Defensive Security Project
by: Nickson Njau

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Today, you will play the role of an 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 business.
- 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 tasked 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's back-end operations

Whoisxml IP Geolocation API

Whoisxml IP Geolocation API

Whoisxml IP Geolocation API for Splunk is a tool designed to provide geolocation data for IP addresses directly within the Splunk platform.

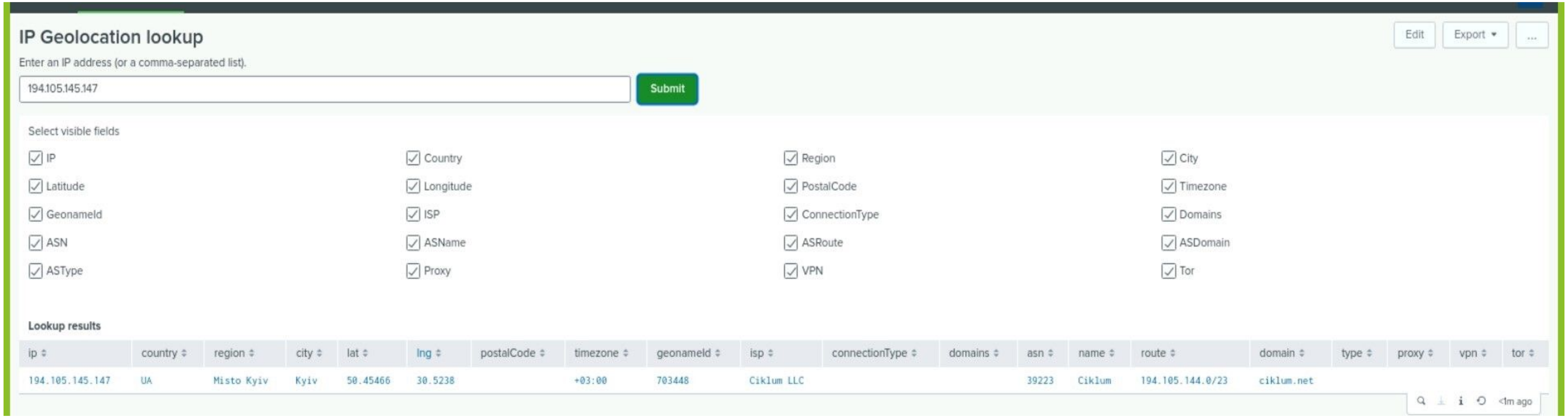
- This add-on allows splunk users to search for geographical information based on the IP addresses present in their logs or datasets. Add-on information:
  - Country
  - City
  - Latitude
  - Longitude
  - Postal Code
  - VPN

This integration allows for the filtering of geographical origins of network traffic, users, or other relevant data points, assisting in security analysis, compliance, and business intelligence. This API retrieves information of IP address data, providing accurate and up-to-date geolocation data to enhance the analysis capabilities of Splunk users.

Whoisxml IP Geolocation API

This tool is helpful for being able to note specific locations of ip addresses better than the cluster map itself.

On the cluster map, it's very easy to miss any small new locations without zooming in and inspecting every country very closely. With this, we were able to find a new clientip location in Kiev, Ukraine.



IP Geolocation lookup

Enter an IP address (or a comma-separated list).

194.105.145.147

Select visible fields

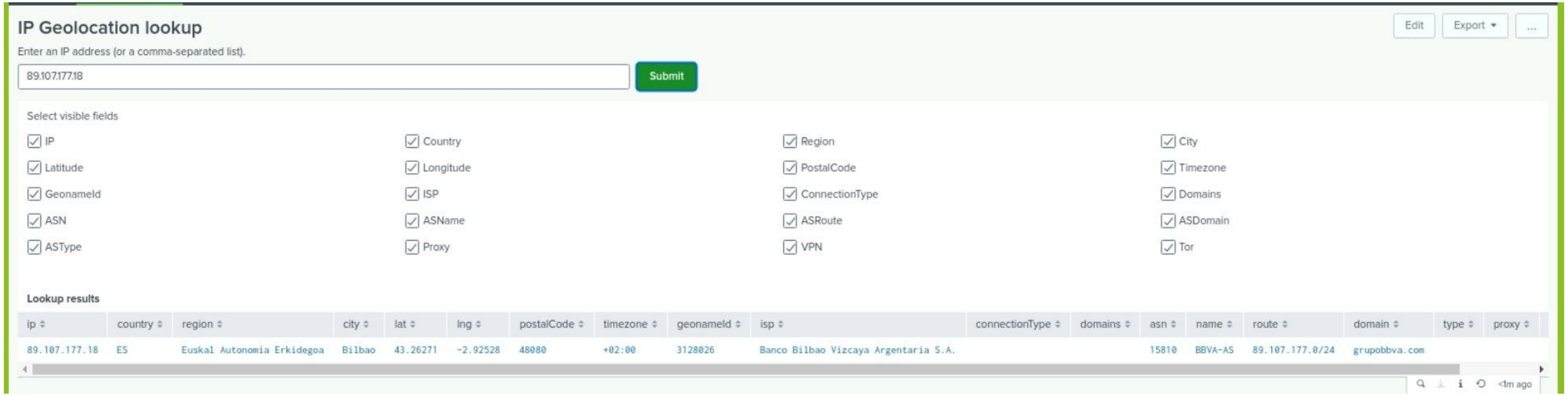
☑ IP ☑ Country ☑ Region ☑ City
☑ Latitude ☑ Longitude ☑ PostalCode ☑ Timezone
☑ GeonameId ☑ ISP ☑ ConnectionType ☑ Domains
☑ ASN ☑ ASName ☑ ASRoute ☑ ASDomain
☑ ASType ☑ Proxy ☑ VPN ☑ Tor

Lookup results

ip	country	region	city	lat	lng	postalCode	timezone	geonameId	isp	connectionType	domains	asn	name	route	domain	type	proxy	vpn	tor
194.105.145.147	UA	Misto Kyiv	Kyiv	50.45466	30.5238		+03:00	703448	Ciklum LLC			39223	Ciklum	194.105.144.0/23	ciklum.net				

Whoisxml IP Geolocation API (example)

Spain



IP Geolocation lookup

Enter an IP address (or a comma-separated list).

89.107.177.18

Submit

Select visible fields

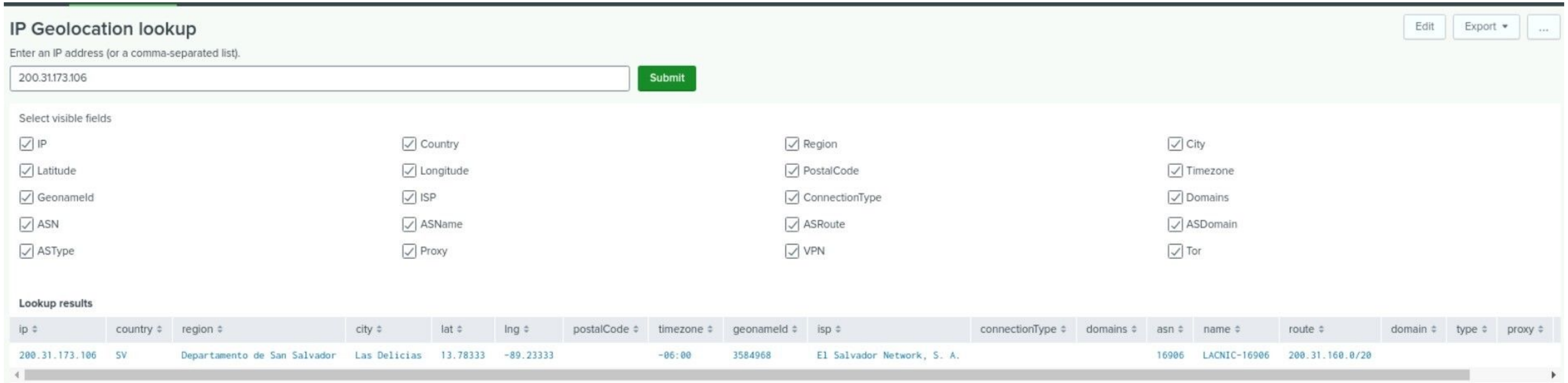
- ☑ IP
- ☑ Latitude
- ☑ GeonameId
- ☑ ASN
- ☑ ASType
- ☑ Country
- ☑ Longitude
- ☑ ISP
- ☑ ASName
- ☑ Proxy
- ☑ Region
- ☑ PostalCode
- ☑ ConnectionType
- ☑ ASRoute
- ☑ VPN
- ☑ City
- ☑ Timezone
- ☑ Domains
- ☑ ASDomain
- ☑ Tor

Lookup results

ip	country	region	city	lat	lng	postalCode	timezone	geonameId	isp	connectionType	domains	asn	name	route	domain	type	proxy
89.107.177.18	ES	Euskal Autonomia Erkidegoa	Bilbao	43.26271	-2.92528	48080	+02:00	3128026	Banco Bilbao Vizcaya Argentaria S.A.			15810	BBVA-AS	89.107.177.0/24	grupobbva.com		

<1m ago

El Salvador



IP Geolocation lookup

Enter an IP address (or a comma-separated list).

