Defensive Security Project

by: Jake Clary, Matt Palmer, Hetvi Patel, Seth Kyker, Sydney Sharp, and Jason Holder.

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

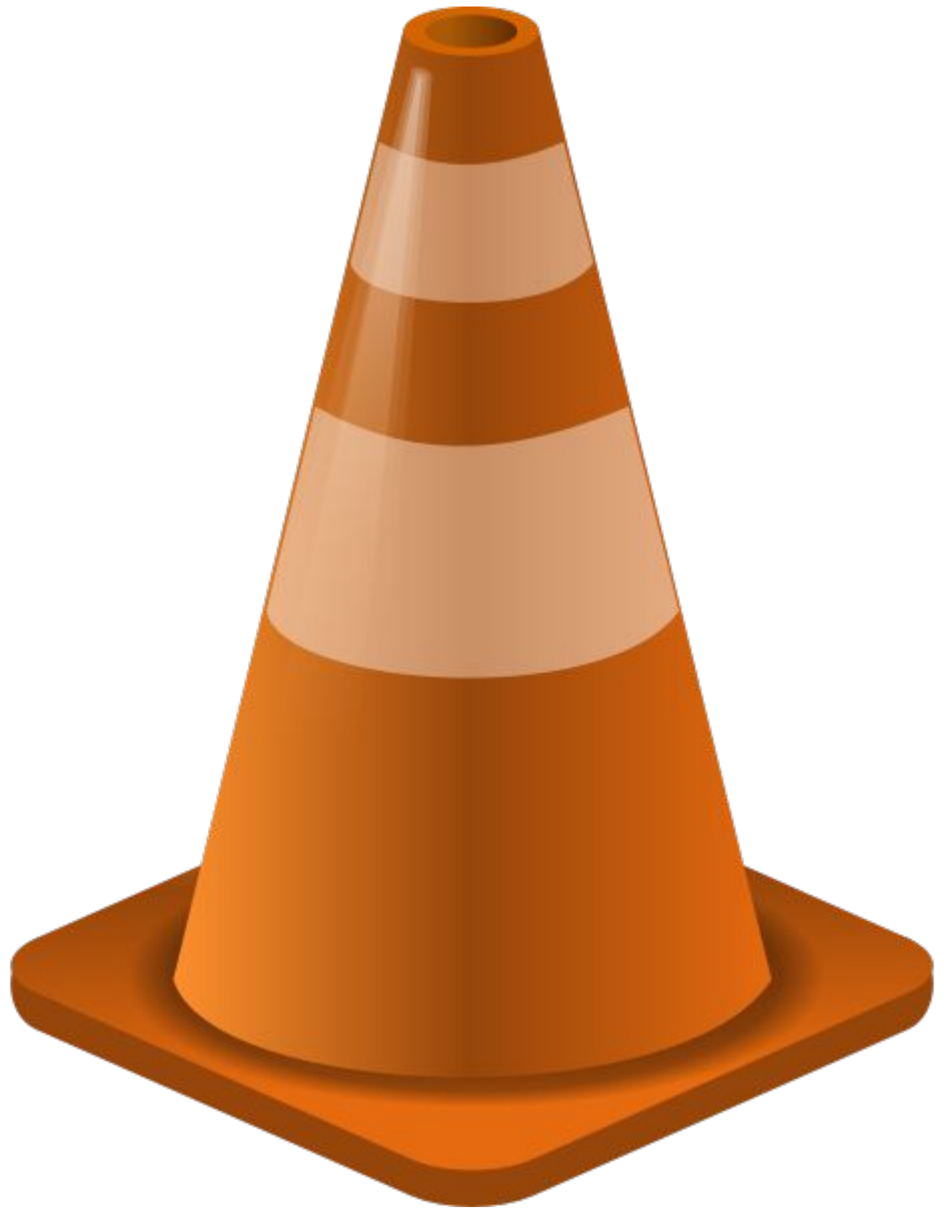
03

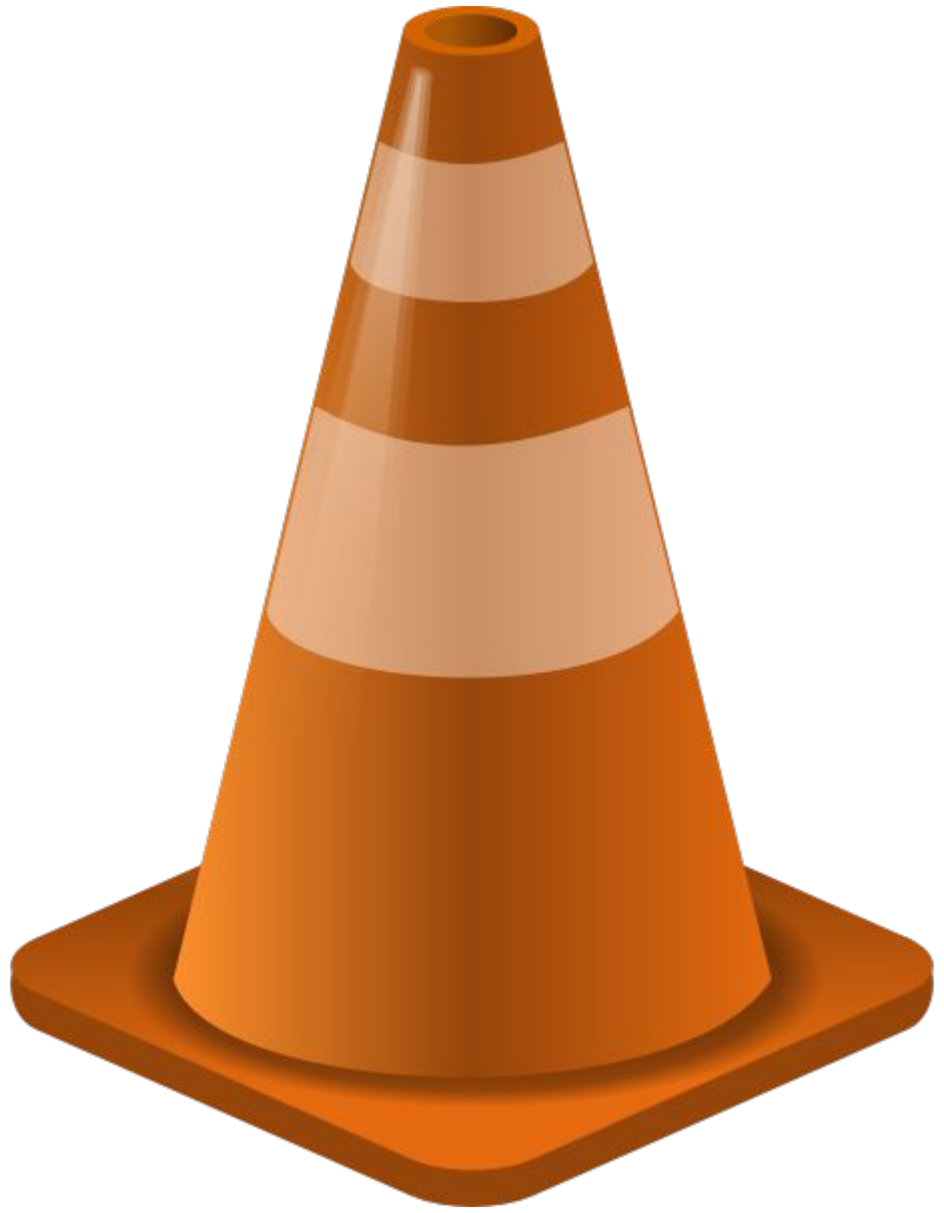
Project Summary & Future Mitigations

Monitoring Environment

Scenario

- We were tasked to observe a websites traffic, set up alerts that are outside of the baseline and alert a SOC analyst if the traffic is outside of the regular traffic.





Website Monitoring App

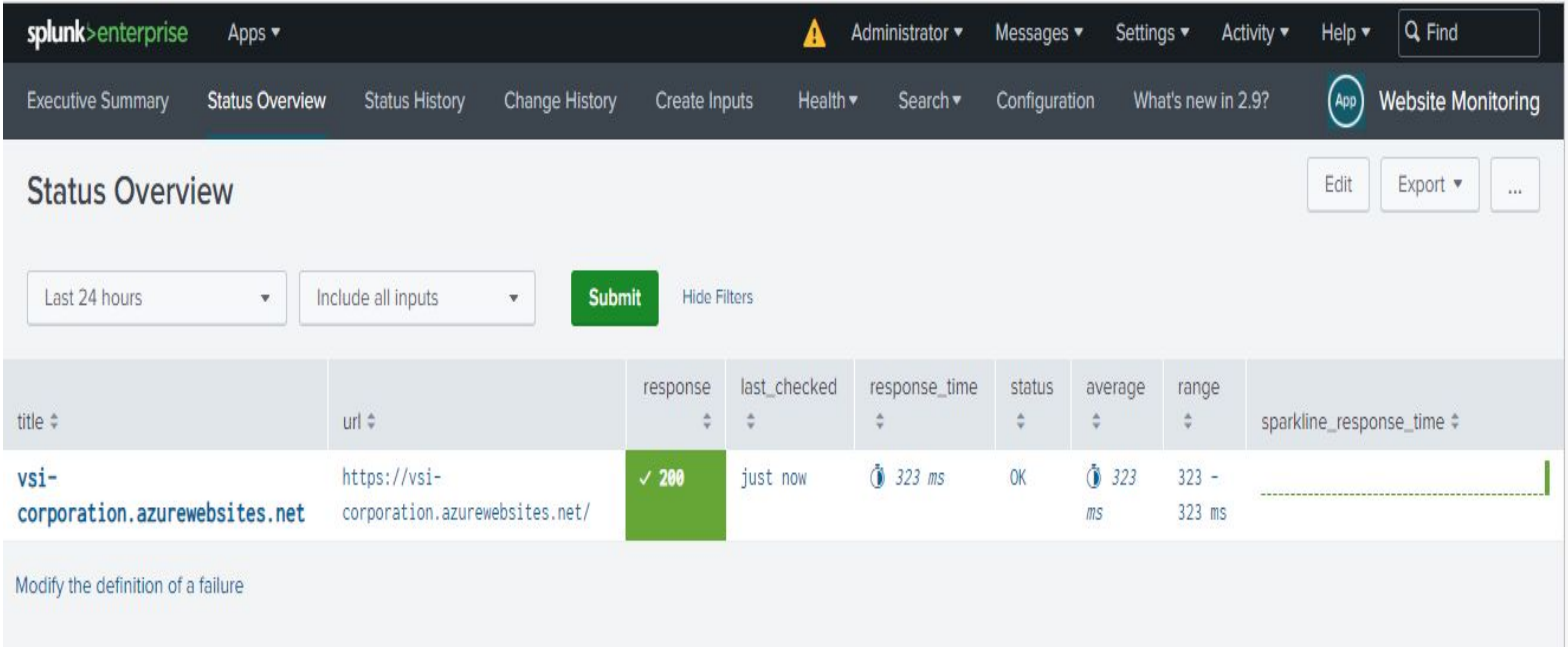
Website Monitoring

We chose the website monitoring tool. This tool allowed us to detect if the website we were monitoring was having any downtime and/or performance problems, and it is easy to set up, taking 5 minutes or less.

