Defensive Security Project
by: Josh Ryan

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

Playing 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 a SOC analyst, we are tasked with using Splunk to monitor against potential attacks on these 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. The networking team has provided us with past logs to help us develop baselines and create reports, alerts, dashboards, and more.

Website Monitoring

Website Monitoring

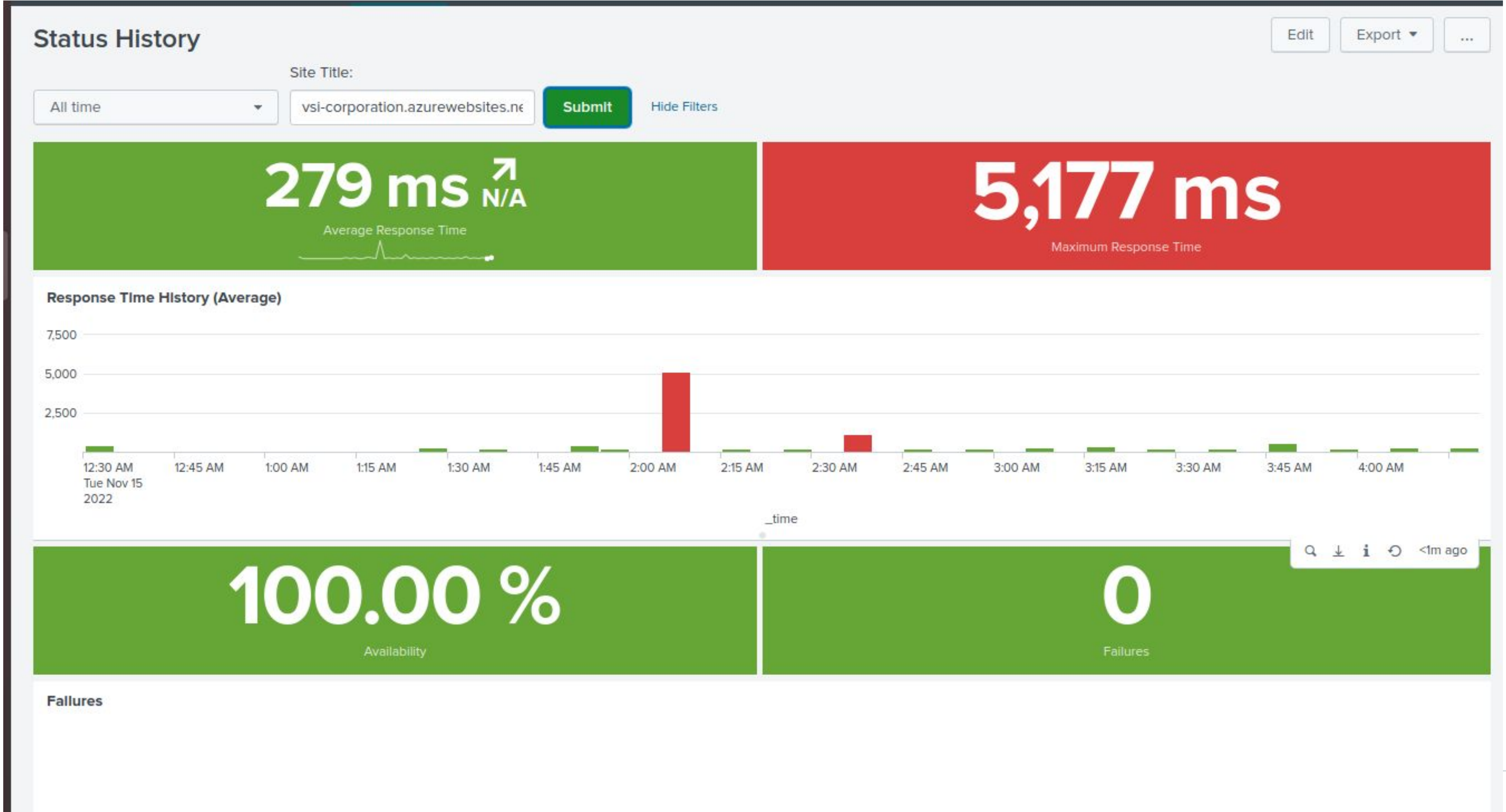
Monitor websites to detect downtime and performance problems. This app uses a modular input that can be setup easily (in 5 minutes or less).

Website Monitoring

This helps get a high level overview on the outages and a historical analysis of the sites responsiveness.

You can check the availability at a glance.

Website Monitoring (no failures reported)



Status History

Edit | Export ▾ | ...

Site Title:

All time ▾ | vsi-corporation.azurewebsites.ne | Submit | Hide Filters

279 ms ↗ N/A

Average Response Time

5,177 ms

Maximum Response Time

Response Time History (Average)

100.00 %

Availability

0

Failures

Failures

Logs Analyzed

1 Windows Logs

The data contained in these windows logs that we analyzed were signatured events including account data such as: account locked out, resetting passwords, successful/failed logins and user accounts that changed.

Also monitored users that made these changes and compared these activities during the attack to the normal day to day activity.

Determined a baseline and threshold for hourly count of the signature an user account was deleted.

2 Apache Logs

A report that shows a table of the different HTTP methods. A report that shows the top 10 domains that referred to VSI's website. A report that shows the count of the HTTP response codes.

An hourly count of HTTP POST methods used. Alerts were also made for hourly counts of activity from a country other than the United States.

Used a geographical map to show the locations and charts to display the count of different URIs.

