Defensive Security Project
by: FATMA KAYGISIZ

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Today, you will play 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, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.
- The VSI products that you 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.

[“Add-On” App]

[Add-On App Name]

[Summary of add-on app chosen]

[Add-On App Name]

[Scenario that illustrates benefit of add-on app]

[Add-On App Name]

[Images for add-on app]

Logs Analyzed

1

Windows Logs

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

2

Apache Logs

Logs for VSI’s main public-facing website, vsi-company.com.

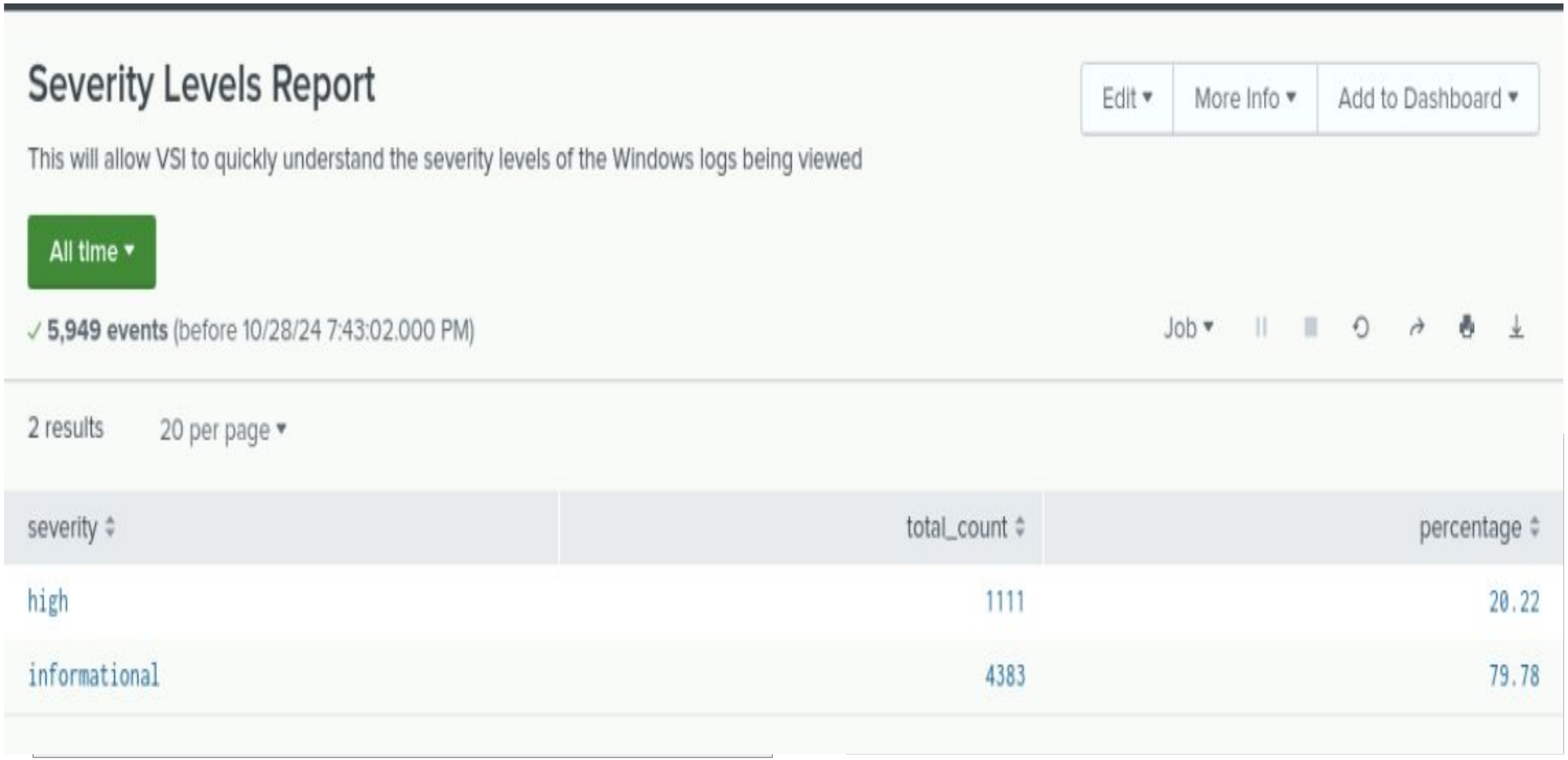
Windows Logs

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

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.

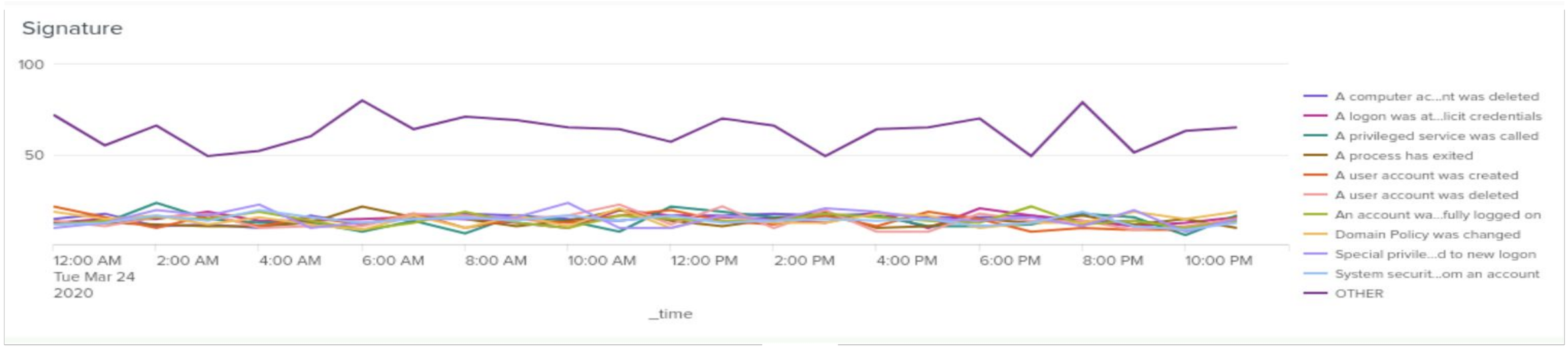
Alerts—Windows

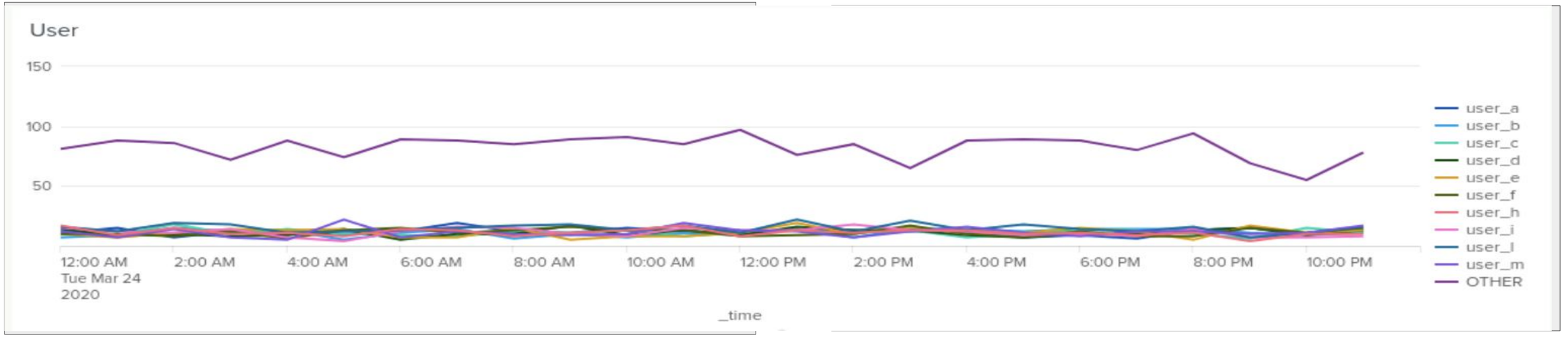
Designed the following alerts:

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

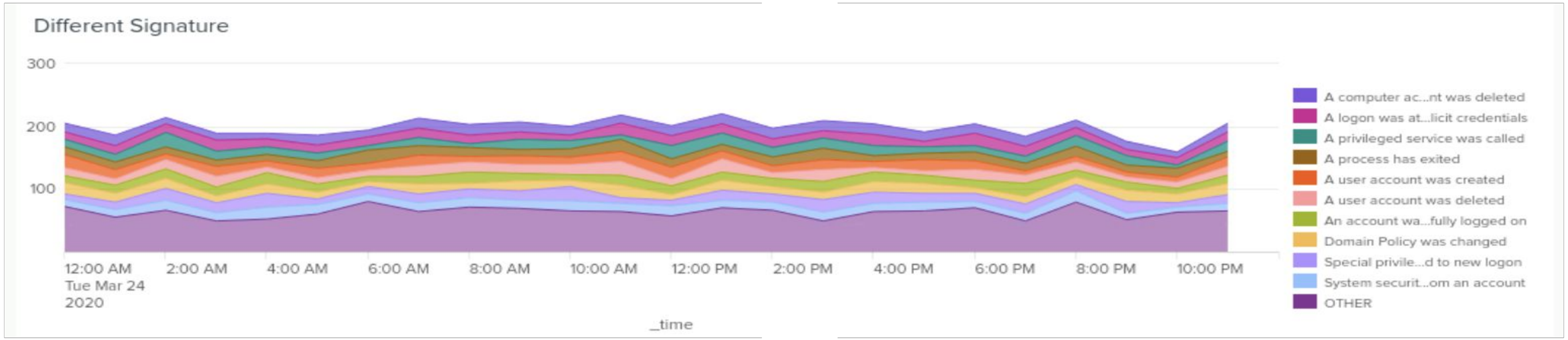
JUSTIFICATION: A baseline of 7-22 seemed on par with a "normal" hour. Exceeding 33 would raise suspicion levels and indicate a problem.