200.31.173.106

Submit

Select visible fields

- ☑ IP
- ☑ Latitude
- ☑ GeonameId
- ☑ ASN
- ☑ ASType
- ☑ Country
- ☑ Longitude
- ☑ ISP
- ☑ ASName
- ☑ Proxy
- ☑ Region
- ☑ PostalCode
- ☑ ConnectionType
- ☑ ASRoute
- ☑ VPN
- ☑ City
- ☑ Timezone
- ☑ Domains
- ☑ ASDomain
- ☑ Tor

Lookup results

ip	country	region	city	lat	lng	postalCode	timezone	geonameId	isp	connectionType	domains	asn	name	route	domain	type	proxy
200.31.173.106	SV	Departamento de San Salvador	Las Delicias	13.78333	-89.23333		-06:00	3584968	El Salvador Network, S. A.			16906	LACNIC-16906	200.31.160.0/20			

Logs Analyzed

1 Windows Logs

These logs contained incidents that occurred on the Windows server. The incident signatures had a correlated ID and severity level, and displayed whether they were a success or failure. Some of these incidents included successful logins, deleted accounts, and user activity on the server.

2 Apache Logs

These logs examine routine activity from the Apache web server for VSI. The activities display the HTTP type, the top 10 domains, and the quantity of each HTTP response code.

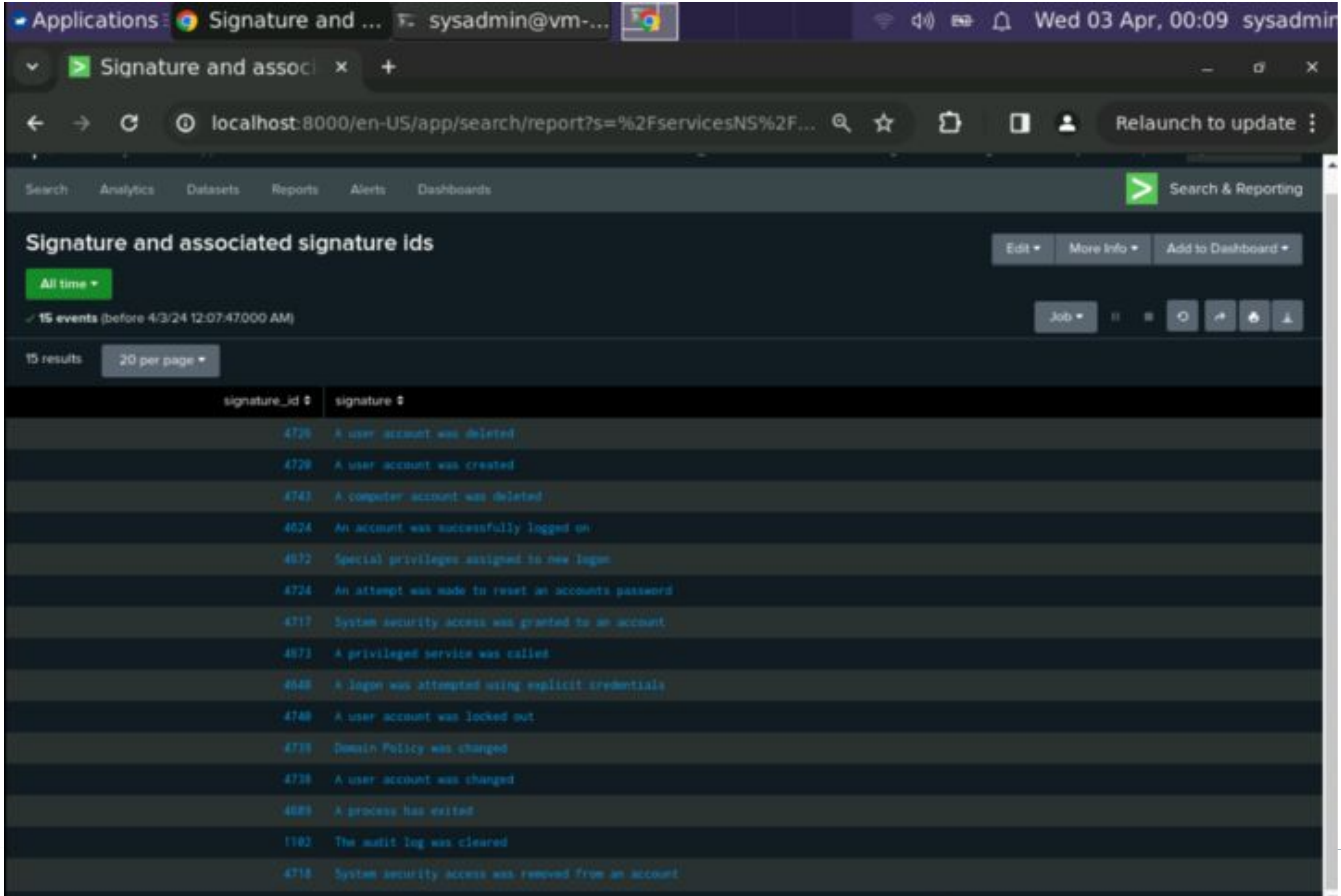
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	**Report Description**
Signature and associated signature IDs	A table of signatures and associated signature IDs
Severity level, count, and percentage	Severity levels with count and percentage of each
Success vs. failure	Comparison of success and failures of windows activities

Images of Reports—Signature and associated signature IDs



Signature and associated signature ids

✓ 15 events (before 4/3/24 12:07:47.000 AM)

15 results

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

Images of Reports—Severity level, count, and percentage

Severity Level,Count and Percentage

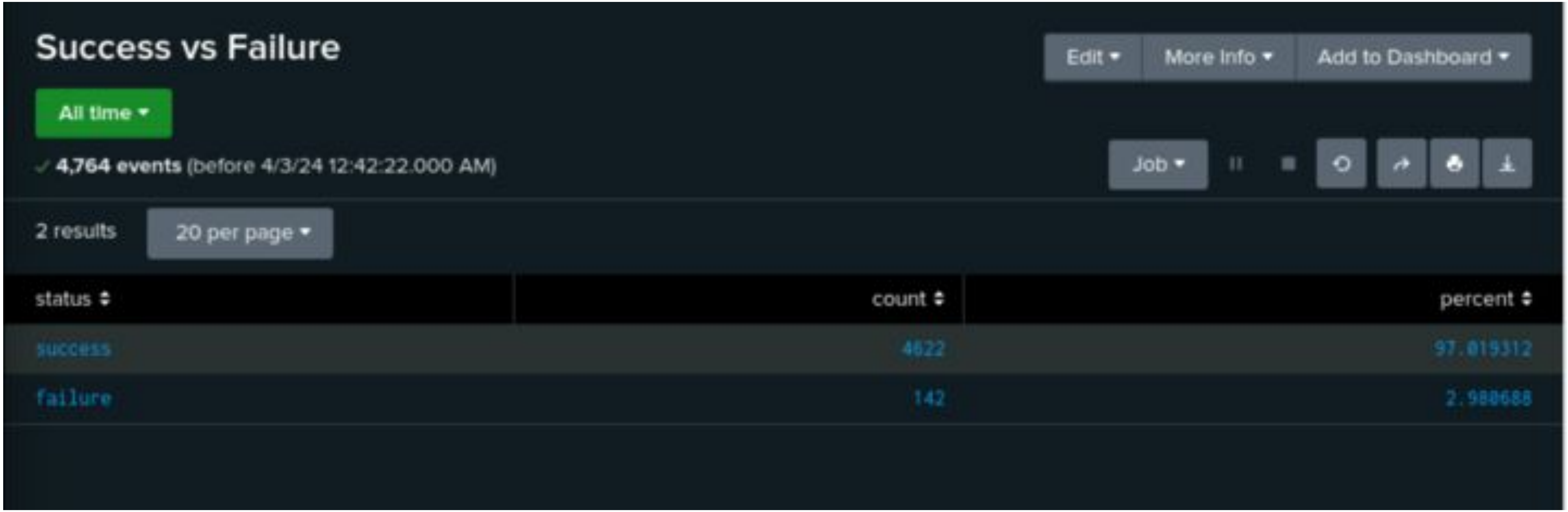
Edit ▾
More Info ▾
Add to Dashboard ▾
All time ▾
Job ▾
20 per page ▾

✓ 4,764 events (before 4/3/24 12:22:29.000 AM)

2 results

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Images of Reports—Success vs. failure



Success vs Failure

✓ **4,764 events** (before 4/3/24 12:42:22.000 AM)

2 results

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
Status failure	An email is sent to SOC@VSI-company.com when the threshold of failed windows activity is crossed.	6	greater than 7

JUSTIFICATION: The average amount of failed Windows activity averaged around 6 to establish our baseline yet never got close to 7. Failures exceeding 7 would certainly indicate suspicious activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful logins	An email is sent to SOC@VSI-company.com when the threshold of successful logins is crossed.	14	greater than 15

JUSTIFICATION: The average amount of logins, designated by signature id “4624,” averaged around 14 to establish 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
User account deleted	An email is sent to SOC@VSI-company.com when the threshold of deleted accounts is crossed.	13	greater than 14

JUSTIFICATION: With the amount of user accounts deleted, designated by signature id “4743” in this log, we were able to determine a baseline of 13 seemed on par with a "normal" hour. Exceeding 14 would raise suspicion levels and indicate a problem.

