Defensive Security Project

by: Cameron Pike, Jaylan Howden, David Stephen, Dylan Nasution and Aeraj Askari

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- We work for VSI corporation
- VSI corporation has experienced multiple attacks, the current suspect is JobeCorp
- Two systems were specifically attacked, the Windows Server, and the Apache Web server
- The Attacks Occurred on March 25th

VirusTotal Malware Lookup for Splunk

VirusTotal Malware Lookup for Splunk

The VirusTotal Malware Lookup

- Uses API’s to allow you to search using the regular “Search & Reporting” search bar
- Allows you to do a reputation check for
  - URL’s
  - Domains
  - IP’s
  - Hash’s
- Can search hundreds of resources and events at once and refer it to the VirusTotal database, instead of copy/pasting the resource into their site one by one

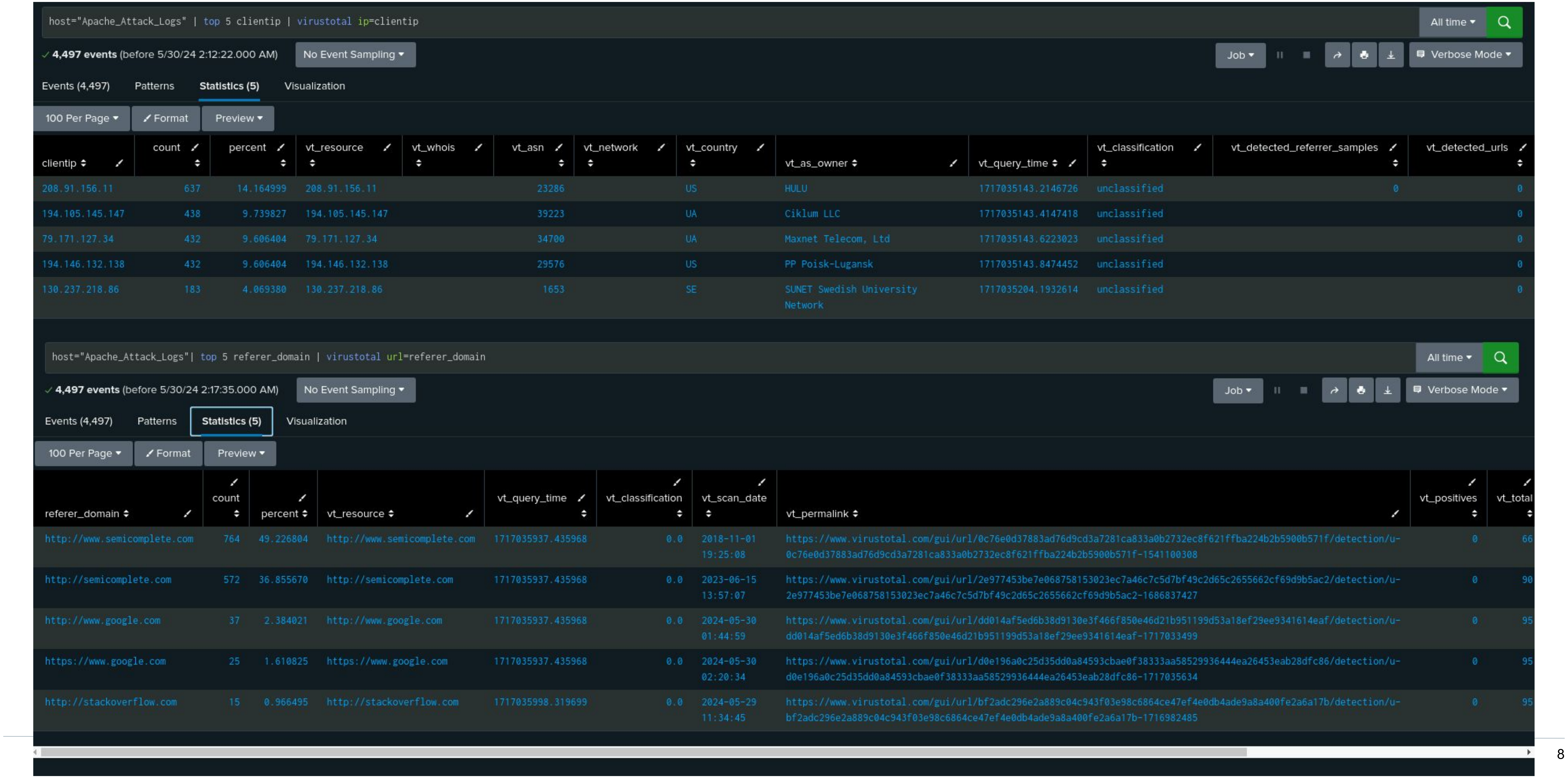
VirusTotal Malware Lookup for Splunk

When looking over logs, VirusTotal allows you to Check IP’s, Domains, URL’s and Hashes

Someone who looks over email logs and has access to the files or their hashes can send that using the add-on inside splunk

That same person can also send IP’s and Domains, All inside splunk allowing someone to check hundreds of IP’s, Domains, URL’s, and Hashes at one time

VirusTotal Malware Lookup for Splunk



```
host="Apache_Attack_Logs" | top 5 clientip | virustotal ip=clientip
```

✓ **4,497 events** (before 5/30/24 2:12:22.000 AM) No Event Sampling

clientip	count	percent	vt_resource	vt_whois	vt_asn	vt_network	vt_country	vt_as_owner	vt_query_time	vt_classification	vt_detected_referrer_samples	vt_detected_urls
208.91.156.11	637	14.164999	208.91.156.11		23286		US	HULU	1717035143.2146726	unclassified	0	0
194.105.145.147	438	9.739827	194.105.145.147		39223		UA	Ciklum LLC	1717035143.4147418	unclassified		0
79.171.127.34	432	9.606404	79.171.127.34		34700		UA	Maxnet Telecom, Ltd	1717035143.6223023	unclassified		0
194.146.132.138	432	9.606404	194.146.132.138		29576		US	PP Poisk-Lugansk	1717035143.8474452	unclassified		0
130.237.218.86	183	4.069380	130.237.218.86		1653		SE	SUNET Swedish University Network	1717035204.1932614	unclassified		0

```
host="Apache_Attack_Logs"| top 5 referer_domain | virustotal url=referer_domain
```