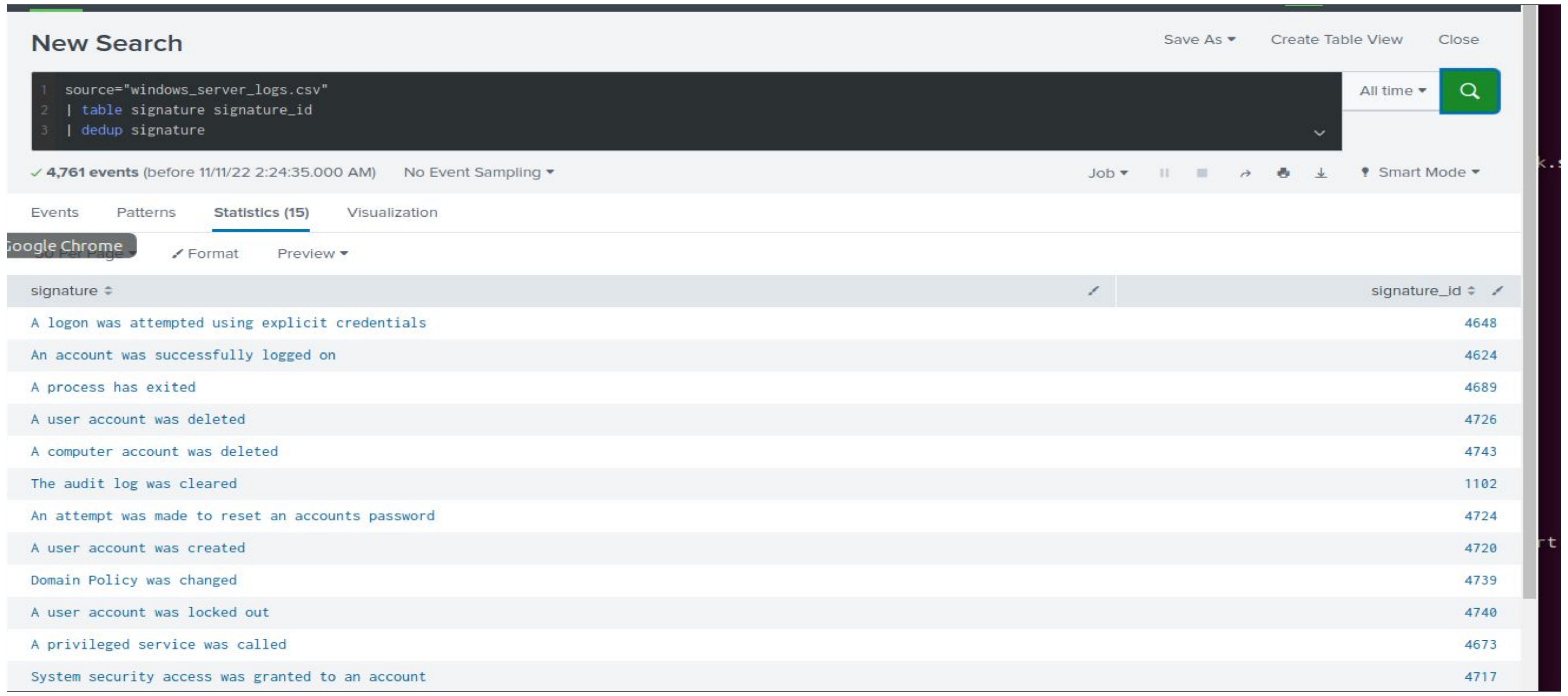
Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Windows Log Report 1	A report with a table of signatures with associated SignatureID.
Windows Log Report 2	A report that provides the count and percent of the severity.
Windows Log Report 3	A report that provides a comparison between the success and failure of Windows activities.

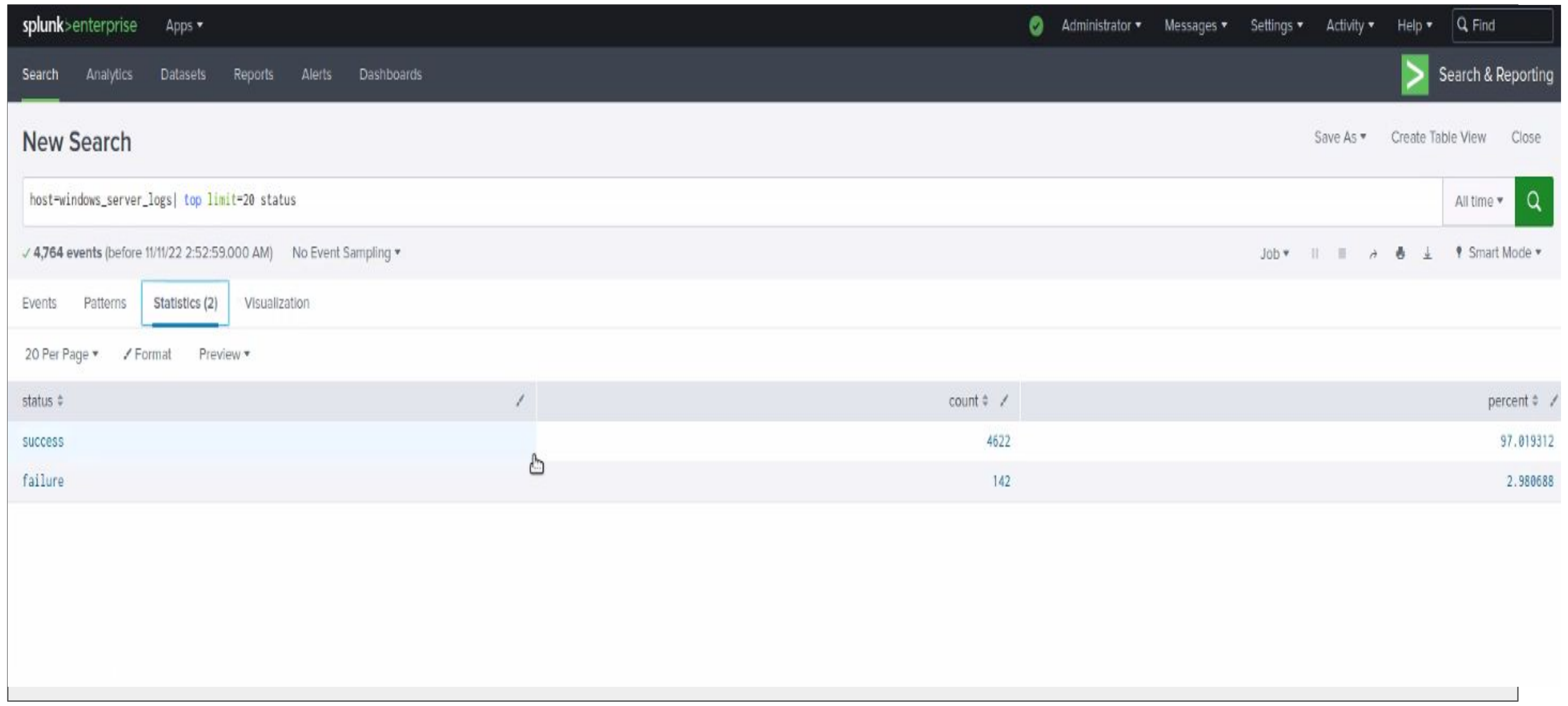
Images of Reports—Windows



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

✓ 4,761 events (before 11/11/22 2:24:35.000 AM)