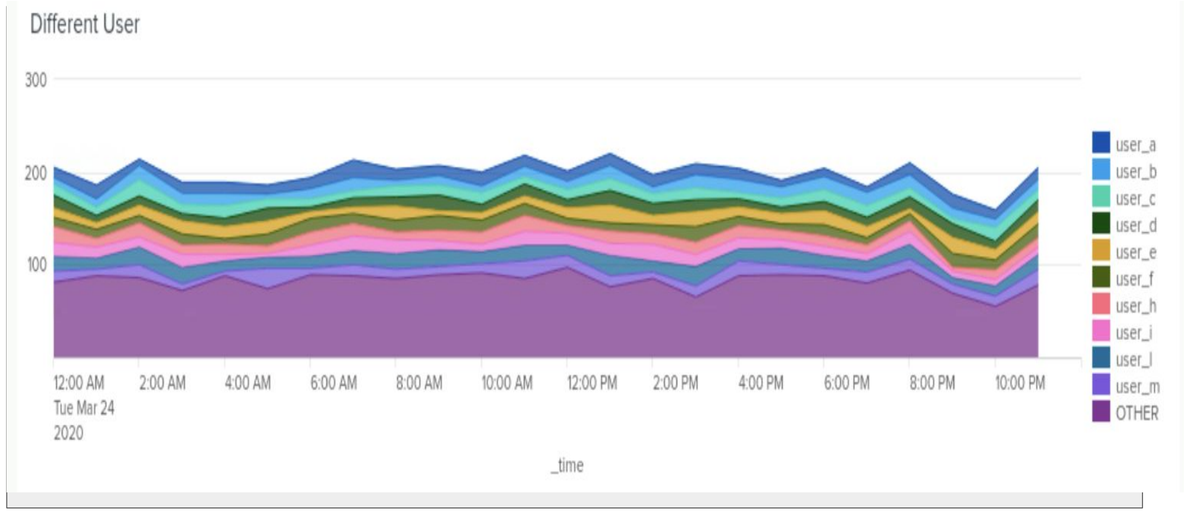
Dashboards—Windows

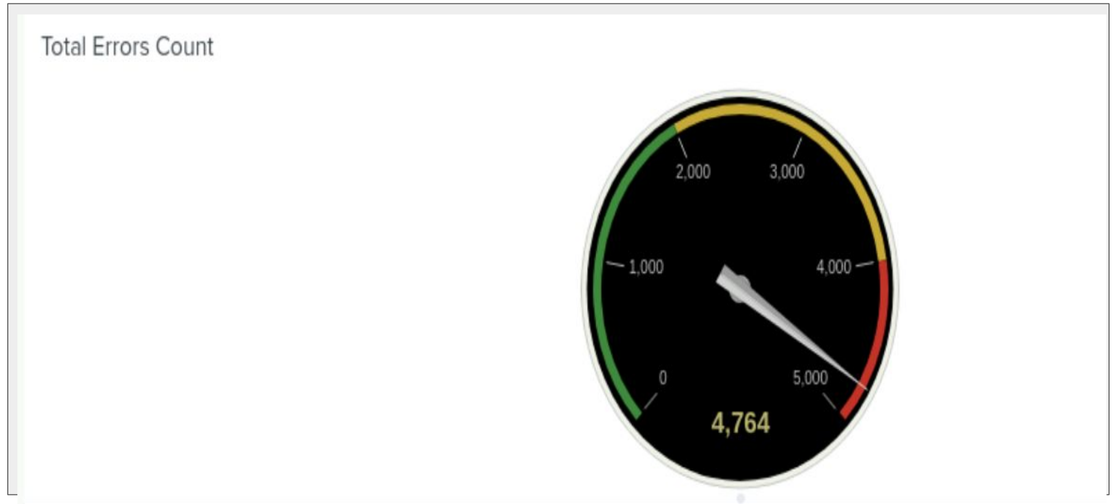




Dashboards—Windows







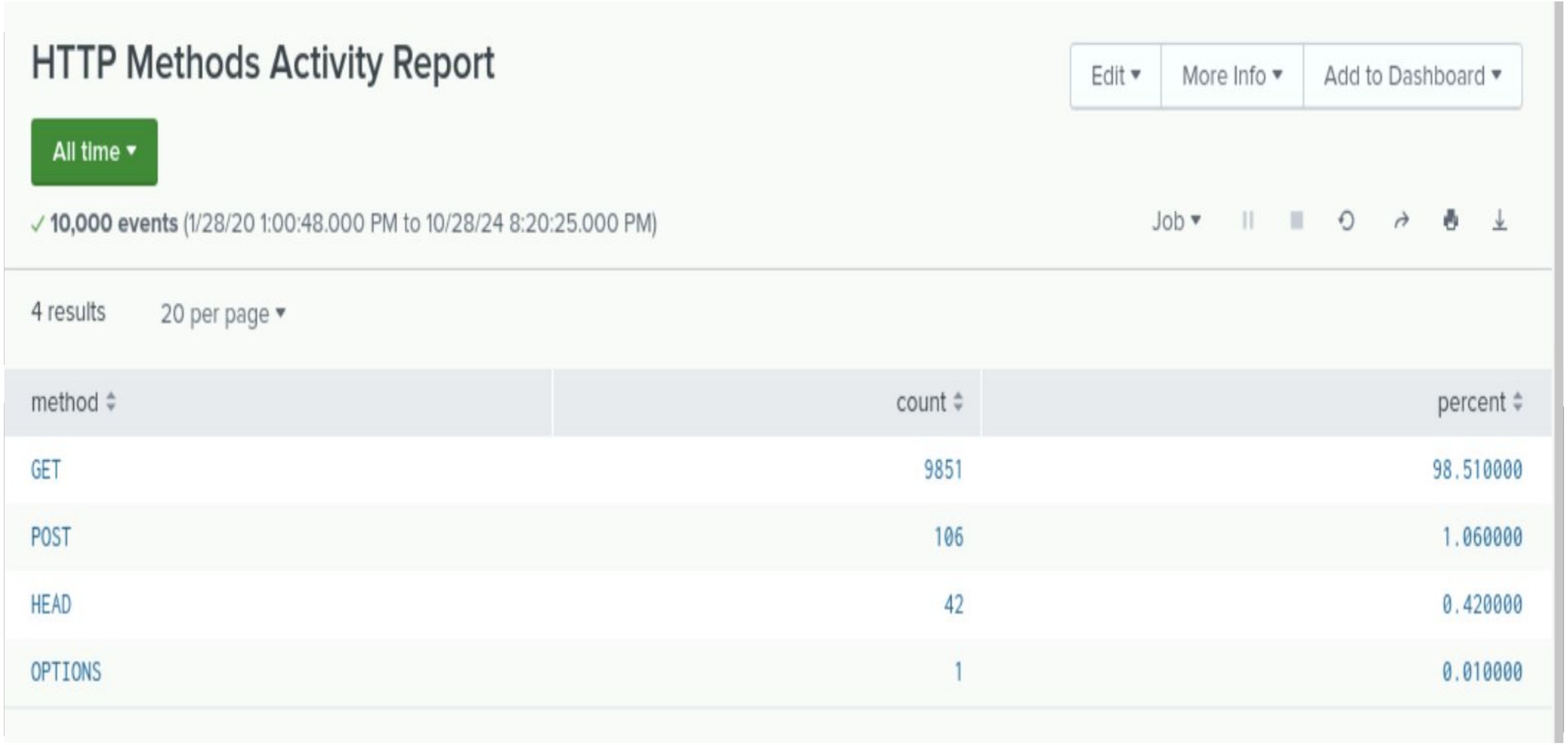
Apache Logs

Reports—Apache

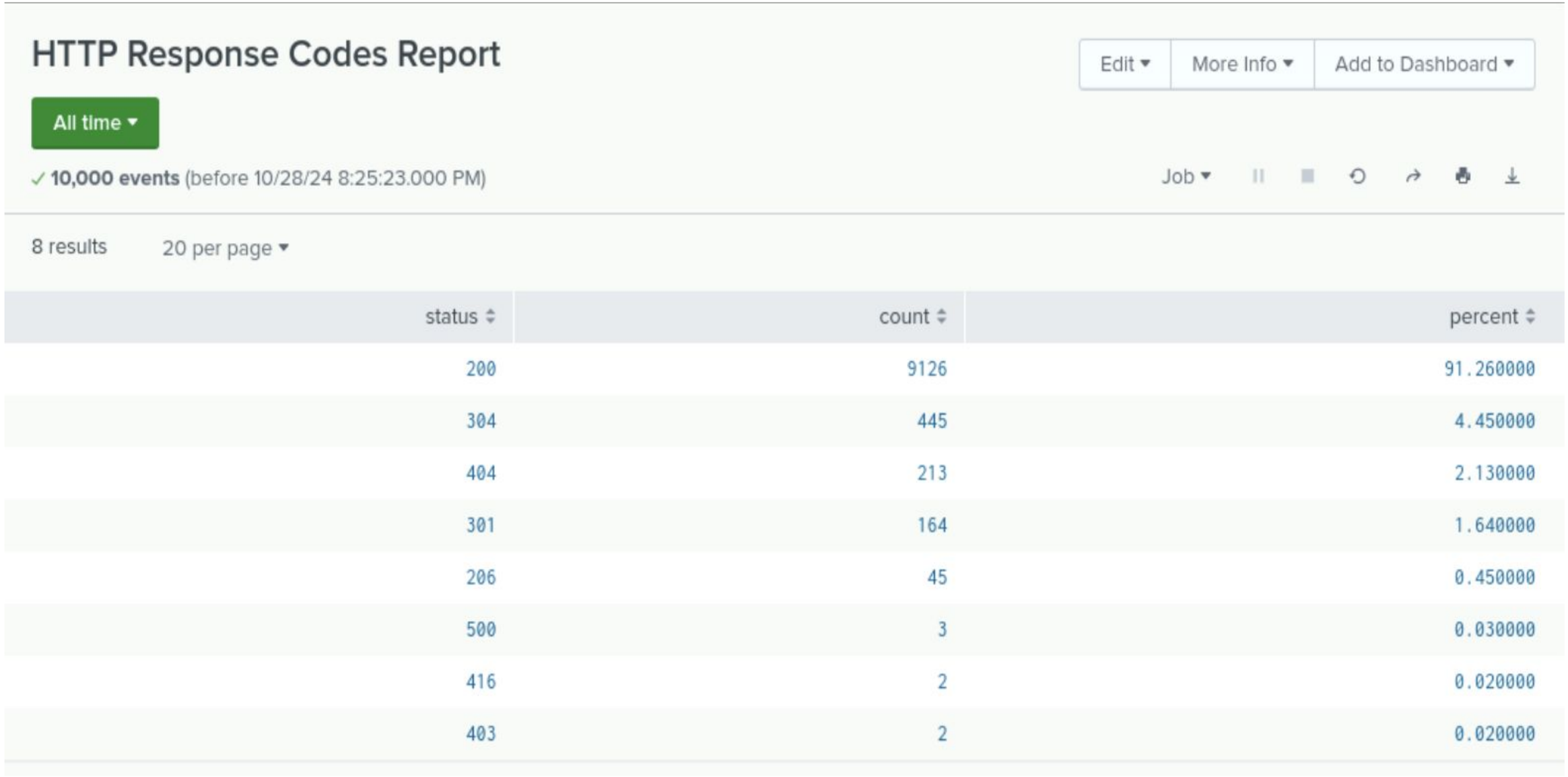
Designed the following reports:

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



Images of Reports—Apache



HTTP Response Codes Report

Edit ▾ | More Info ▾ | Add to Dashboard ▾

All time ▾

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

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.

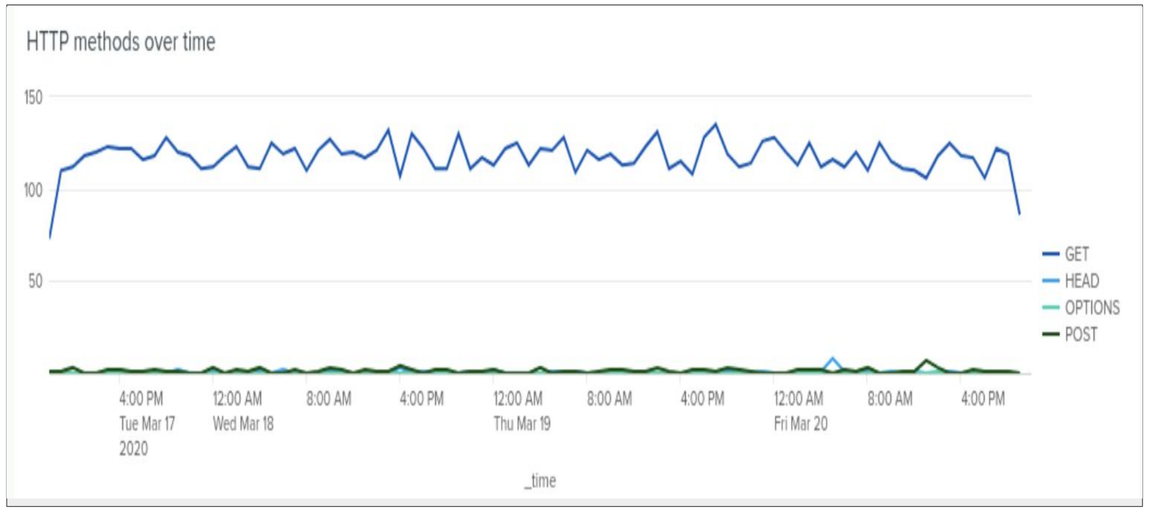
Alerts—Apache

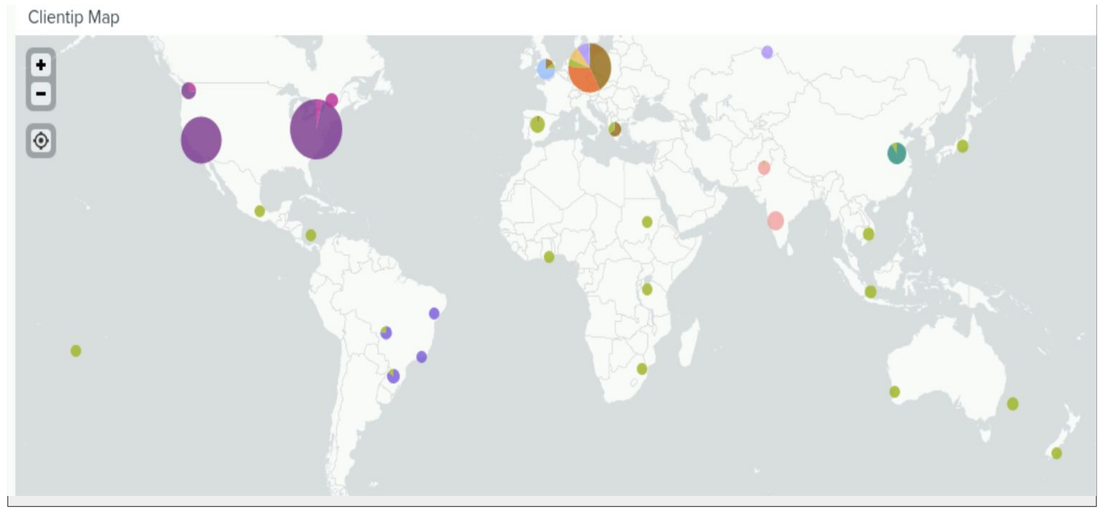
Designed the following alerts:

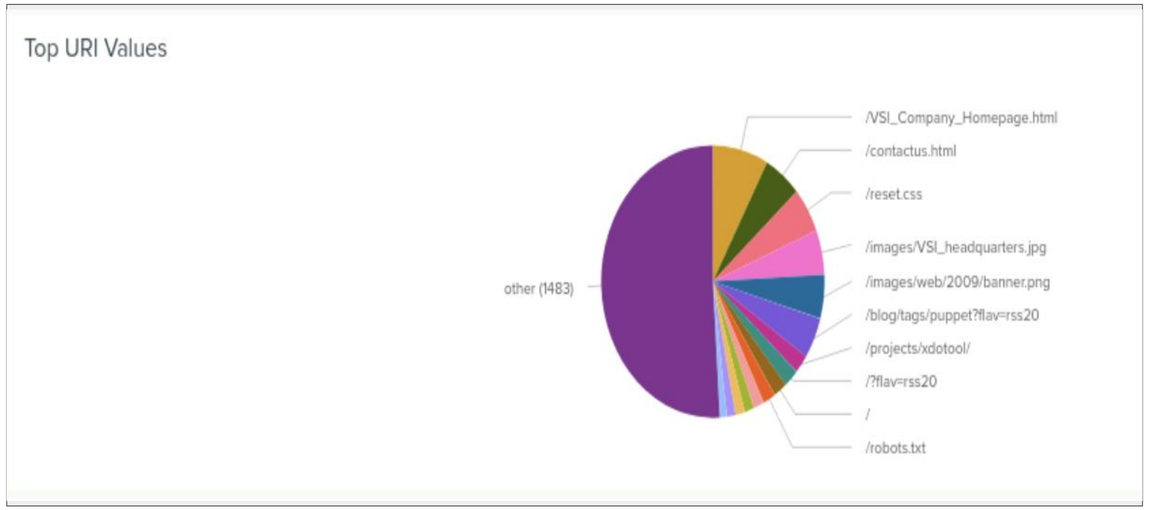
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Method Alert	Alert if the hourly count of the HTTP POST method exceeds the threshold.	Lower: 0 Upper: 7	10

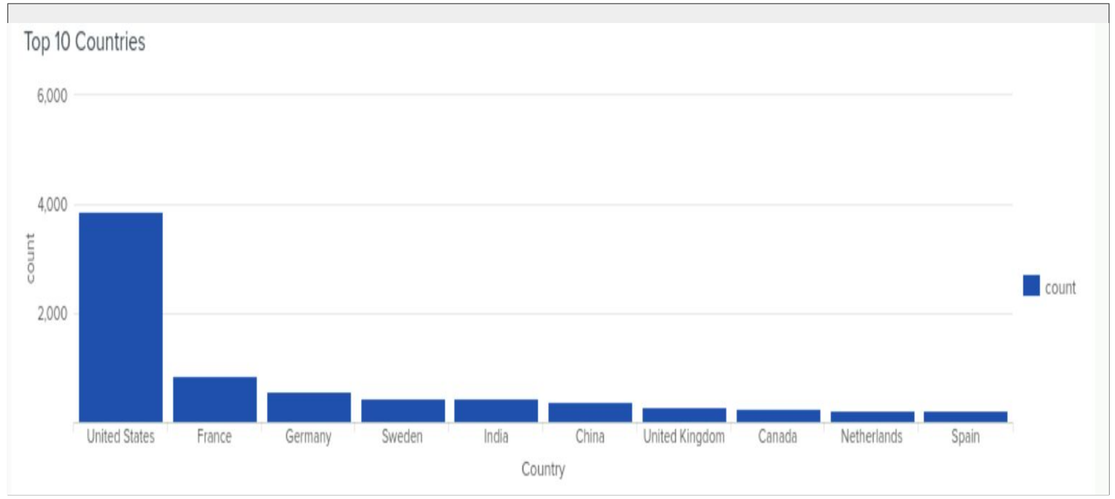
JUSTIFICATION: Most events per hour hovered between 1 and 4 and never surpassed 7. A threshold of 10 seemed like a number that would be out of reach of "normal" hourly events but small enough to catch malicious activity.

Dashboards—Apache



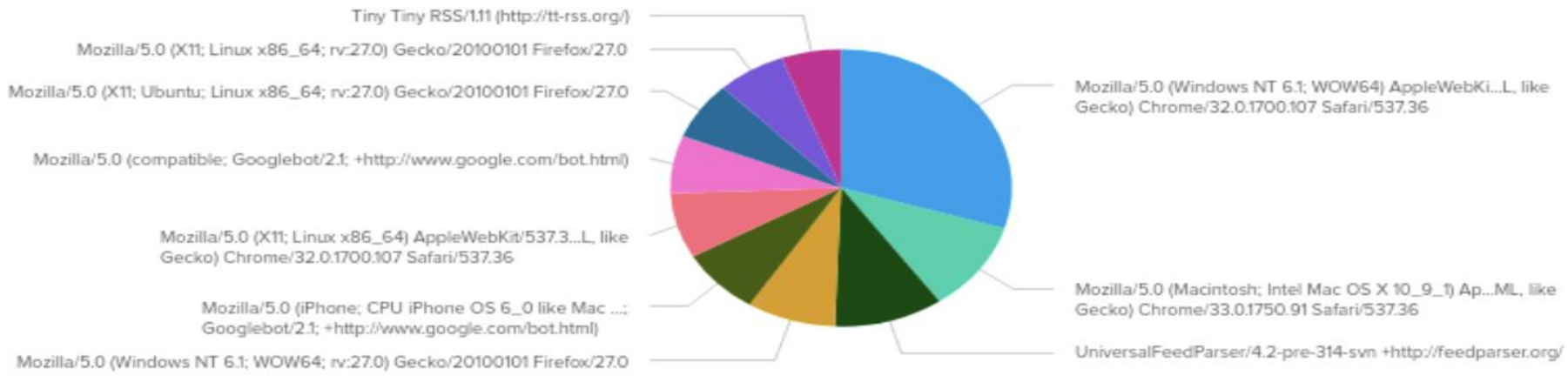






Dashboards—Apache

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 more successes than failures after the attack.

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.

Attack Summary—Windows

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

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.

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.

Attack Summary—Windows

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

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.

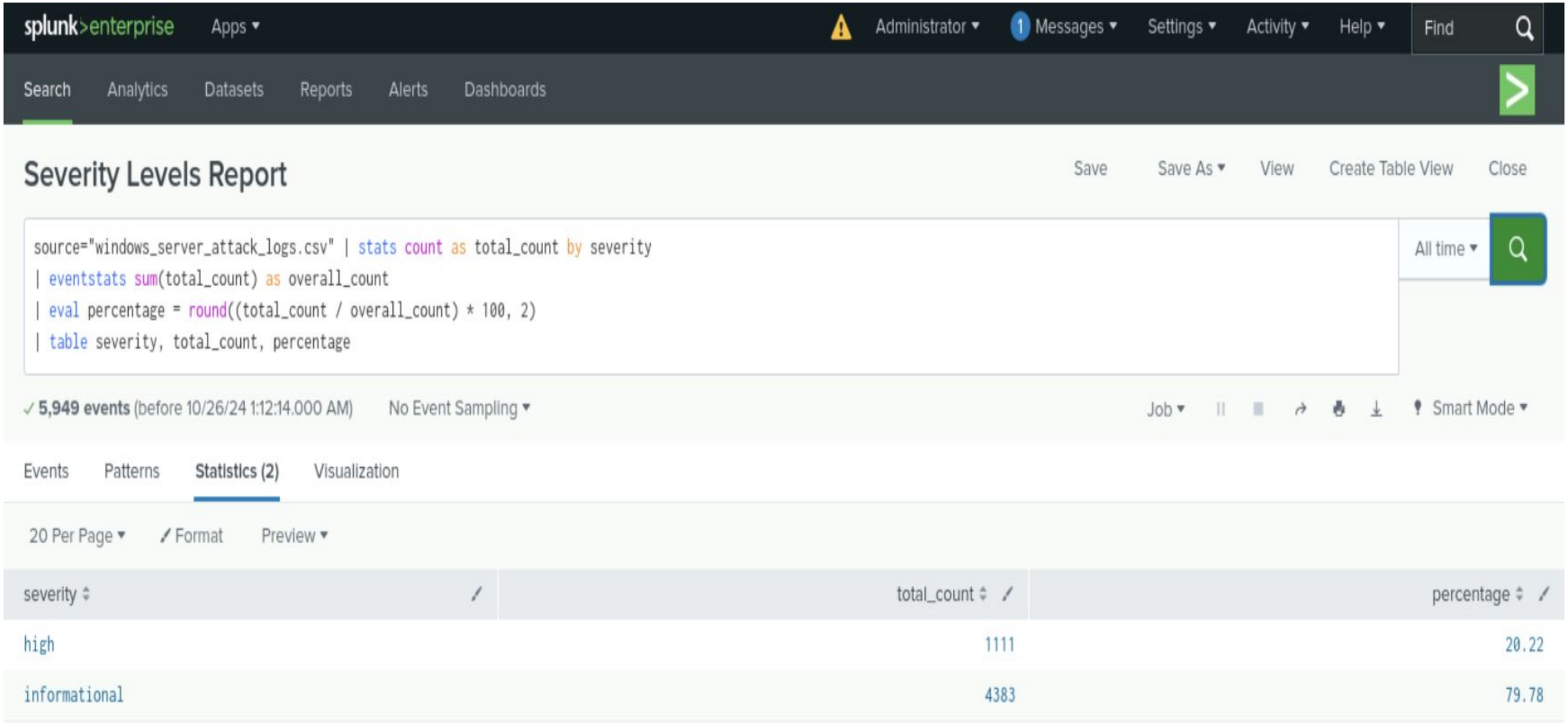
8- Dashboard analysis for signatures with pie charts:

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

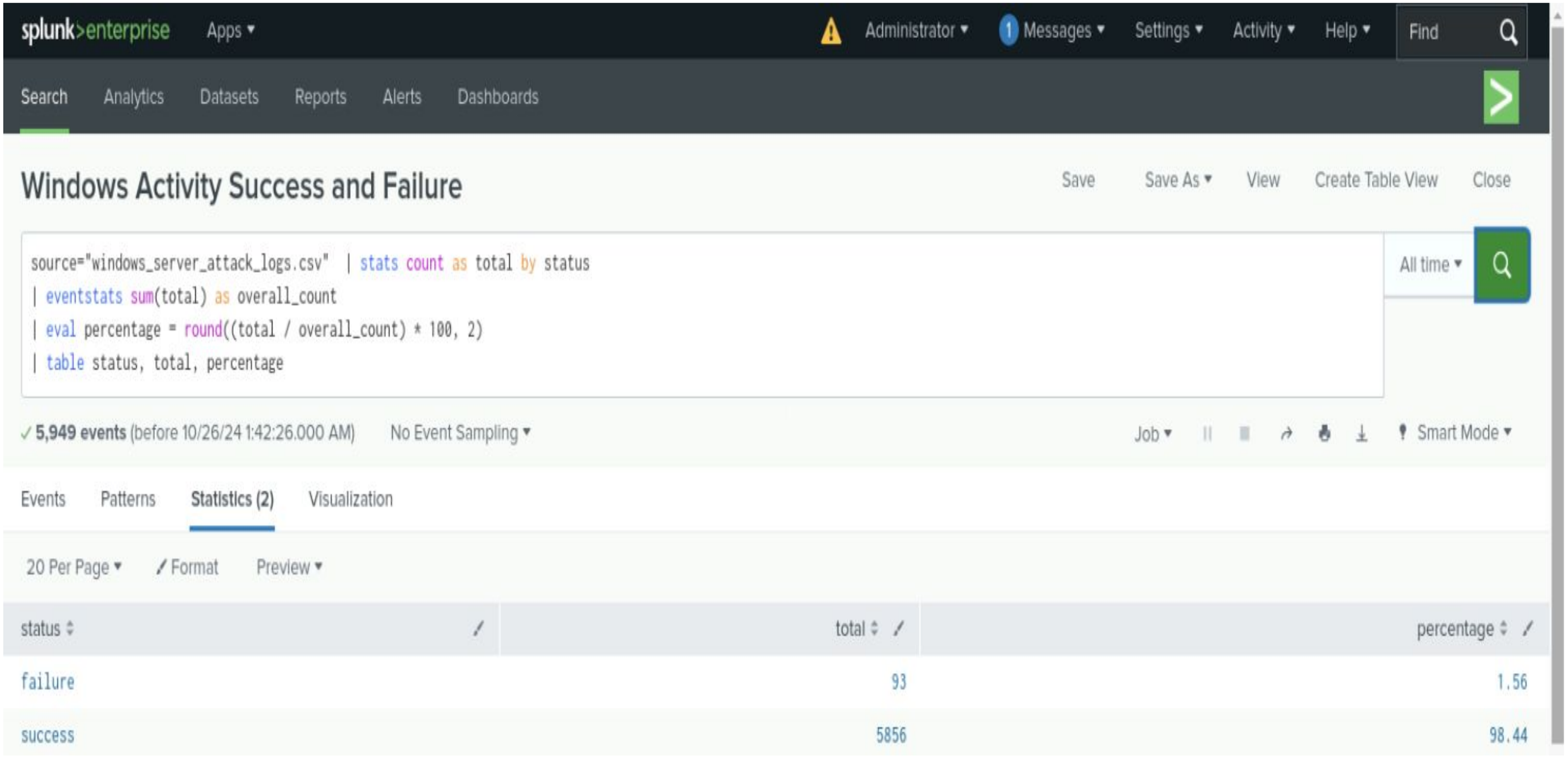
9- Dashboard analysis for users with pie charts:

- There was increased activity for user_a and user_k.