Website Monitoring

In addition to this tool's ability to tell us if the website is alive or having performance issues, this add on also gives us information about the server. It provides a response code, when it was last checked, the response time, status, the average time as well as the range.

Website Monitoring



Status Overview

Last 24 hours ▾

Include all inputs ▾

title	url	response	last_checked	response_time	status	average	range	sparkline_response_time
vsi-corporation.azurewebsites.net	https://vsi-corporation.azurewebsites.net/	✓ 200	just now	323 ms	OK	323 ms	323 - 323 ms	

Modify the definition of a failure

Logs Analyzed

1 Windows Logs

These logs contained information for:

- signature ID’s in the environment, such as an account was deleted, a password was changed, or an account was successfully logged on.
- severity levels, such as information and high.
- Status, labeling it as success or failure
- and the different users

2 Apache Logs

These logs contained information such as:

- The different HTTP methods
- The domains that refer to the website
- HTTP response codes
- Client IP location’s from all over the world
- Different URI’s that have visited or used the site
-

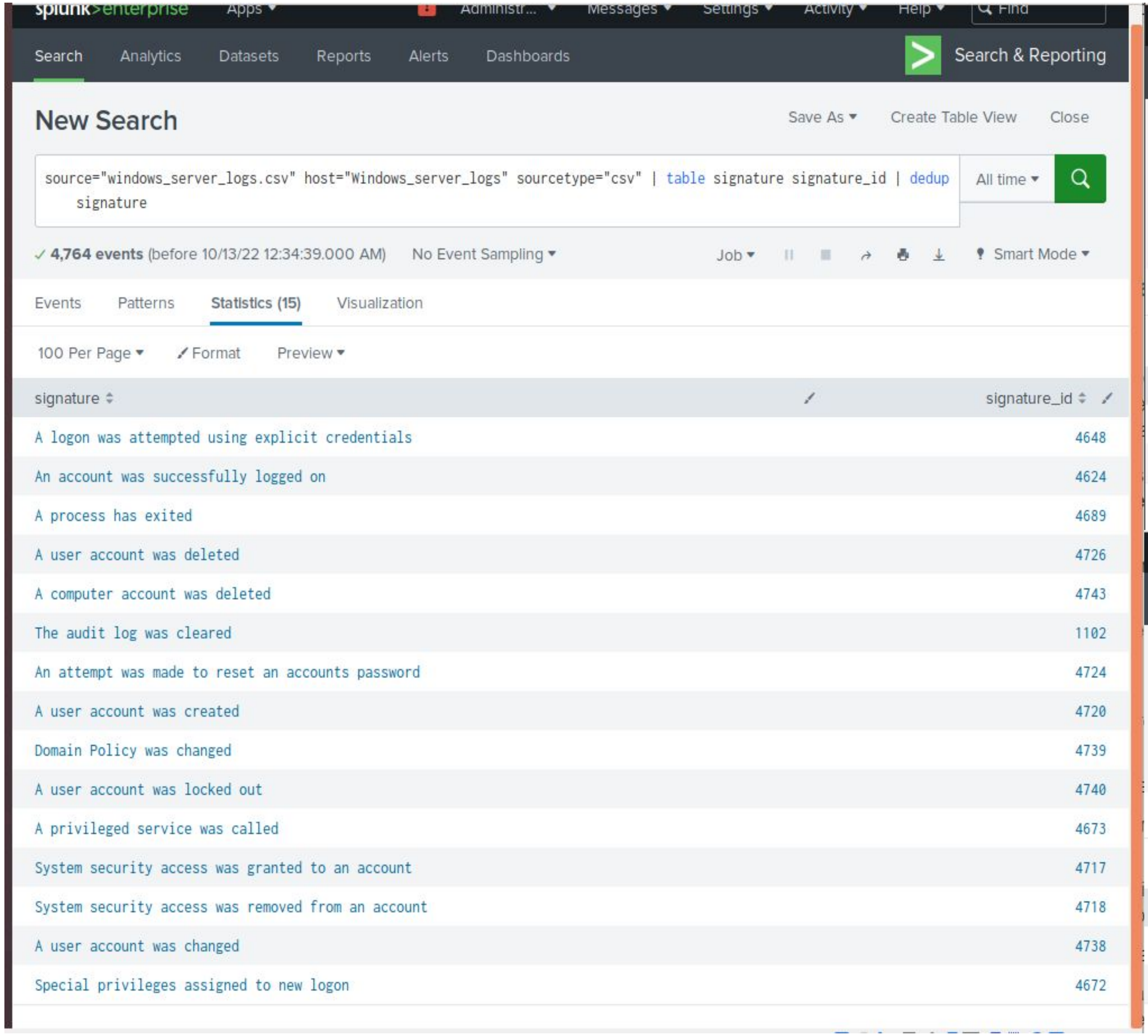
Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Analysis for severity	There was suspicious activity. We found 2222 items listed that were high severity.
Analysis for failed activities	We found suspicious changes in failed activities through decreased failures. There were only 186 failures meaning there was a decrease of 240 failed activities.