✓ **4,497 events** (before 5/30/24 2:17:35.000 AM) No Event Sampling

referer_domain	count	percent	vt_resource	vt_query_time	vt_classification	vt_scan_date	vt_permalink	vt_positives	vt_total
http://www.semicomplete.com	764	49.226804	http://www.semicomplete.com	1717035937.435968	0.0	2018-11-01 19:25:08	https://www.virustotal.com/gui/url/0c76e0d37883ad76d9cd3a7281ca833a0b2732ec8f621ffba224b2b5900b571f/detection/u-0c76e0d37883ad76d9cd3a7281ca833a0b2732ec8f621ffba224b2b5900b571f-1541100308	0	66
http://semicomplete.com	572	36.855670	http://semicomplete.com	1717035937.435968	0.0	2023-06-15 13:57:07	https://www.virustotal.com/gui/url/2e977453be7e068758153023ec7a46c7c5d7bf49c2d65c2655662cf69d9b5ac2/detection/u-2e977453be7e068758153023ec7a46c7c5d7bf49c2d65c2655662cf69d9b5ac2-1686837427	0	90
http://www.google.com	37	2.384021	http://www.google.com	1717035937.435968	0.0	2024-05-30 01:44:59	https://www.virustotal.com/gui/url/dd014af5ed6b38d9130e3f466f850e46d21b951199d53a18ef29ee9341614eaf/detection/u-dd014af5ed6b38d9130e3f466f850e46d21b951199d53a18ef29ee9341614eaf-1717033499	0	95
https://www.google.com	25	1.610825	https://www.google.com	1717035937.435968	0.0	2024-05-30 02:20:34	https://www.virustotal.com/gui/url/d0e196a0c25d35dd0a84593cbae0f38333aa58529936444ea26453eab28dfc86/detection/u-d0e196a0c25d35dd0a84593cbae0f38333aa58529936444ea26453eab28dfc86-1717035634	0	95
http://stackoverflow.com	15	0.966495	http://stackoverflow.com	1717035998.319699	0.0	2024-05-29 11:34:45	https://www.virustotal.com/gui/url/bf2adc296e2a889c04c943f03e98c6864ce47ef4e0db4ade9a8a400fe2a6a17b/detection/u-bf2adc296e2a889c04c943f03e98c6864ce47ef4e0db4ade9a8a400fe2a6a17b-1716982485	0	95

Logs Analyzed

1 Windows Logs

The Windows logs contain data consisting of:

- Signature IDs
- Error codes
- Account deletion
- Source ip addresses

2 Apache Logs

The Apache logs contain data consisting of:

- HTTP methods
- Response codes e.g. 404 errors
- Client location data
- URI scheme information

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Severity in Windows Attack Logs	This report shows the severity of the Windows logs and percentage.
Failed activities	This report shows the levels of success and failure on the Windows Server.
Windows Signature ID	This report shows the signature and the ID number that is linked to it.

Images of Reports—Windows

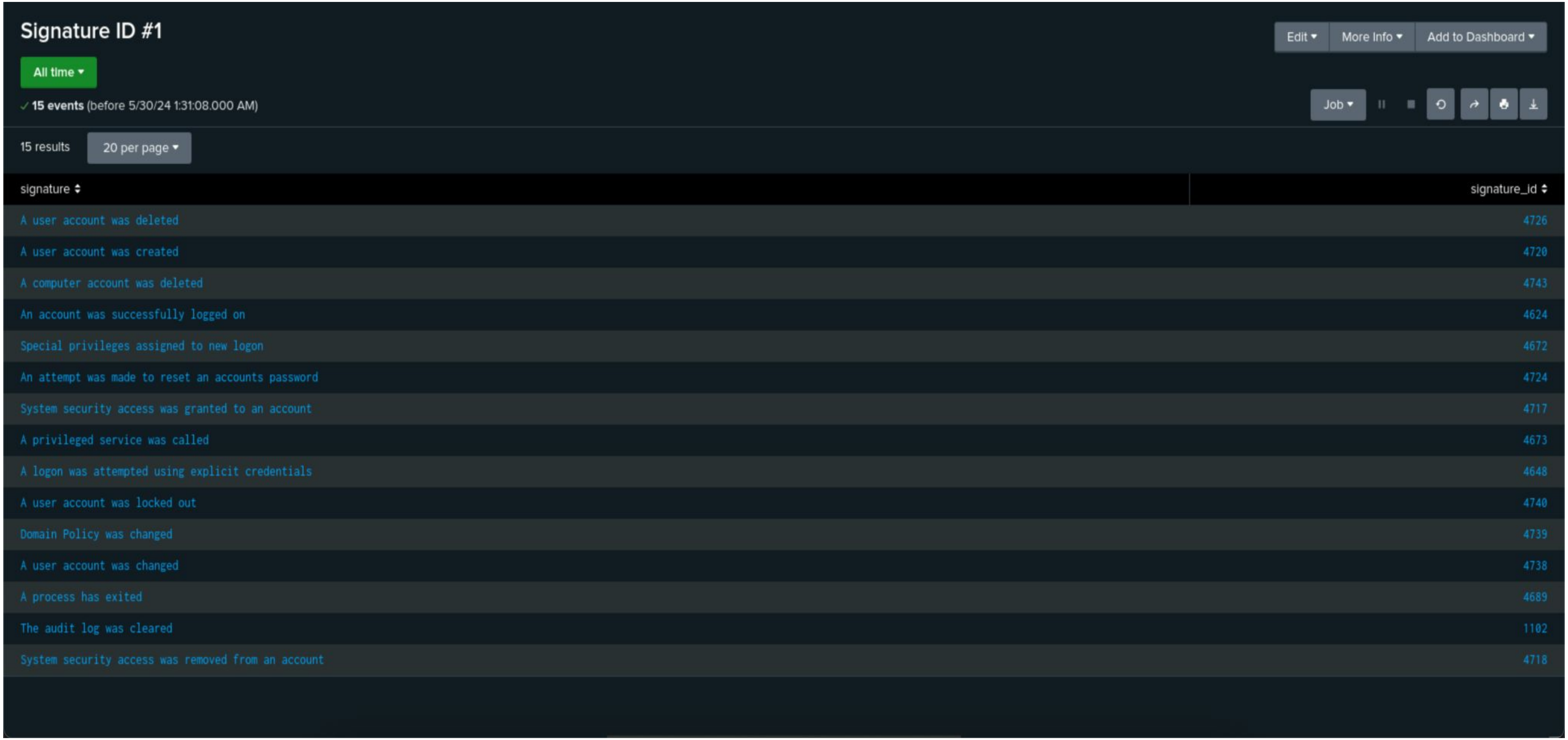
Server severity
All time ▾
Edit ▾
More Info ▾
Add to Dashboard ▾
Job ▾
20 per page ▾

✓ **4,764 events** (before 5/30/24 1:28:23.000 AM)

2 results

severity ⬍	count ⬍	percent ⬍
informational	4435	93.094039
high	329	6.905961

Images of Reports—Windows



Signature ID #1

✓ **15 events** (before 5/30/24 1:31:08.000 AM)

15 results

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
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

Images of Reports—Windows

Windows failed activities

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

✓ **4,764 events** (before 5/30/24 1:33:46.000 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
Failed Windows login attempts	This alert activates once the threshold is meet on failed Windows logins in a hour	6	10

JUSTIFICATION: Our team determined that a baseline for failed logins within the hour would be 6. From that determination we made the threshold for the alert at 10 failed login attempts per hour.

