Defensive Security Project

by:

Alessandro Sant,
Neil Starkie,
Mark Vennare,
Shane Mandarino,
Shajee Islam,
Jun Millado,
Younis Kessler,
Tanvir Shah

Table of Contents

This document contains the following resources:

01

Monitoring Environment

-Addon App
-Windows Logs
-Apache Logs

02

Attack Analysis

-Signature & User value over Time
-Different User and Signature Counts
- URI & HTTP methods

03

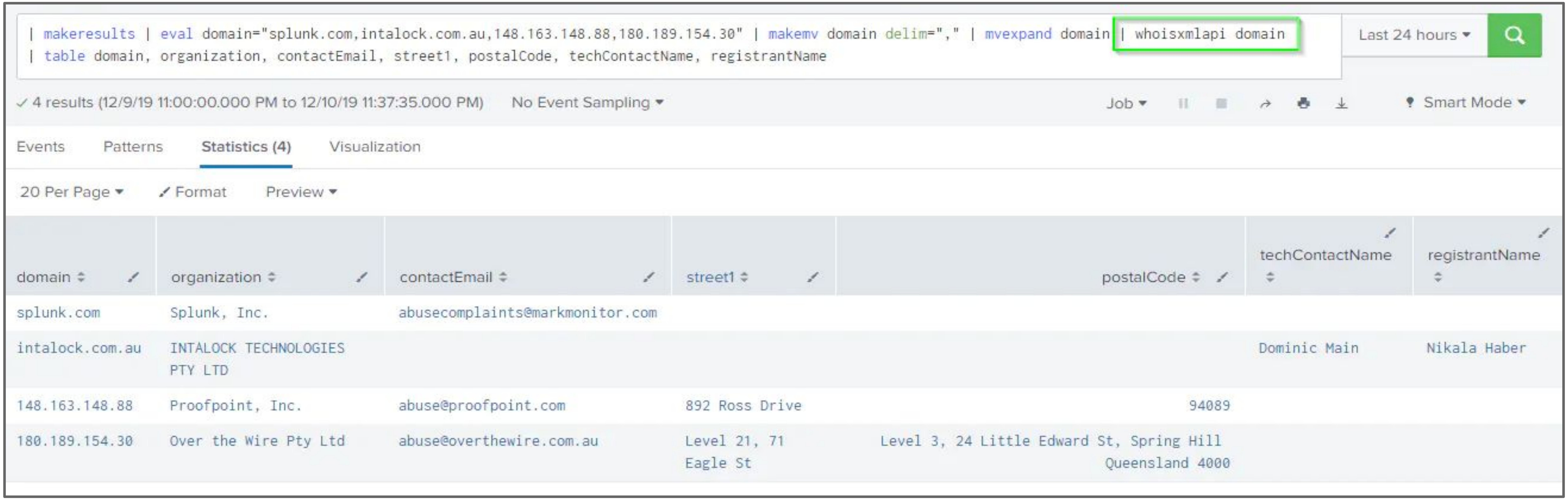
Project Summary & Future Mitigations

-Overall findings of the attack
- Actions, Users & Value findings
- Mitigations

Monitoring Environment

WhoisXML IP Geolocation API
(addon app)

Enhancing VSI’s Security with WhoisXML IP Geolocation API



```
| makeresults | eval domain="splunk.com,intalock.com.au,148.163.148.88,180.189.154.30" | makemv domain delim="," | mvexpand domain | whoisxmlapi domain
| table domain, organization, contactEmail, street1, postalCode, techContactName, registrantName
```

✓ 4 results (12/9/19 11:00:00.000 PM to 12/10/19 11:37:35.000 PM)

domain	organization	contactEmail	street1	postalCode	techContactName	registrantName
splunk.com	Splunk, Inc.	abusecomplaints@markmonitor.com				
intalock.com.au	INTALOCK TECHNOLOGIES PTY LTD				Dominic Main	Nikala Haber
148.163.148.88	Proofpoint, Inc.	abuse@proofpoint.com	892 Ross Drive	94089		
180.189.154.30	Over the Wire Pty Ltd	abuse@overthewire.com.au	Level 21, 71 Eagle St	Level 3, 24 Little Edward St, Spring Hill Queensland 4000		

Benefits and Integration of WhoisXML IP Geolocation API

- ❖ **Deep Contextualization**: Precise geolocation data for IP's, aiding in tracking potential threat origins.
- ❖ **Enhanced Monitoring**: Insights into connected domains, network information, and timezones.
- ❖ **Real-time and Historical Data**: Access to billions of historical DNS data points.
- ❖ **Integrated Cybersecurity**: Easily integratable with Splunk, enhancing VSI's security operations center.
- ❖ **Access Discovery Management**: With the growth of VSI, knowing our digital footprint is essential. The tool aids in discovering and monitoring all IP-related assets, ensuring no endpoint goes unnoticed or unprotected.

Practical Implementation for VSI

A Realistic Scenario of a VSI Attack

OH NO! It's a calm Thursday evening at VSI when suddenly, the alarm goes off!

- **Initial Breach Attempt**: An unknown IP tries to access VSI's administrative webpage. The IP's origin is unfamiliar and not linked to any of VSI's global offices or known partners.
- **WhoisXML IP Geolocation API Activation**: Before the IP can gain deeper access, the WhoisXML IP Geolocation tool in Splunk identifies the suspicious IP's geographical location and its recent online activities.
- **Threat Classification**: The IP is linked to previous cyber-attacks on similar VR companies in another region. With this intel the system flags this as a high-priority threat.
- **Immediate Response**: Automated protocols restrict access for the identified IP, and an alert is sent to VSI's security team for a deeper investigation.
- **Post-Incident**: Using WhoisXML API, VSI's SOC team conducts a detailed analysis of the breach attempt. The team identifies potential patterns and refines security protocols to safeguard against future attempts from similar origins.

Windows Logs

Logs Analyzed

1 Windows Logs

1. User account logs
   a. Successful user account login
   b. User account creation
   c. User account deletion
   d. Computer account deletion
   e. Special privileges assigned to new logon
   f. Privilege service was called
2. Process IDs
3. User Session
4. Process Success vs Failure
5. Actions (success, modified, created, cleared, deleted, false)

2 Apache Logs

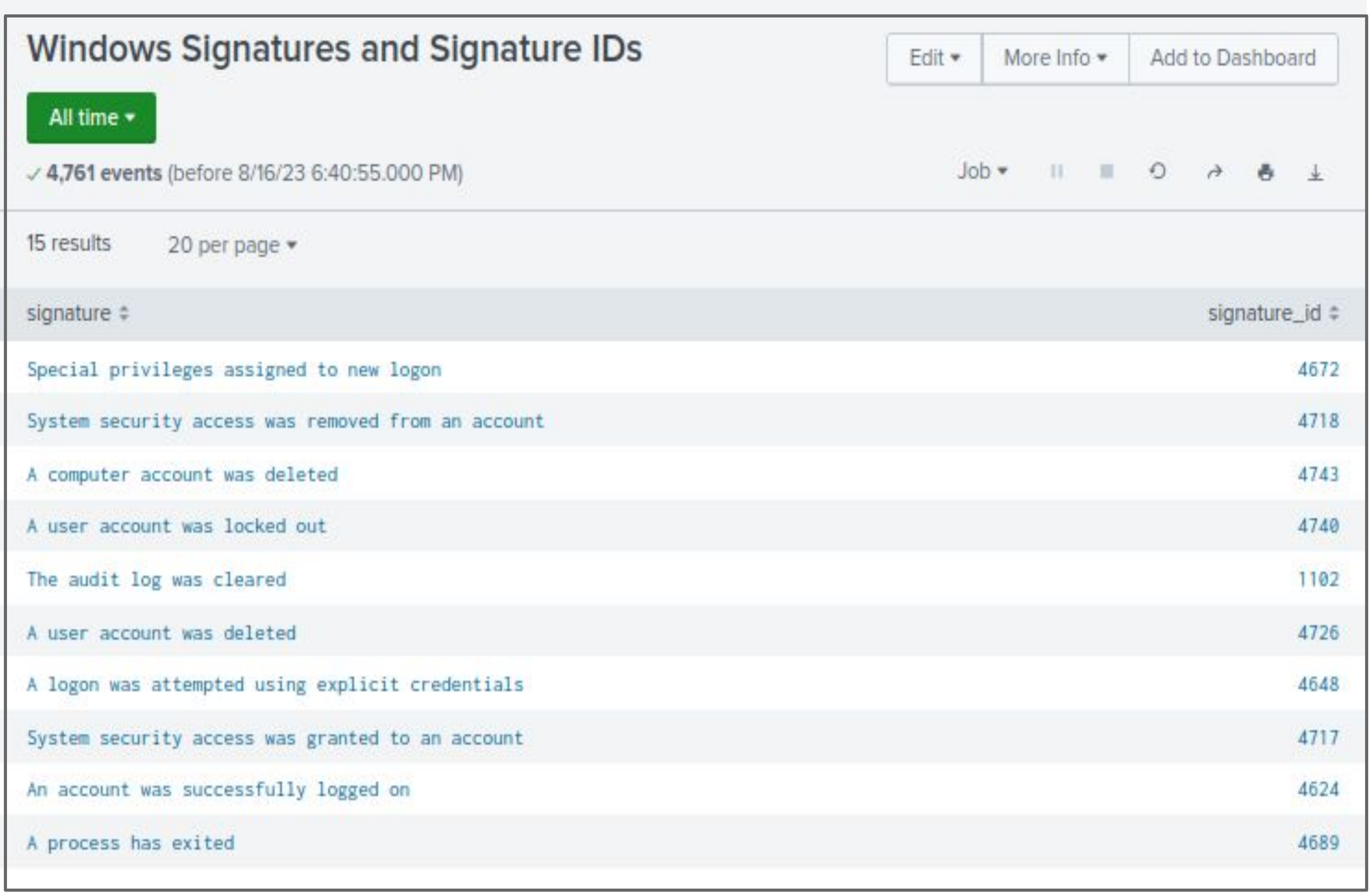
1. HTTP Methods
   a. Referrer domains
   b. Count of HTTP response code
   c. Countries & Location based on the “Clientip”
   d. URI Count
   e. Agents Count

Reports—Windows

Designed the following reports:

Report Name	Report Description
Windows_severity_report	Creates a report comparing the counts of high severity events vs “informational” events.
Windows_Signature_and_Signature_IDs	Records the count of Signature events and Signature IDs.
Success_vs_Failure_Windows_Activities	Records the success vs failure events of processes on the server.