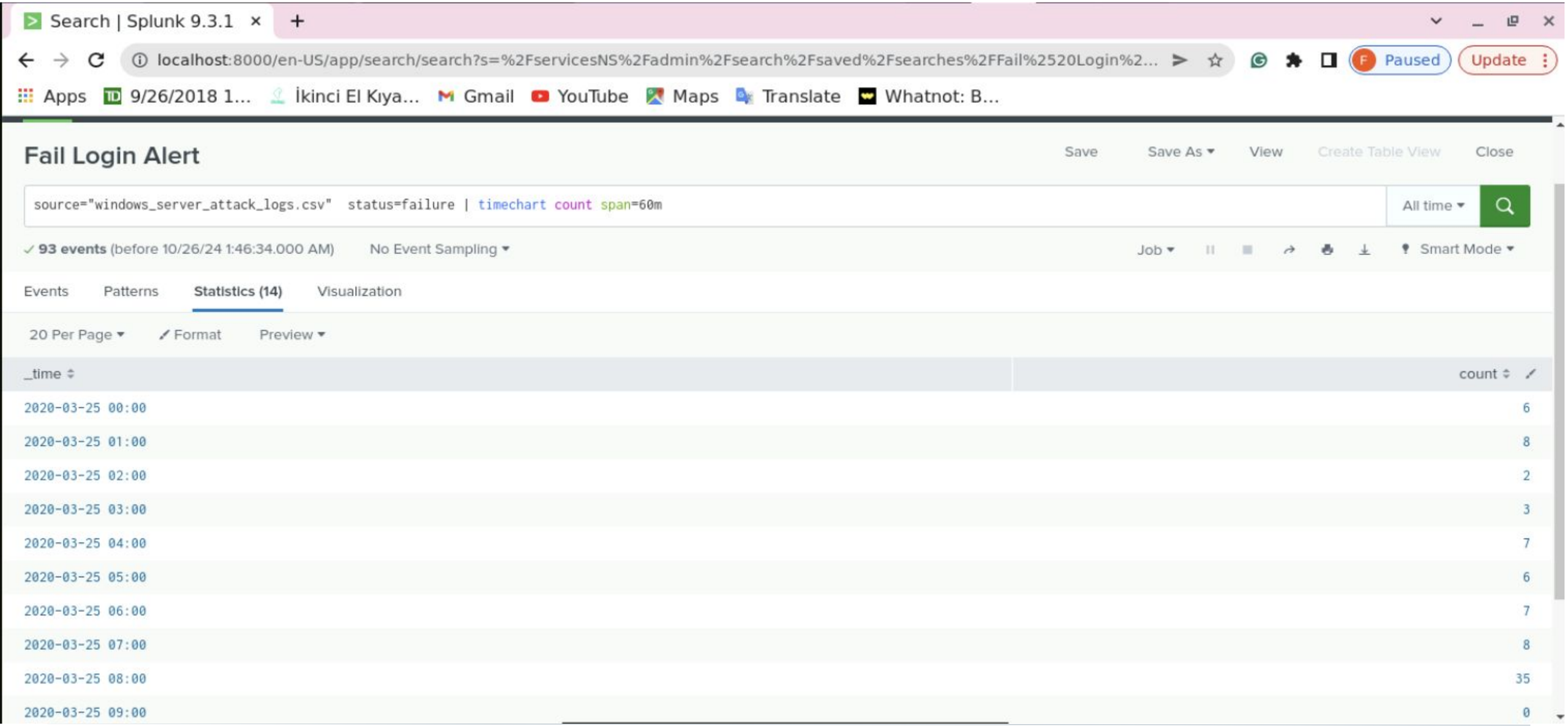
Screenshots of Attack Logs



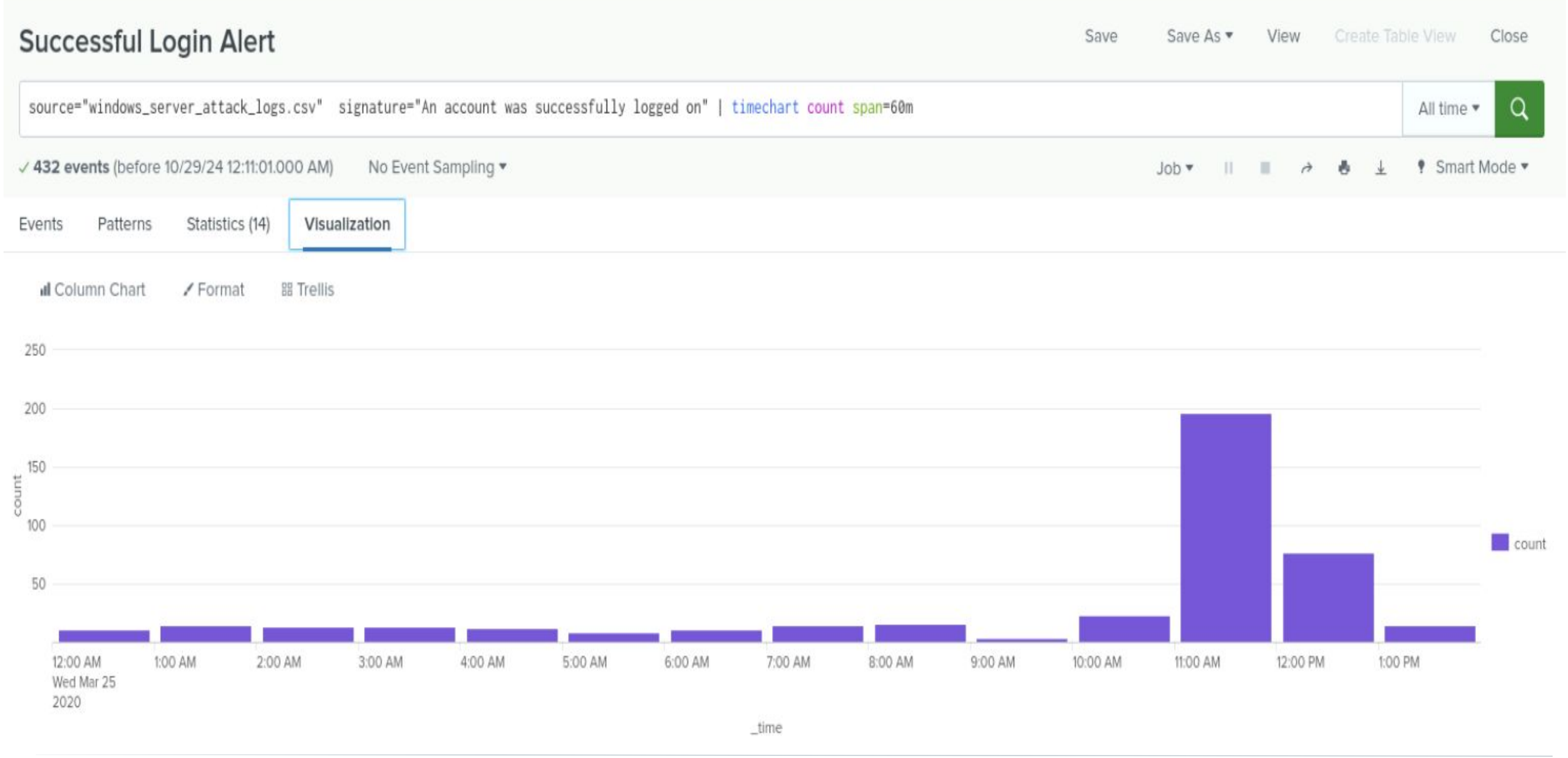
Screenshots of Attack Logs



Screenshots of Attack Logs



Screenshots of Attack Logs



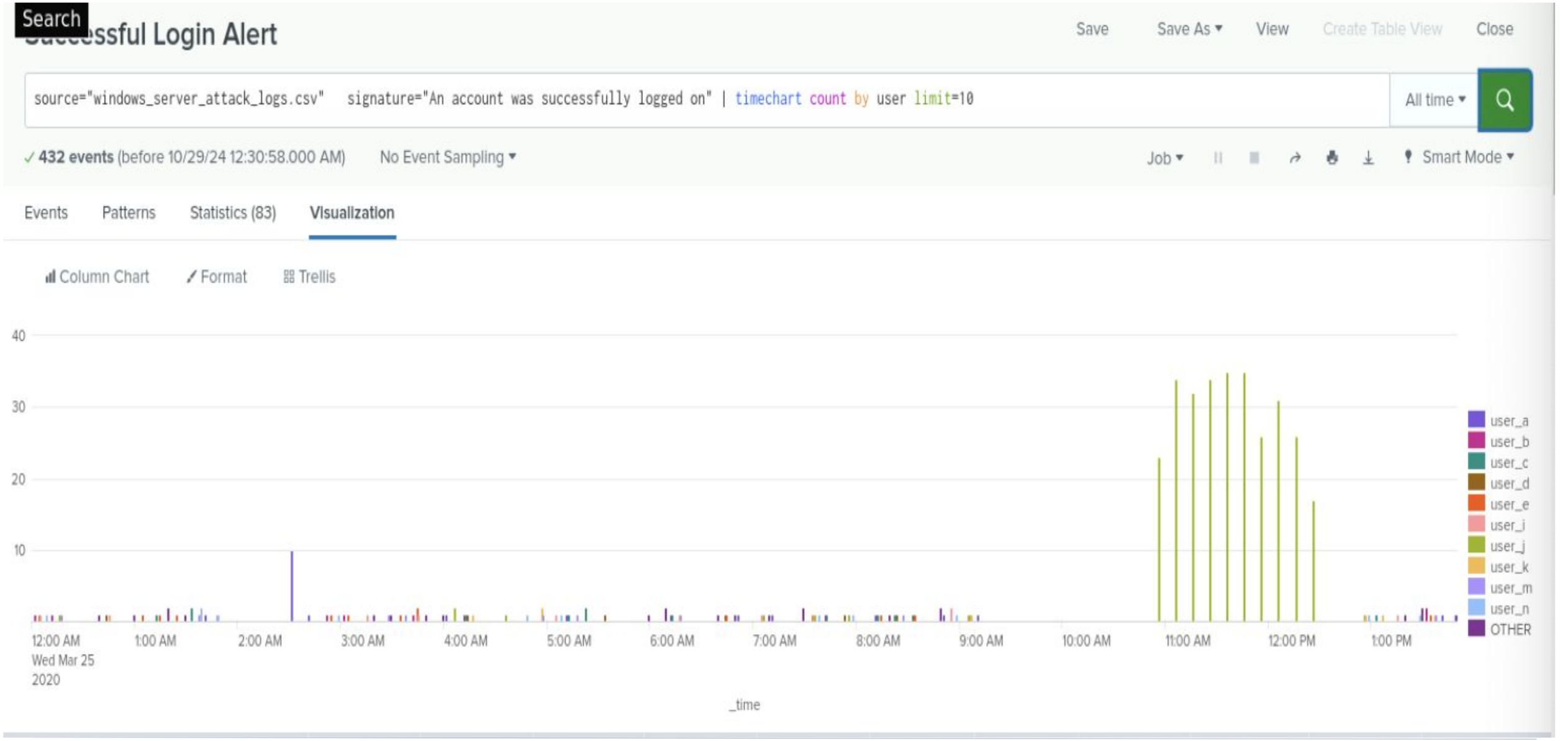
Screenshots of Attack Logs

Events | Patterns | **Statistics (14)** | Visualization

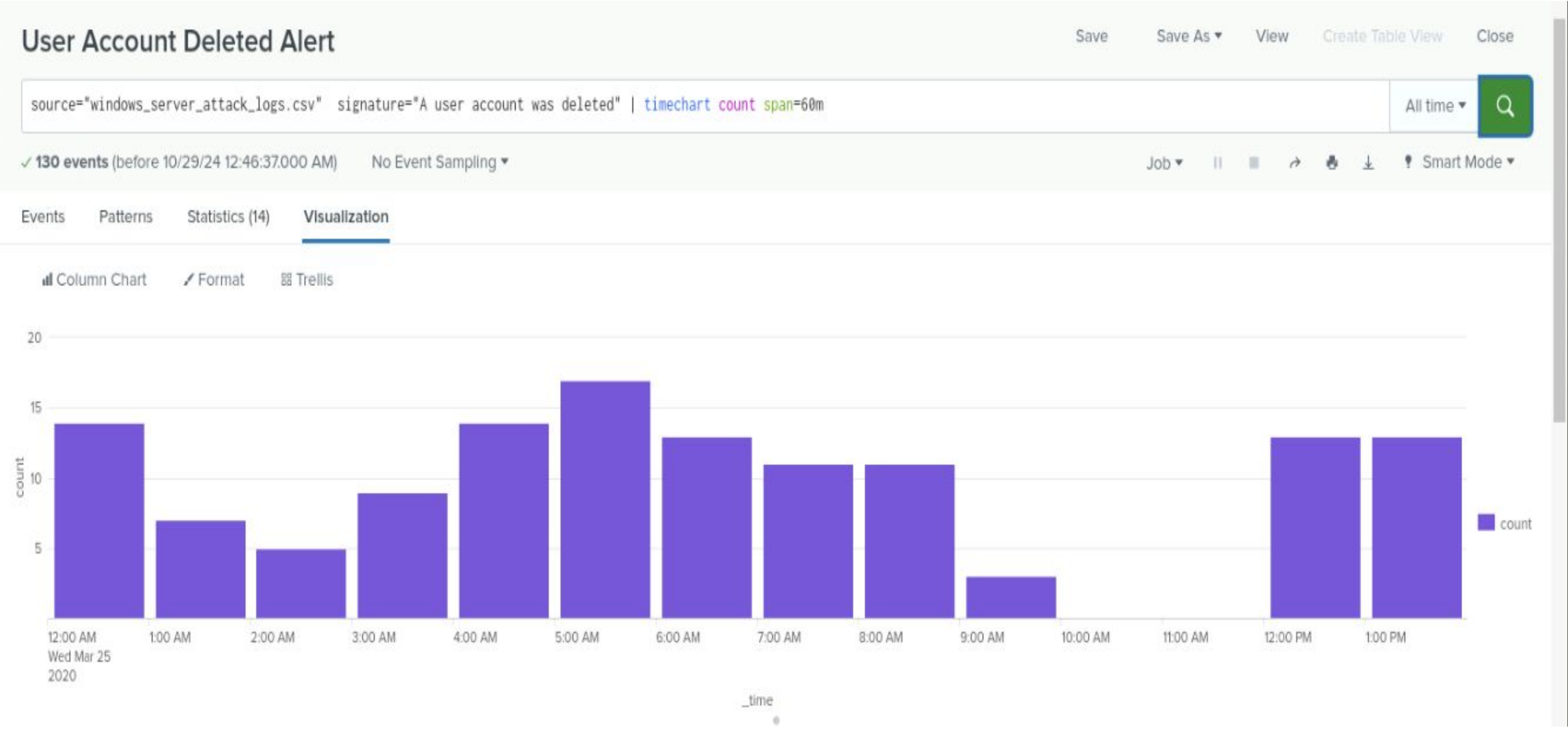
20 Per Page ▾ | Format | Preview ▾

_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

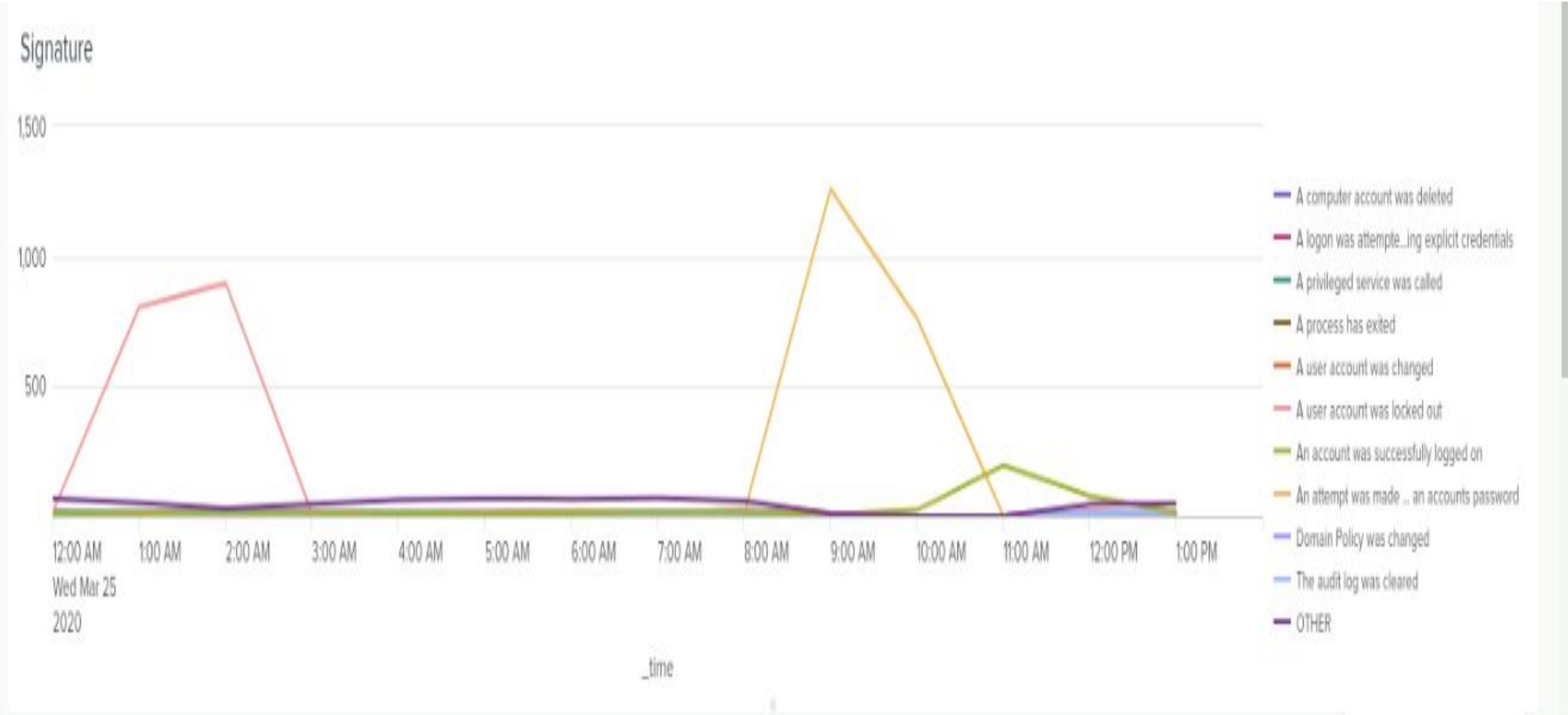
Screenshots of Attack Logs



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

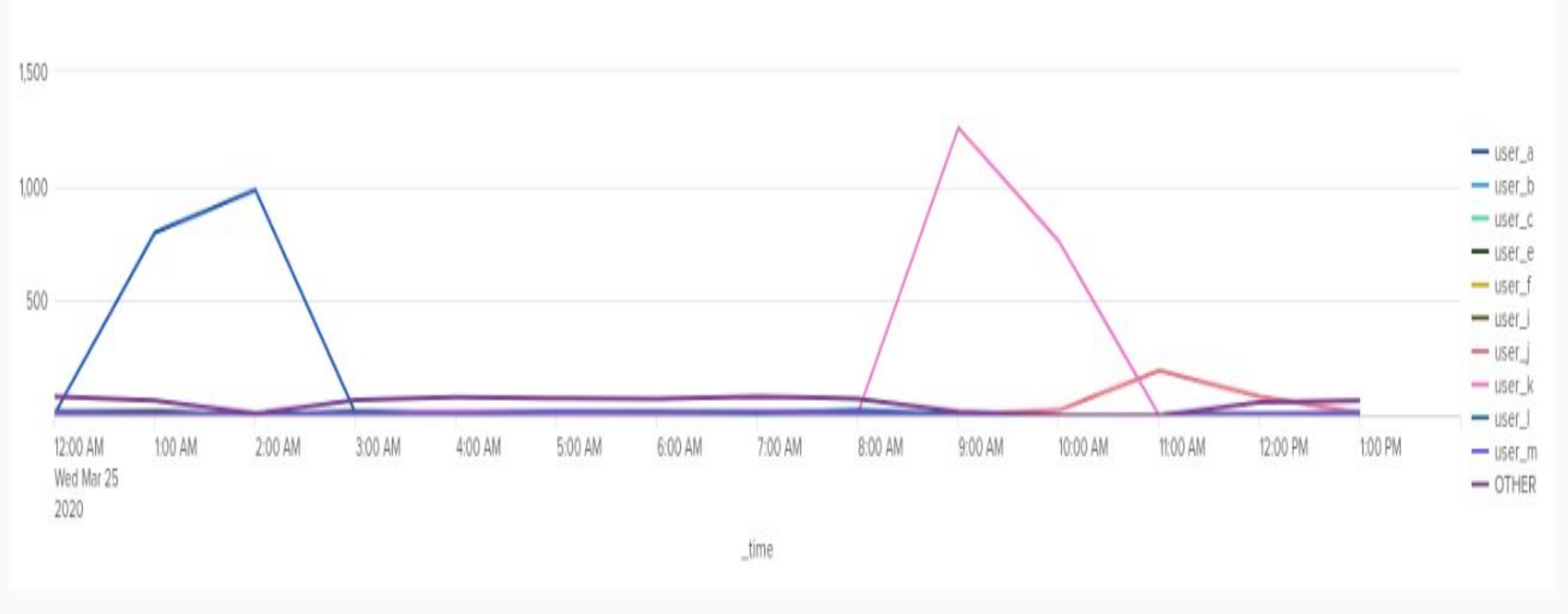
✓ **5,949 events** (before 10/26/24 3:39:16.000 PM) No Event Sampling Job Smart Mode