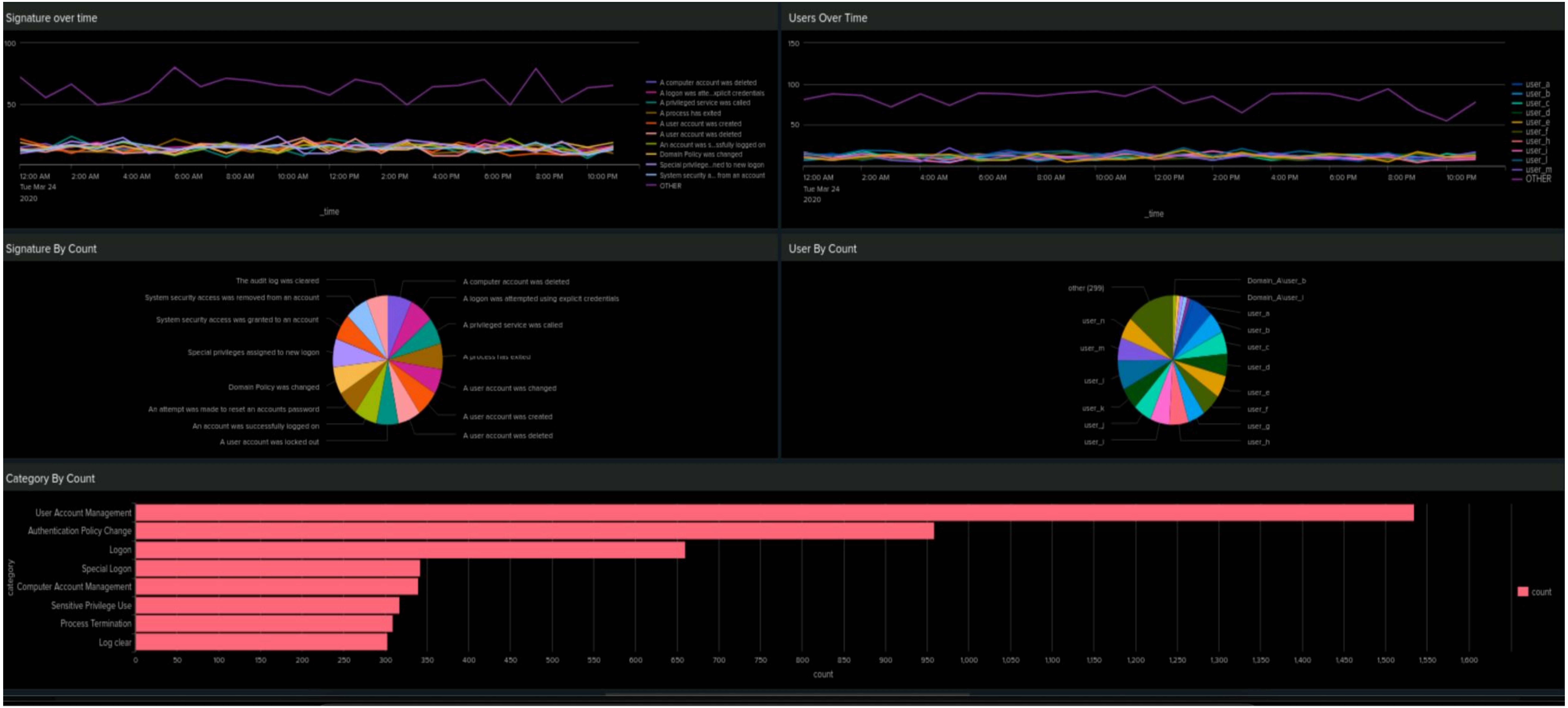
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Windows logins	This alert activates when the threshold for successful windows logins is met within the hour	15	25

JUSTIFICATION: Our team decided that a baseline for successful windows logins by getting an average for logins per hour which was 15. We set the threshold at 25 as that would detect suspicious activity but also at the same time false positives would be low.

Dashboards—Windows


Signature over time
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 atte...xplicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was s...ssfully logged on
Domain Policy was changed
Special privilege...ned to new logon
System security a... from an account
OTHER
Users Over Time
150
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
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_l
user_m
OTHER
Signature By Count
The audit log was cleared
System security access was removed from an account
System security access was granted to an account
Special privileges assigned to new logon
Domain Policy was changed
An attempt was made to reset an accounts password
An account was successfully logged on
A user account was locked out
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 created
A user account was deleted
User By Count
other (299)
user_n
user_m
user_l
user_k
user_j
user_i
Domain_A\user_b
Domain_A\user_i
user_a
user_b
user_c
user_d
user_e
user_f
user_g
user_h
Category By Count
category
User Account Management
Authentication Policy Change
Logon
Special Logon
Computer Account Management
Sensitive Privilege Use
Process Termination
Log clear
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
1,400
1,450
1,500
1,550
1,600
count
count