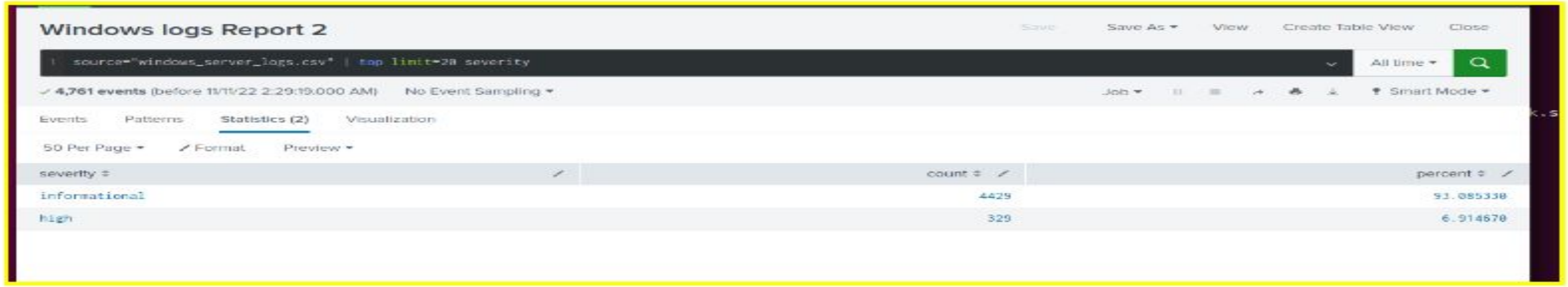
signature	signature_id
A logon was attempted using explicit credentials	4648
An account was successfully logged on	4624
A process has exited	4689
A user account was deleted	4726
A computer account was deleted	4743
The audit log was cleared	1102
An attempt was made to reset an accounts password	4724
A 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



```
host=windows_server_logs| top limit=20 status
```

✓ 4,764 events (before 11/11/22 2:52:59.000 AM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

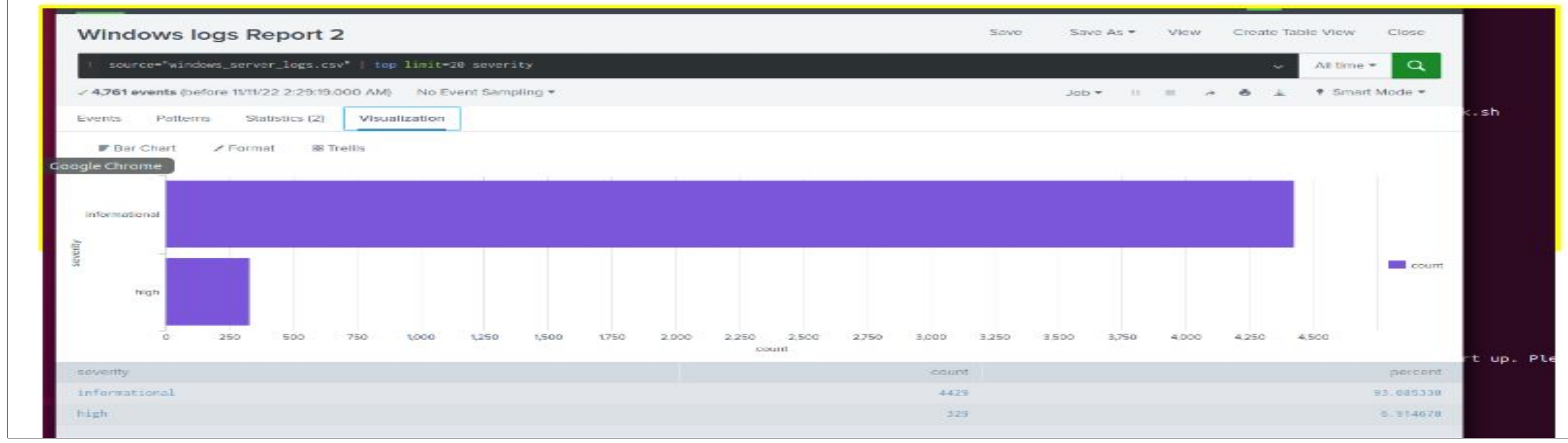


Windows logs Report 2

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

✓ 4,761 events (before 11/11/22 2:29:19.000 AM)

severity	count	percent
informational	4429	93.085330
high	329	6.914670



Windows logs Report 2

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

✓ 4,761 events (before 11/11/22 2:29:19.000 AM)

severity	count	percent
informational	4429	93.085330
high	329	6.914670

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Window logs Alert 1	Baseline and threshold for hourly level of failed Windows activity	6	13

JUSTIFICATION: The baseline was approximately 6 because the low was around 3 and high was round 10. Nothing exceeded 10 so an alert threshold of 13 was within reason.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Alert 2	Determined a baseline and threshold for hourly count of the signature an account was successfully logged on. Created an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.	13.5	23

JUSTIFICATION: The baseline was an approximate tally of the low vs high. The threshold was certainly much higher than any other hour found so was well outside the scope of the typical day.