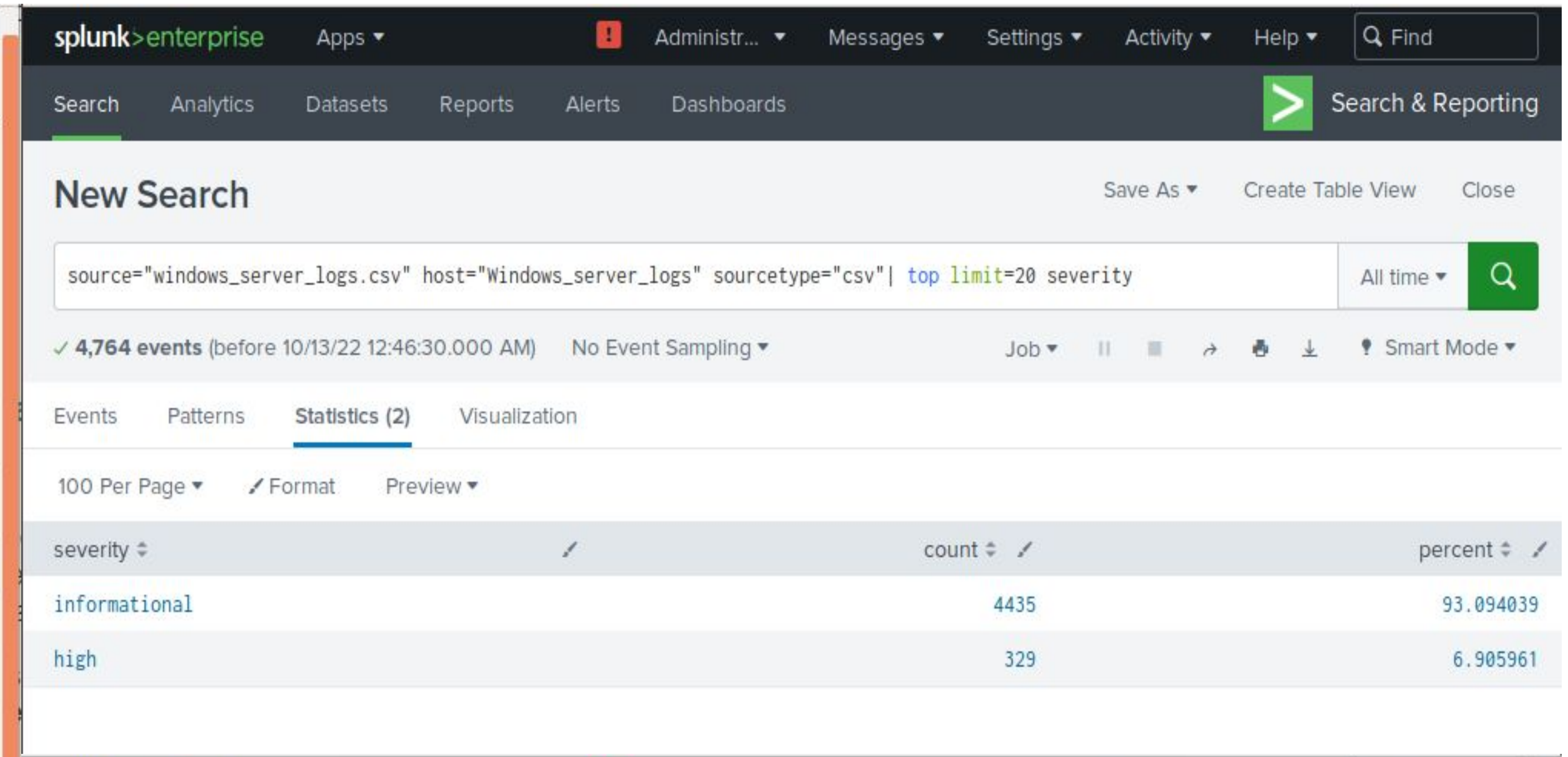
Images of Reports—Windows



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

✓ 4,764 events (before 10/13/22 12:34:39.000 AM) No Event Sampling

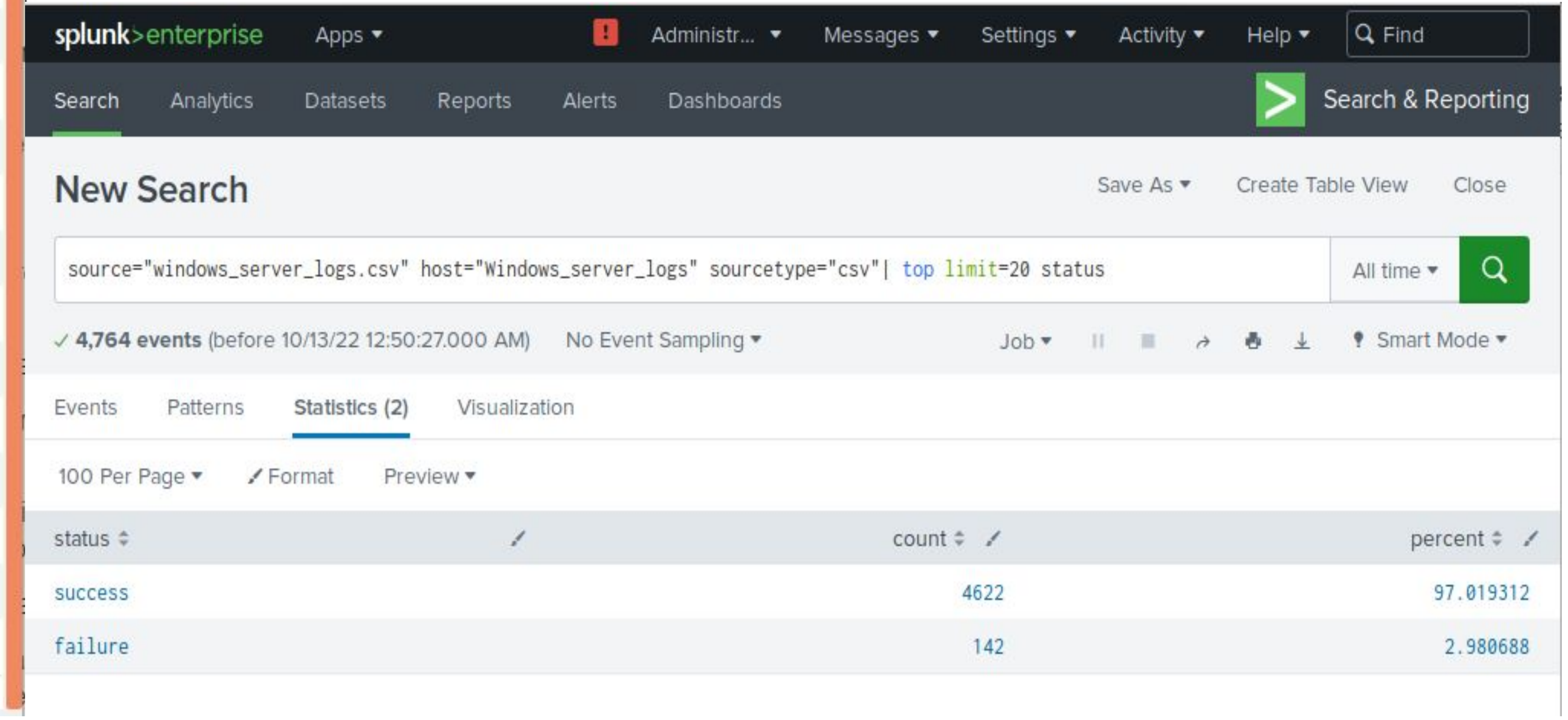
signature	signature_id
A logon was attempted using explicit credentials	4648
An account was successfully logged on	4624
A process has exited	4689
A user account was deleted	4726
A computer account was deleted	4743
The audit log was cleared	1102
An attempt was made to reset an accounts password	4724
A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



```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=20 severity
```

✓ 4,764 events (before 10/13/22 12:46:30.000 AM) No Event Sampling

severity	count	percent
informational	4435	93.094039
high	329	6.905961



```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=20 status
```

✓ 4,764 events (before 10/13/22 12:50:27.000 AM) No Event Sampling

status	count	percent
success	4622	97.019312
failure	142	2.980688

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	Failed Windows Status	10 in 60 mins	20 failed events in 60 minutes

JUSTIFICATION: We felt that 20 failed events in 60 minutes would be abnormal considering it is double the amount of the baseline.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins	Suspicious Amount Of Successful Logins	20 successful logins in 60 minutes	More than 25 accounts successfully logged in.

JUSTIFICATION: The amount of maximum successful logins never went above 21 in the 1 hour time frame. We set the baseline to 20 logins and set an alert to trigger when more than 25 accounts successfully login in a 1 hour window.

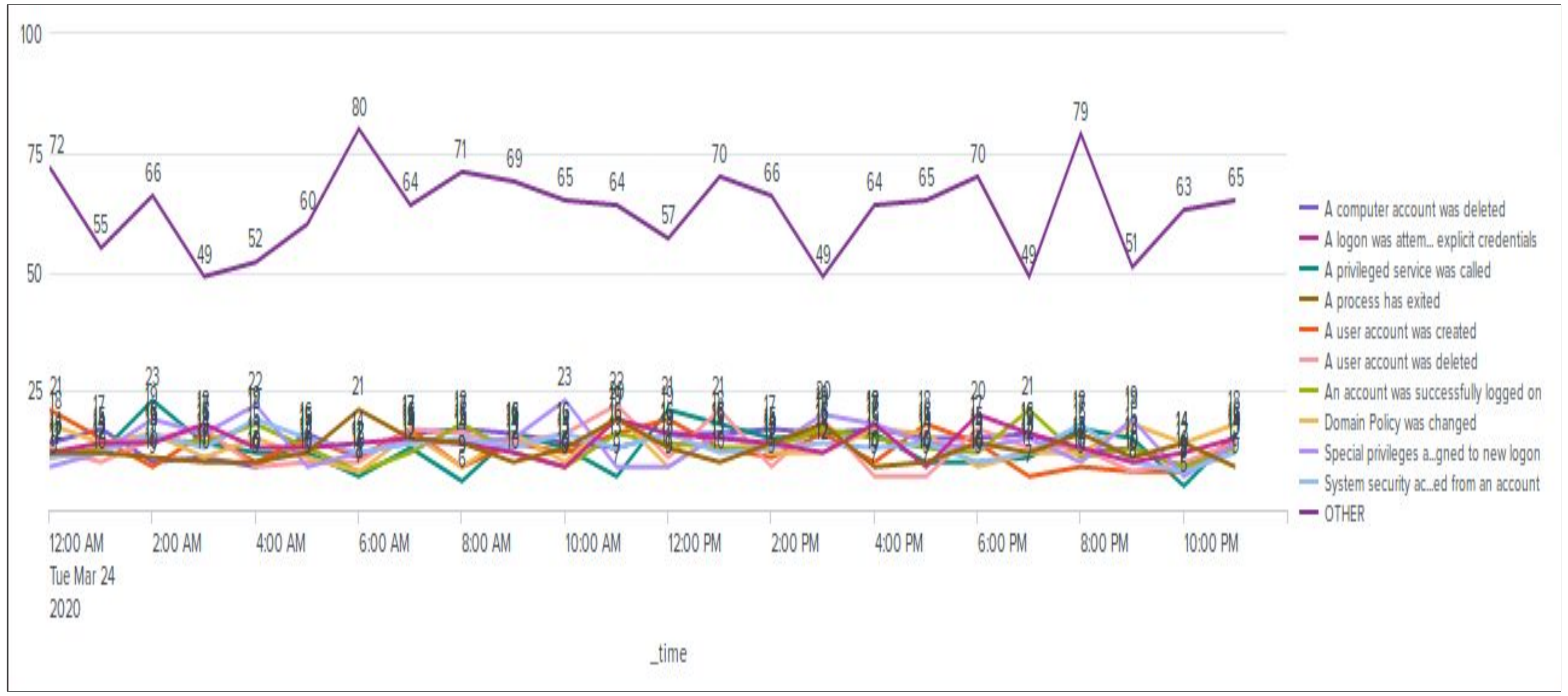
Alerts—Windows

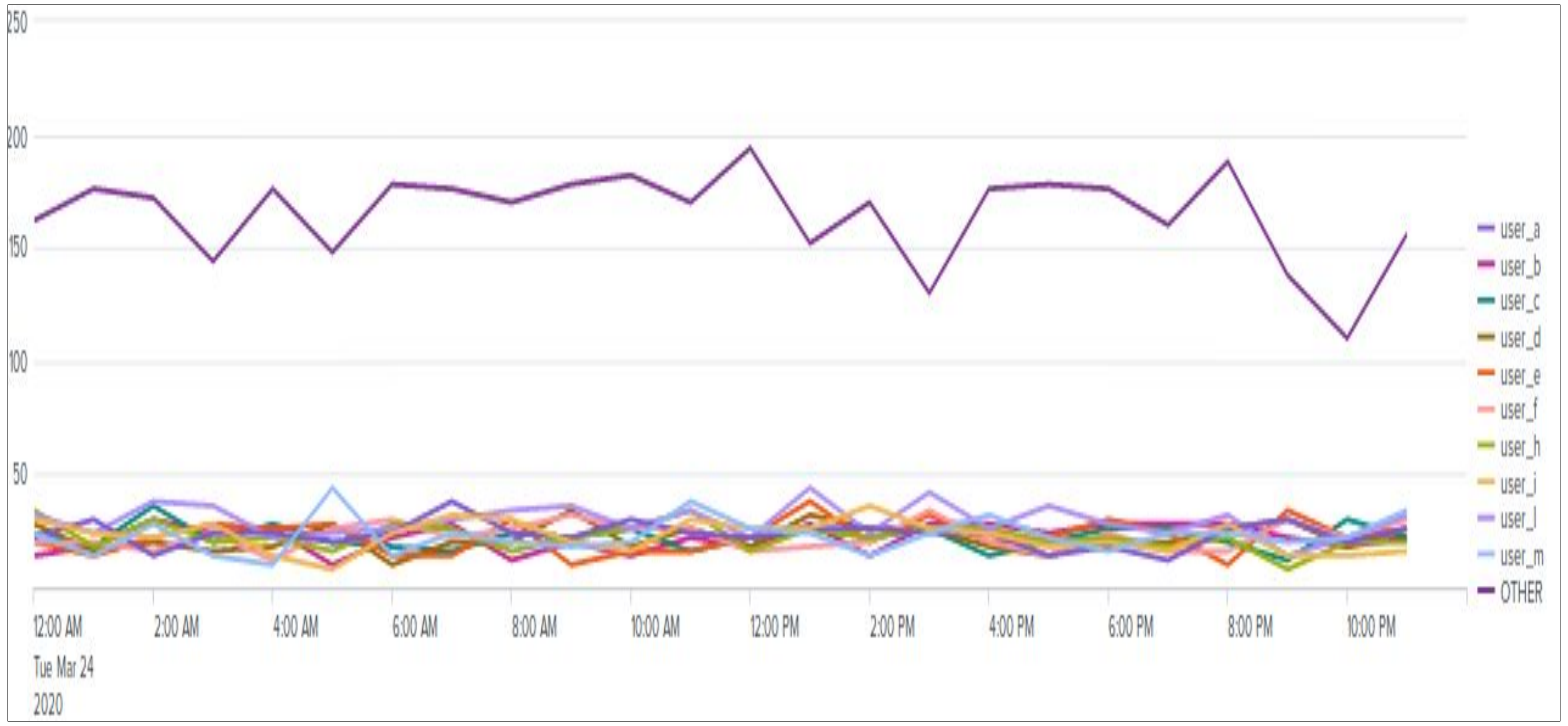
Designed the following alerts:

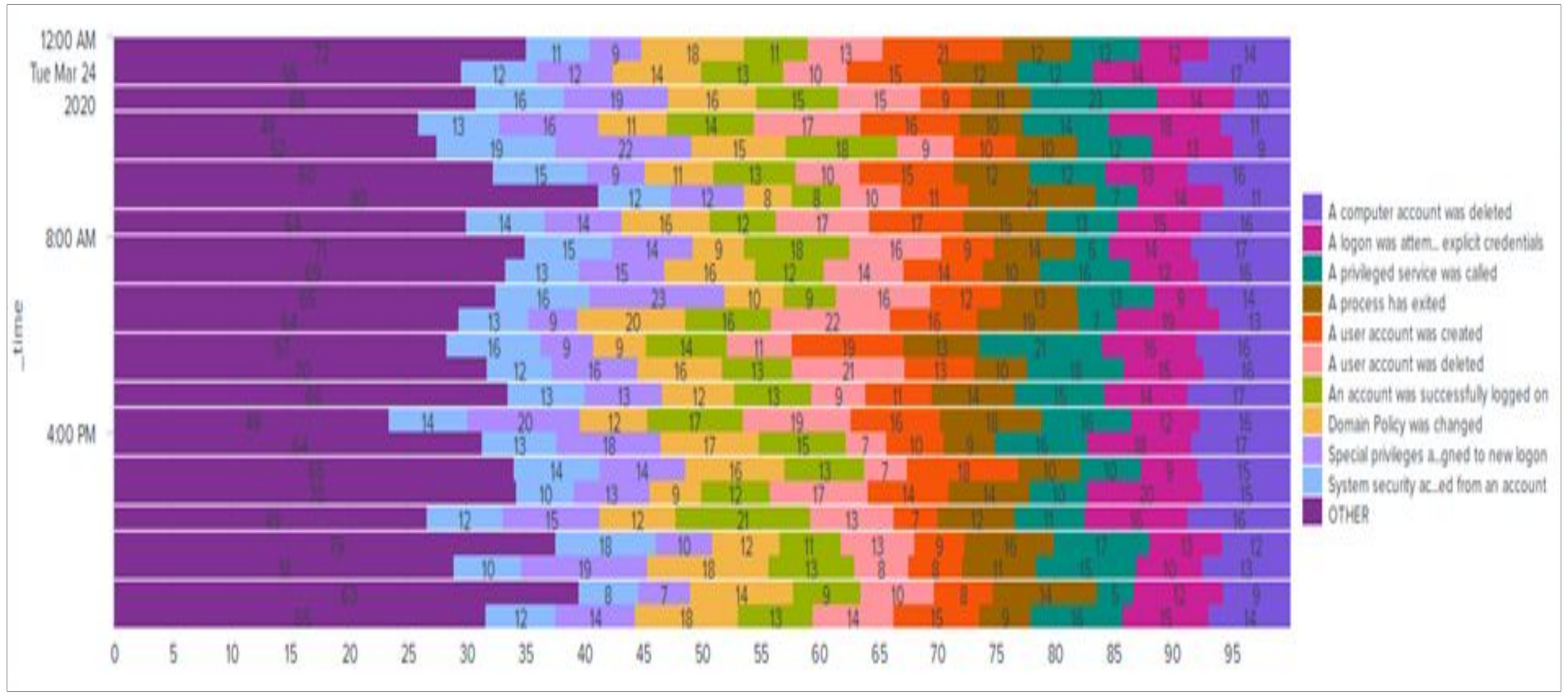
Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Was Deleted	Suspicious Amount Of Accounts Deleted	20 accounts deleted in 60 minutes	25 accounts deleted in 60 minutes

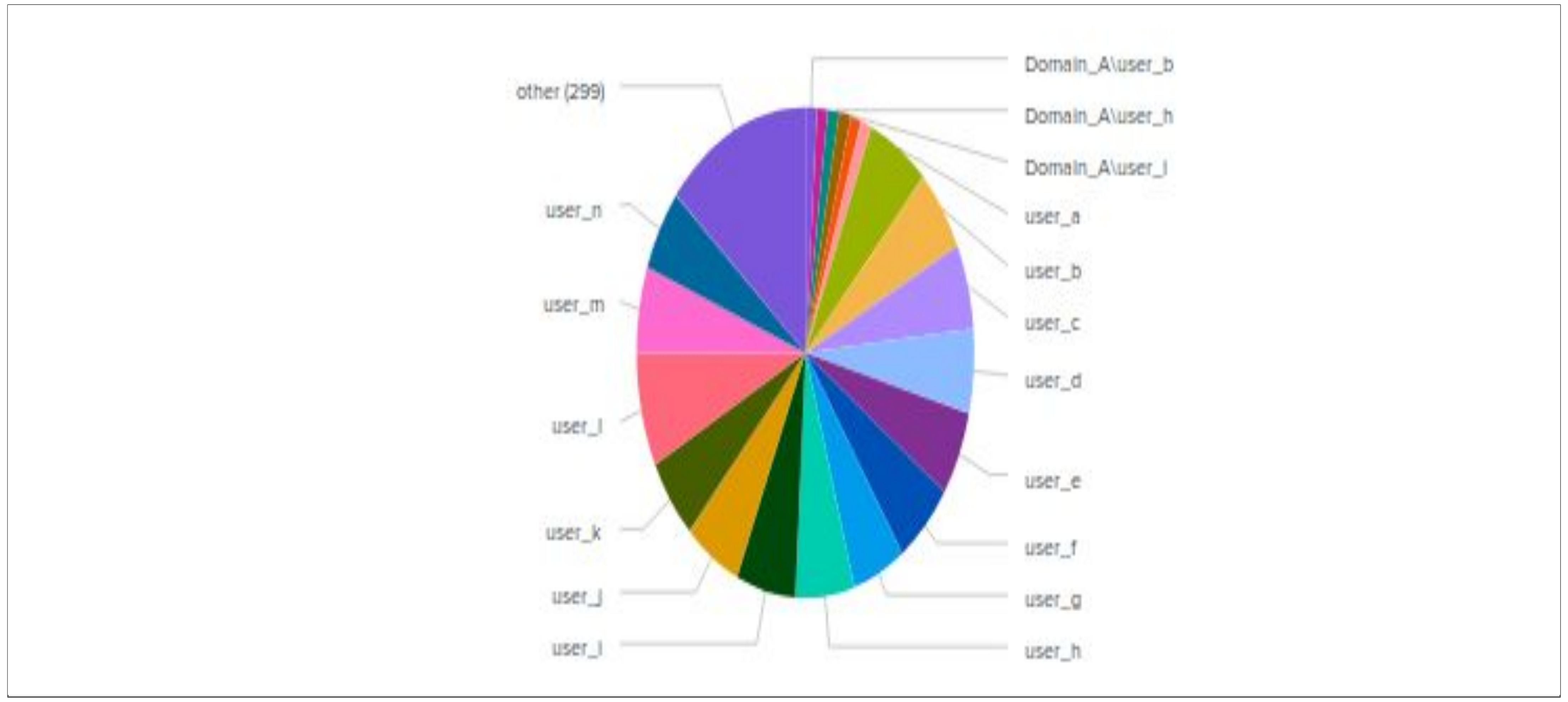
JUSTIFICATION: We felt that setting the threshold to 25 accounts being deleted in 60 minutes would provide some room for increased activity but also detection for abnormal activity.

Dashboards—Windows









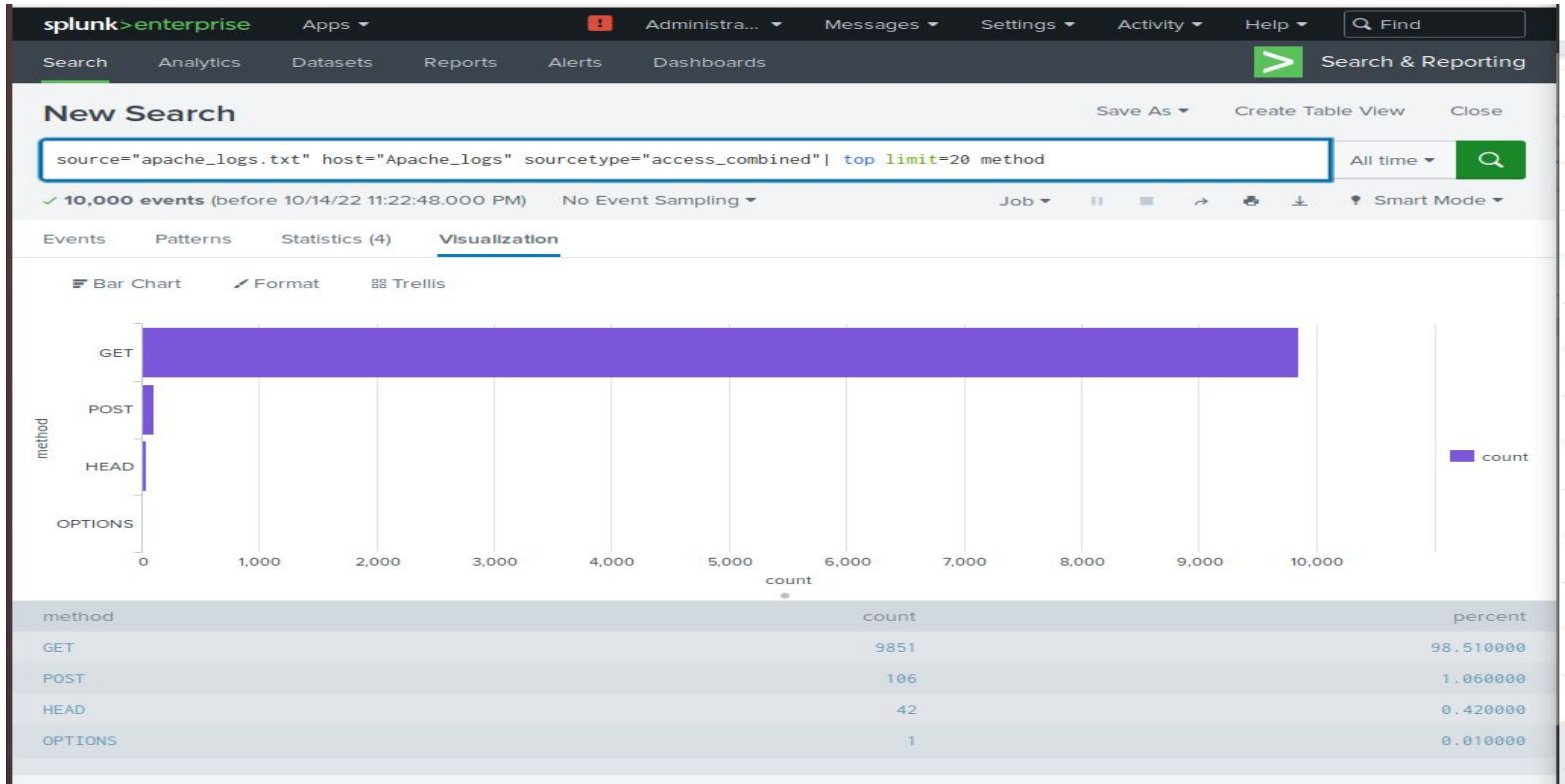
Apache Logs

Reports—Apache

We designed the following reports:

Report Name	Report Description
HTTP Methods Table	A report that shows a table of the different HTTP methods.
Top 10 Referrer Domains	A report that shows the top 10 domains that refer to VSI’s website.
HTTP Response Codes	A report that shows the count of each HTTP response codes

Images of Reports—Apache

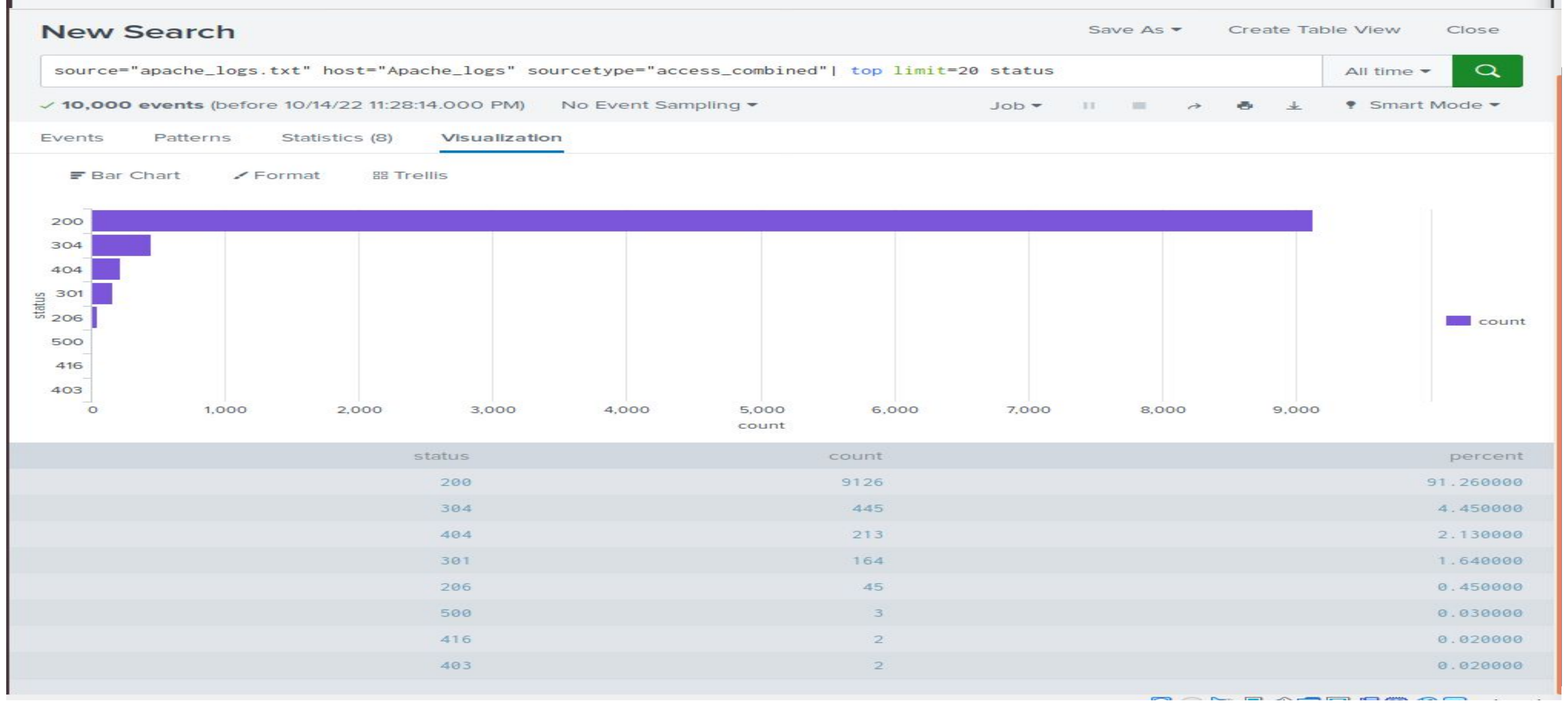


New Search

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=20 method
```

✓ 10,000 events (before 10/14/22 11:22:48.000 PM)

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

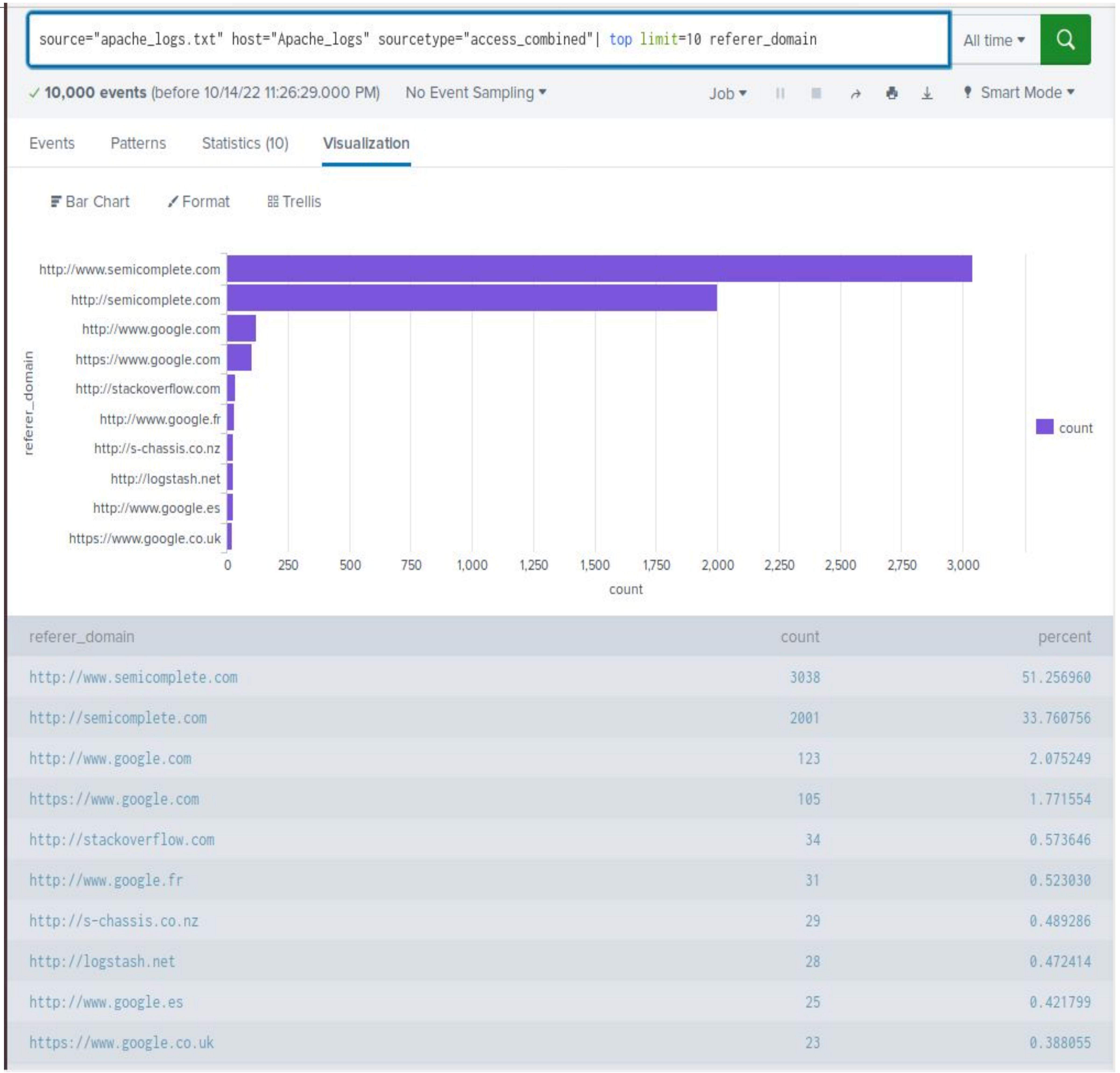


New Search

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=20 status
```

✓ 10,000 events (before 10/14/22 11:28:14.000 PM)