Dashboards—Windows

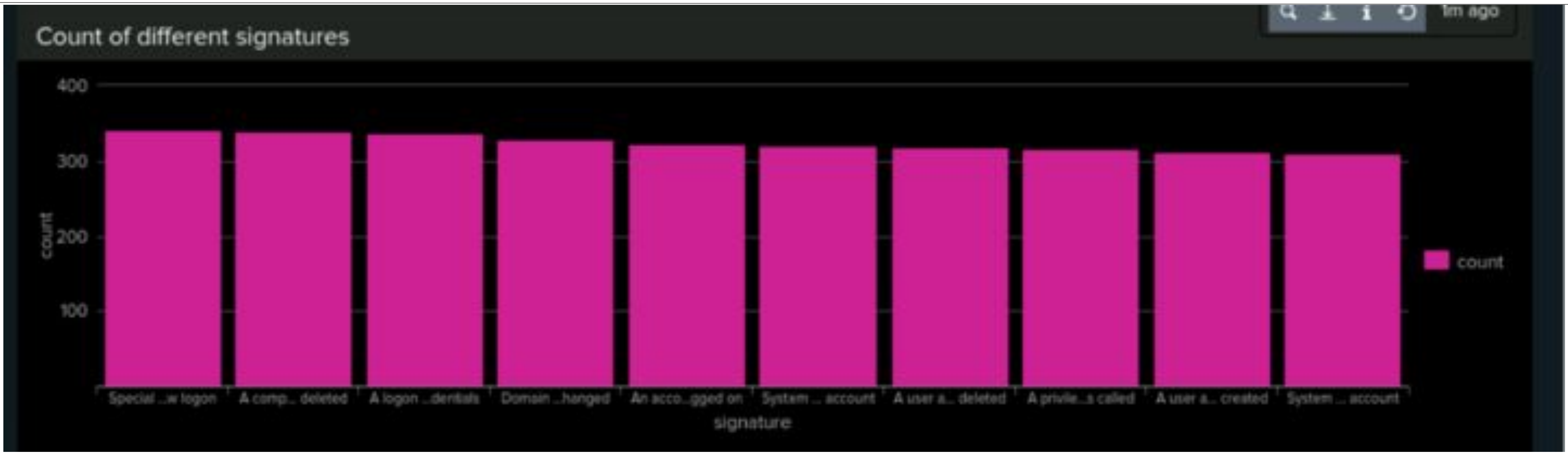
Trends for signatures over time

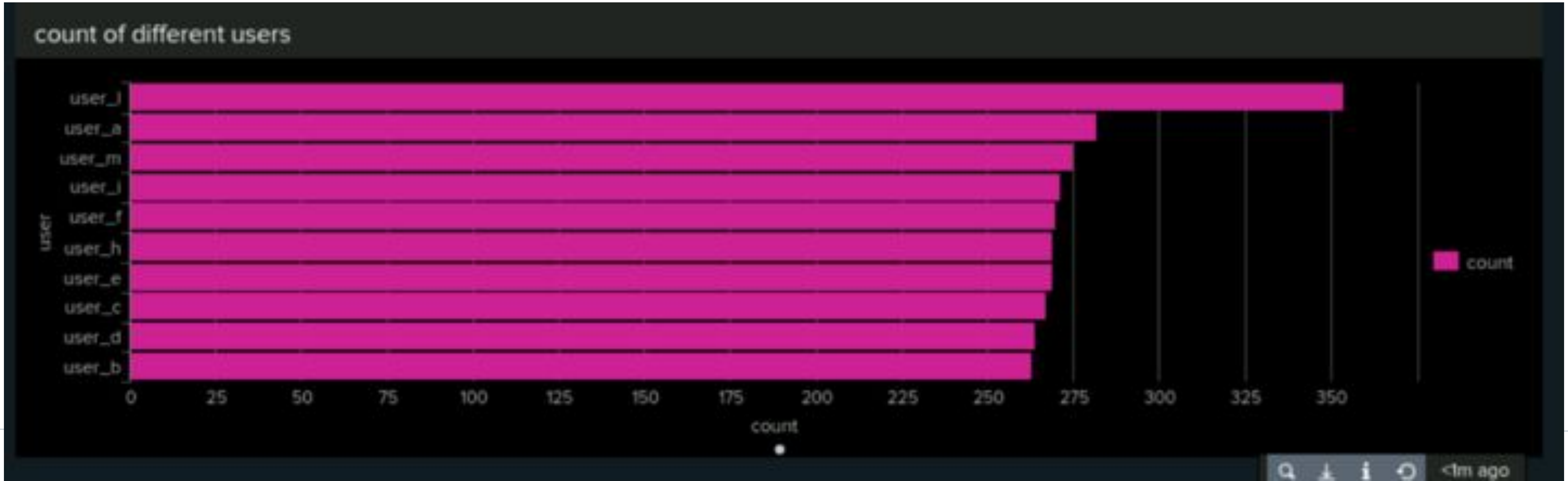
Trends for signature_id
100
50
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials.
A privileged service was called
A process has exited
A user account 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 was removed from an account
OTHER

Different User field values over time

100
75
50
25
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
_time
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_j
user_m
OTH