Reports—Windows

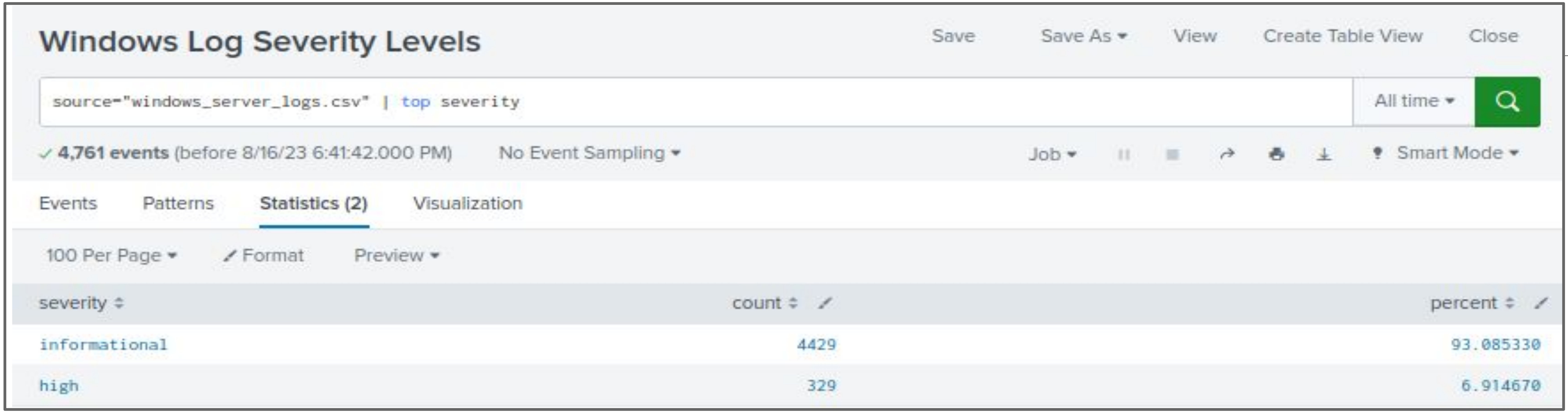


Windows Signatures and Signature IDs

✓ **4,761 events** (before 8/16/23 6:40:55.000 PM)

15 results   20 per page ▾

signature	signature_id
Special privileges assigned to new logon	4672
System security access was removed from an account	4718
A computer account was deleted	4743
A user account was locked out	4740
The audit log was cleared	1102
A user account was deleted	4726
A logon was attempted using explicit credentials	4648
System security access was granted to an account	4717
An account was successfully logged on	4624
A process has exited	4689

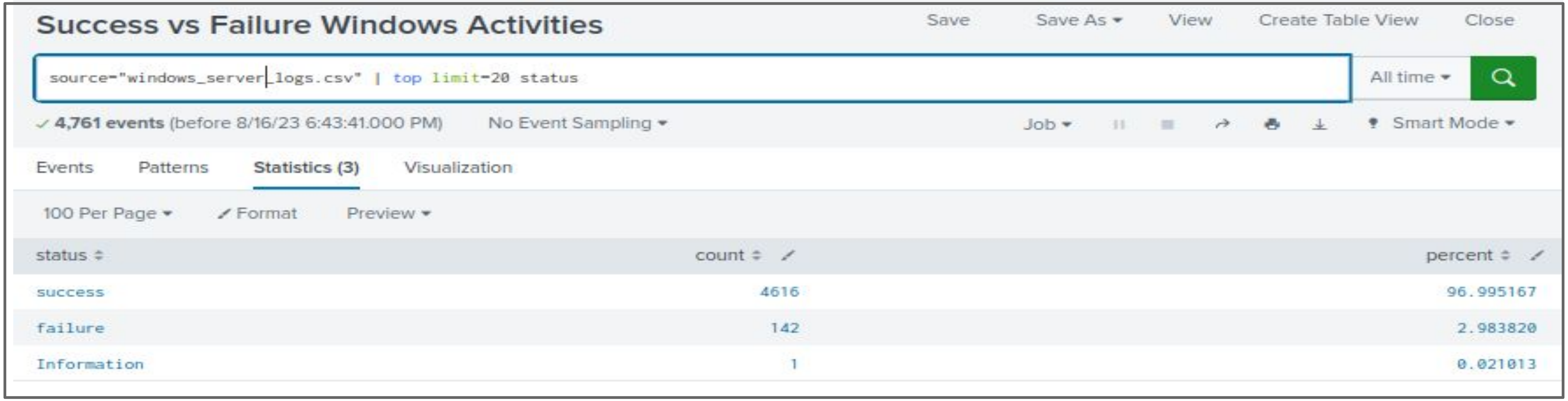


Windows Log Severity Levels

```
source="windows_server_logs.csv" | top severity
```

✓ 4,761 events (before 8/16/23 6:41:42.000 PM)

severity	count	percent
informational	4429	93.085330
high	329	6.914670



Success vs Failure Windows Activities

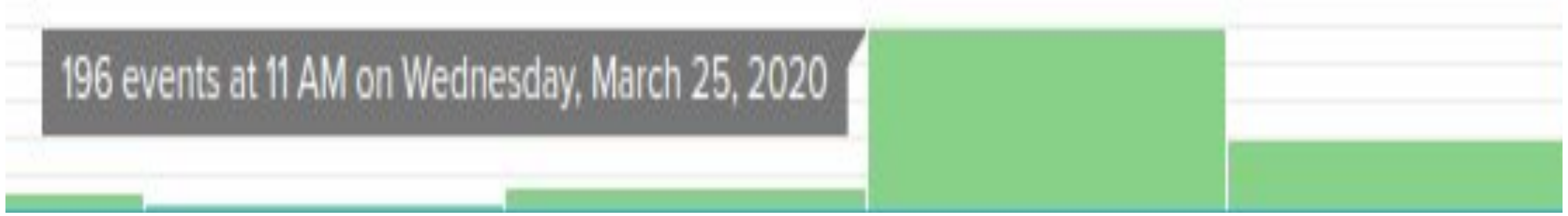
```
source="windows_server_logs.csv" | top limit=20 status
```

✓ 4,761 events (before 8/16/23 6:43:41.000 PM)

status	count	percent
success	4616	96.995167
failure	142	2.983820
Information	1	0.021013

Alerts—Windows

Designed the following alerts:



Alert Name	Alert Description	Alert Baseline	Alert Threshold
Average Hourly Count of Successful Logged on	This alert will go off if the amount of logins go past regular activity	8-21	[25]

JUSTIFICATION: We chose the alert baseline to be 8-21 because the normal number of events ranges from lowest 8 to the highest 21 on any given hour. We chose our alert threshold to be 25 because the highest number of successful logins is 21. To avoid any false positives we wanted to aim a little higher than the highest number of successful log in events. In the example our group provided we see that an attack was made and it was an event count of 196 which will set off our alert because our threshold is 25.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Failed Activities	Alerts for number of failed windows activities above the threshold. A failed activity generally means some action, process or request that did not successfully complete. This can be a login or a service that didn't start or run as expected.	10-12	17

JUSTIFICATION: We set the baseline between 10-12 as this is where most of the normal activity seemed to be in the pre-attack log. Then using the stats stdev function we found that one standard deviation was 6.8, and so we set the threshold to one standard deviation above baseline activity.

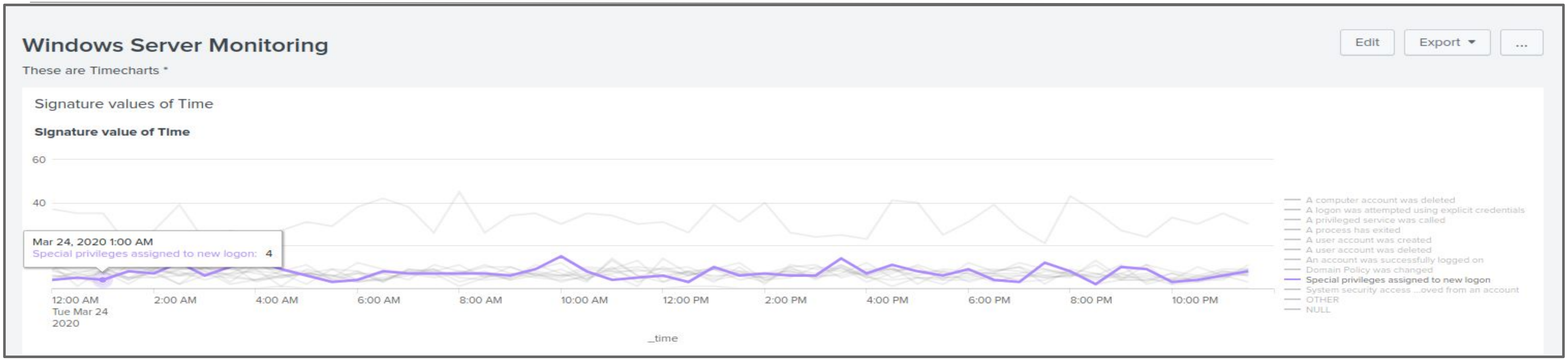
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted	This alert will be triggered when user Accounts are deleted higher than our threshold	7-22	15

JUSTIFICATION: Our threshold was set to 15, and there seemed to be activity peak in the attack log at 5AM (17 counts of account deletion). It seems that our threshold may have been too low and resulted in a false positive. In the future we would change this threshold to a higher number such as 25-30.