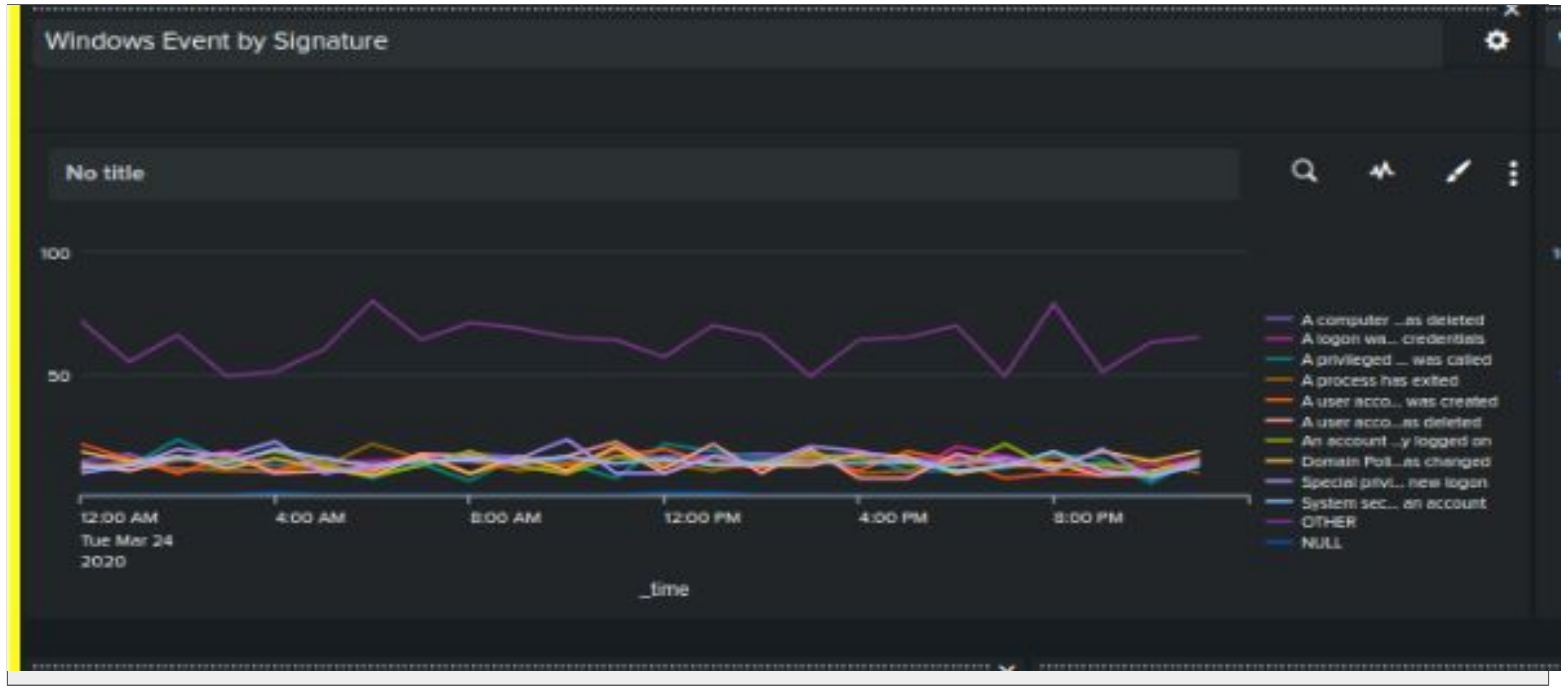
Alerts—Windows

Designed the following alerts:

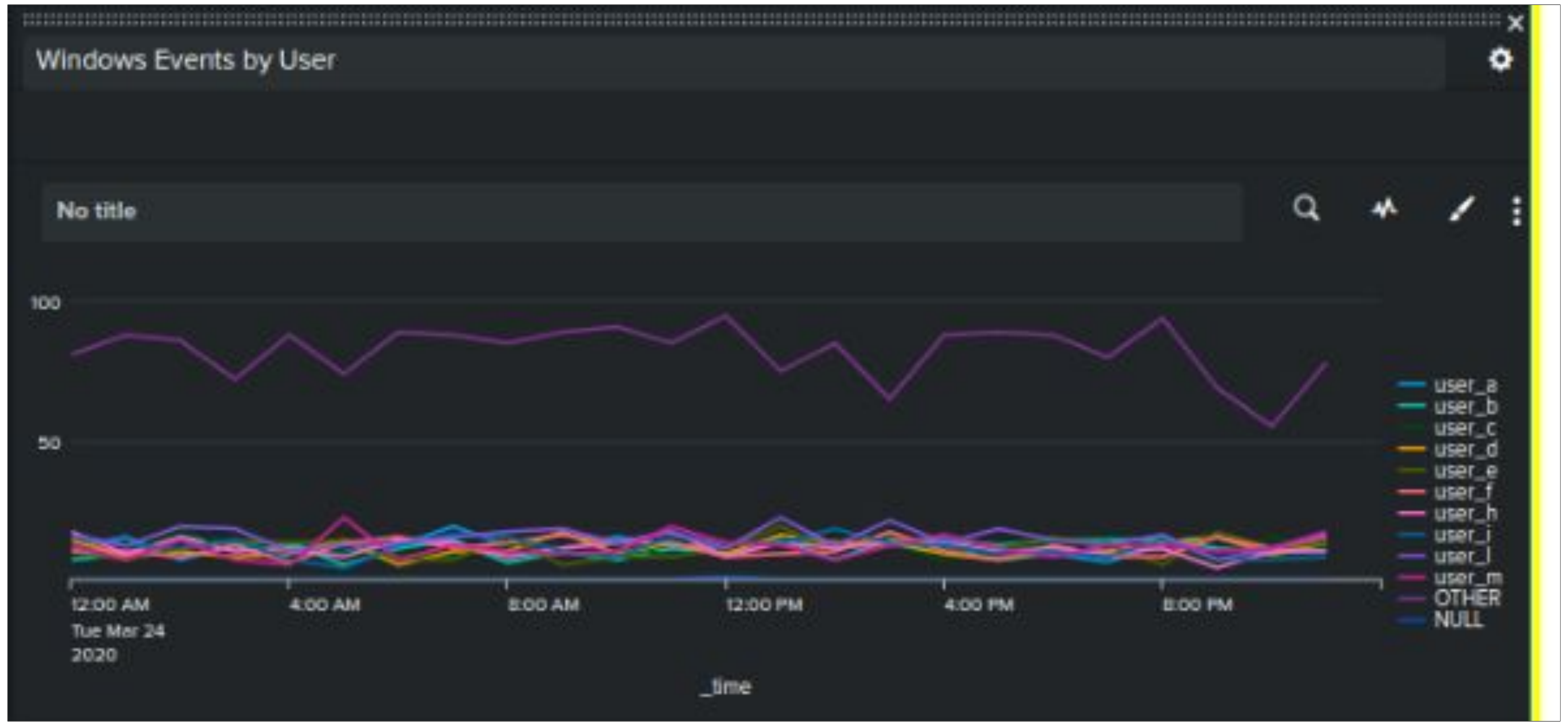
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert 3	Determine a baseline and threshold for hourly count of the signature a user account was deleted. Designed the alert based on the corresponding SignatureID. Created an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.	around 13	26