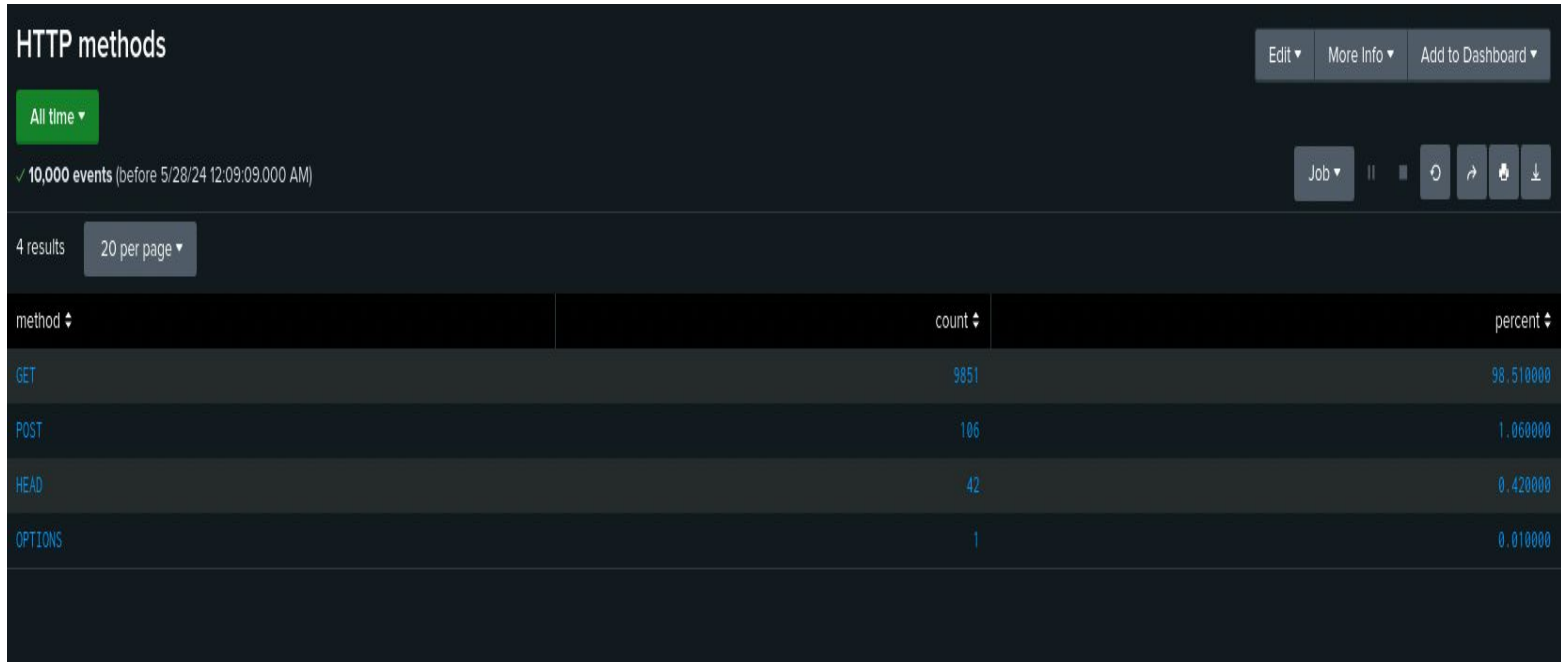
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	This report offers insights into the types of HTTP activities requested from VSI's web server, detailing various HTTP methods (such as GET, POST, HEAD, etc.)
Top Ten Domains	A report that highlights the top 10 domains that refer to VSI, helping us to identify any suspicious referrers.
HTTP Response Codes	A report that details the count of each HTTP response code, providing insight into any unusual levels of HTTP responses.

Images of Reports—Apache

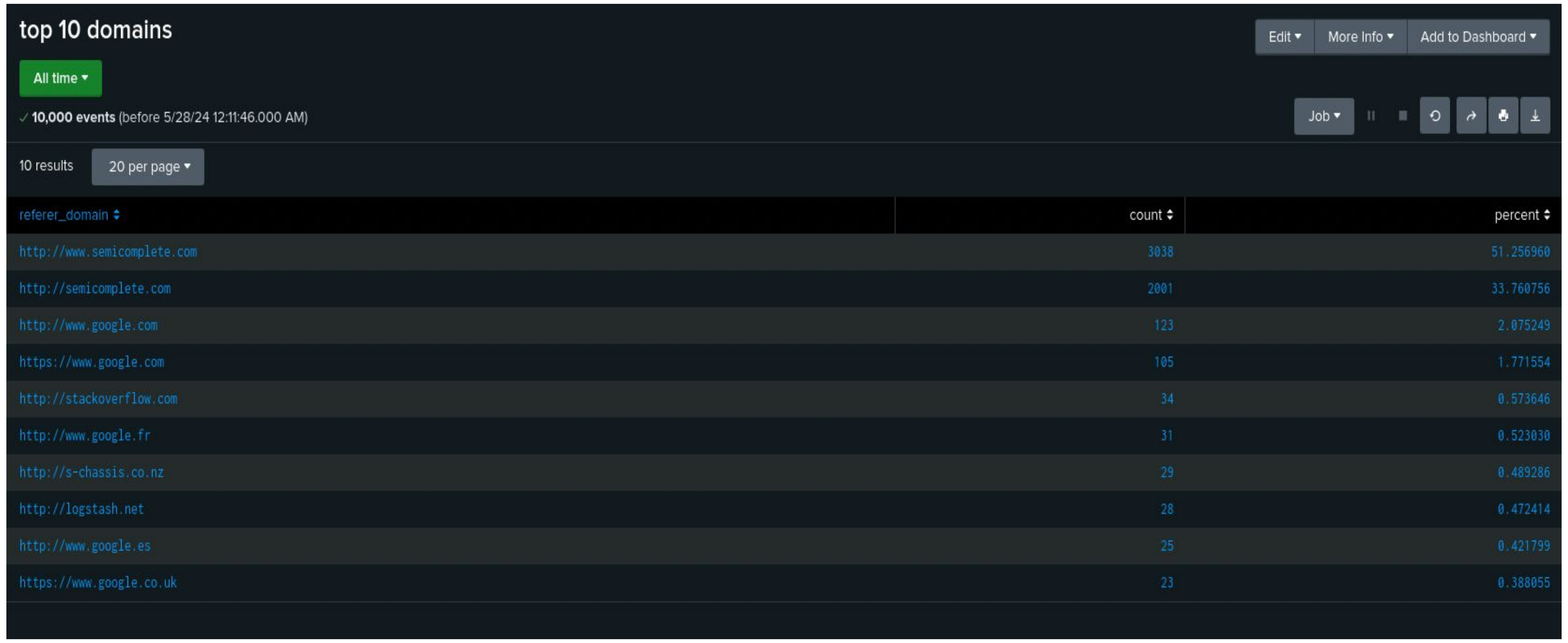


HTTP methods

✓ **10,000 events** (before 5/28/24 12:09:09.000 AM)