Screenshots Dashboards — Windows



Windows Server Monitoring

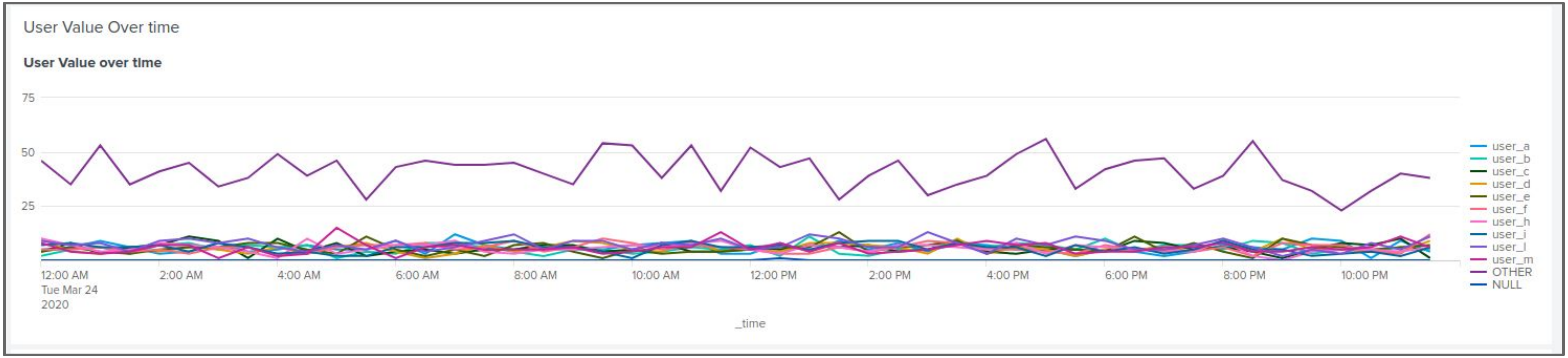
These are Timecharts *

Signature values of Time

Signature value of Time

Mar 24, 2020 1:00 AM
Special privileges assigned to new logon: 4

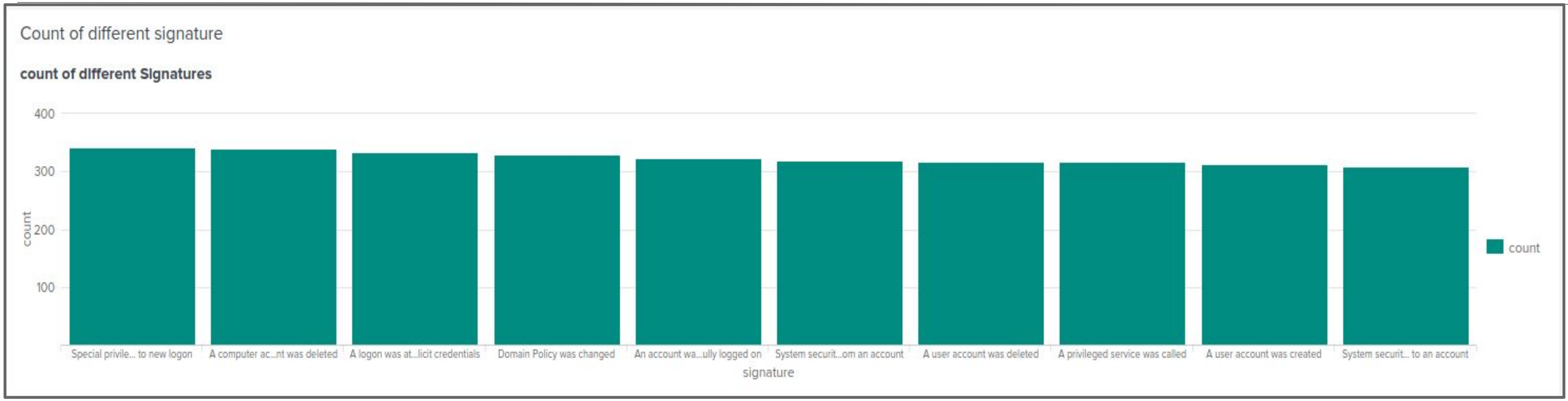
Edit
Export ▾
...
60
40
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access ...oved from an account
OTHER
NULL



User Value Over time

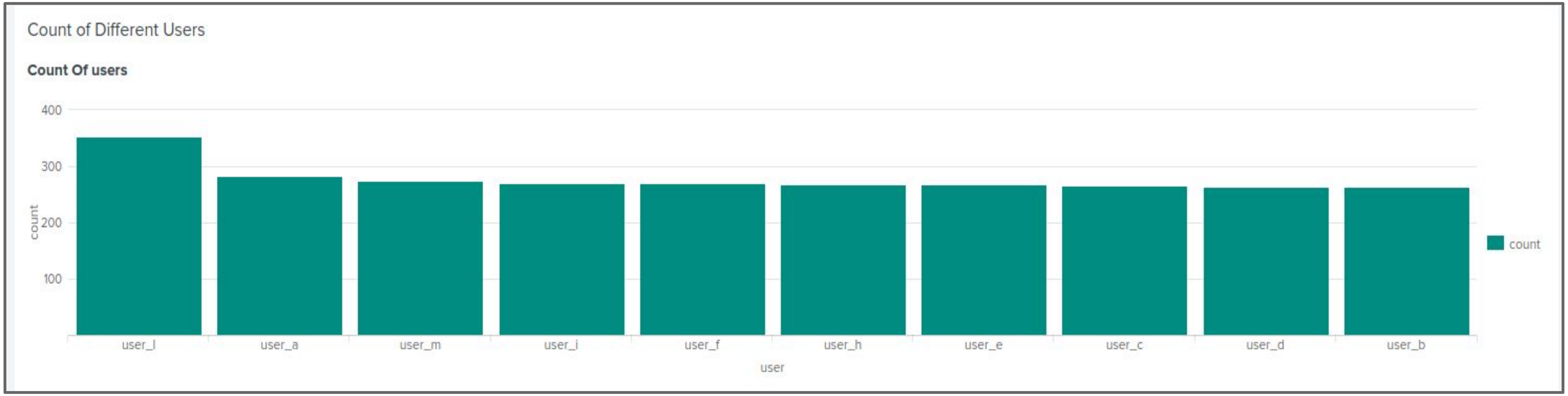
User Value over time

Count of Signatures & Users —Windows



Count of different signature

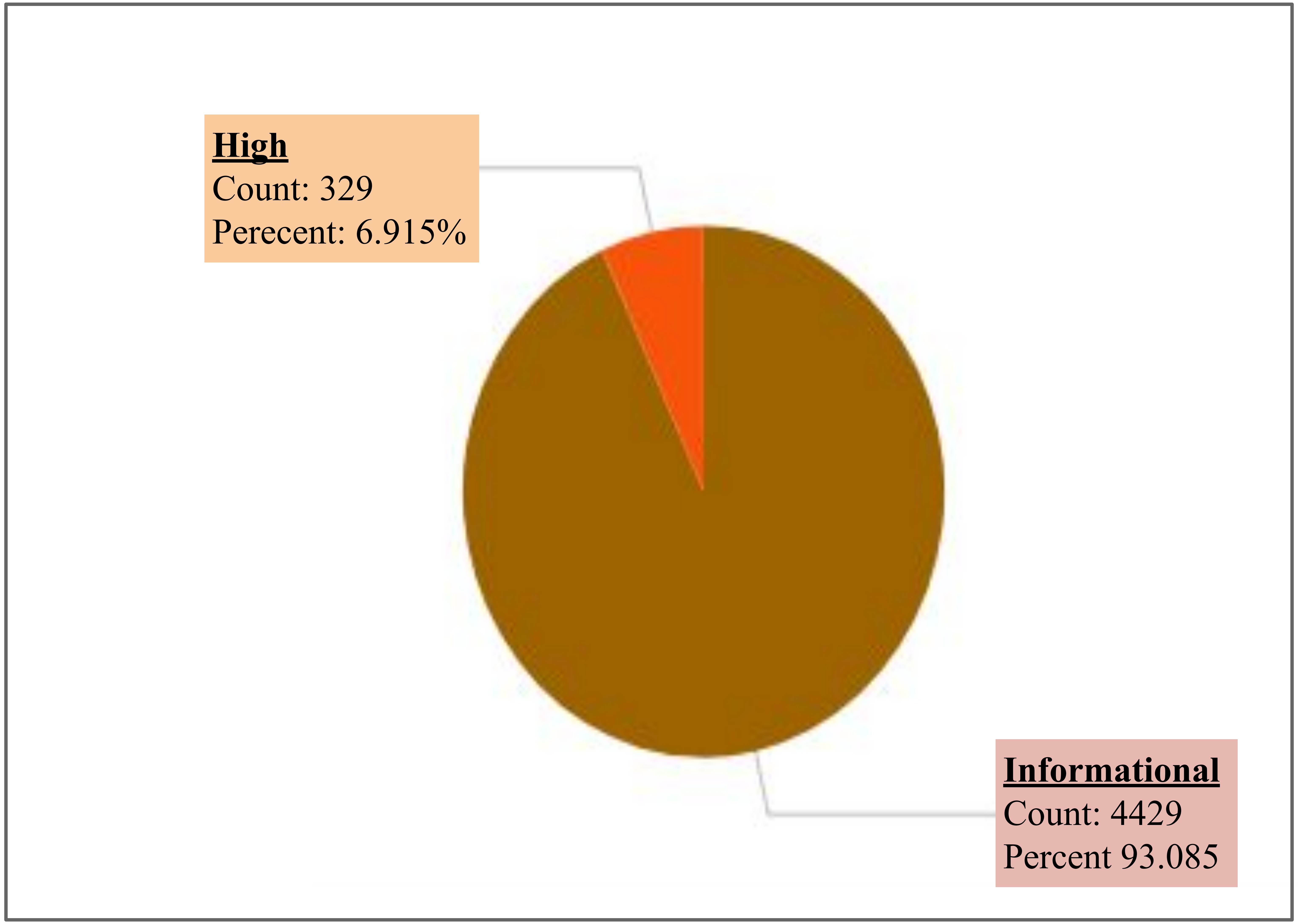
count of different Signatures



Count of Different Users

Count Of users

Dashboards Pie Chart before attack—Windows



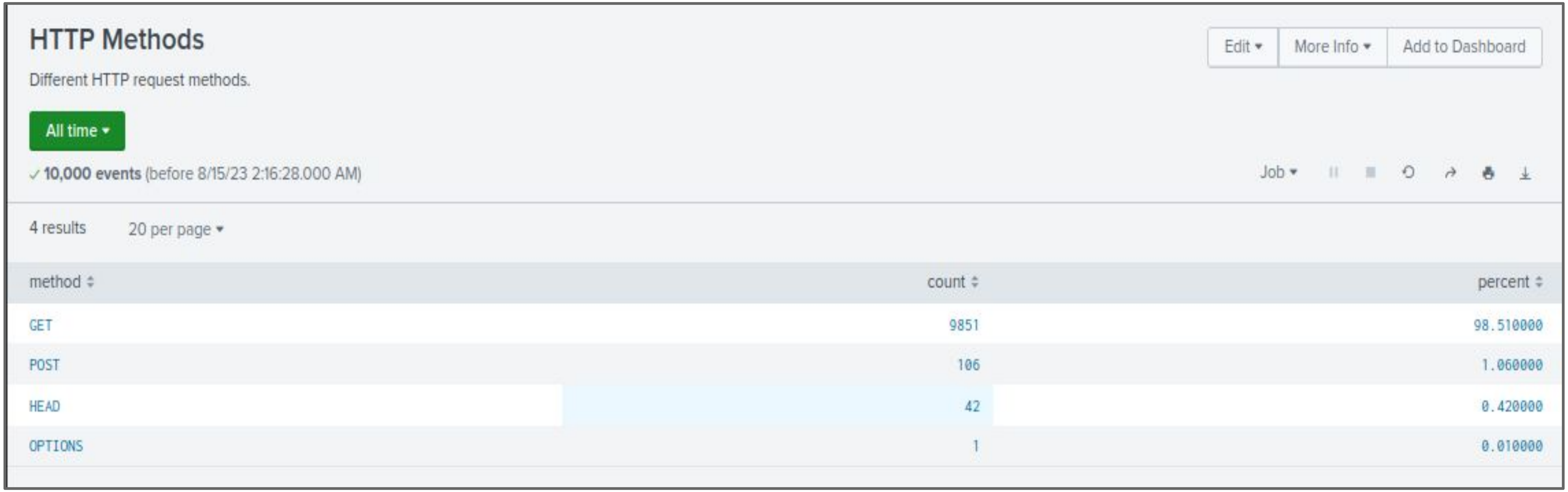
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods Report	This will offer valuable understanding regarding the nature of HTTP activities being solicited towards the web server of the VSI.
Top ten domains of VSI Report	This will aid VSI in recognizing potentially questionable sources of referral traffic.
HTTP response Report	This will offer understanding into potentially abnormal patterns of HTTP responses.