JUSTIFICATION: The baseline was an approximate tally of the low vs high. The threshold was certainly much higher than any other hour found so was well outside the scope of the typical day.

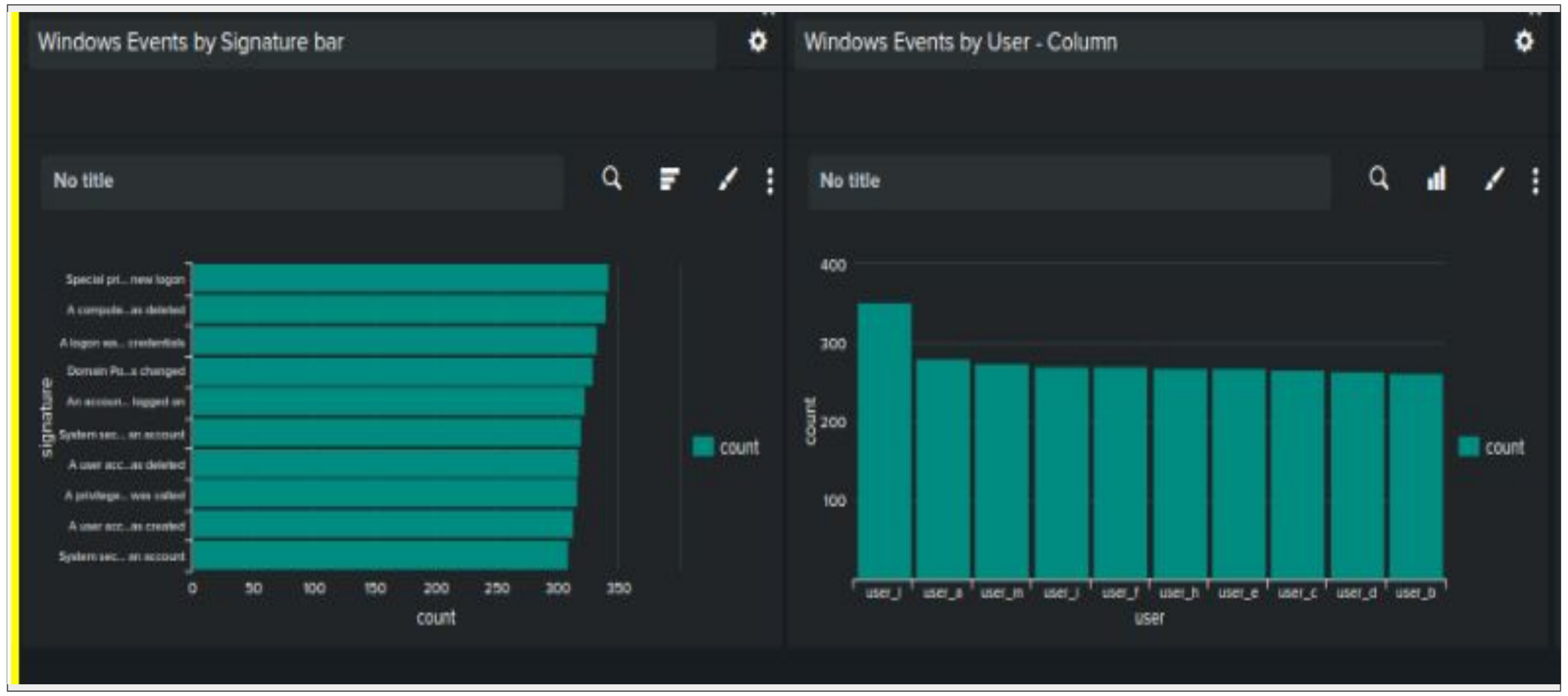
Dashboards—Windows


Windows Event by Signature

No title


Windows Events by User

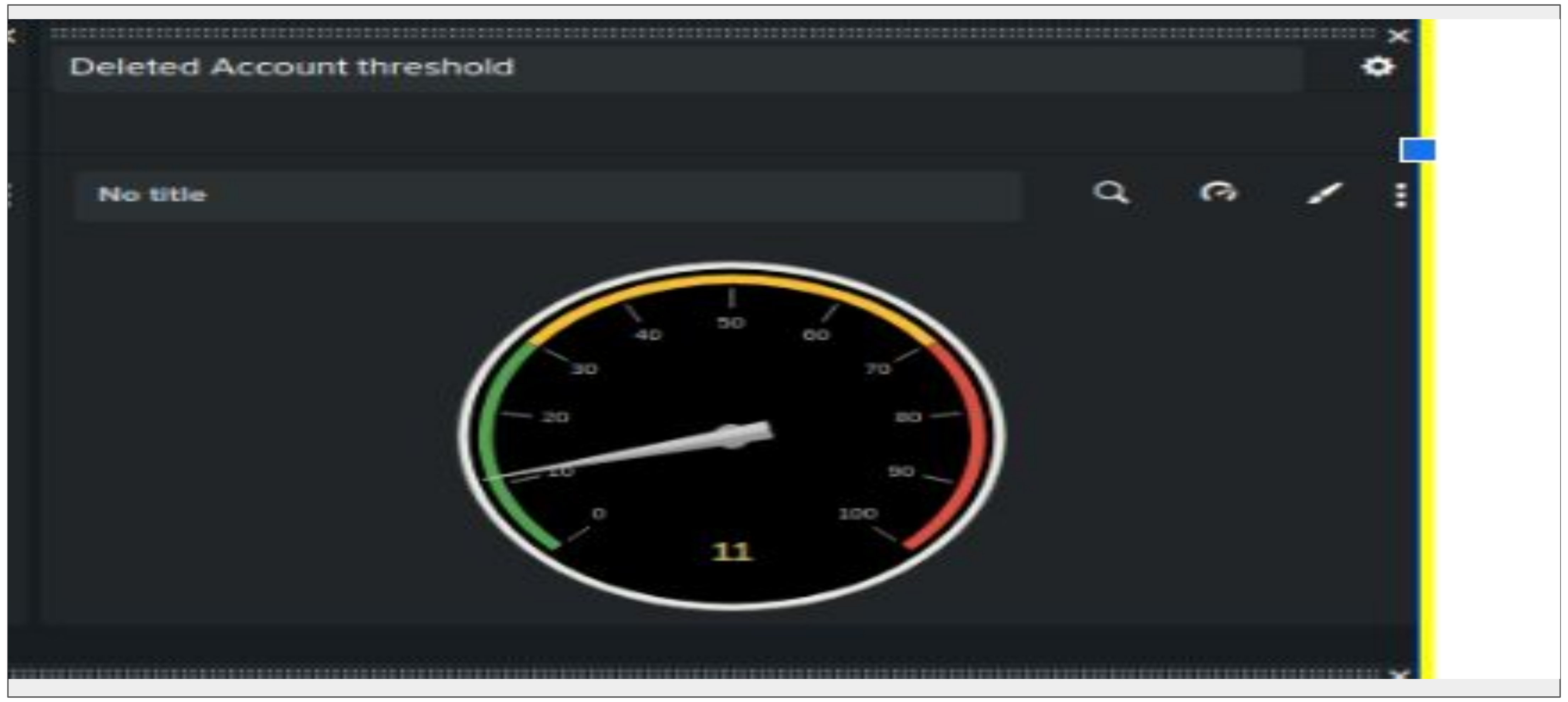
No title


Windows Events by Signature bar

No title

Windows Events by User - Column

No title


Deleted Account threshold

No title

Dashboards—Windows

Windows Event by Signature
No title
100
50
12:00 AM
Tue Mar 24
2020
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
_time
A computer ...as deleted
A logon wa... credentials
A privileged ... was called
A process has exited
A user acco... was created
A user acco...as deleted
An account ...y logged on
Domain Poli...as changed
Special privi... new logon
System sec... an account
OTHER
NULL
Windows Events by User
No title
100
50
12:00 AM
Tue Mar 24
2020
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
_time