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

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

All time

✓ **5,949 events** (before 10/26/24 3:54:26.000 PM) No Event Sampling

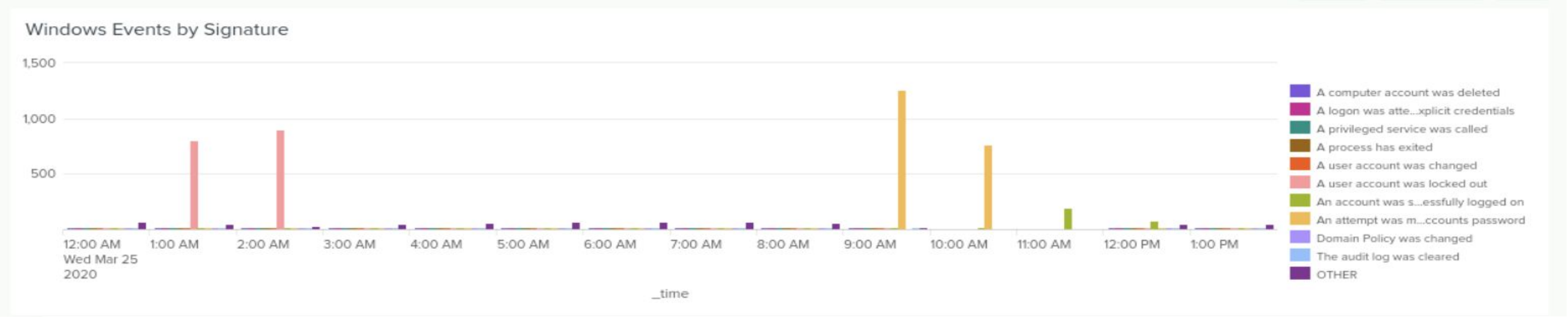
Job Smart Mode

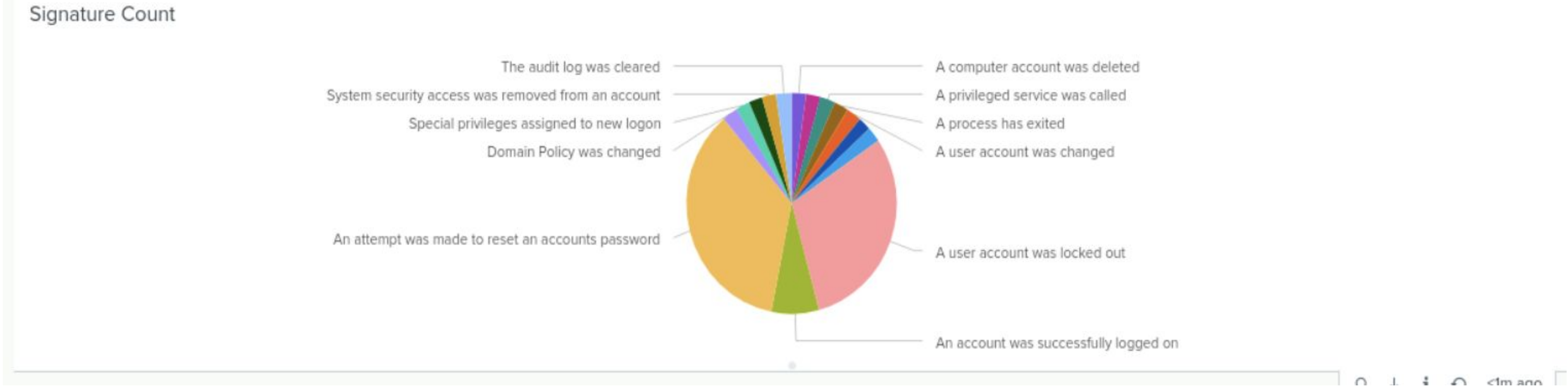
Events Patterns **Statistics (14)** Visualization

20 Per Page Format Preview

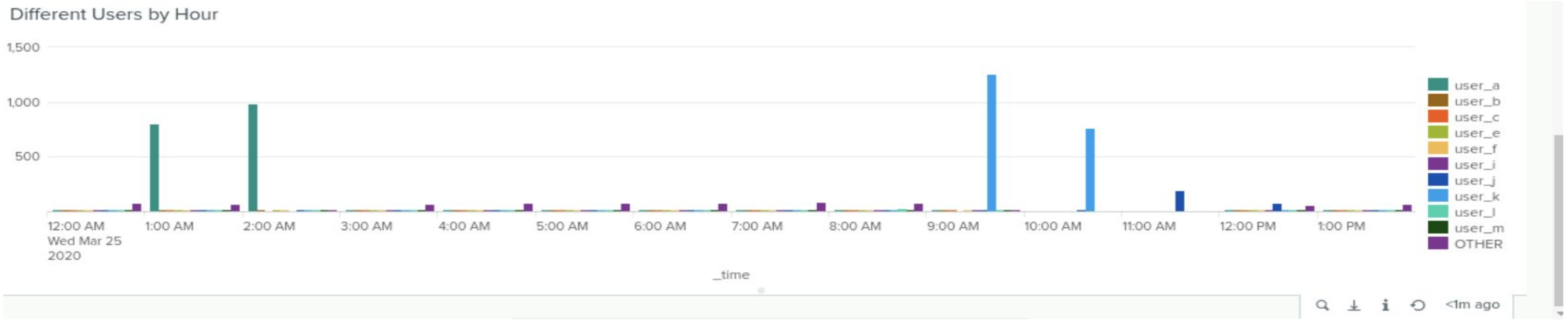
_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16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

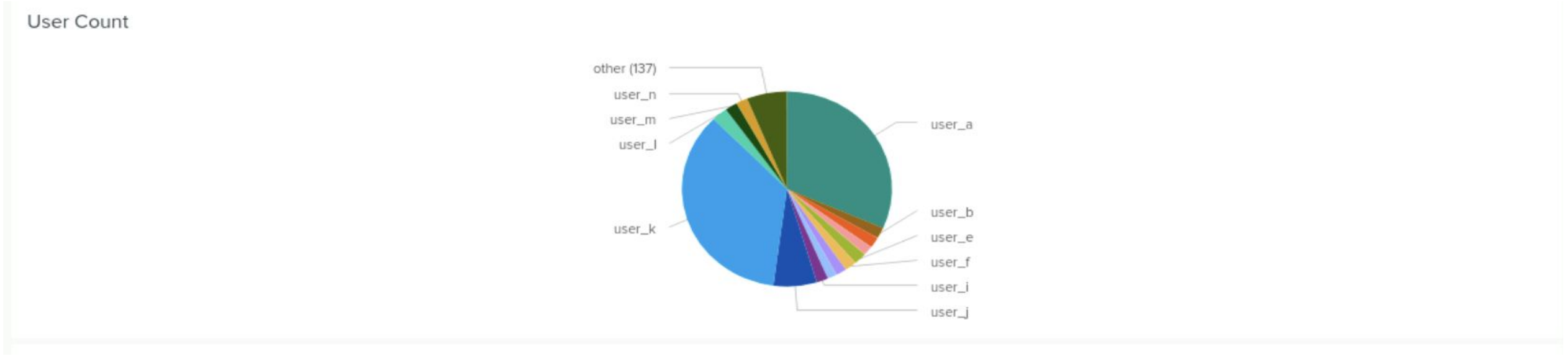
Screenshots of Attack Logs





Screenshots of Attack Logs





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.

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.

Attack Summary—Apache

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

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.

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.