4 results

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

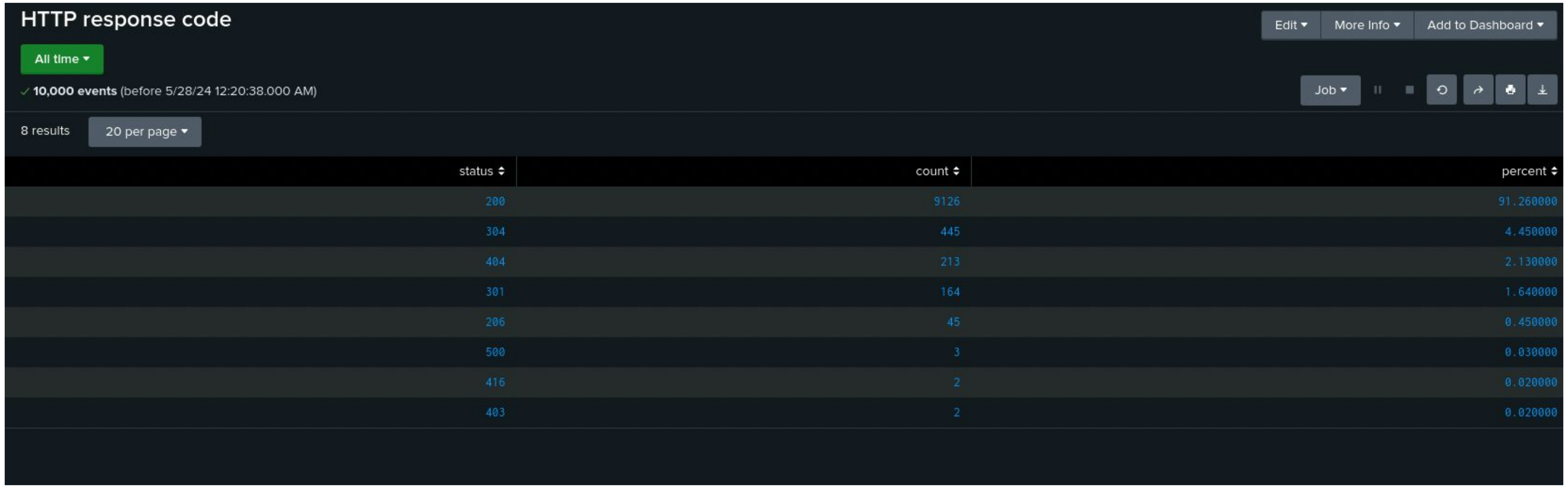


top 10 domains

✓ **10,000 events** (before 5/28/24 12:11:46.000 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



HTTP response code

✓ **10,000 events** (before 5/28/24 12:20:38.000 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
Hourly Activity from any Country then the U.S.	An alert created to monitor hourly activity from any country besides the United States. This alert will be triggered when the specified threshold is reached.	120	150

JUSTIFICATION: We determined the baseline to be 120, as this was the average amount of activity across time. We set the alert at 150 as we believe that a higher number may an indicator of a potential attack, and would prevent too many false positives.

Alerts—Apache

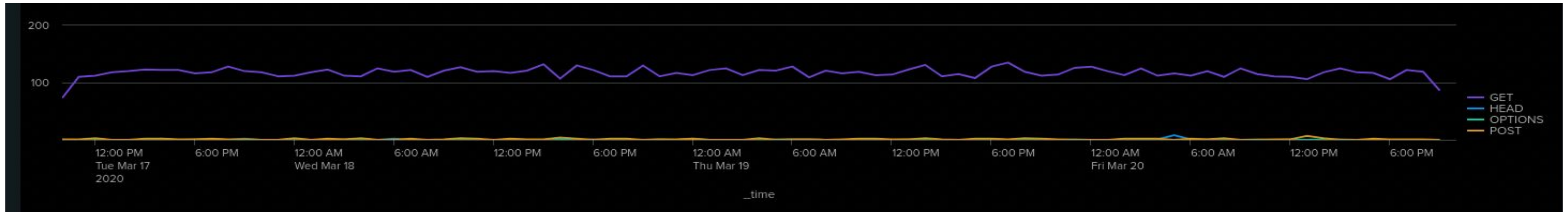
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of the HTTP POST Method	An alert created to monitor the hourly count of the HTTP POST method. This alert will be triggered when the specified threshold is reached.	2	4

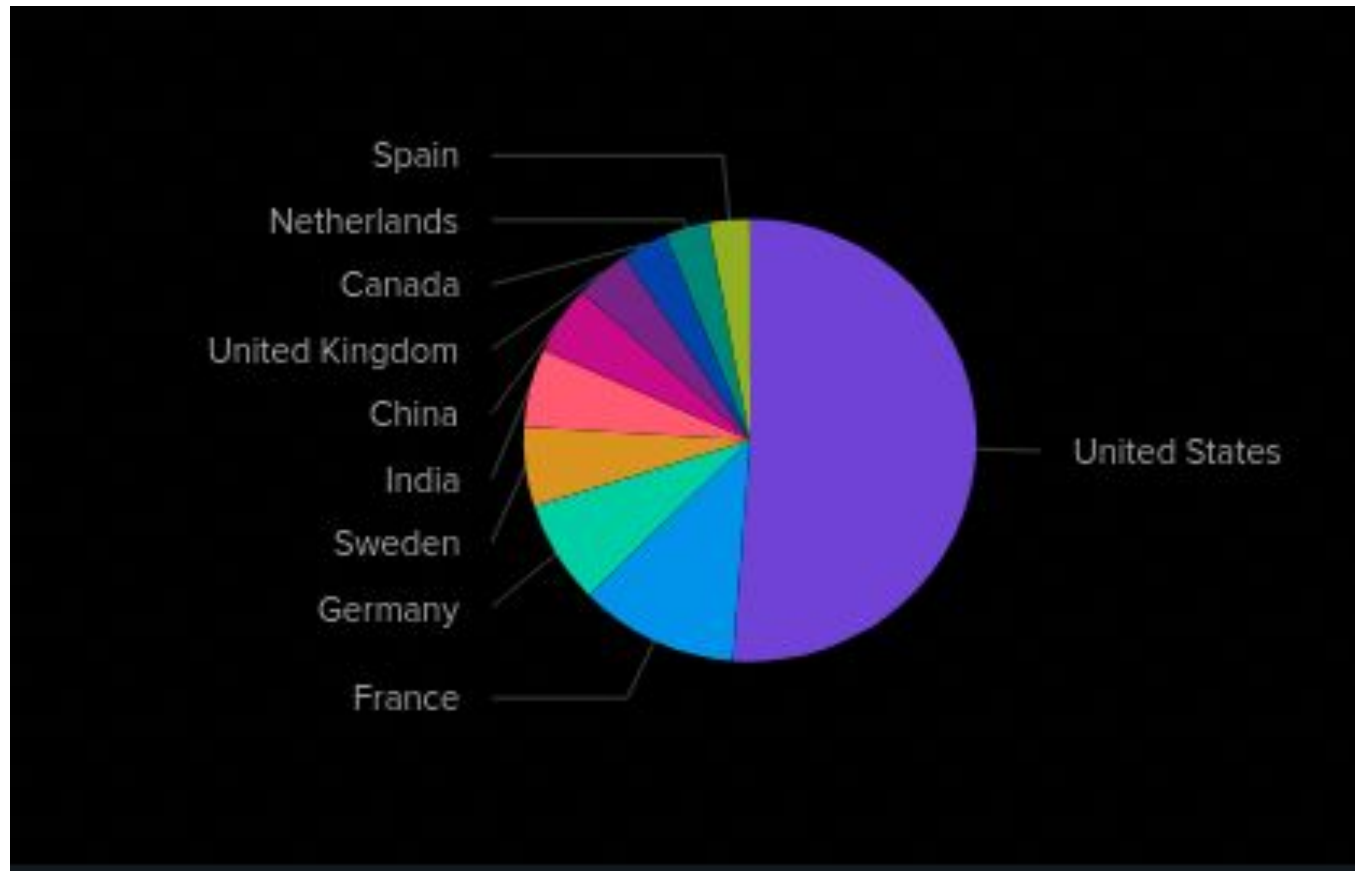
JUSTIFICATION: We determined the baseline for this was 2, as this was the average across all time. We set the alert level at 4 because of the nature of what POST could mean with regards to a potential attack, and that even if there are false positives, it is better to be safe than sorry.