HTTP Methods — Apache



HTTP Methods

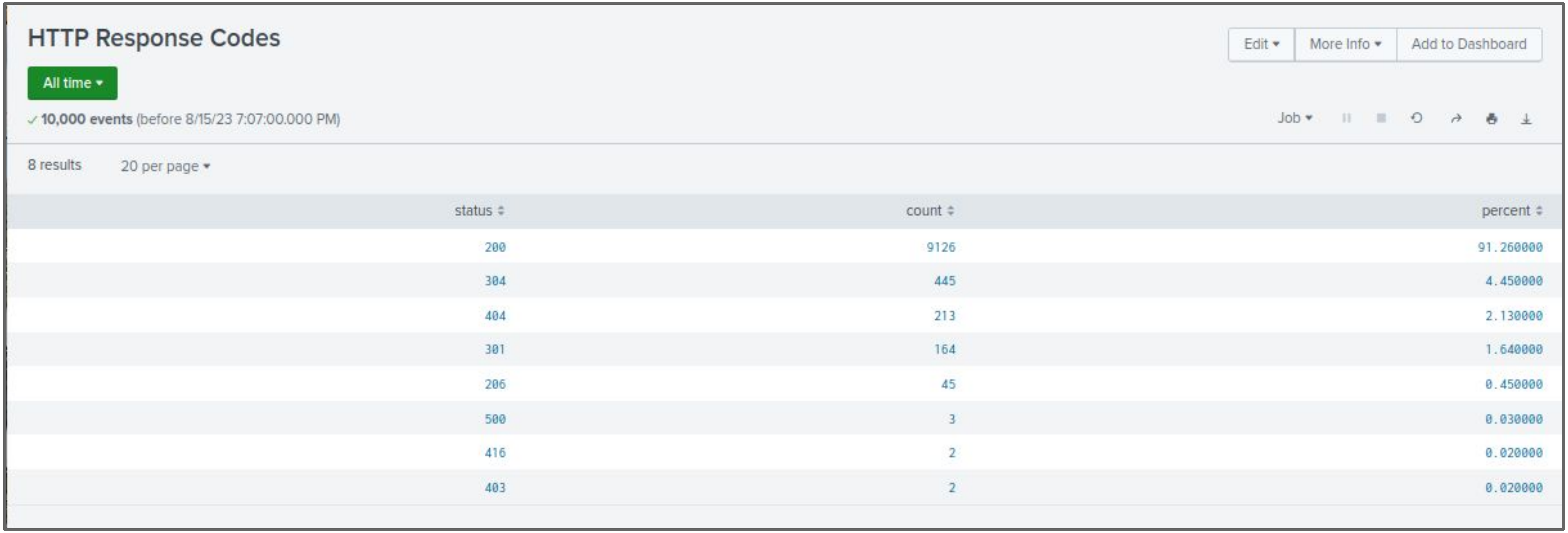
Different HTTP request methods.

✓ **10,000 events** (before 8/15/23 2:16:28.000 AM)

4 results

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

HTTP Response Code — Apache



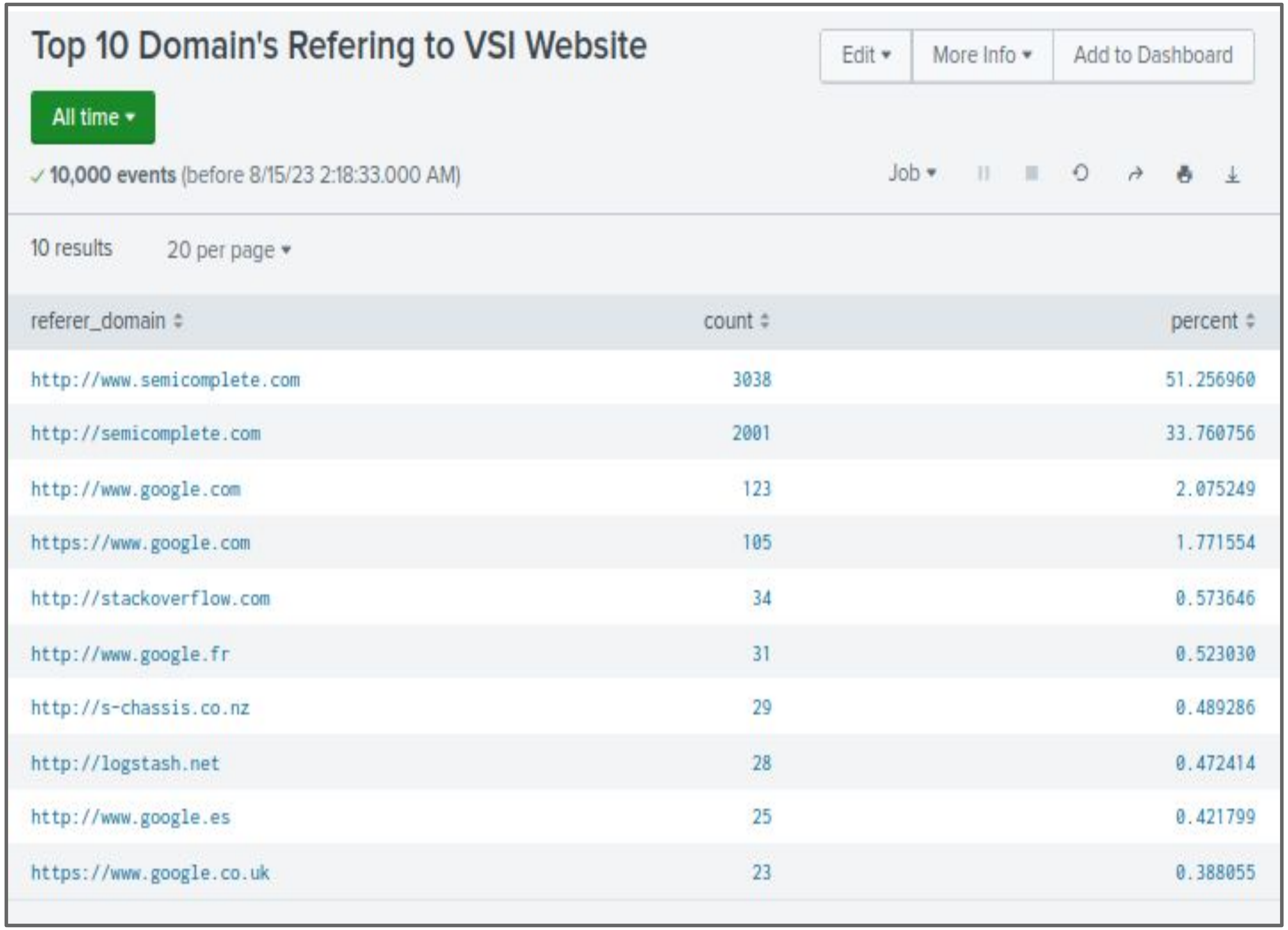
HTTP Response Codes

✓ 10,000 events (before 8/15/23 7:07:00.000 PM)

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

HTTP VSI Domains — Apache



✓ 10,000 events (before 8/15/23 2:18:33.000 AM)

10 results

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

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of HTTP POST method]	[This alert will be triggered when the threshold is past the alarming rate.]	[1-10]	[12]

JUSTIFICATION: We chose the alert baseline 1-10 because when we scanned the number of events for the day it had a low of 1 event and high of 10 event. Our alert threshold is 12 because we did not want false positives by putting it at 8 because it is to close to the max of the baseline. When we hit the attack there was an attack with a count of 1296 which would set off our threshold and everything was within our baseline.

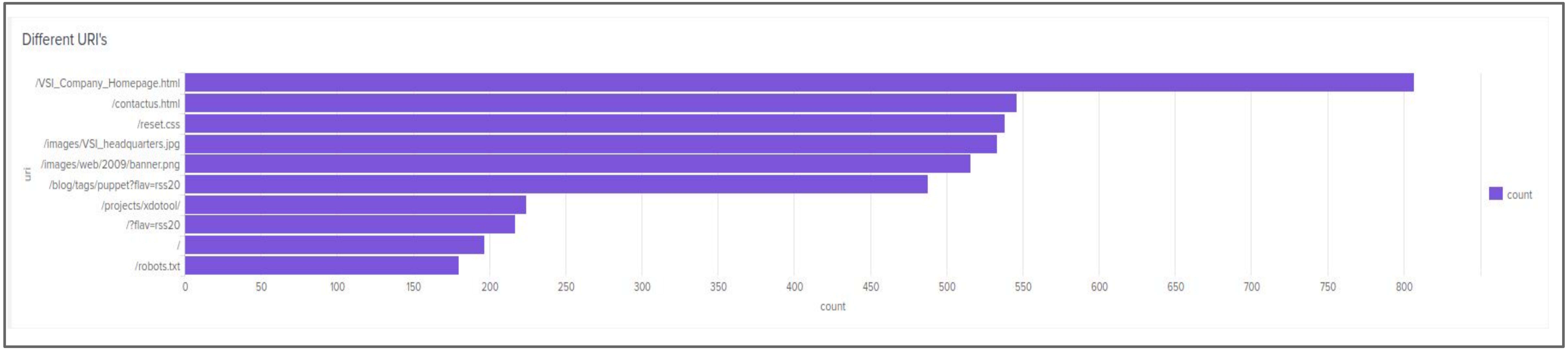
Alerts—Apache

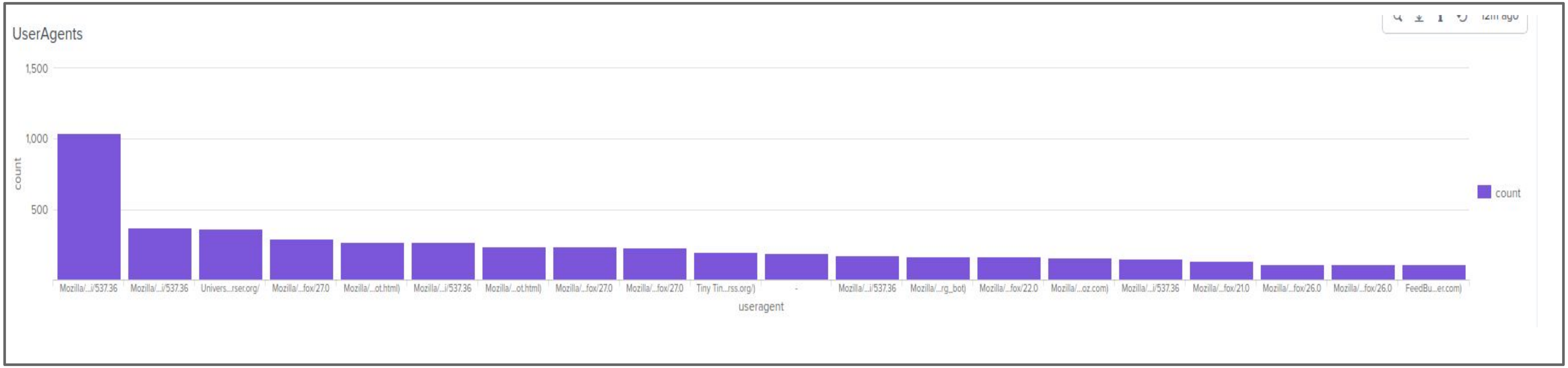
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International IP Threshold	This is an alert that monitors the iplocation of clients originating outside of the United States.	0-130	175