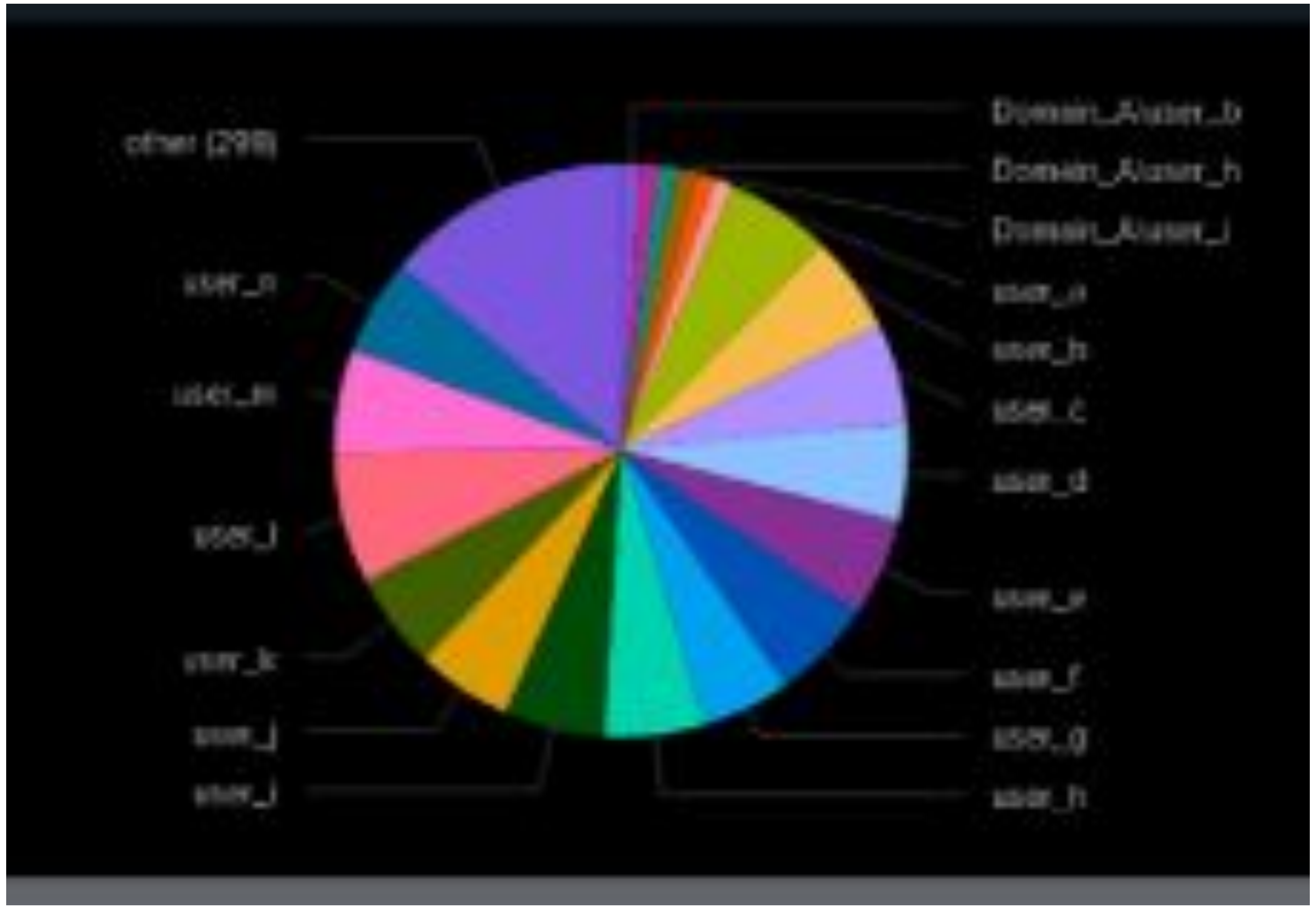
Dashboards—Windows



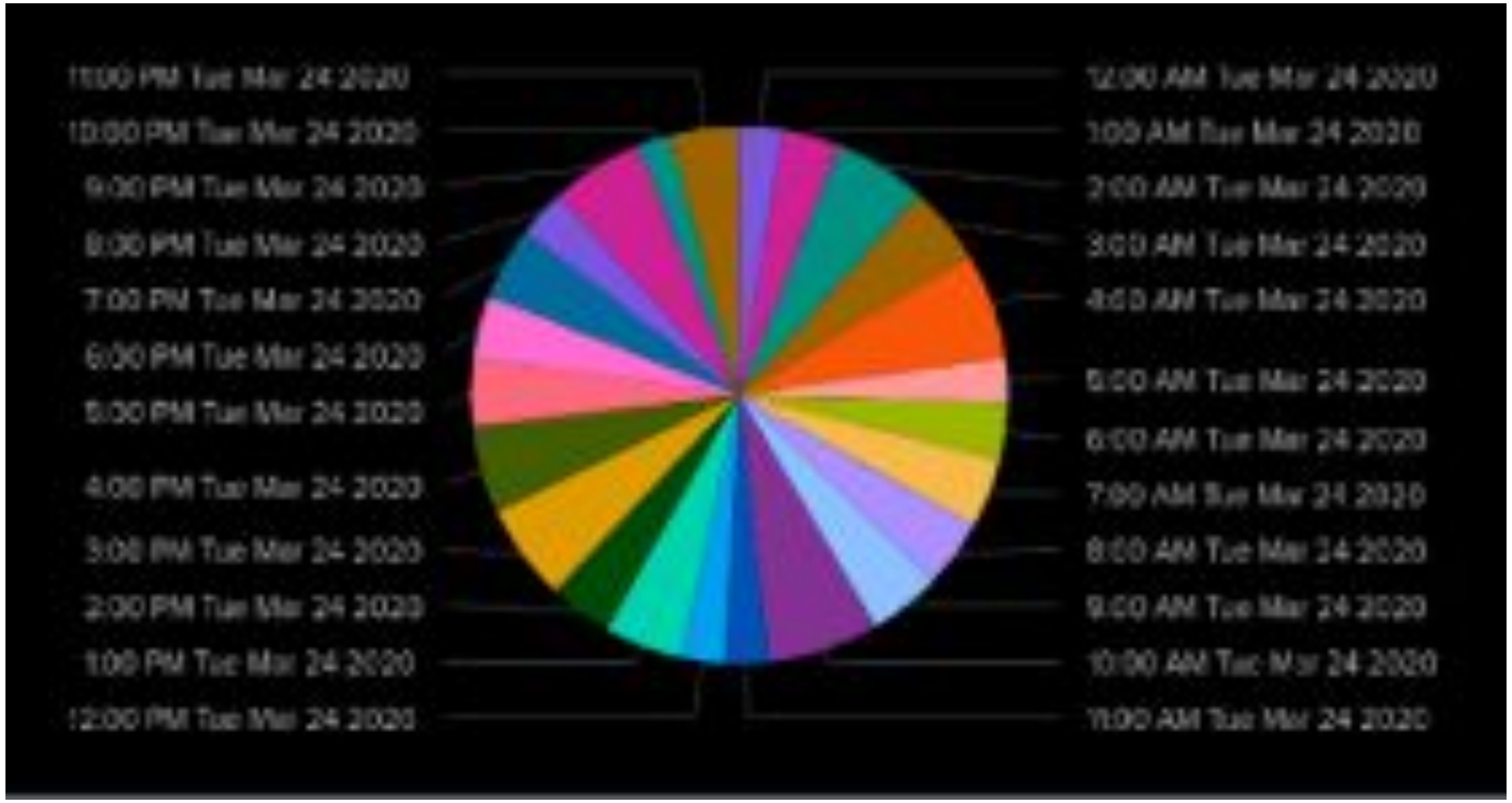


Dashboards—Windows

Different user counts



Timechart signature ID



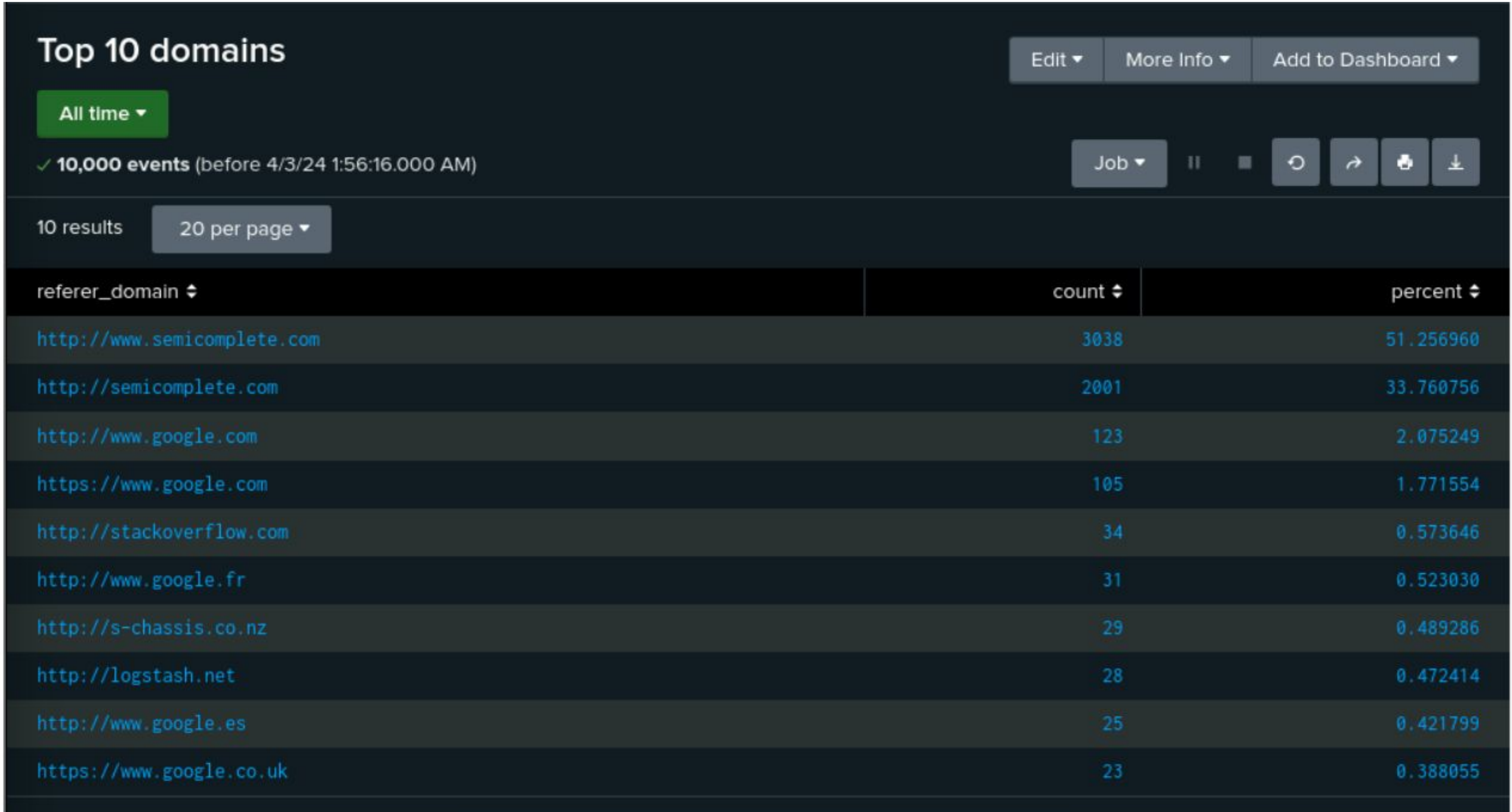
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Provides insight into the type of HTTP activity being requested against VSI's web server.
Top 10 Domains	Shows the top 10 domains that refer to VSI's website.
Count of HTTP Response Code	Shows the count of each HTTP response code.