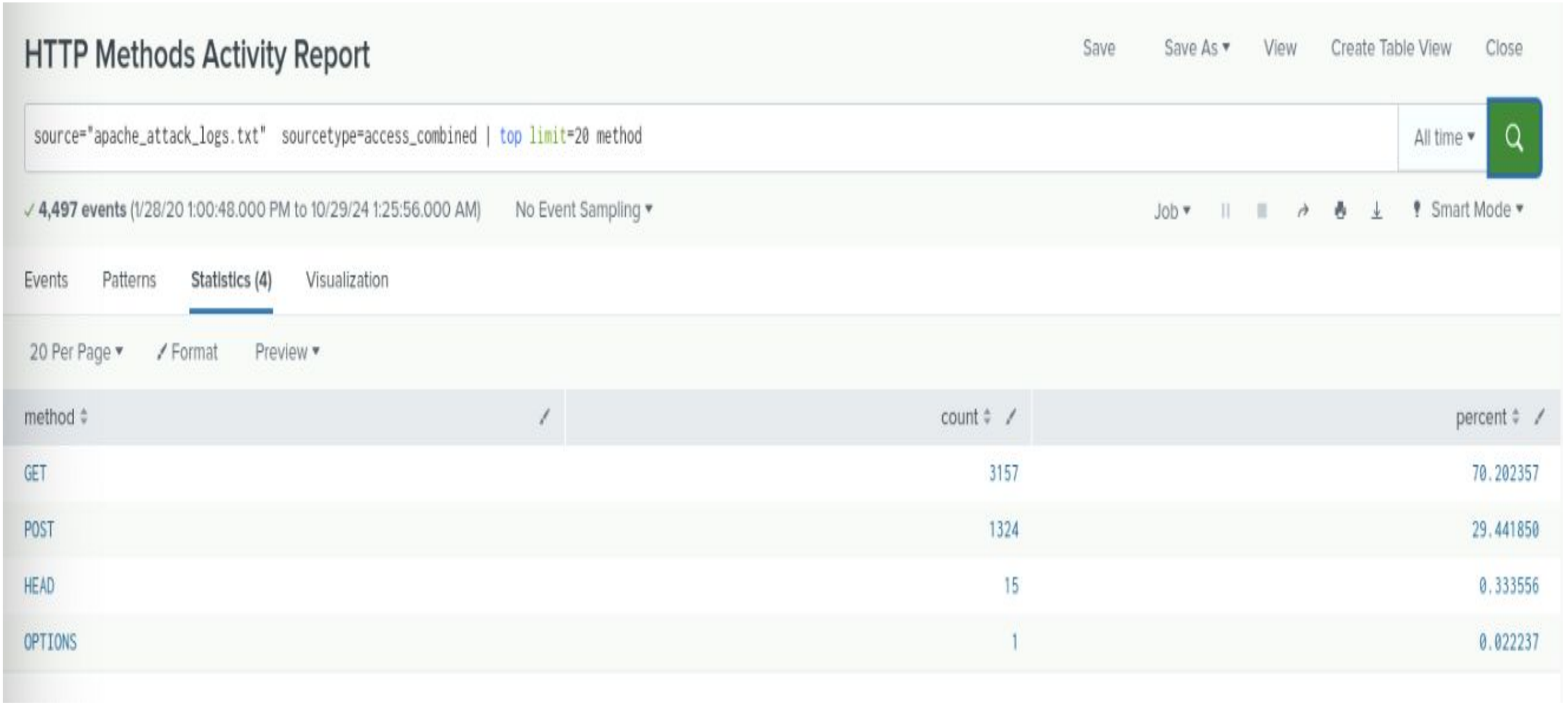
Attack Summary—Apache

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

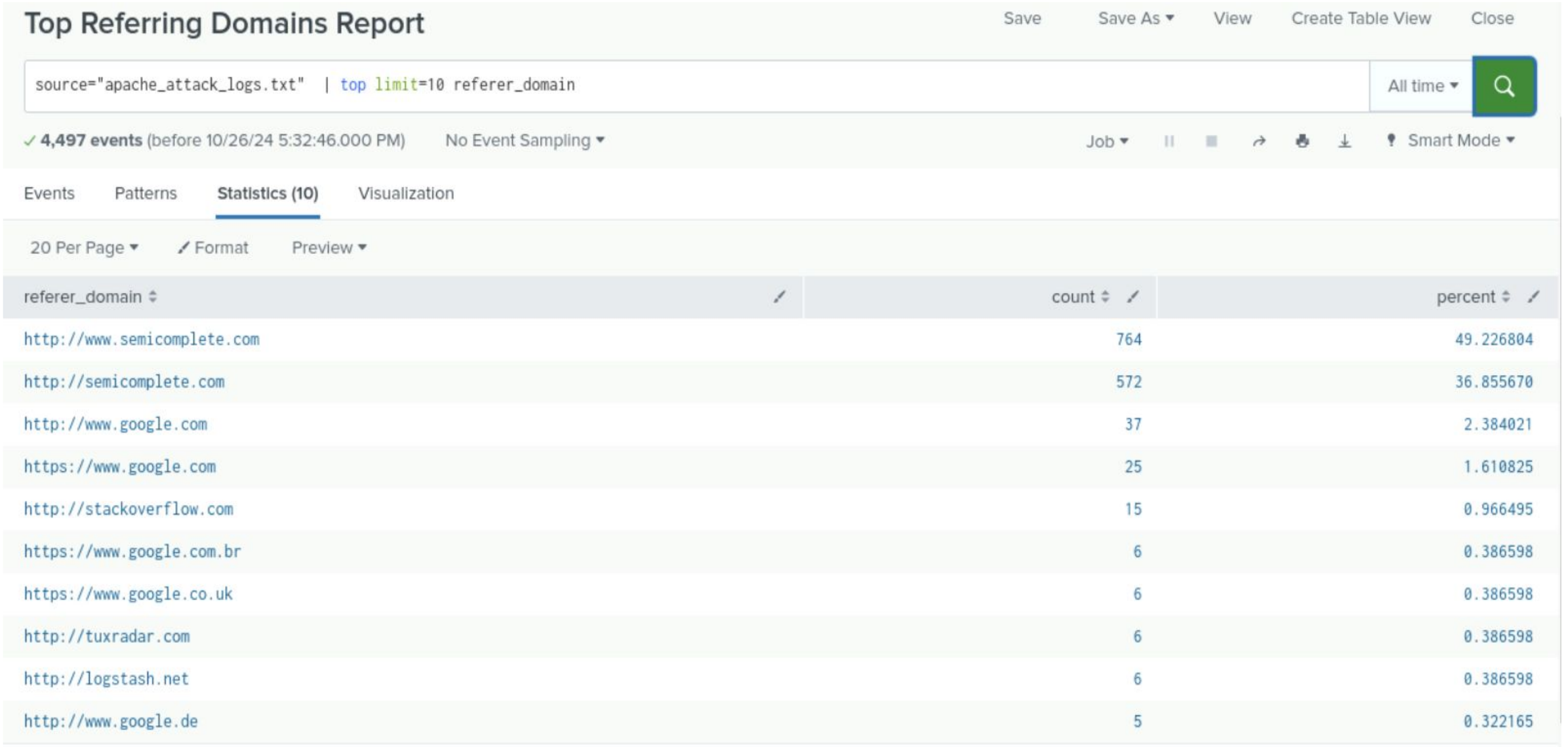
8- Dashboard analysis for URI Data:

- 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



Screenshots of Attack Logs



Top Referring Domains Report

Save Save As View Create Table View Close

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

All time

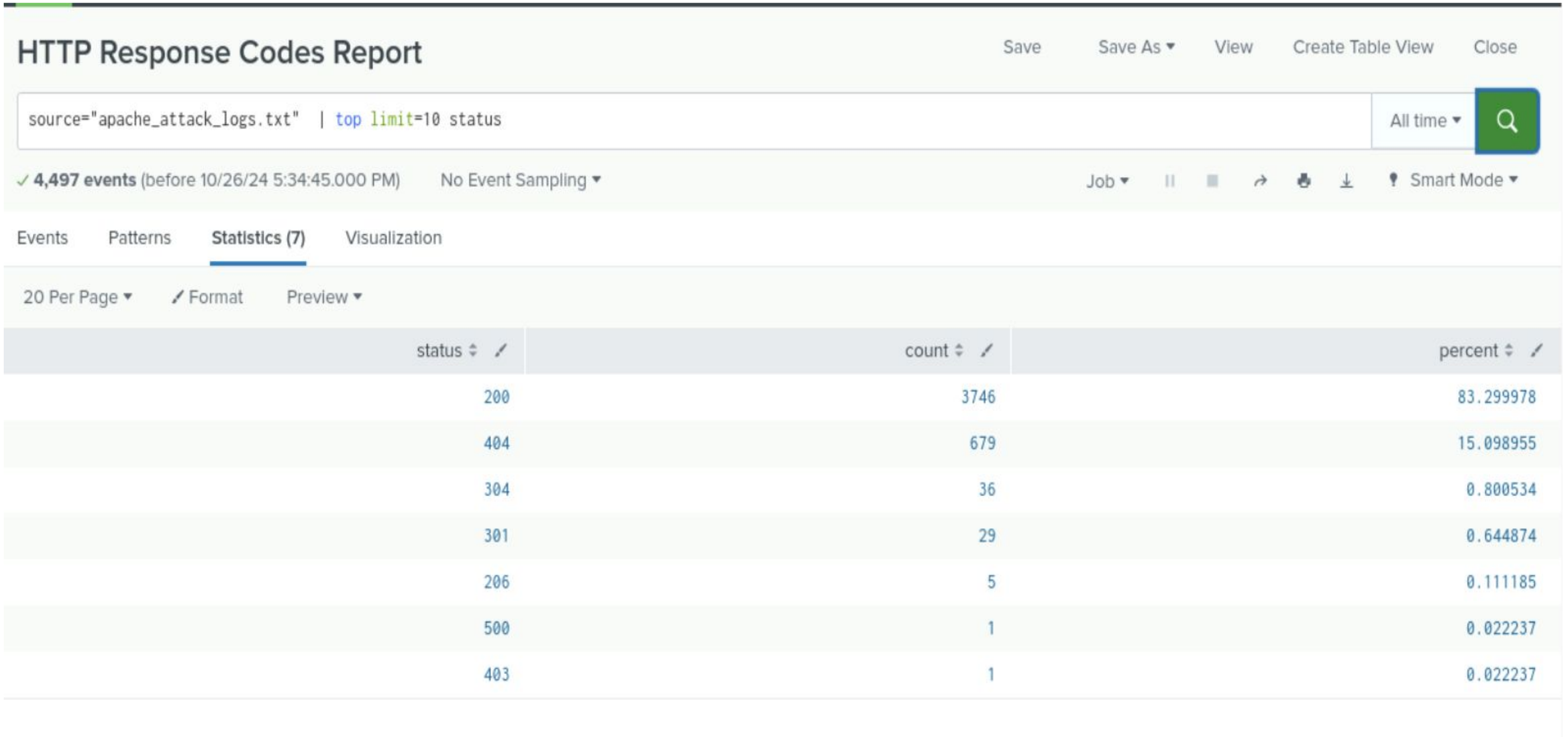
✓ 4,497 events (before 10/26/24 5:32:46.000 PM) No Event Sampling Job Smart Mode

Events Patterns Statistics (10) Visualization

20 Per Page Format Preview

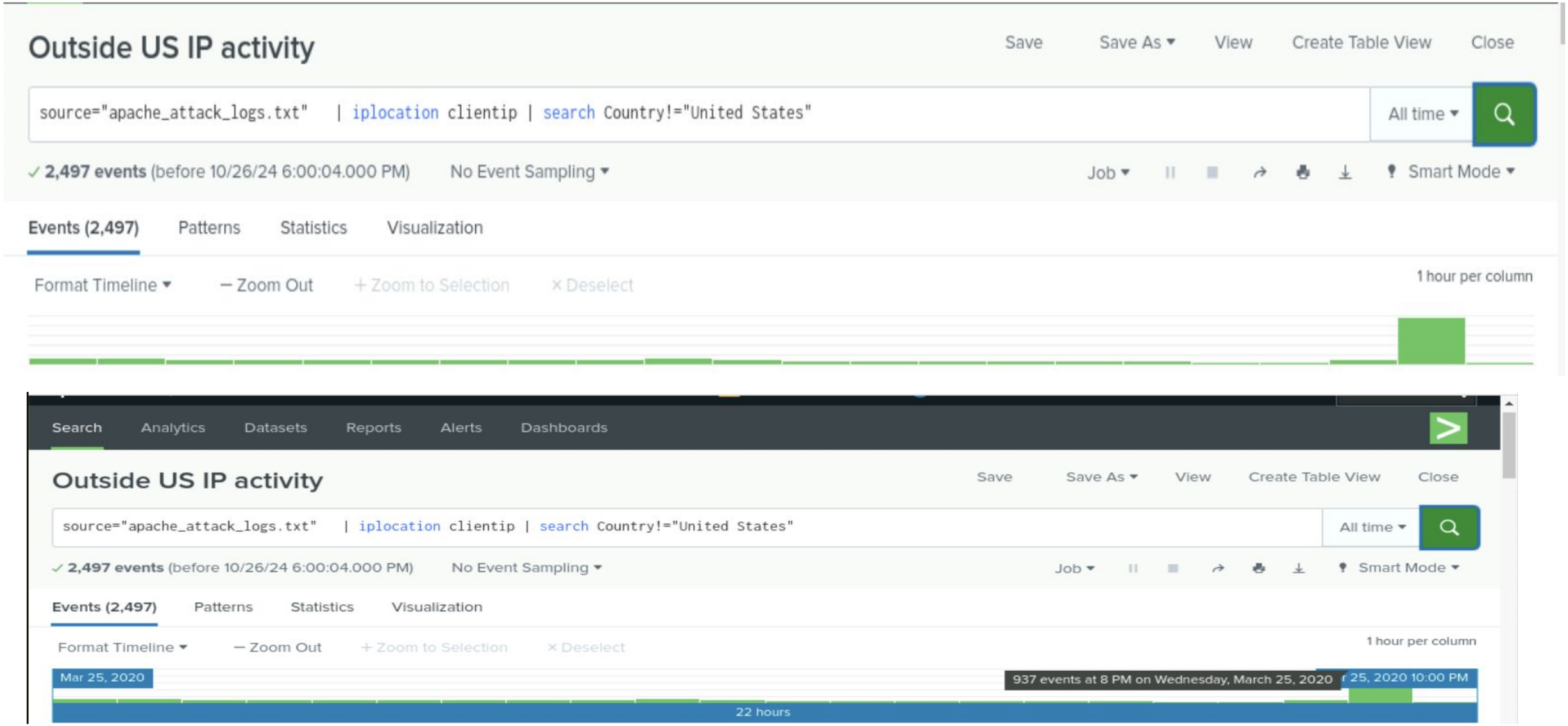
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com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