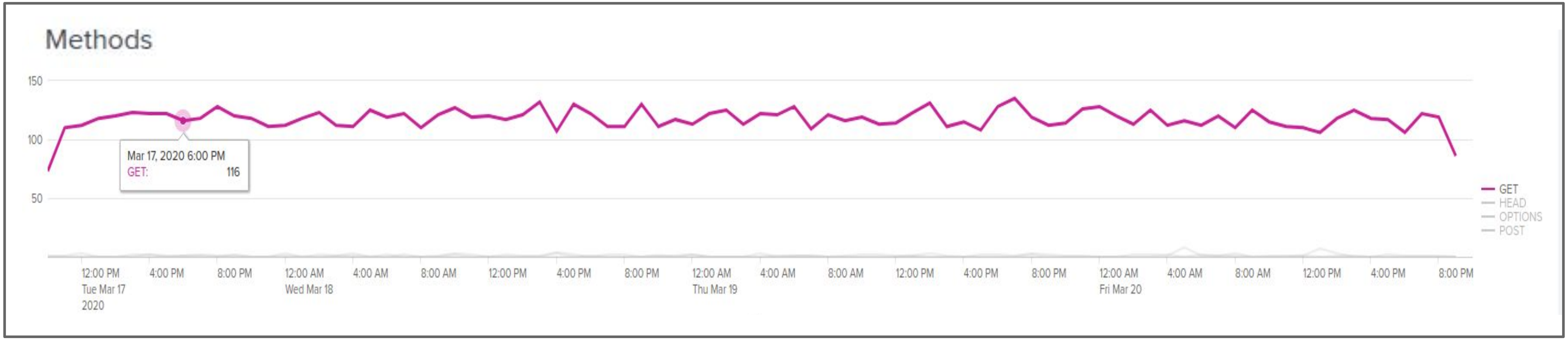
JUSTIFICATION:
The business is primarily an American business and so there is limited IP origination from outside of the USA. Therefore a sudden spike of visits from outside the USA may indicate suspicious activity. Baseline seemed to range from 0 to 130, and so we set our threshold ~25% above normal at 175.

Different URI`s & Agents—Apache

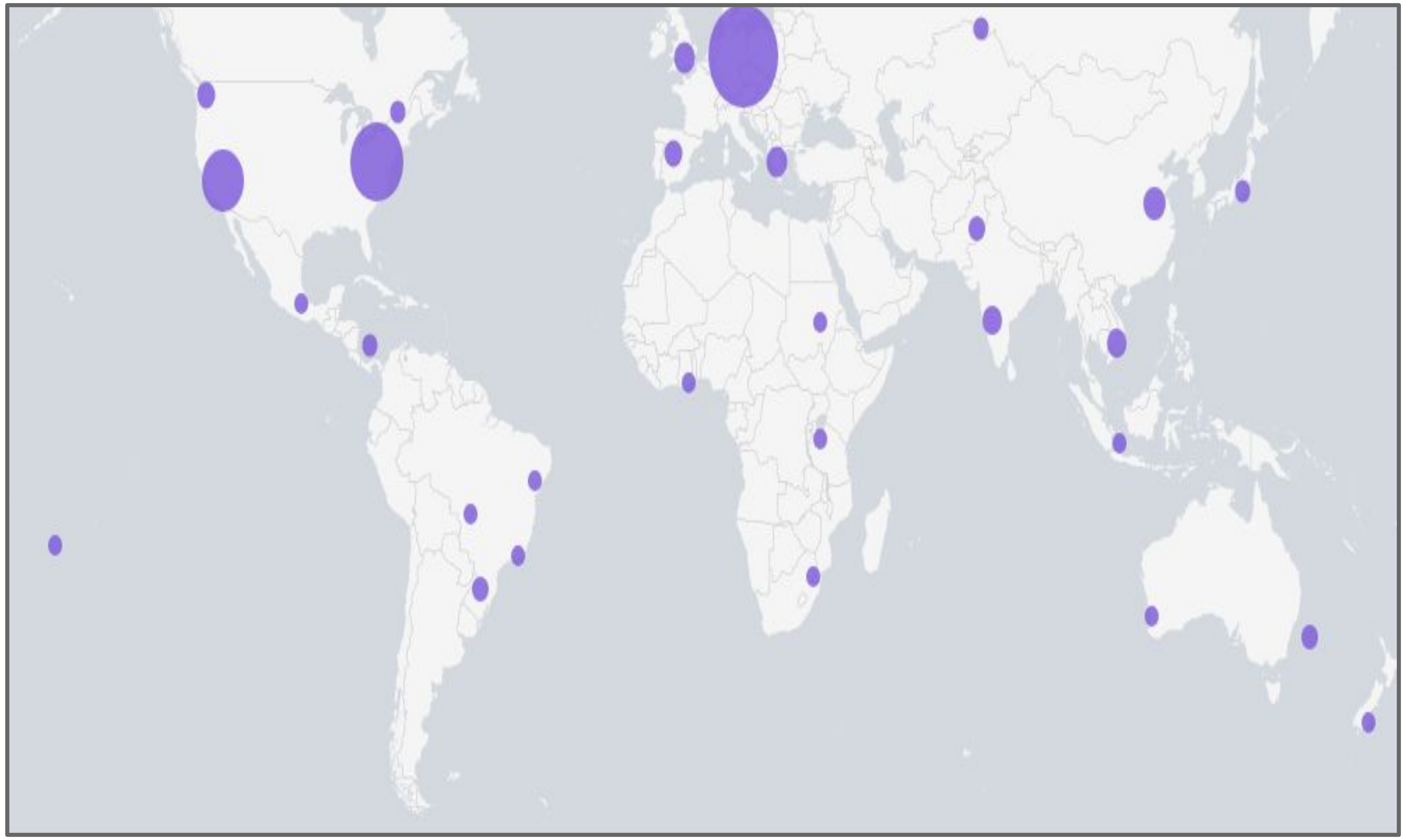


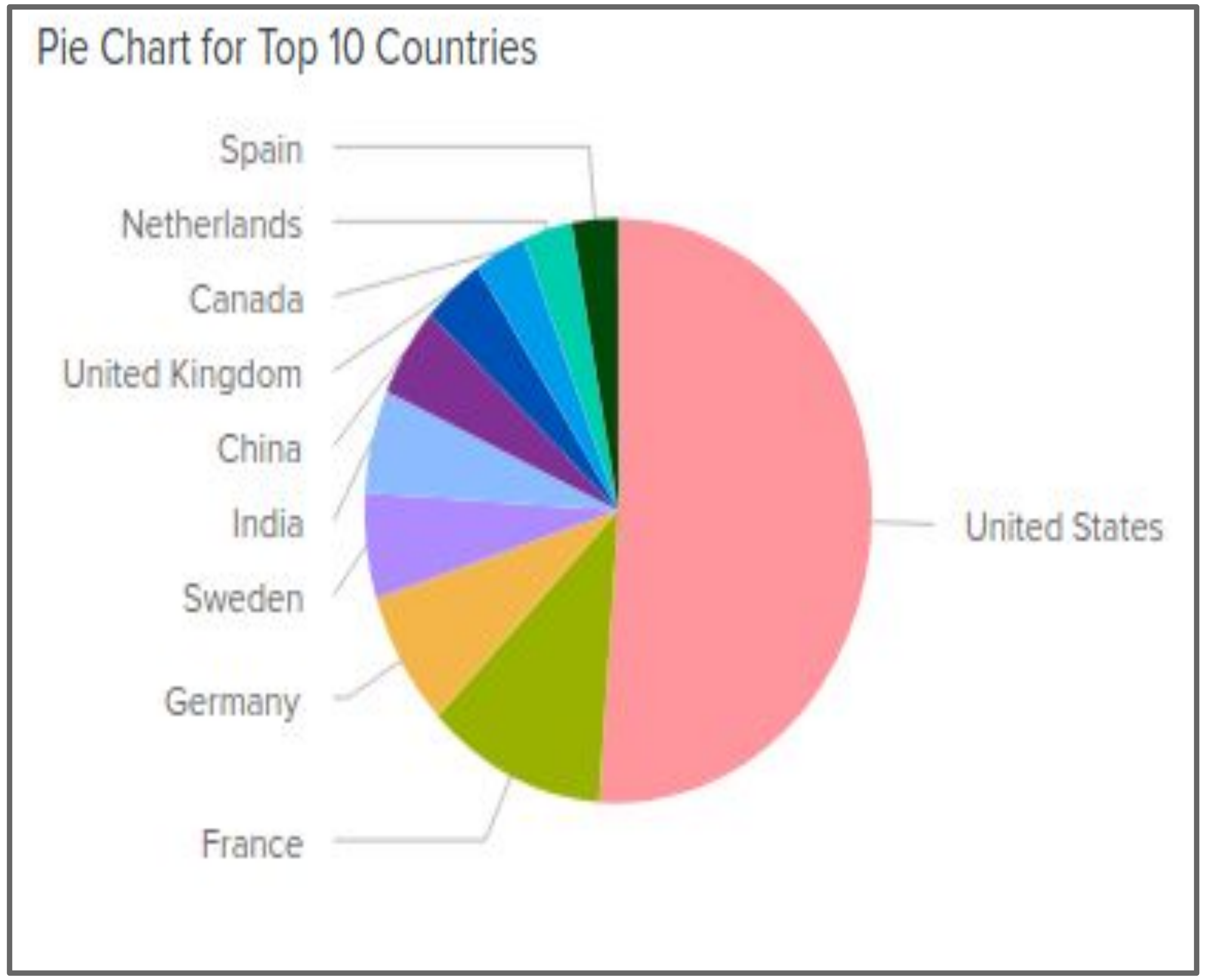


Dashboard Methods — Apache



Geolocation — Apache





Attack Analysis

Attack Summary—Windows

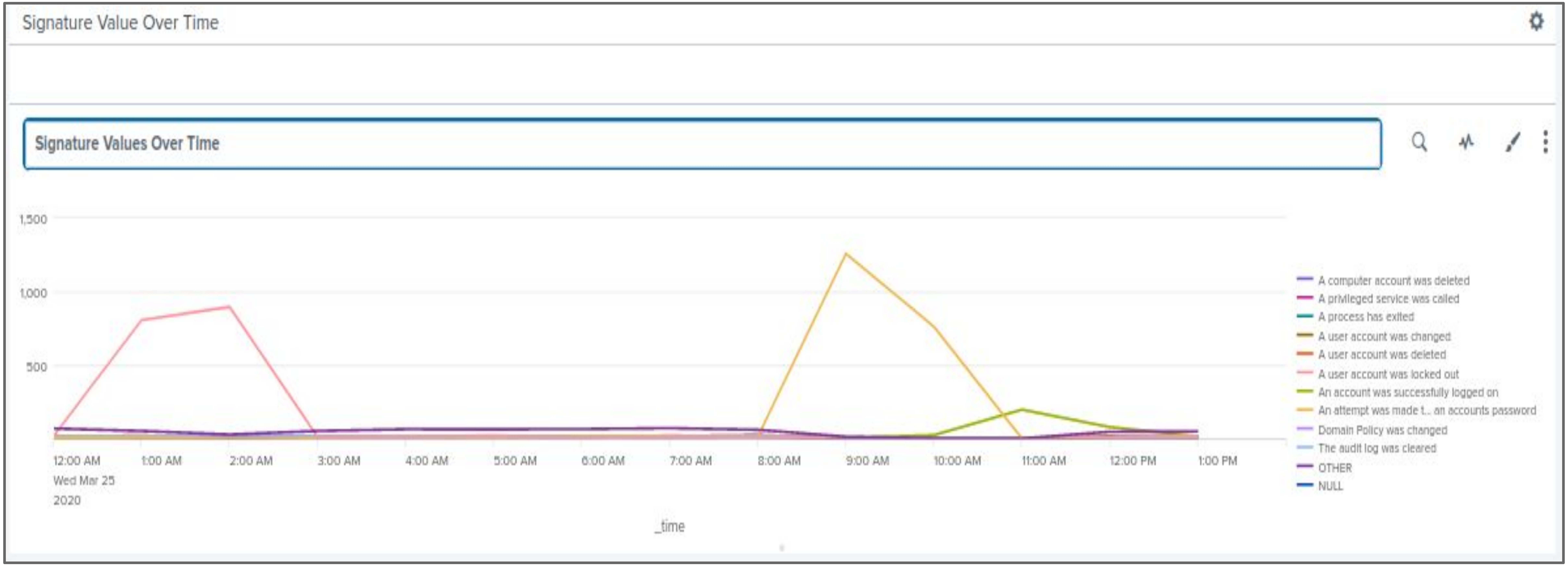
It appears that two users were attacking the system in two different ways.