Dashboards—Apache

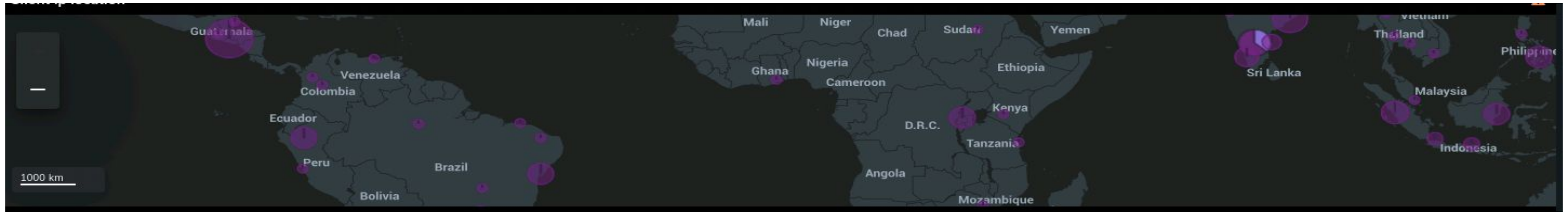
HTTP Methods



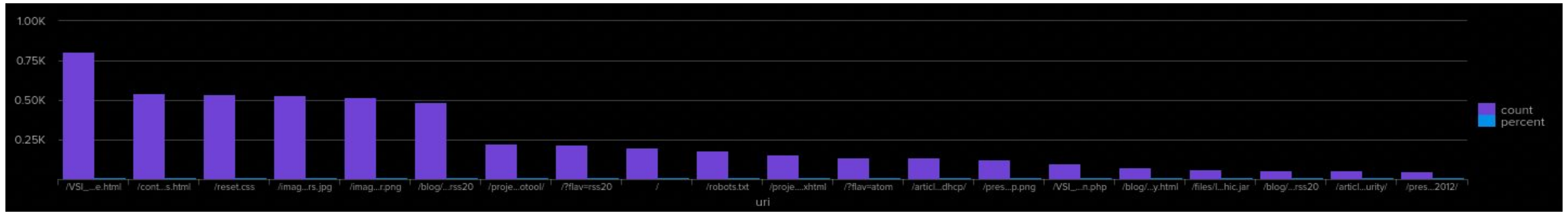
Count of Top 10 Countries



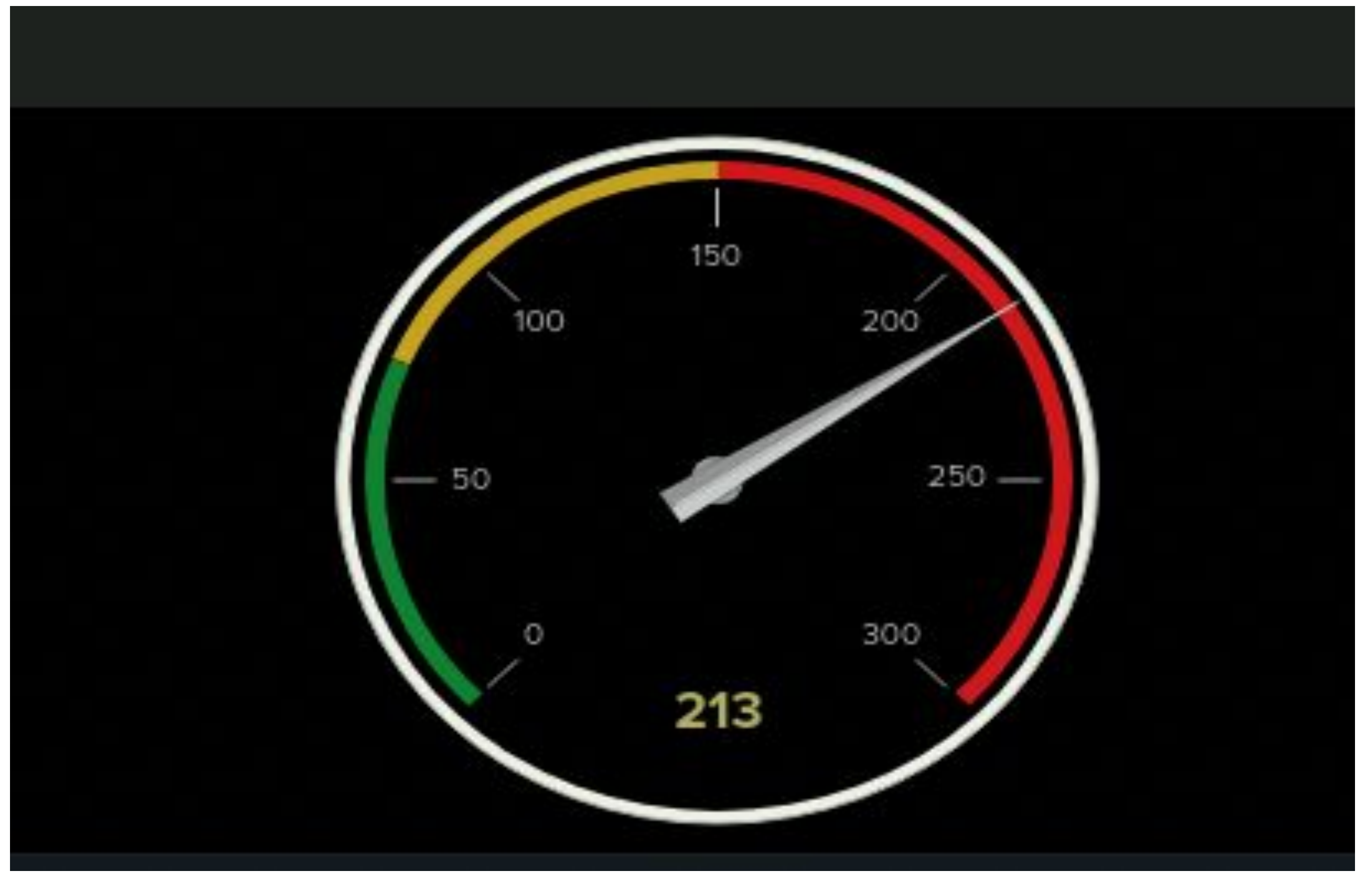
Client IP Location



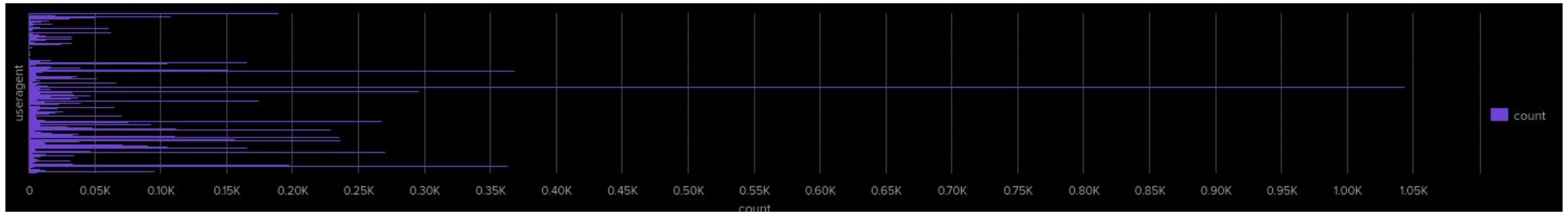
URIs



404 Error Count



User Agents



Attack Analysis

Attack Summary—Windows

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

- Count share of high severity events increased by 13%

Attack Summary—Windows

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

- Failed Windows Activity events (35) from 8-9 AM on Wednesday, March 25, 2020
  - Threshold was 5, should increase to 7 or 8
- Successful Logins events (196) from user_j from 11 Am to 12 PM on March 25, 2020 (attacker could be doing reconnaissance or trying to get persistence, also could be bot activity)