Images of Reports—Top 10 Domains



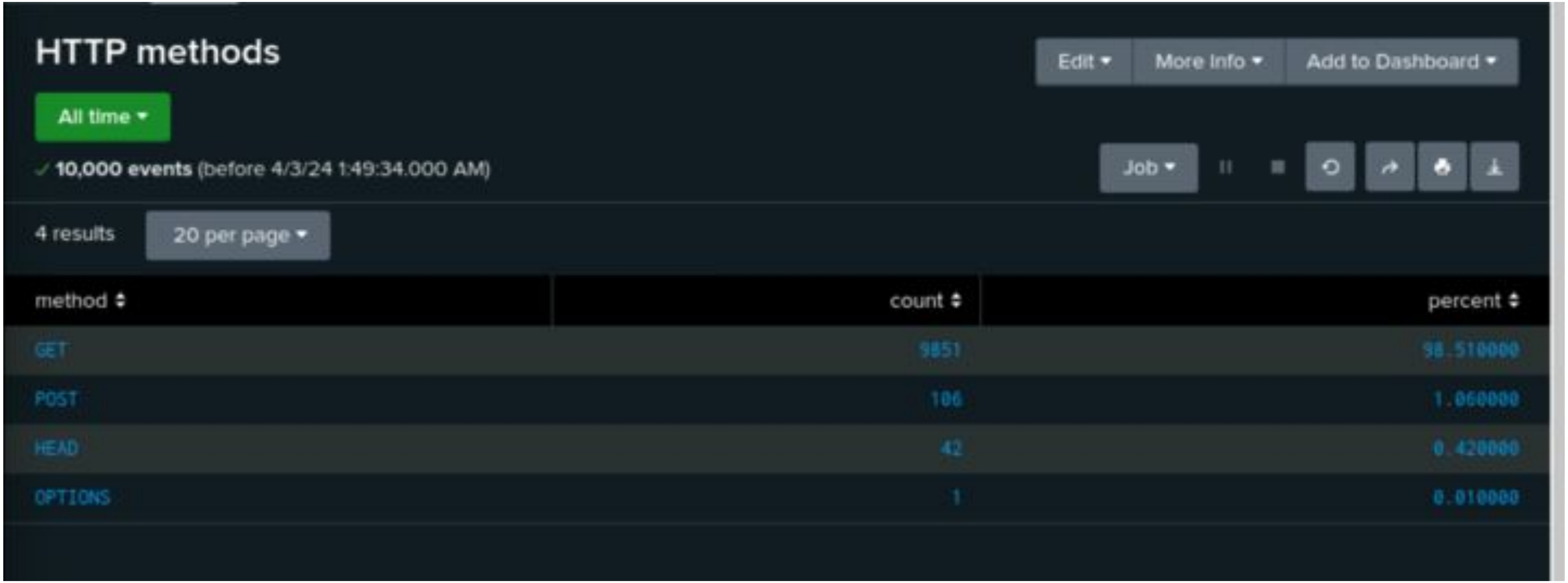
Top 10 domains

✓ **10,000 events** (before 4/3/24 1:56:16.000 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

Images of Reports—HTTP Methods



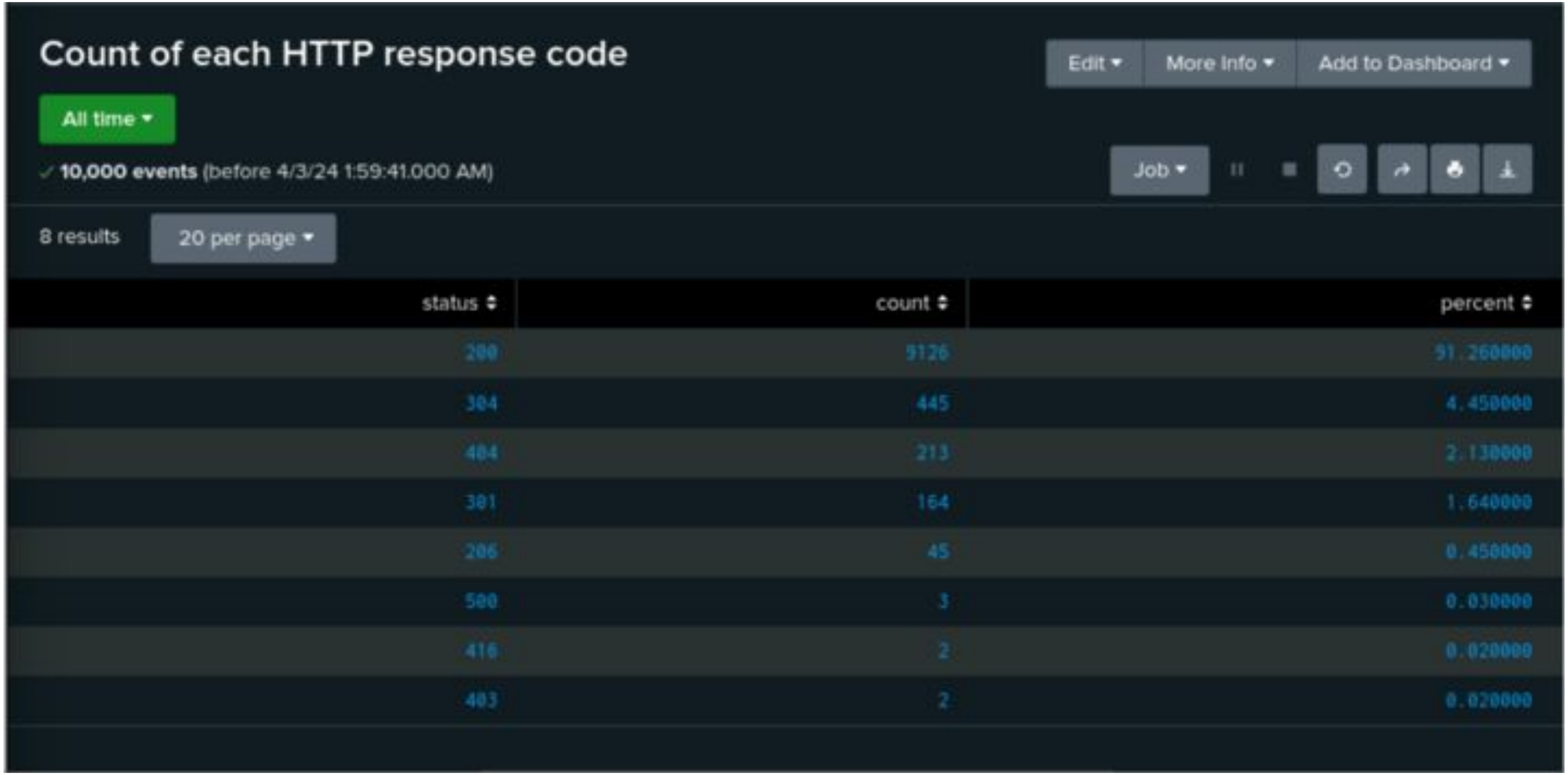
HTTP methods

✓ **10,000 events** (before 4/3/24 1:49:34.000 AM)

4 results

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

Images of Reports—Count of HTTP Response Code



Count of each HTTP response code

✓ **10,000 events** (before 4/3/24 1:59:41.000 AM)

8 results

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-USA Activity	Alert if the hourly activity from any country besides the United States exceeds the threshold.	94	95 or above

JUSTIFICATION: 94 events in a hour seemed standard in the logs, yet exceeding 95 seemed unlikely on a normal day. Seeing any number of events greater than the threshold would indicate issues.