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_l
user_m
OTHER
NULL
Windows Events by Signature bar
No title
signature
Special pri... new logon
A compute...as deleted
A logon wa... credentials
Domain Po...s changed
An accoun... logged on
System sec... an account
A user acc...as deleted
A privilege... was called
A user acc...as created
System sec... an account
0
50
100
150
200
250
300
350
count
count
Windows Events by User - Column
No title
400
300
200
100
count
user_l
user_a
user_m
user_i
user_f
user_h
user_e
user_c
user_d
user_b
user
count
Deleted Account threshold
No title
0
10
20
30
40
50
60
70
80
90
100
11
Windows Events by User - Table
No title
user
count
percent

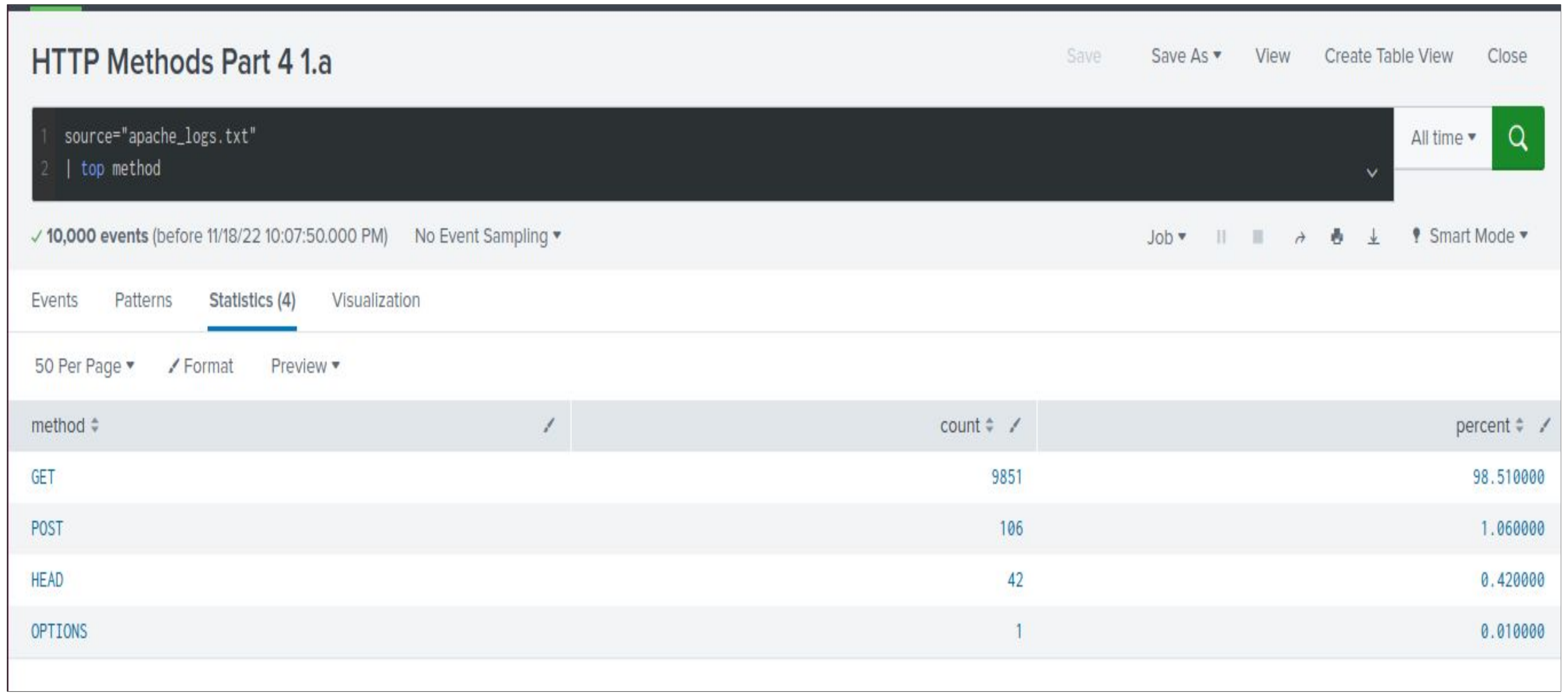
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	**Report Description**
HTTP Methods Part 4 1.a	A report that shows a table of the different HTTP methods
VSIs website	A report that shows the top 10 domains that referred to VSI's website
HTTP response report 2	A report that shows the count of the HTTP response codes