Screenshots of Attack Logs

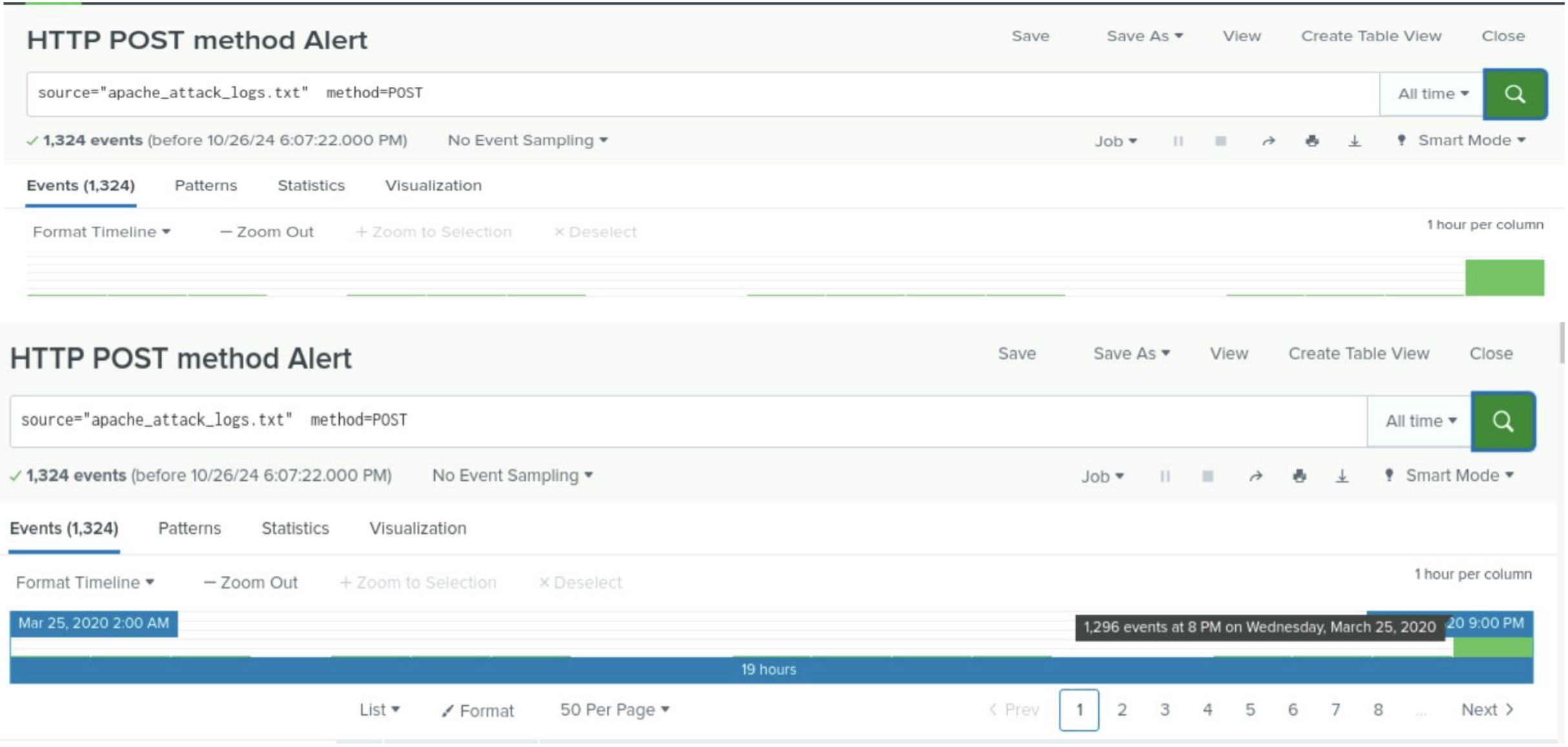


status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

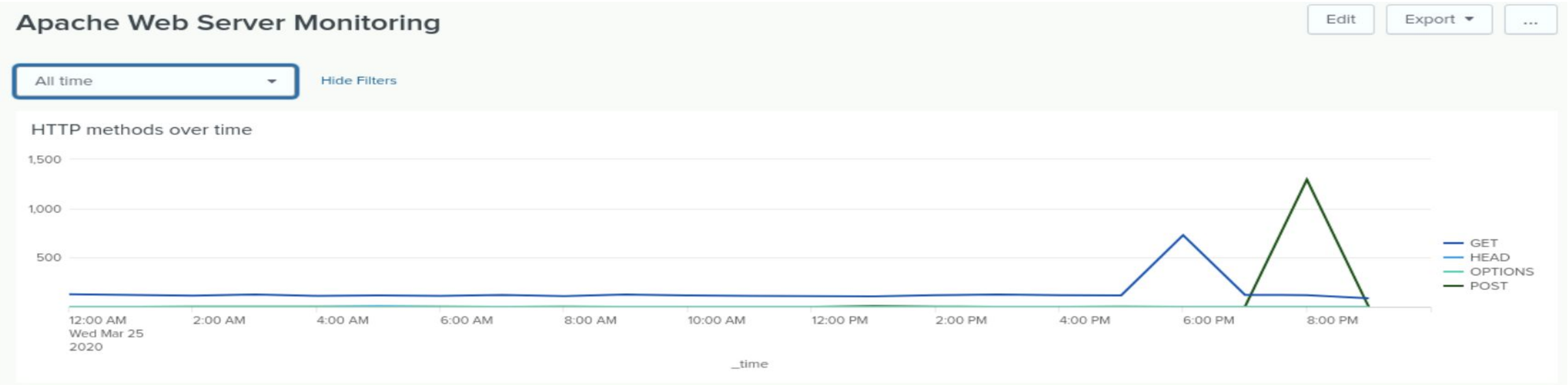
Screenshots of Attack Logs

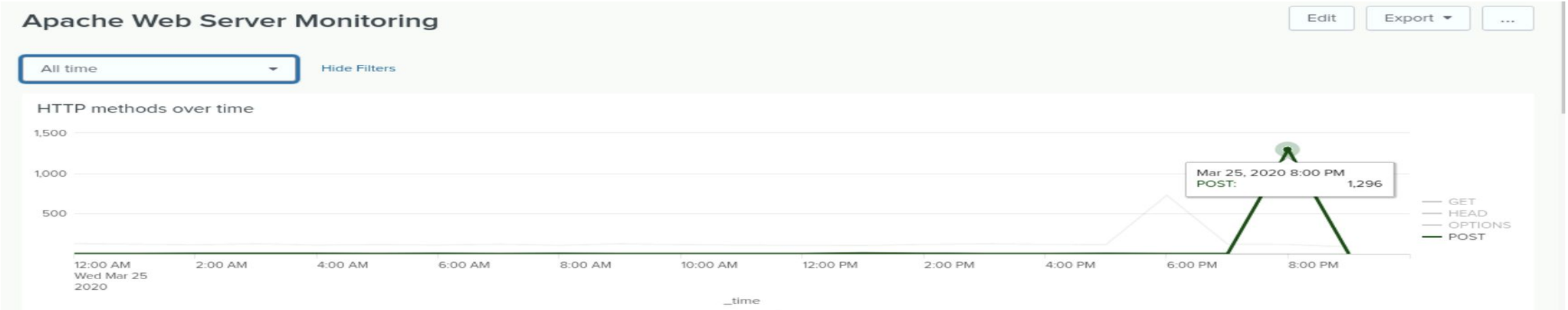


Screenshots of Attack Logs

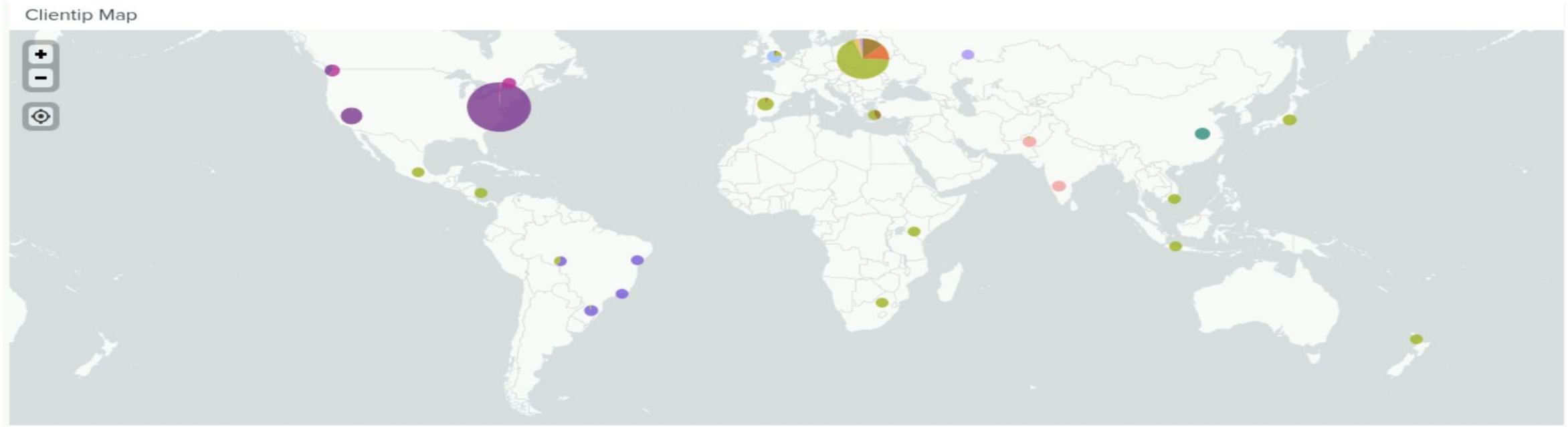


Screenshots of Attack Logs





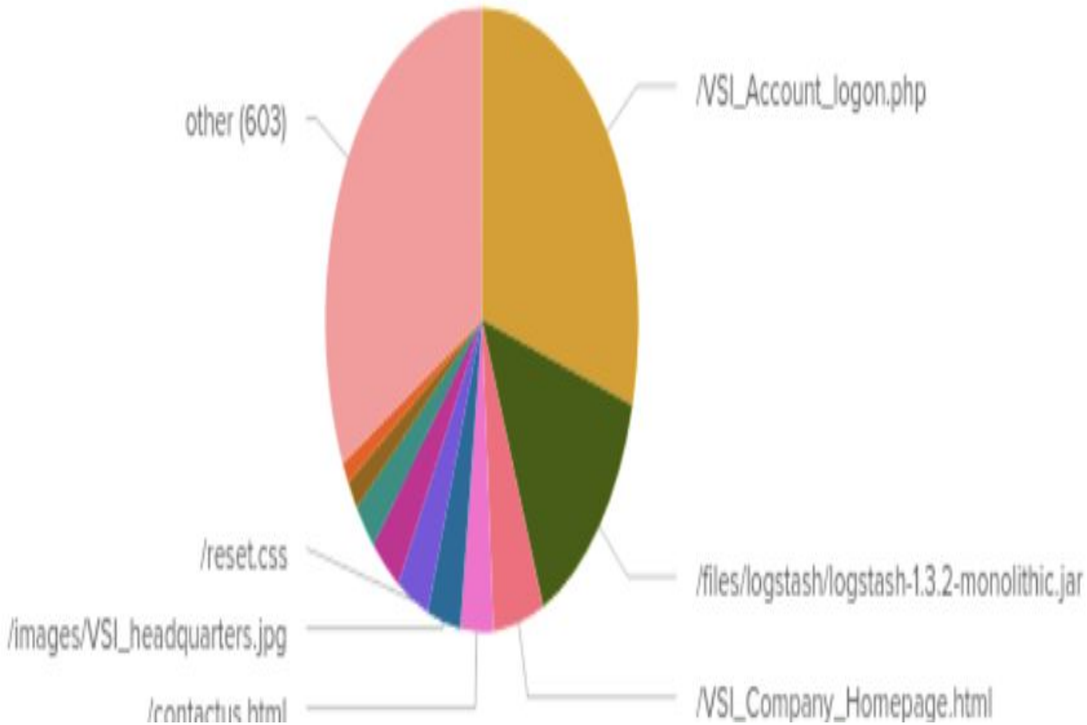
Screenshots of Attack Logs



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.