The logs suggest that user_a and user_k were involved in suspicious activity:

- User_a was active during the hours of midnight to 3AM, which correspond to an increase in user accounts being locked out.
- Meanwhile, user_k showed increased activity during the hours of 8AM to 11AM which correspond to an increase in attempts made to reset account passwords.

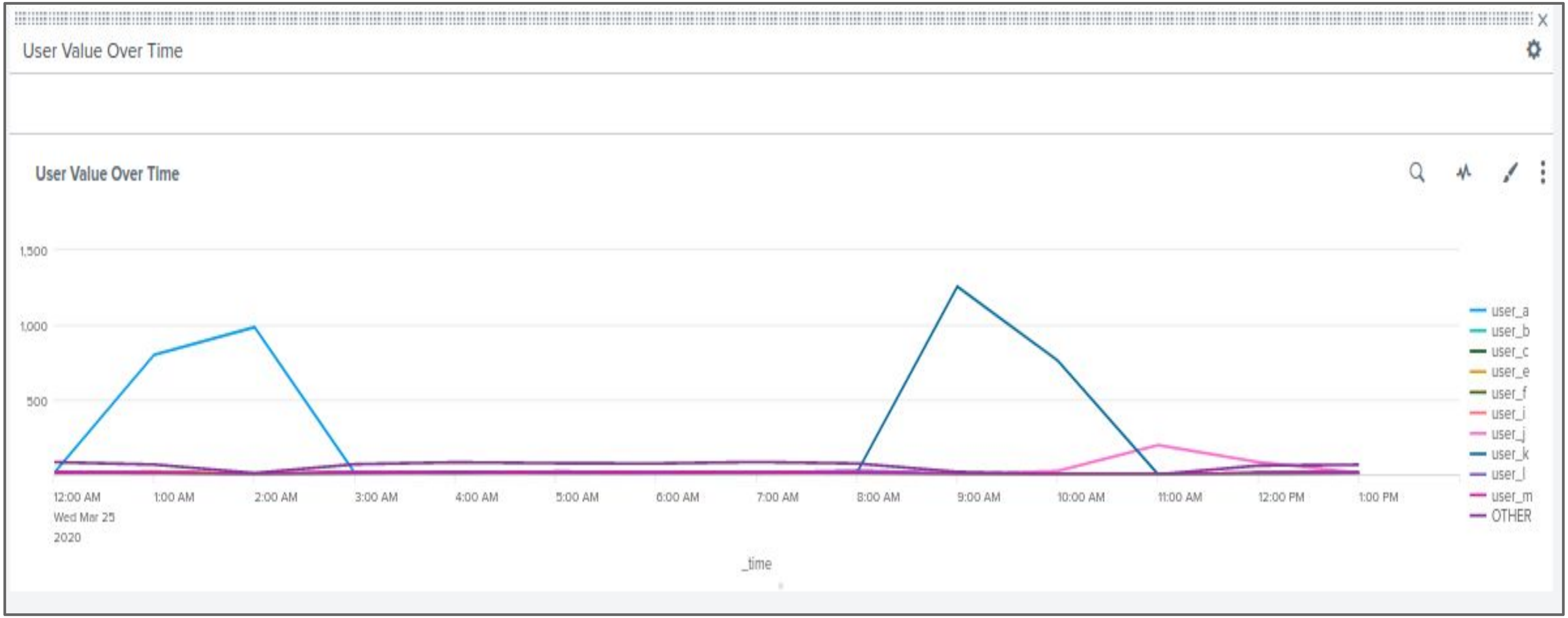
- We analyzed the attack logs on the Windows Server
- Signature Values:
  - User Account Locked Out:
    - from 12AM to 3AM event count total 1701 (805 from 12AM - 1AM, and 896 from 8AM - 11AM).
  - Attempt to Reset Account Password
    - from 8AM - 11AM event count total 2019 (1258 from 8AM - 9AM, and 761 from 10AM - 11AM).

Signature V.O.T— Windows attack logs

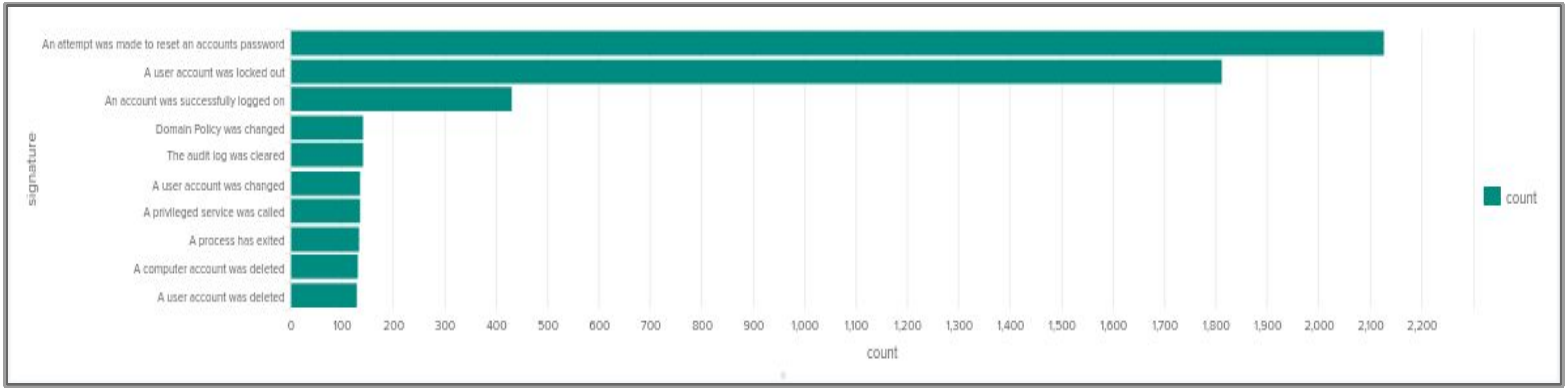


Signature Value Over Time
Signature Values Over Time
1,500
1,000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was successfully logged on
An attempt was made t... an accounts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL

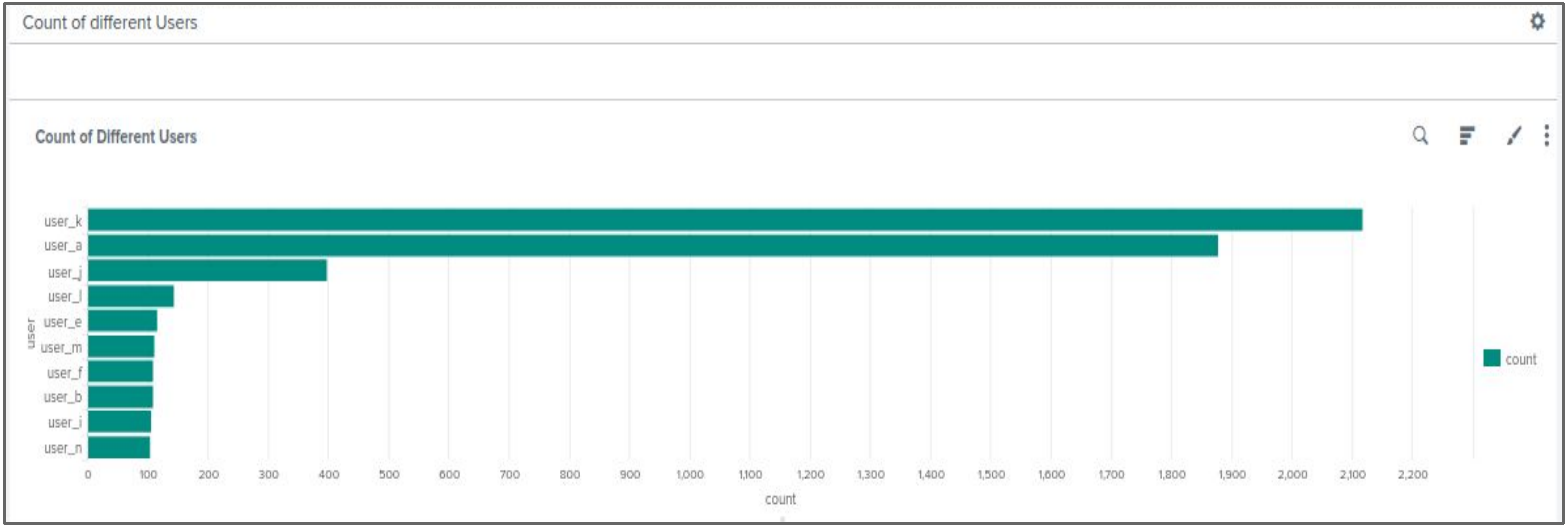
User V.O.T— Windows attack logs



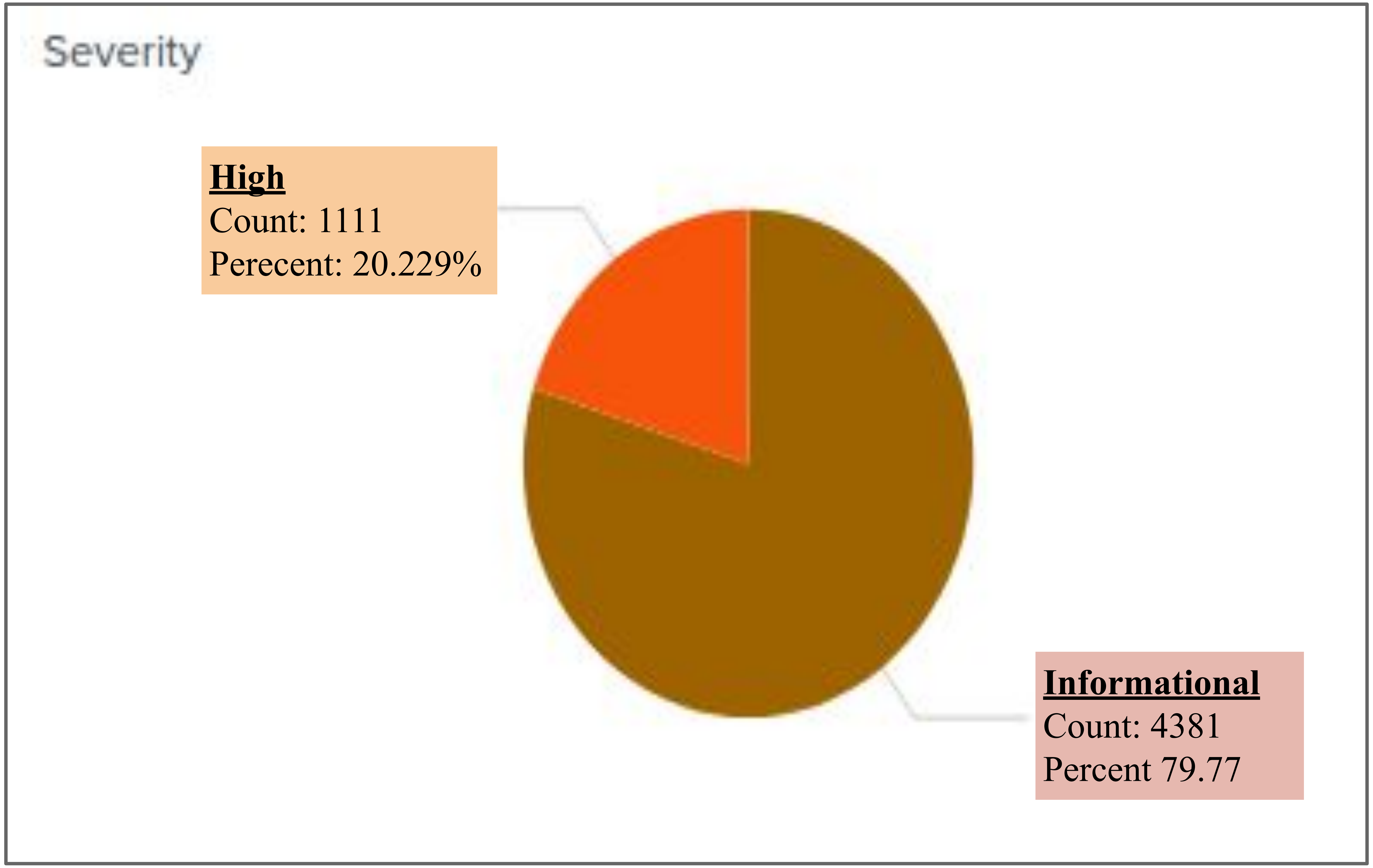
Count of Different Signatures — Windows attack logs



Count of Different Users — Windows attack logs



Severity Pie Chart Attack Log— Windows attack logs



High
Count: 1111
Perecent: 20.229%

Informational
Count: 4381
Percent 79.77

Attack Summary—Apache

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

- It appears that there was a DoS or DDoS attack on the Apache Web Server.
- There was a significant increase in POST requests from 7PM - 9PM
- The URI with the highest count was the VSI_Account_Logon page
- The country with the largest increase in IP traffic origination was the Ukraine

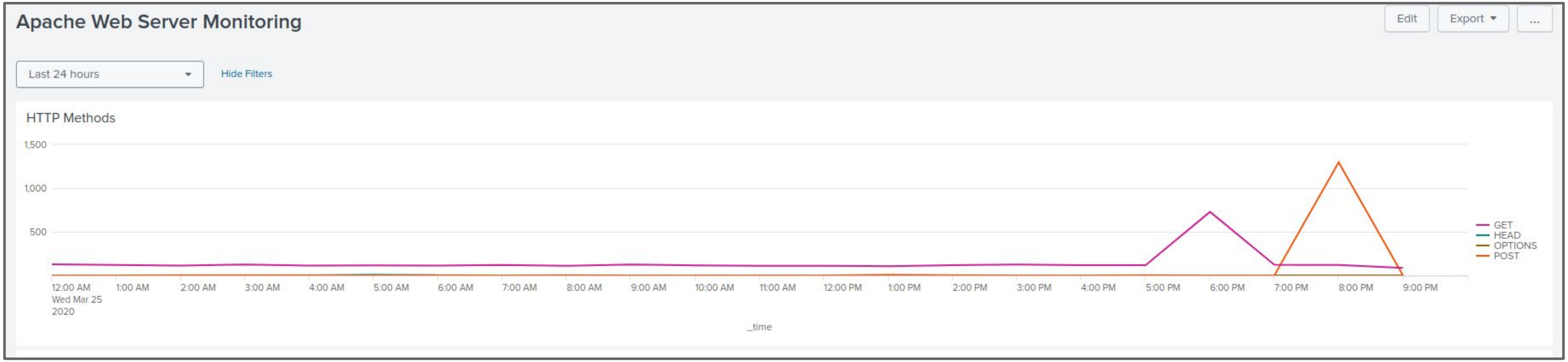
It appears that some malicious actors from Ukraine conducted a DoS attack by brute forcing the VSI_Account_Logon page with POST requests, effectively decreasing the server's capacity for normal traffic and potentially affecting the business.

Attack Summary—Apache

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

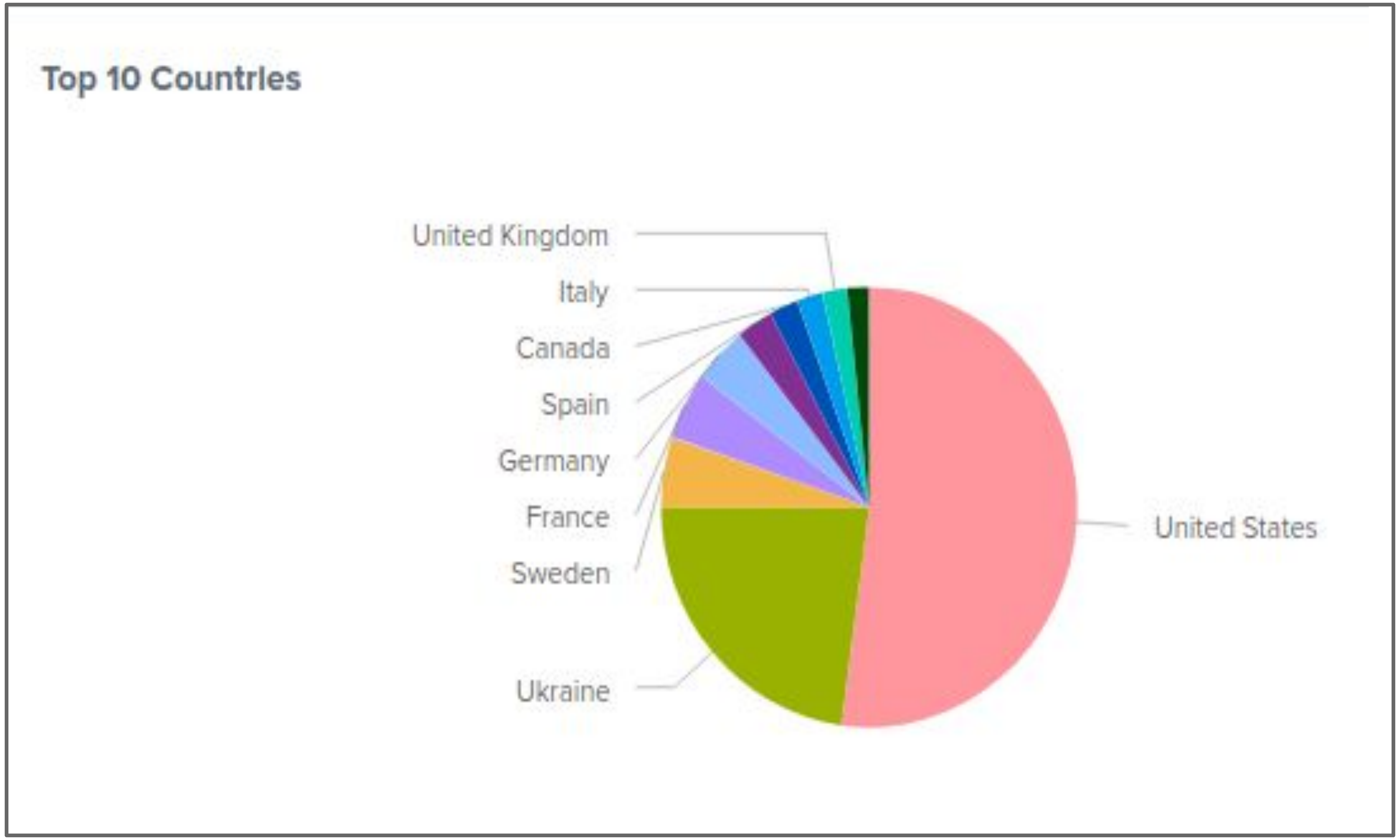
- ALERT: International Activity
  - Threshold 175 (baseline 0-130) - CORRECT
  - International activity peaked at 937 counts requests
- ALERT: HTTP POST Activity
  - Threshold 12 (baseline 0-10) - CORRECT
  - HTTP POST activity peaked at 1296 POST requests