Alerts—Apache

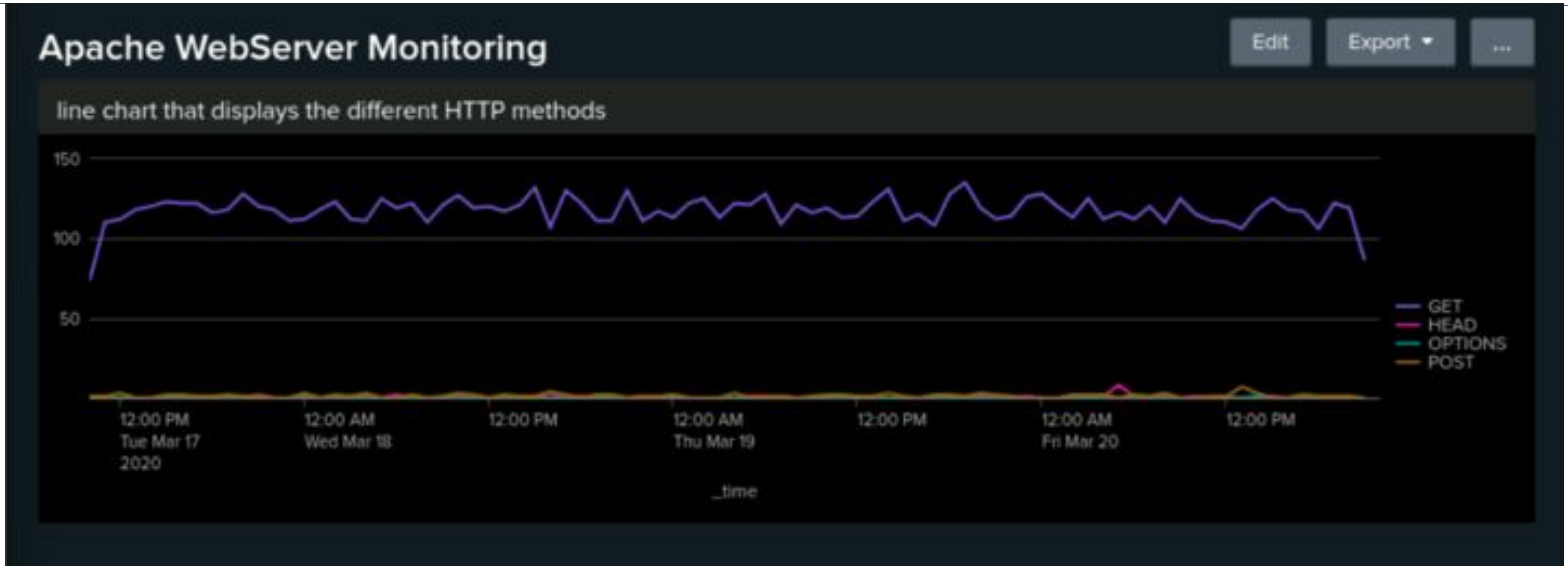
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Count	Alert if the hourly count of the HTTP POST method exceeds the threshold	3	4 or above

JUSTIFICATION: Most events per hour hovered between 1 and 3 and never surpassed 3. A threshold of 4 seemed like a number that would be out of reach of "normal" hourly events but small enough to catch malicious activity.

Dashboards—Apache

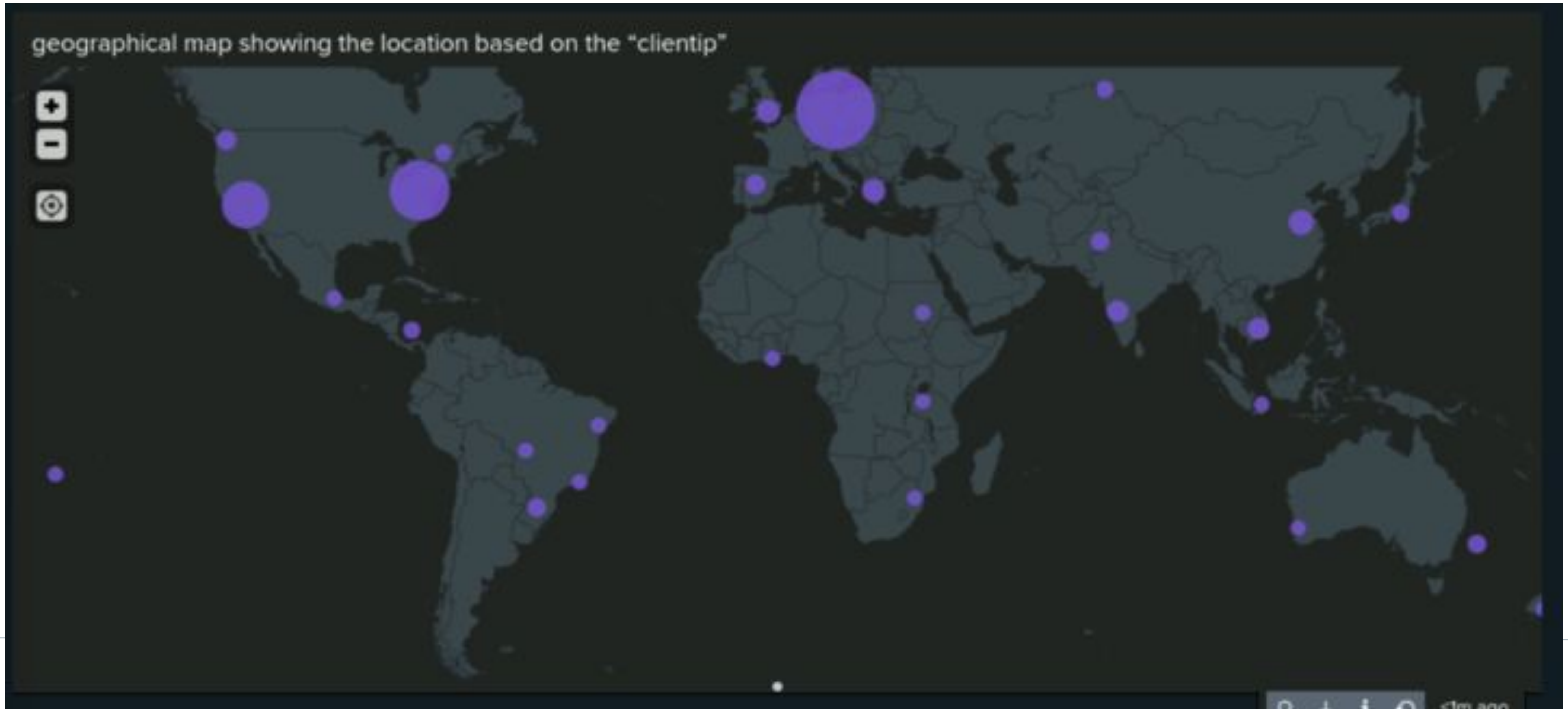
Different HTTP methods



Apache WebServer Monitoring

line chart that displays the different HTTP methods

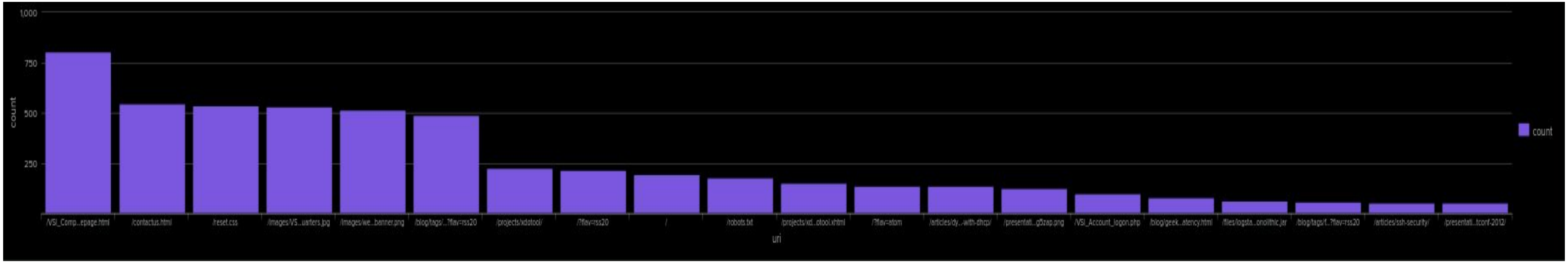
Geographical map



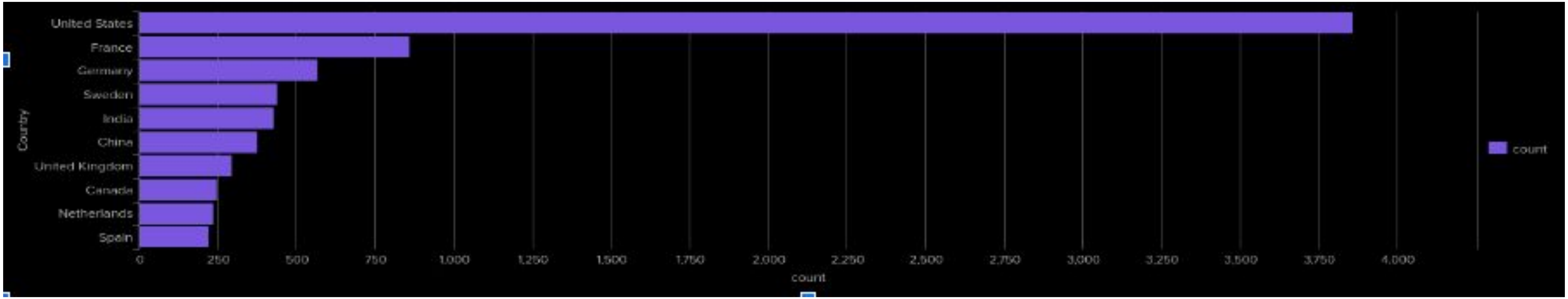
geographical map showing the location based on the “clientip”