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000



```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ 10,000 events (before 10/14/22 11:26:29.000 PM)

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

Alerts—Apache

We designed the following alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Visiting IPs Alert	Monitors international activity	~650 IPs outside of the US in an hour	More than 935 IP’s visiting from outside of the US in an hour

JUSTIFICATION: We determined that 935 visiting IPs an hour would provide some room for increased activity but also detection for abnormally high activity.

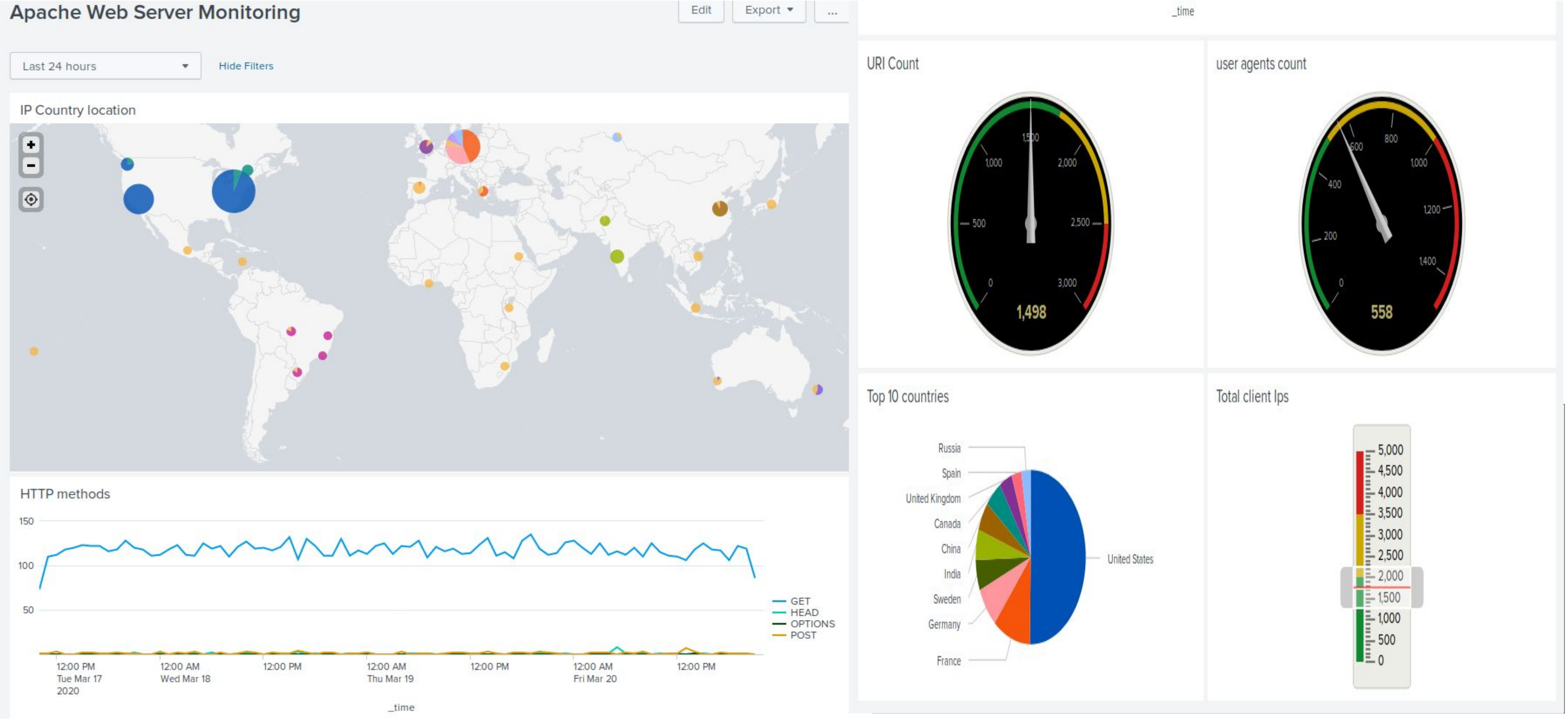
Alerts—Apache

We designed the following alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Activity Alert	Monitors HTTP POST requests	~35 POST's in an hour.	An alert will be sent after 40 POST's are made in an hour.

JUSTIFICATION: We determined that 40 POST's an hour would provide some room for increased activity but also detection for abnormally high activity.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows Reports

- Severity
  - Informational decreased by 8,766
  - High increased by 1,235
- Status
  - Success increased by 7,090