Images of Reports—Apache

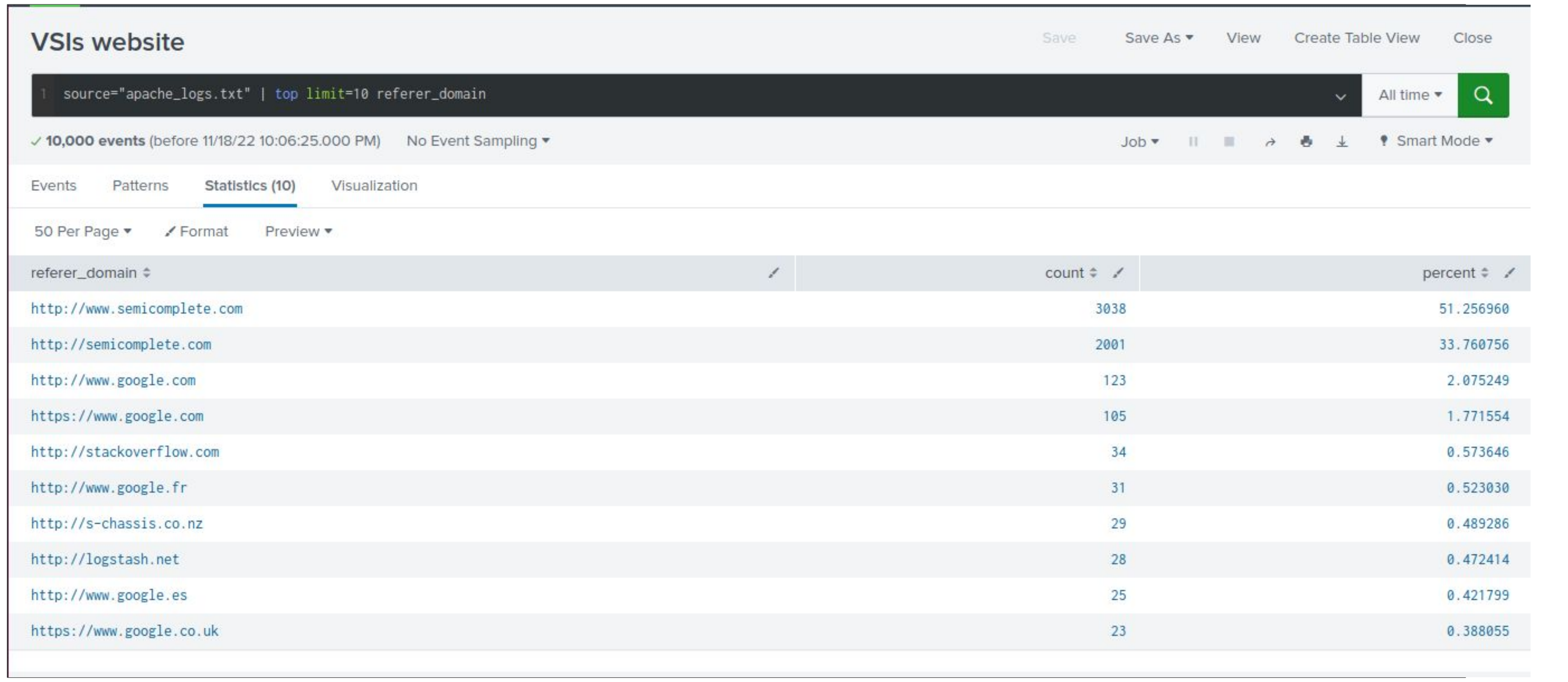


HTTP Methods Part 4 1.a

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

✓ 10,000 events (before 11/18/22 10:07:50.000 PM) No Event Sampling ▾

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

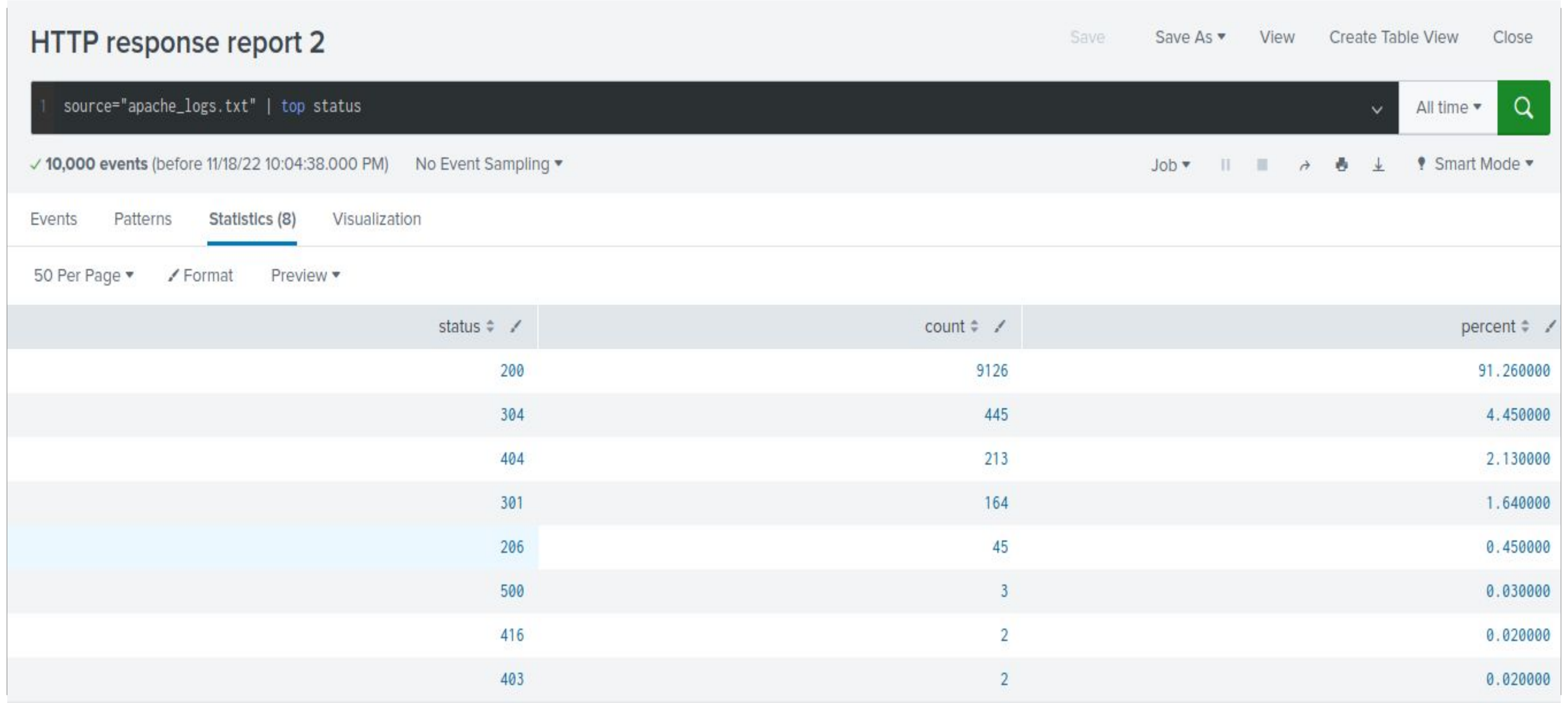


VSIs website

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

✓ 10,000 events (before 11/18/22 10:06:25.000 PM) No Event Sampling ▾

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 report 2