Dashboards—Apache

Different URIs

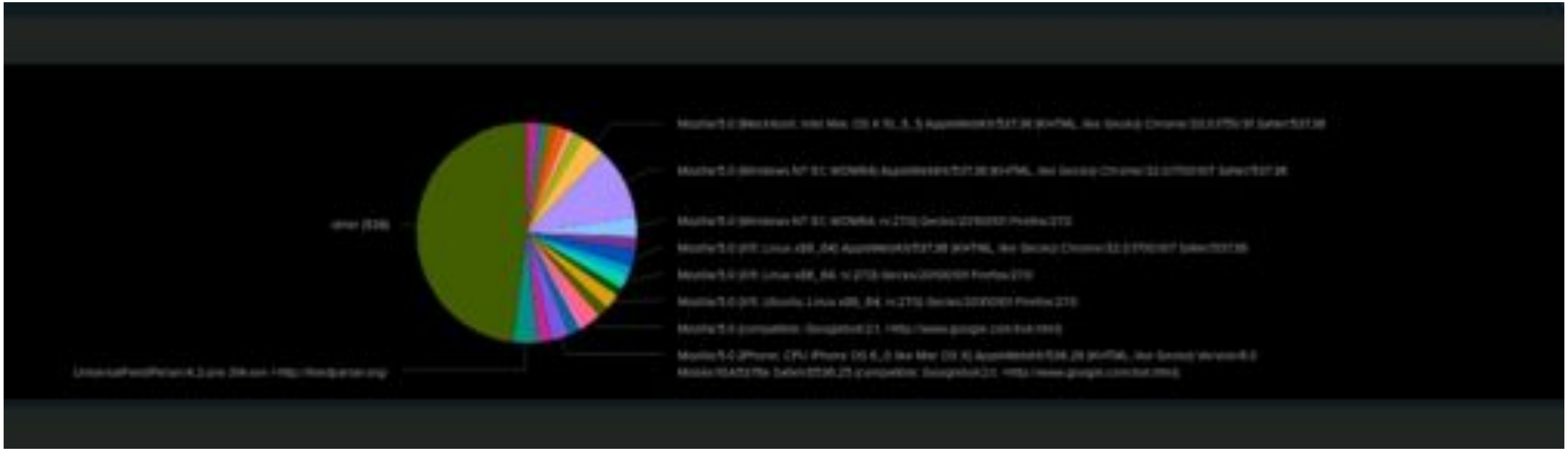


Top 10 Countries

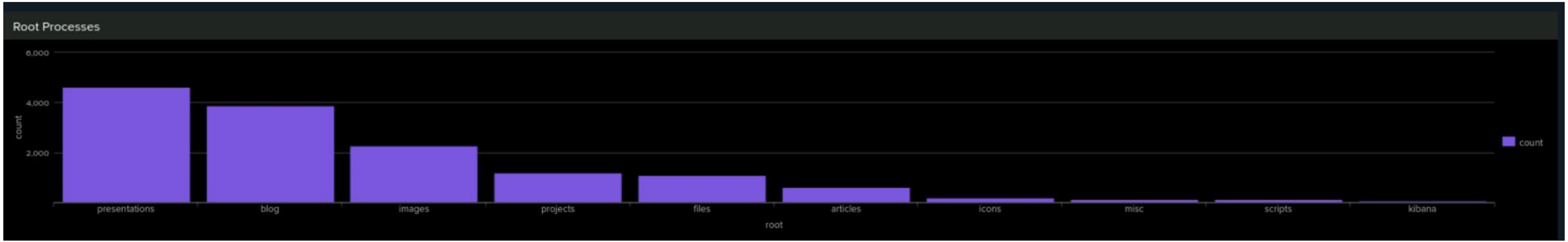


Dashboards—Apache

User Agents



Root Processes



Attack Analysis

Attack Summary—Windows

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

- Upon analyzing Windows attack logs, it was found that the Windows attack system exhibited more severity levels in the "high" category(20%) compared to almost 7% in the "high" category observed before the attack. Furthermore, there were more successes(97% to 98%) than failures(2.9% to 1.5%) noted after the attack. Alert analysis indicated a suspicious volume of failed windows activity. Specifically, 35 failed logins occurred at 8 am on 3/25/2020, exceeding the threshold, with no recommended changes. Additionally, suspicious volumes of successful logins were detected, with 1256 events recorded in one hour, primarily attributed to the user "user_k" logging in at 10 am to 1 pm on 3/25/2020. The alert threshold of >15 was exceeded, suggesting a sufficient threshold.

Attack Summary—Windows

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

- An alert analysis indicated a suspicious volume of failed activity. There was a suspicious volume of deleted accounts, with the threshold set to >14. Notable signatures included "A user account was locked out" and "An attempt was made to reset an account's password," with specific start and stop times for each signature. "A user account was locked out" occurred from 12:00 am to 3:00 am, while "An attempt was made to reset an account's password" happened from 8:00 am to 11 am, peaking at 896 and 1258, respectively. Successful logons happened from 10:00 am to 1:00pm and peaked 196.

Attack Summary—Windows

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

Findings from dashboards analyzing attack logs revealed suspicious activity associated with 3 users:

- User_a (locked out) 12am - 3am
- User_k (password reset) 8am-11am
- User_j (an account successfully logged on) 10am-1PM

Attack Summary—Windows

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

Findings from our alerts when analyzing the attack logs indicated the following:
We detected a suspicious volume activity in 3 hour increments:

- User locked out 12am - 3am
- Password reset 8am-11am
- An account successfully logged on 10am-1PM

Our thresholds were set a little bit lower than they were supposed to be, but our alert would have been triggered for all 3 alerts not long after suspicious activity started.

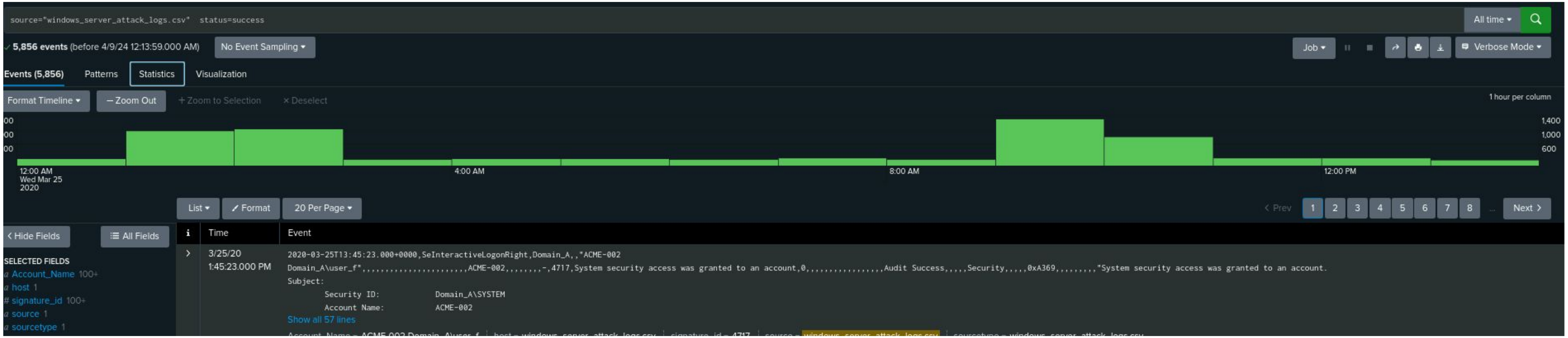
Attack Summary—Windows

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

- Suspicious activity was observed in two users, User_A and User_K. User_A's activity occurred from 12 am to 3 am, while User_K's activity spanned from 8 am to 11 am. The peak count of different users was 984 for User_A and 1256 for User_K.
- There was suspicious activity associated with signatures, particularly "A user account was locked out" and "An attempt was made to reset an account's password," both exhibiting very high volumes of activity. The first signature lasted from 12 am to 3 am, while the second occurred from 8 am to 11 am. "A user account..." peaked at a count of 896, and "An attempt..." peaked at 1258.