  - Failure increased by 44

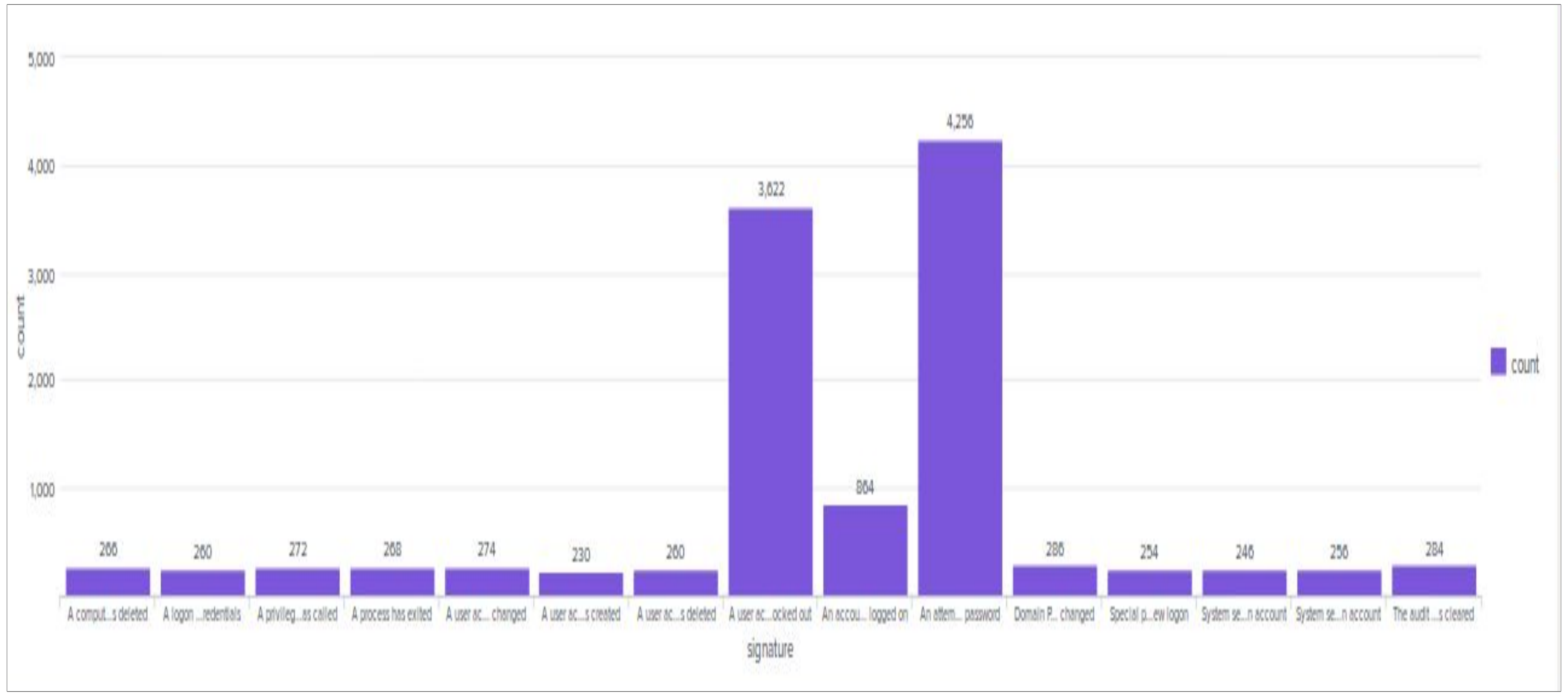
Attack Summary—Windows Alerts

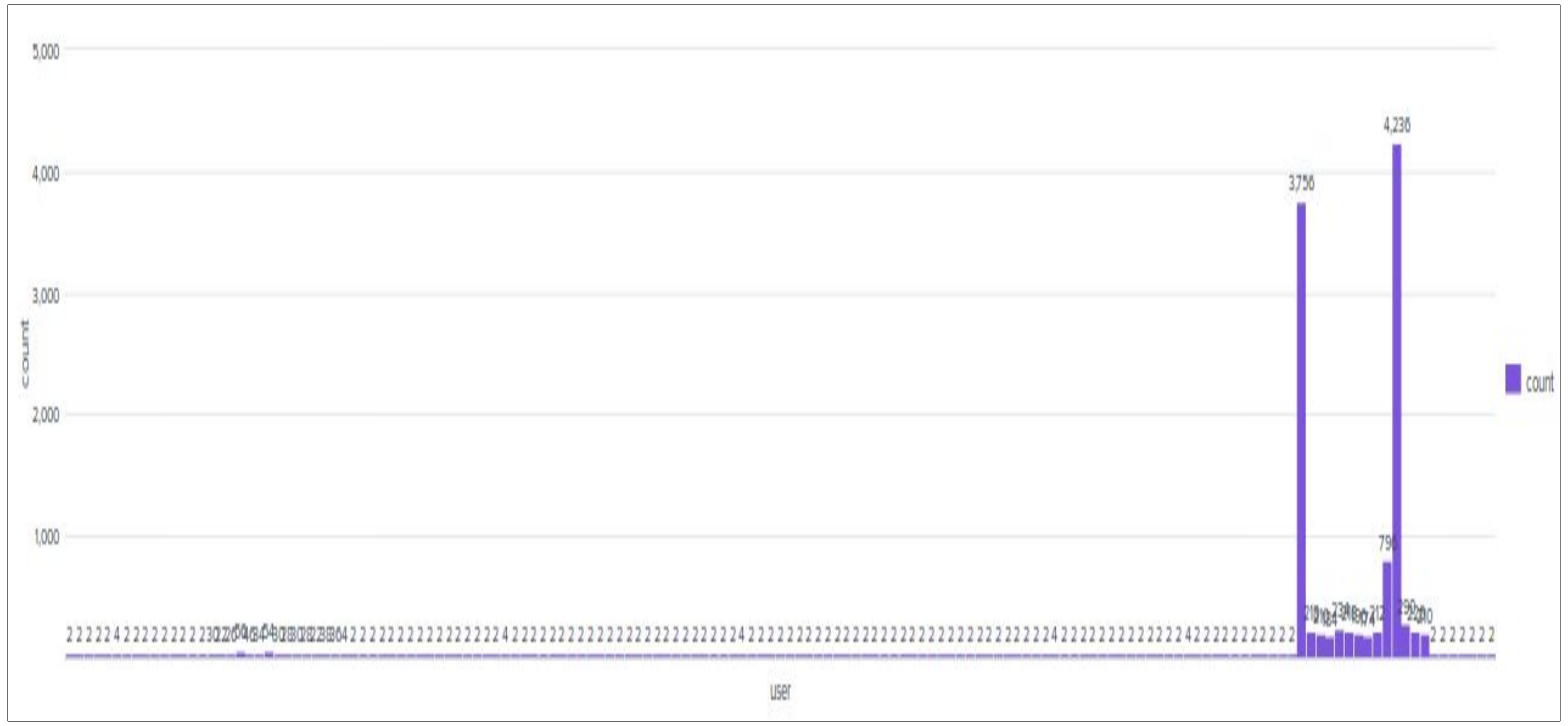
- There was an elevated number of failed windows activities, which would set off our alert.
  - On 03/25/2020,
    - Start-time: 1:00 AM
    - Peak: 9:00 AM (2,586 success)
    - End-time: 11:00 AM
- There was a little bit of a jump in successful logins, which would set off our alert.
  - On 03/25/2020,
    - Start-time: 1:00 AM
    - Peak: 8:00 AM (32 Logons)
    - End-time: 8:00 AM
- We didn’t detect an unusual amount of deleted accounts.

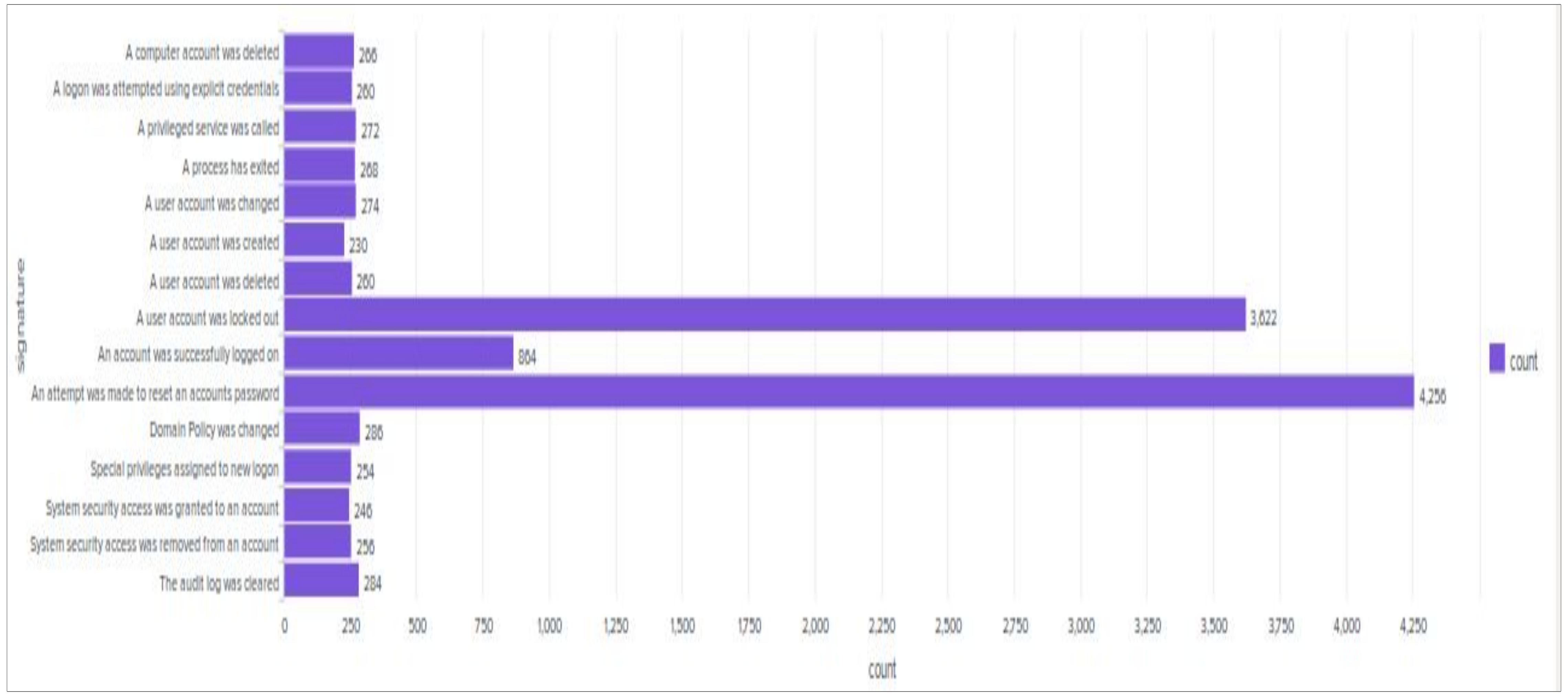
Attack Summary—Windows Dashboards

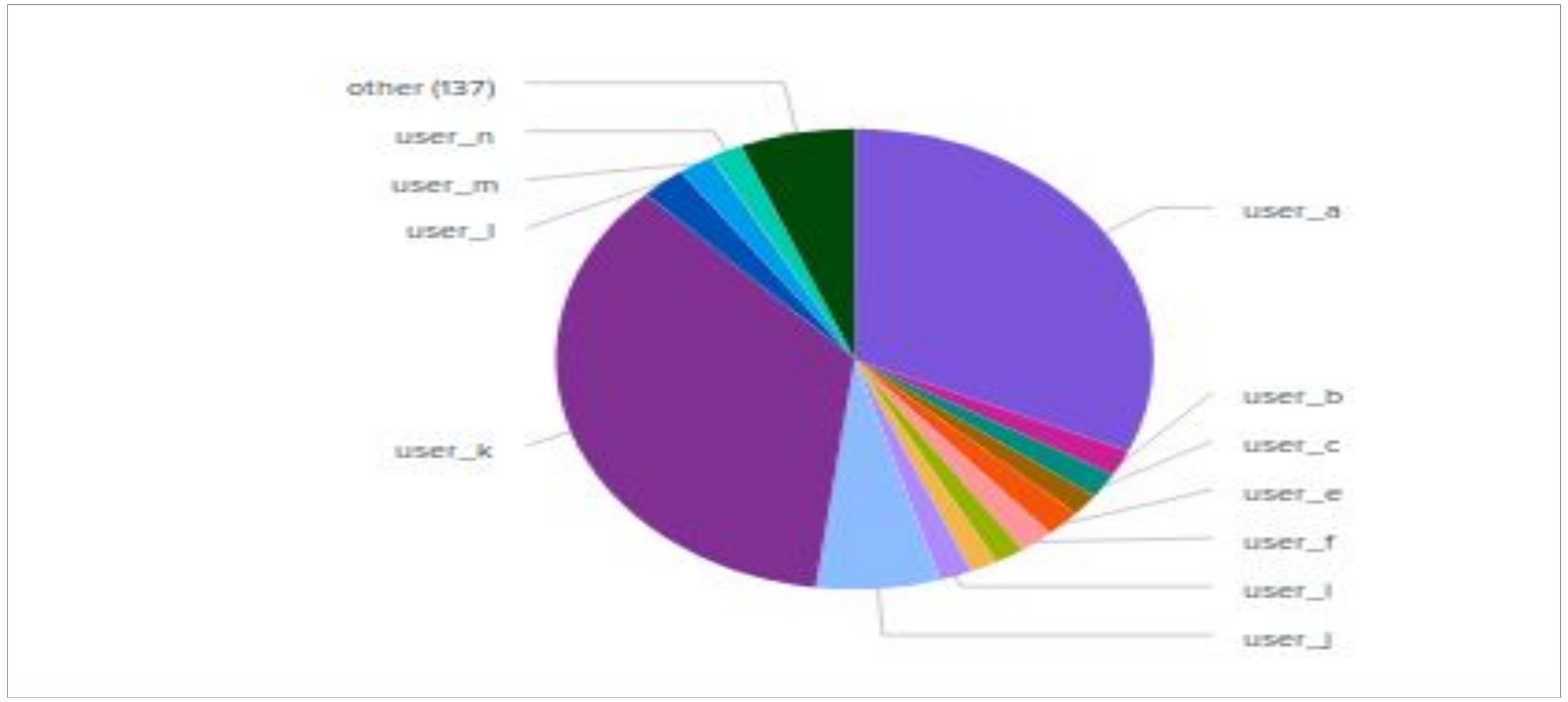
- 3,622 user accounts were locked
    - On 03/25/2020,
        - Start-time: 12:00 AM
        - Peak: 2:00 AM (1,792 incidents)
        - End-time: 3:00 AM
- 4,256 attempts were made to reset an account passwords
    - On 03/25/2020,
        - Start-time: 8:00 AM
        - Peak: 9:00 AM (2,516 incidents)
        - End-time: 11:00 AM

Dashboards—Windows Attack Logs



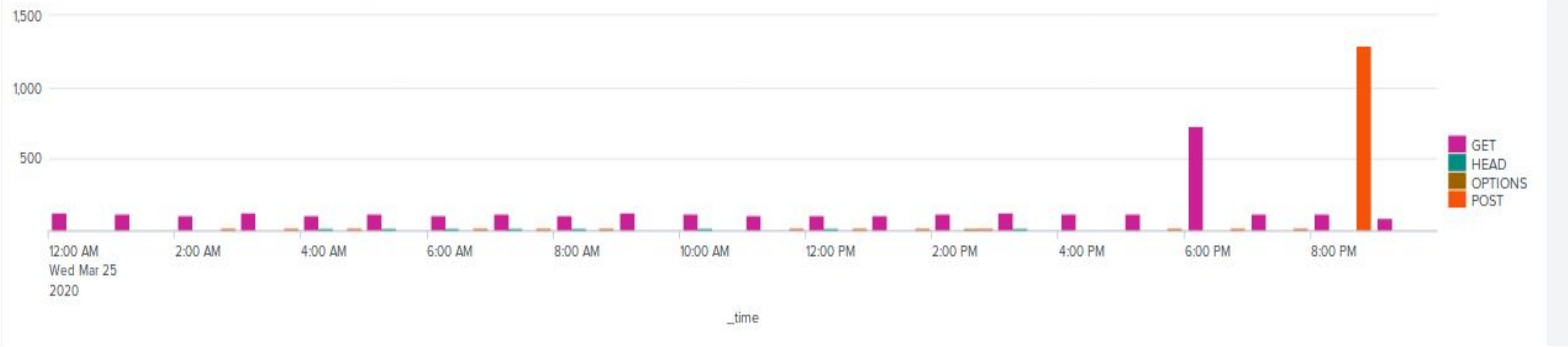






Attack Summary—Apache

- Drop in GET requests.
  - From 49k to 3k