  - Threshold was 15 which seems to perform well

Attack Summary—Windows

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

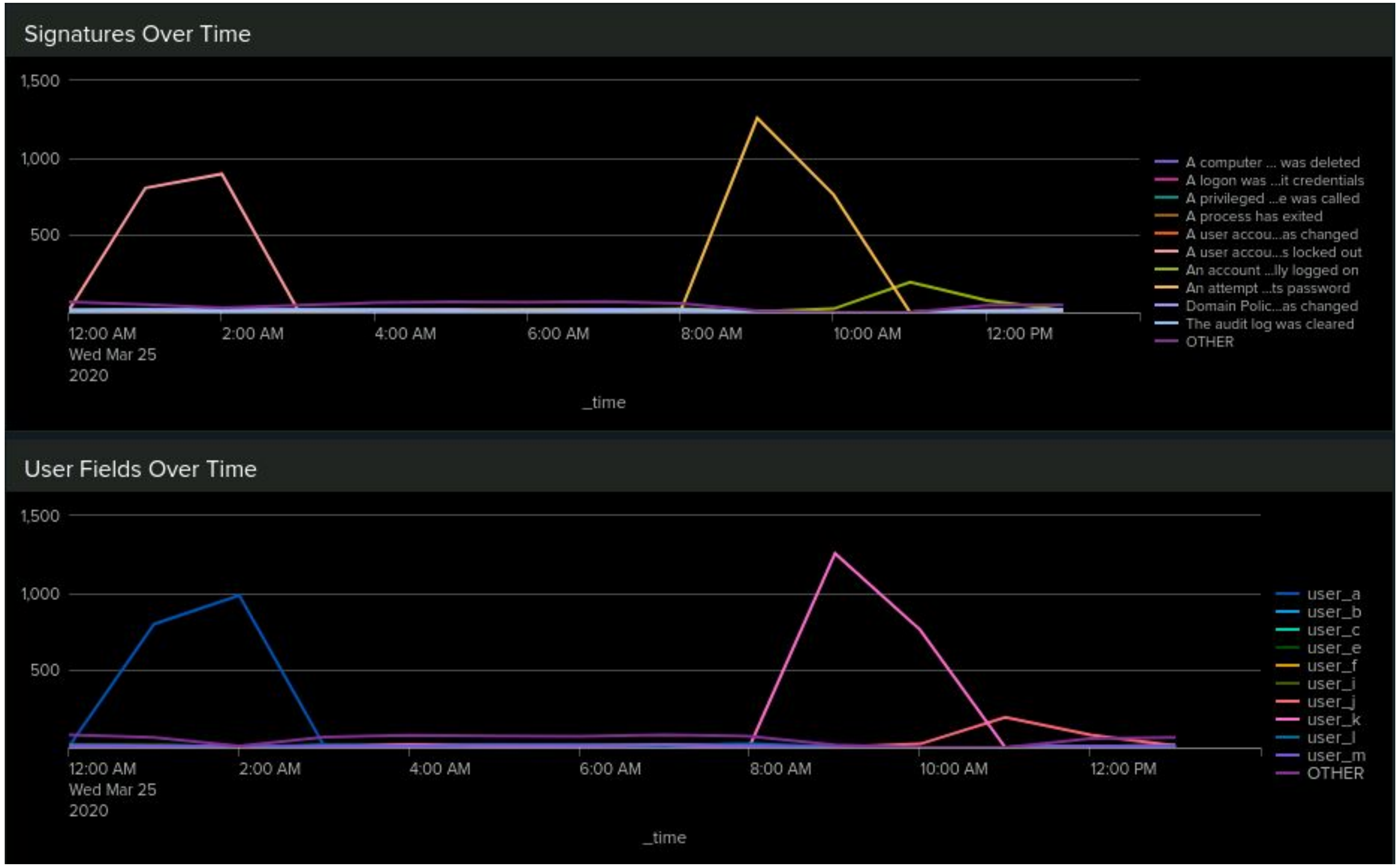
Signatures

- At 9 AM an attempt was made to reset an account’s password 1258 times and 761 times at 10 AM.
- At 1 AM a user account was locked out 805 times and 896 times at 2 AM.

Users

- The user user_a had 799 events at 1 AM and 984 events at 2 AM.
- The user user_k had 1256 events at 9 AM and 761 events at 10 AM.
- The accounts user_a and user_k were likely compromised

Screenshots of Attack Logs



Attack Summary—Apache

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

- The number of POSTs increased by 28%.
- The number of 404 response codes increased by about 10%.

