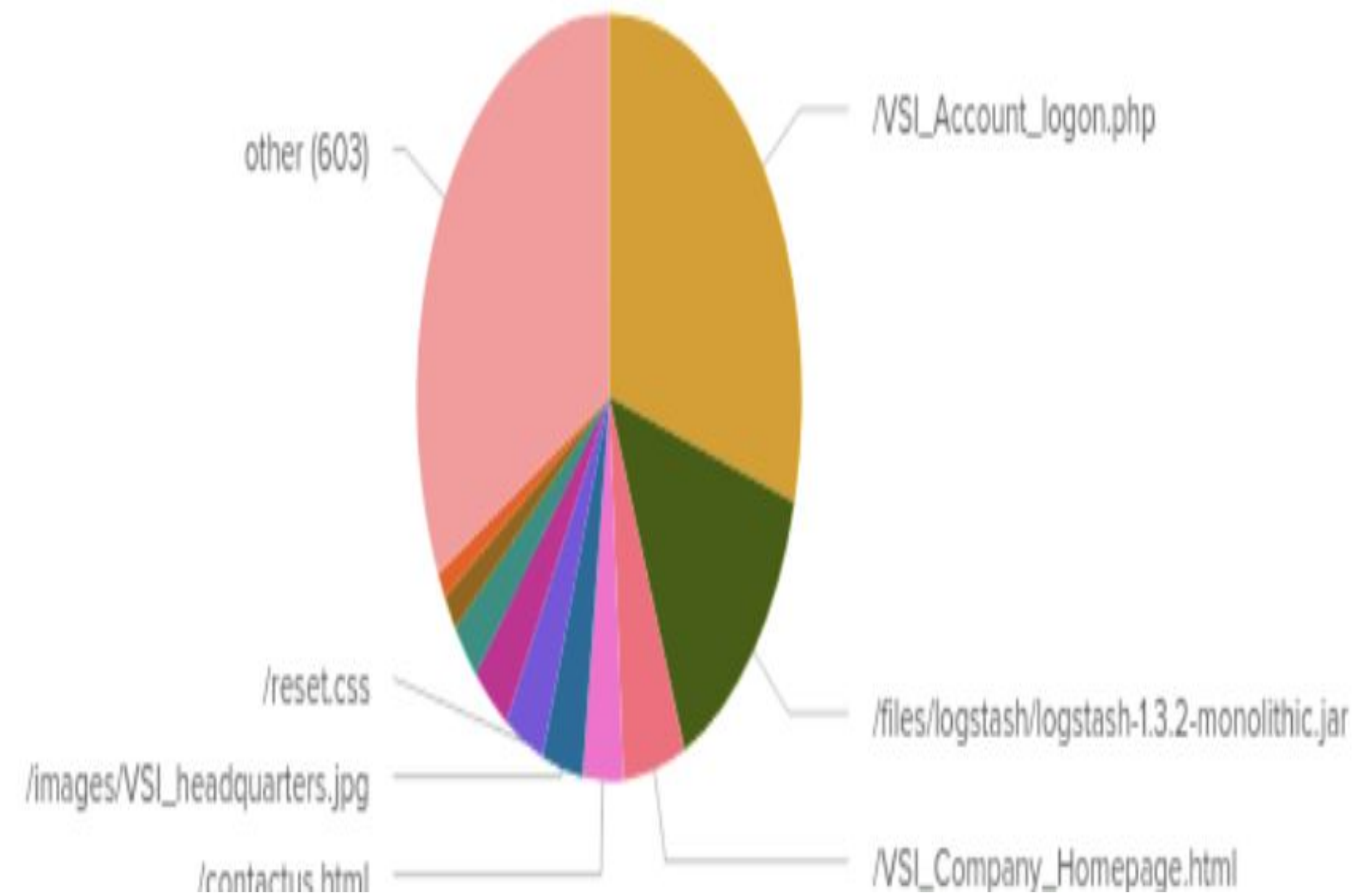
# Screenshots of Attack Logs



# Screenshots of Attack Logs

---

Top URI Values



# Summary and Future Mitigations

# Project 3 Summary

---

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

Our investigation revealed that on March 25th, VSI experienced multiple attacks targeting their Windows and Apache servers. These attacks primarily involved brute force password spamming originating from various regions and countries around the globe.

- To protect VSI from future attacks, what future mitigations would you recommend?
  - Require MFA (Multi-Factor Authentication) for all user accounts, adding an additional layer of security beyond just passwords (the first line of defense against Brute Force attacks).
  - Limit the number of login attempts from a single IP address within a specified timeframe to deter brute force attacks
  - Divide the network into segments to limit access to critical systems and minimize the impact of an attack.