- Hike in Post request
  - From ~500 to 1k+



Attack Summary—Apache

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

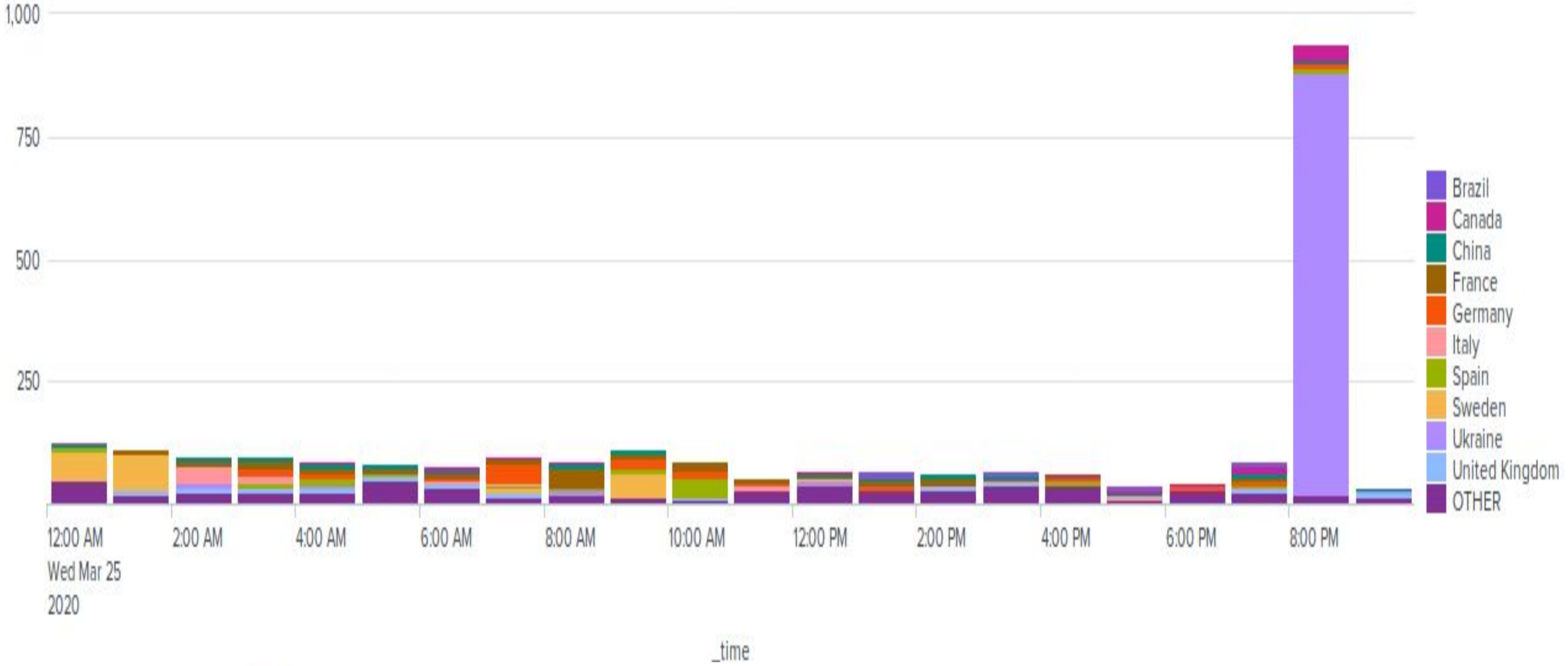
- 1k+ HTTP requests made from Ukraine
  - most of them were POST requests
  - On 03/25/2020,
    - Start-time: 6:00 PM (~700 GET requests)
    - Peak: 8:00 PM (1,296 POST requests)
    - End-time: 9:00 PM

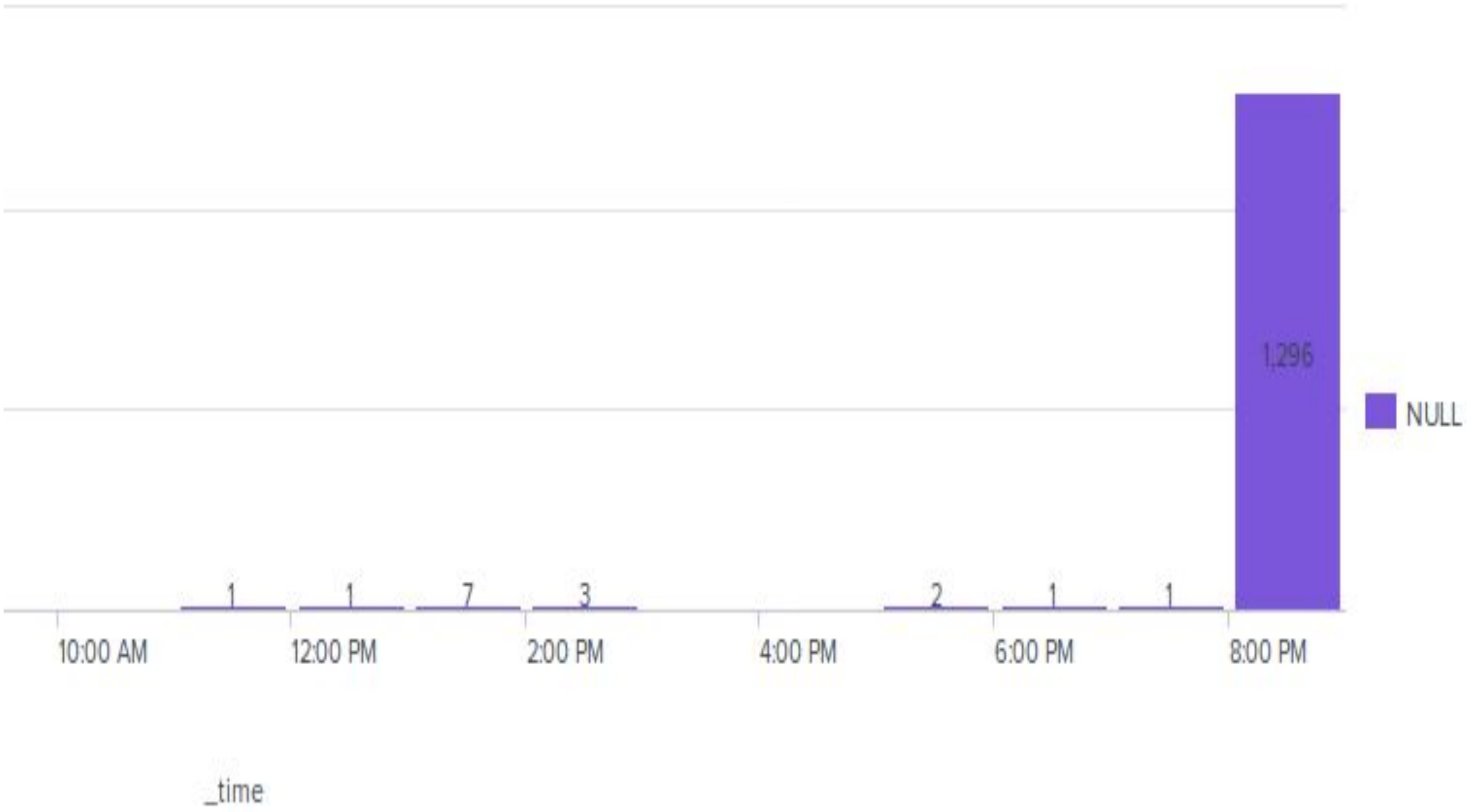
Attack Summary—Apache

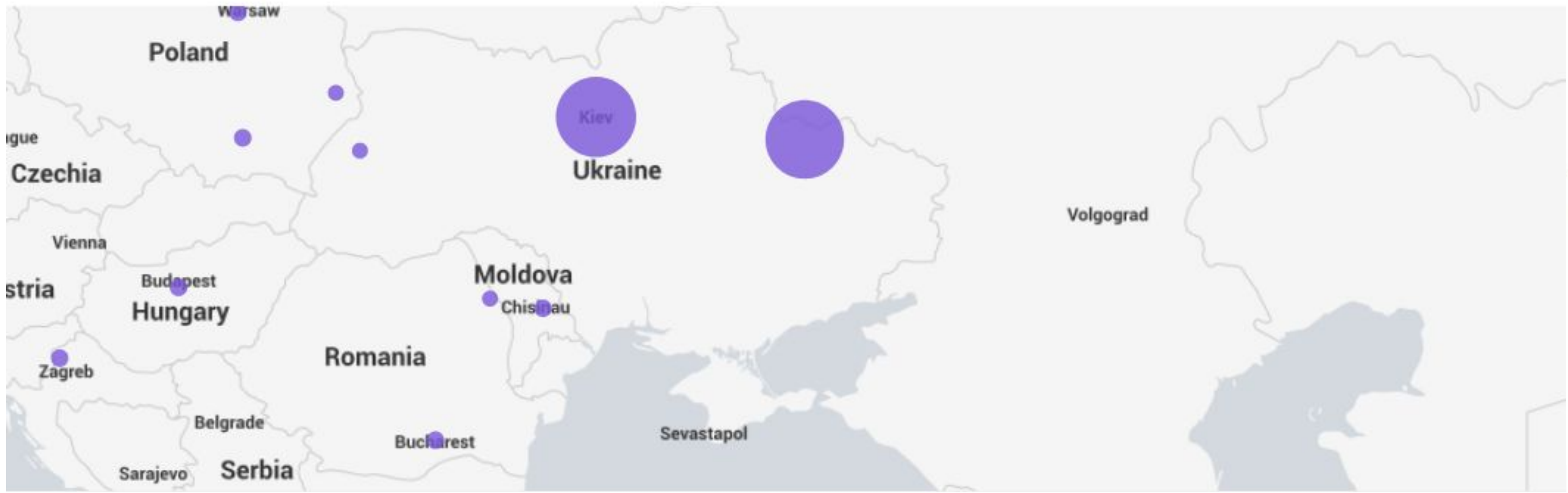
Summarize your findings from your dashboards when analyzing the attack logs.

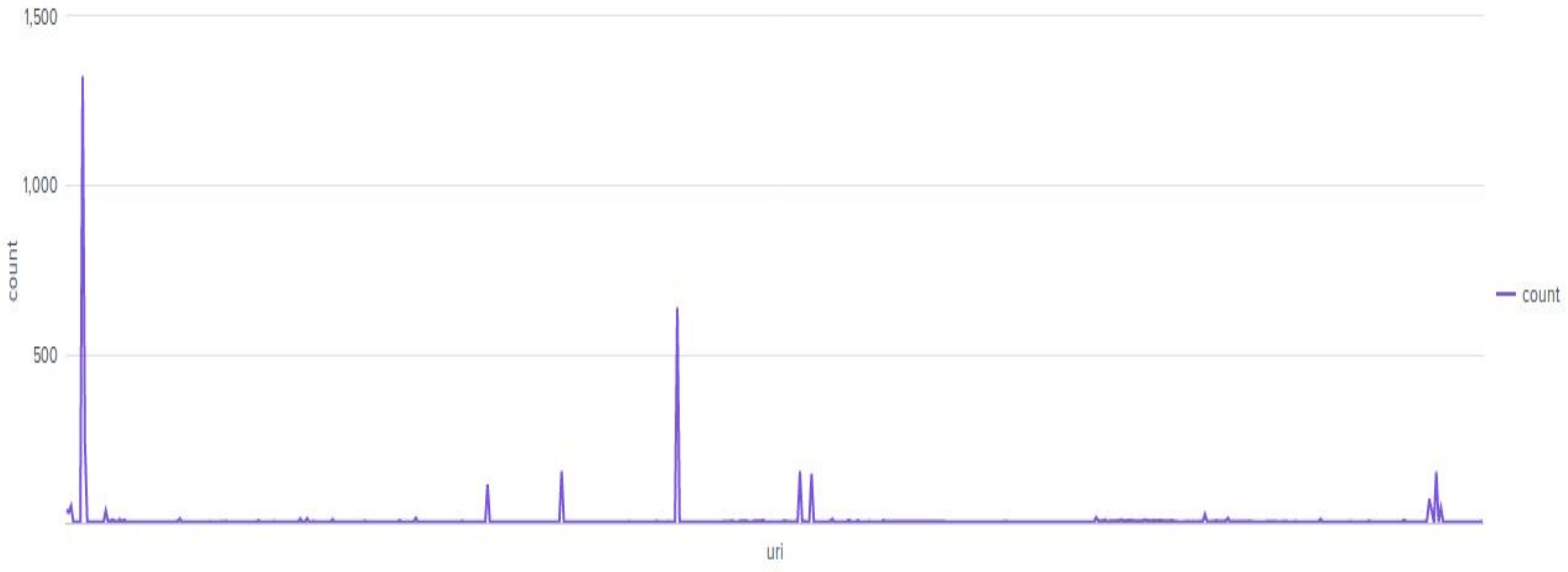
- There was increased HTTP POST methods, as well as an increase of activity in Kiev, Ukraine. These occurrences happened simultaneously on march 25, 2020, at 8pm so they are most likely connected.

Screenshots of Attack Logs









Summary and Future Mitigations

Project 3 Summary

- According to the evidence gathered, it is likely that a brute force attack happened on the windows servers and a DDoS happened on the Apache servers.

- To protect VSI from future attacks,
  - Enforce strong passwords, use multifactor authentication for windows
  - Implement cloud computing as well as stronger bandwidth for apache