Attack Summary—Apache

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

- The count of the hours it occurred in was mostly over 100 events per hour from 6 AM March 19 to 9 AM March 20.
- 1296 POST requests at 8 PM March 25, 2020

Attack Summary—Apache

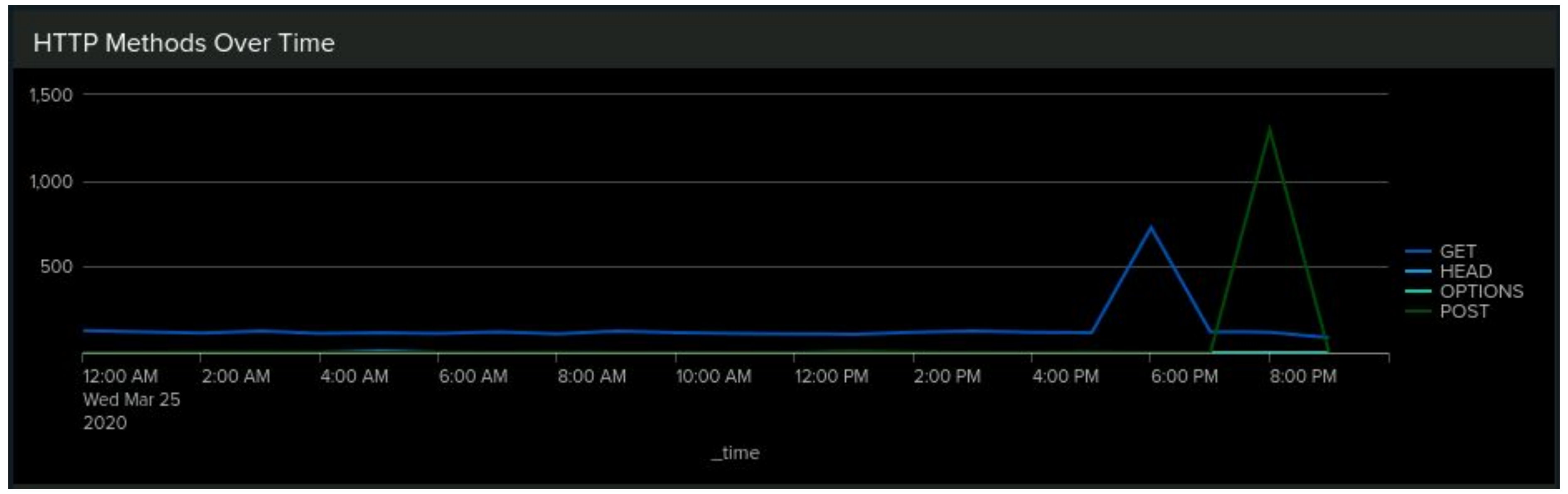
Summarize your findings from your dashboards when analyzing the attack logs.

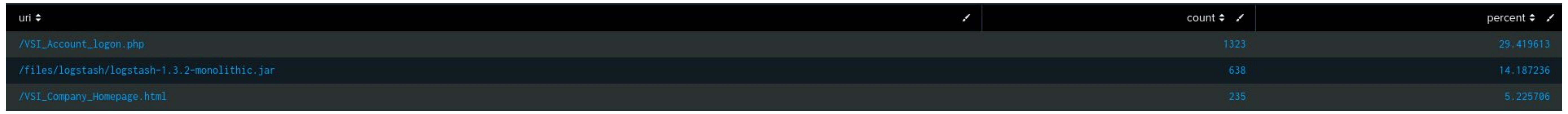
- POST method used for attack.
- High request volume from Kyiv, Ukraine and Kharkiv, Ukraine.
- /VSI_Account_logon.php is the URI being hit the most.

Conclusion

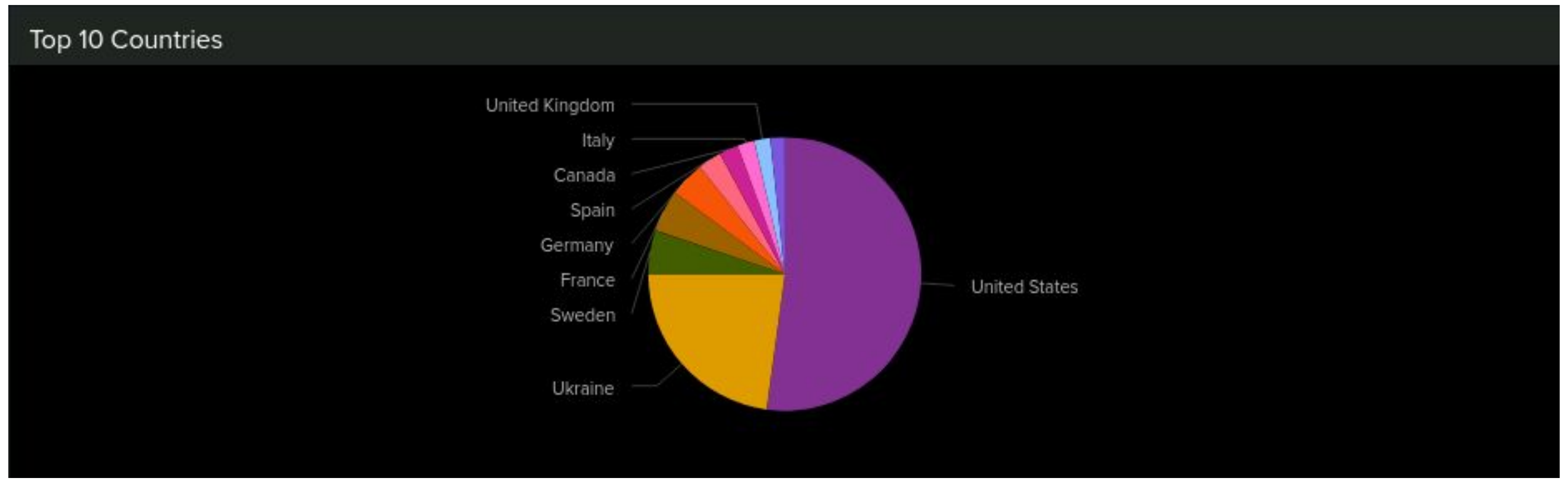
- The attacker was trying to bruteforce login to the webpage and kept failing resulting in many POST requests and many 404 status codes.

Screenshots of Attack Logs





uri	count	percent
/VSI_Account_logon.php	1323	29.419613
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187236
/VSI_Company_Homepage.html	235	5.225706



Summary and Future Mitigations

Project 3 Summary

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

  - /VSI_Account_logon.php was victim to brute force password guessing, XSS, etc. There were attacks on user accounts on the Windows server.

- To protect VSI from future attacks, what future mitigations would you recommend?
  - To prevent Windows accounts from being compromised, rotate passwords regularly, implement 2FA on all accounts, and decrease the amount of allowed login attempts before lockout. Trigger alert if too many lockouts.
  - To prevent brute forcing on the web page, identify and block IPs sending login requests if too many attempts are made.