URI & HTTP Methods Attack Log - Apache

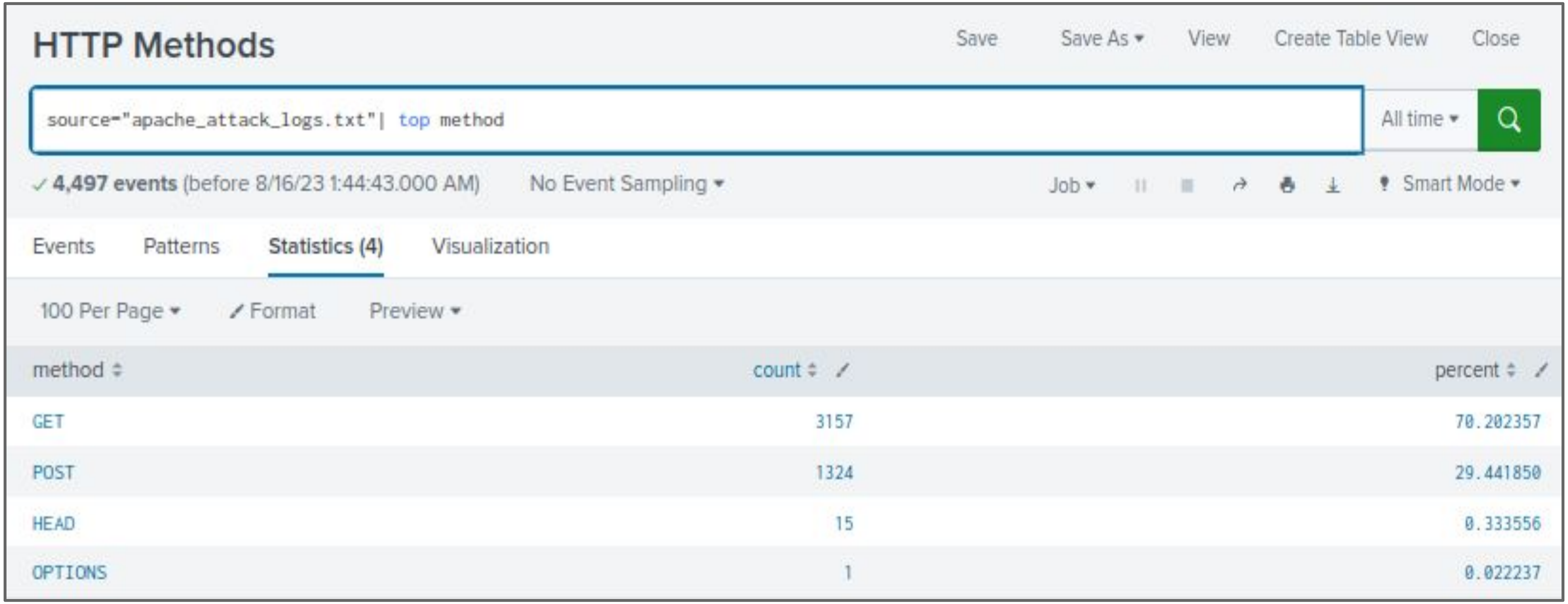


URI's
/VSI_Account_logon.php
/files/logstash/logstash-1.3.2-monolithic.jar
/VSI_Company_Homepage.html
/contactus.html
/images/VSI_headquarters.jpg
/reset.css
/images/web/2009/banner.png
/blog/tags/puppet?flav=rss20
/projects/xdotool/
/?flav=rss20
uri
0
50
100
150
200
250
300
350
400
450
500
550
600
650
700
750
800
850
900
950
1,000
1,050
1,100
1,150
1,200
1,250
1,300
1,350
count
count

Country Pie Chart Attack Log - Apache



HTTP Methods Attack Report — Apache

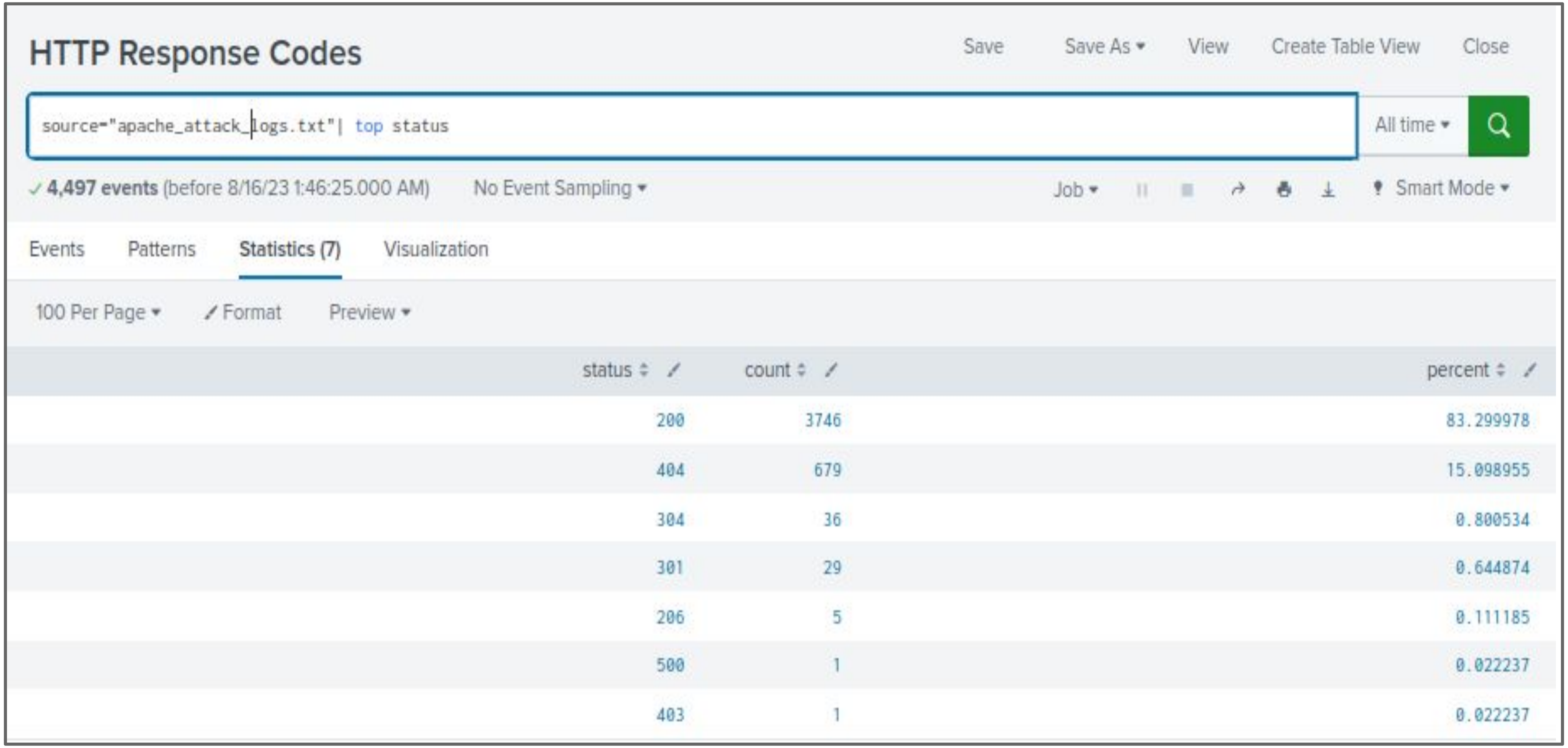


```
source="apache_attack_logs.txt"| top method
```

✓ 4,497 events (before 8/16/23 1:44:43.000 AM)

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

HTTP Response Codes Attack Report — Apache

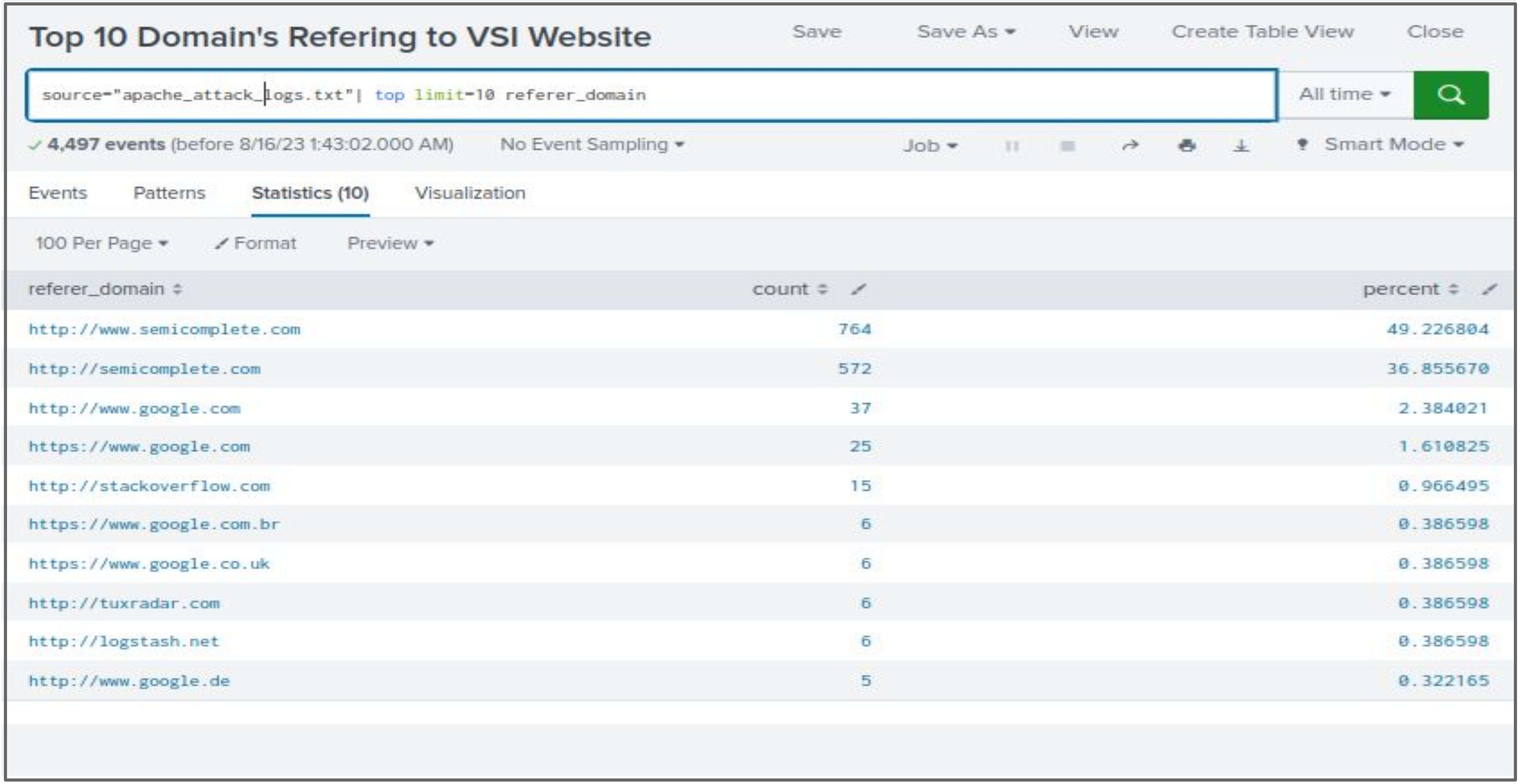


```
source="apache_attack_logs.txt"| top status
```

✓ 4,497 events (before 8/16/23 1:46:25.000 AM) No Event Sampling ▾

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

VSI Domains Attack Report — Apache



Top 10 Domain's Refering to VSI Website

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

✓ 4,497 events (before 8/16/23 1:43:02.000 AM)

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

Summary and Future Mitigations

Project 3 Summary

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

During distinct hours, two users, user_a and user_k, engaged in targeted malicious activities: locking out accounts and attempting password resets, hinting at a possible coordinated attack. Additionally, a separate Denial of Service attack from Ukraine intensely targeted the Apache Web Server's VSI_Account_Logon page, marked by a surge in POST requests between 7PM - 9 PM. These anomalies surpassed set alert thresholds, indicating heightened malicious activity.

Project 3 Future Mitigations

- **To protect VSI from future attacks, what future mitigations would you recommend?**

  User behaviour Analytics: Implement a UBA solution to detect unusual activities from user accounts, especially during off-hours.

  Rate Limiting: Introduce rate-limiting on critical pages such as VSI_Account_Logon.

  Geo-IP Blocking: Considering the significant malicious traffic originating from Ukraine, temporary Geo-IP based blocking can be considered, especially during times of increased threat perception.

  Multi-Factor Authentication: Implement MFA for all user accounts

  Regular Backups: Ensure regular backups of critical data are taken and stored securely offsite. This ensures data integrity and availability in case of any breaches.