Screenshots of Windows Attack Logs

Successful Logins

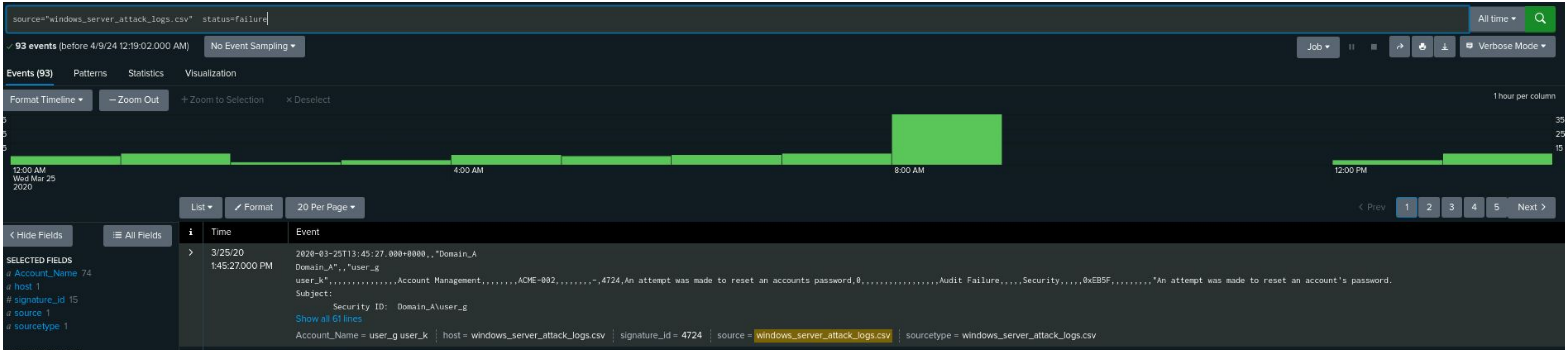


```
source="windows_server_attack_logs.csv"  status=success
```

✓ **5,856 events** (before 4/9/24 12:13:59.000 AM) No Event Sampling ▾

i	Time	Event
>	3/25/20 1:45:23.000 PM	2020-03-25T13:45:23.000+0000,SeInteractiveLogonRight,Domain_A,,"ACME-002 Domain_A\user_f",,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4717,System security access was granted to an account,0,,,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"System security access was granted to an account. Subject: Security ID: Domain_A\SYSTEM Account Name: ACME-002 Show all 57 lines

Failed Logins



```
source="windows_server_attack_logs.csv"  status=failure
```

✓ **93 events** (before 4/9/24 12:19:02.000 AM) No Event Sampling ▾

i	Time	Event
>	3/25/20 1:45:27.000 PM	2020-03-25T13:45:27.000+0000,,"Domain_A Domain_A",,"user_g user_k",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0xEB5F,,,,,,,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_A\user_g Show all 61 lines Account_Name = user_g user_k | host = windows_server_attack_logs.csv | signature_id = 4724 | source = windows_server_attack_logs.csv | sourcetype = windows_server_attack_logs.csv

Attack Summary—Apache

Summarize your findings from your reports when analyzing the attack logs

Findings from our reports when analyzing the attack logs indicated the following:

- We saw an increase in POST requests by around 1,200.
- There were no suspicious changes in referrer domains.
- The number of 404 response codes increased by almost 500.

Attack Summary—Apache

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

Findings from our alerts when analyzing the attack logs indicated the following:

- We detected a suspicious volume of international activity between 8pm and 9pm on March 25, reaching a peak of 957 events during that hour.
- We detected a suspicious volume of HTTP POST activity between 8pm and 9pm on March 25, reaching a peak of 1,296 events during that hour

Our threshold for international activity was set appropriately, whereas our threshold for HTTP POST activity was set a bit lower than needed, however our alert would have triggered for both alerts shortly after any suspicious activity started.

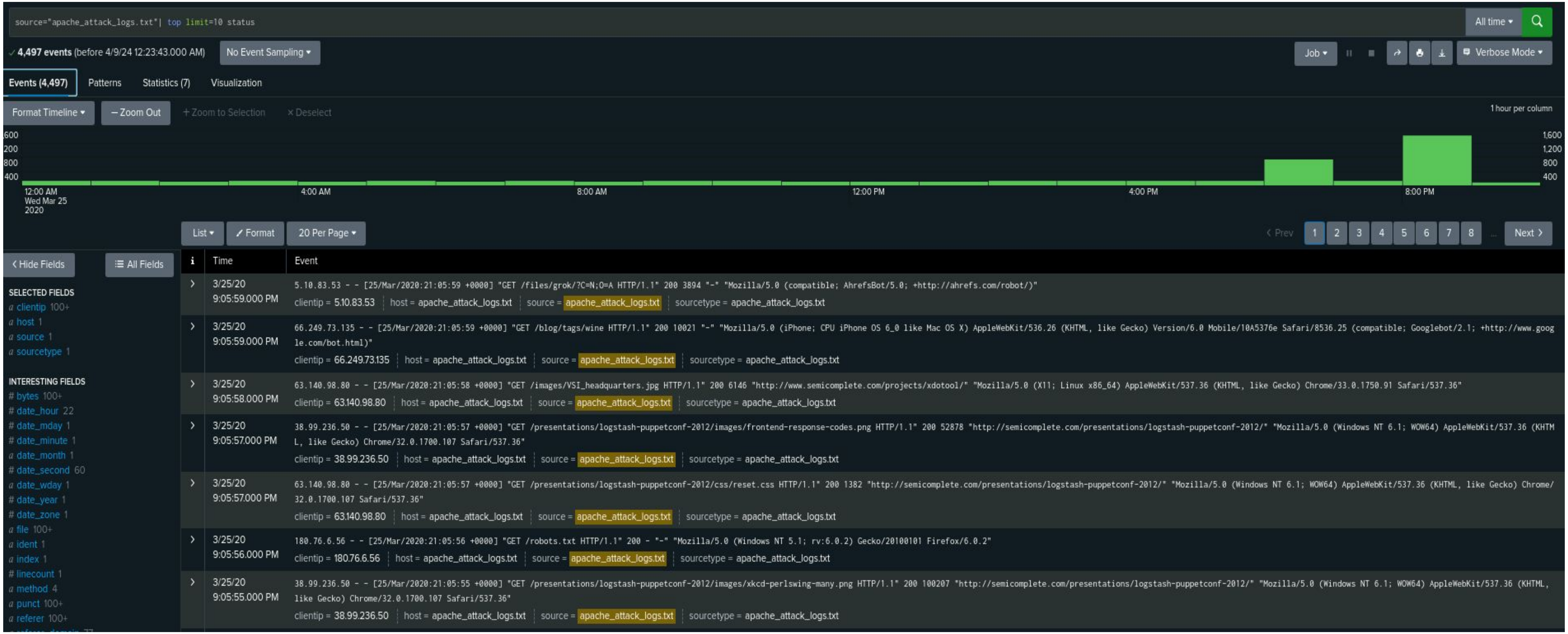
Attack Summary—Apache

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

Findings from our dashboards when analyzing the attack logs are as follows:

- Our Time Chart of HTTP methods revealed suspicious volumes of GET and POST methods. Specifically, the GET attack occurred from 5 pm to 7 pm and peaked with a count of 729, while the POST attack spanned from 7 pm to 9 pm and peaked with a count of 1,296.
- Our Cluster Map revealed suspicious activity from several cities, including Kiev (439) and Kharkiv (433), all exhibiting high volumes of activity.
- Our URI Data flagged "/VSI_Account_logon.php" as having suspiciously high volume.

Screenshots of Apache Attack Logs



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

✓ **4,497 events** (before 4/9/24 12:23:43.000 AM) No Event Sampling

SELECTED FIELDS
- a clientip 100+
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # bytes 100+
- # date_hour 22
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- # date_zone 1
- a file 100+
- a ident 1
- a index 1
- # linecount 1
- a method 4
- a punct 100+
- a referer 100+

i	Time	Event

›	3/25/20
	9:05:59.000 PM
		`5.10.83.53 - - [25/Mar/2020:21:05:59 +0000] "GET /files/grok/?C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"`
		clientip = 5.10.83.53 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

›	3/25/20
	9:05:59.000 PM
		`66.249.73.135 - - [25/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"`
		clientip = 66.249.73.135 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

›	3/25/20
	9:05:58.000 PM
		`63.140.98.80 - - [25/Mar/2020:21:05:58 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"`
		clientip = 63.140.98.80 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

›	3/25/20
	9:05:57.000 PM
		`38.99.236.50 - - [25/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"`
		clientip = 38.99.236.50 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

›	3/25/20
	9:05:57.000 PM
		`63.140.98.80 - - [25/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/css/reset.css HTTP/1.1" 200 1382 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"`
		clientip = 63.140.98.80 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

›	3/25/20
	9:05:56.000 PM
		`180.76.6.56 - - [25/Mar/2020:21:05:56 +0000] "GET /robots.txt HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"`
		clientip = 180.76.6.56 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

›	3/25/20
	9:05:55.000 PM
		`38.99.236.50 - - [25/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/images/xkcd-perlswing-many.png HTTP/1.1" 200 100207 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"`
		clientip = 38.99.236.50 ┆ host = apache_attack_logs.txt ┆ source = apache_attack_logs.txt ┆ sourcetype = apache_attack_logs.txt

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 on both its Windows and Apache servers. These attacks primarily involved brute-force attacks originating from various regions and countries worldwide.

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

  To safeguard VSI from future attacks, we recommend implementing the following mitigations:

  Adoption of two-factor authentication, serving as the primary defense mechanism against brute-force attacks.

  Implementation of user lockout mechanisms after a specified number of unsuccessful login attempts to deter and mitigate potential future attacks