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

✓ 10,000 events (before 11/18/22 10:04:38.000 PM) No Event Sampling ▾

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
Apache alert Baseline and threshold	A baseline and threshold for hourly count of activity from countries outside the United States	Around 70-80	143

JUSTIFICATION: The activity in a typical day didn’t surpass 120 so we estimated a threshold of 143.

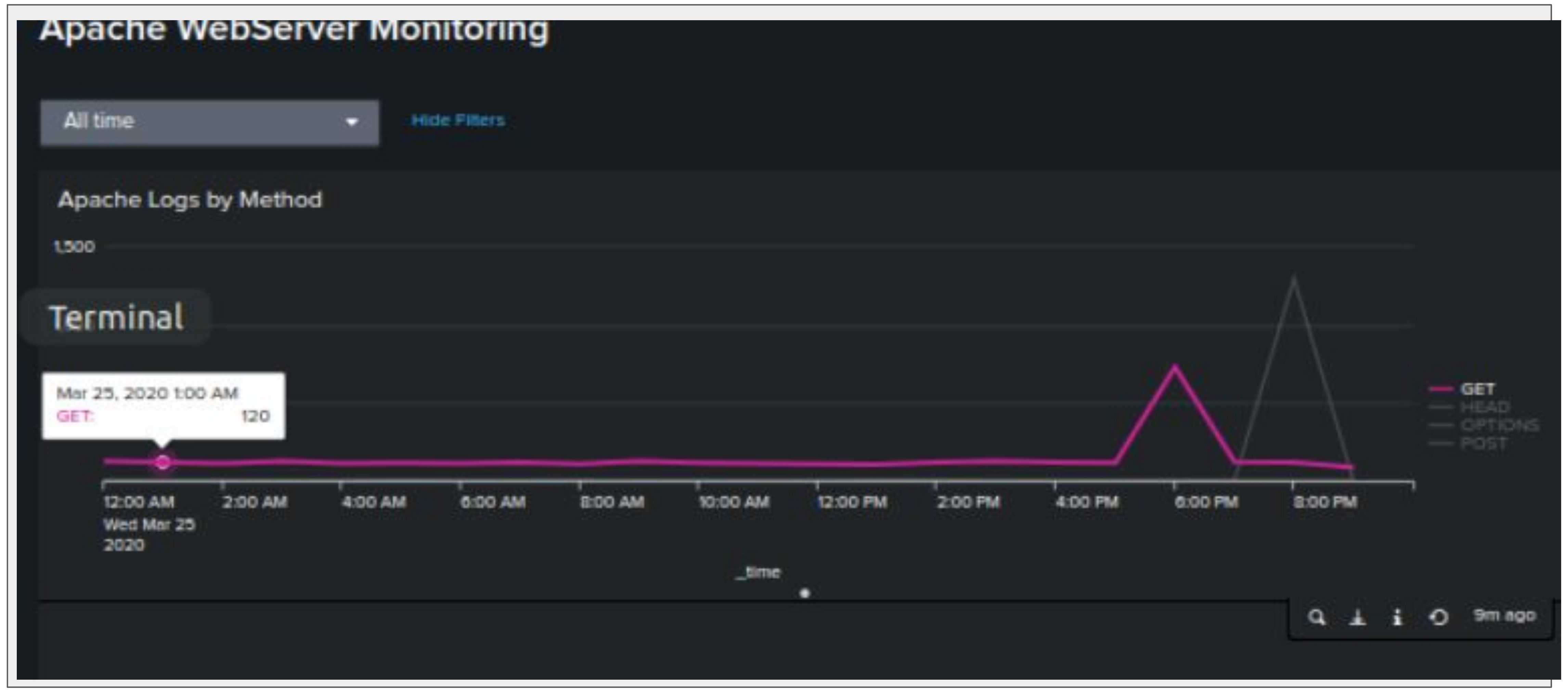
Alerts—Apache

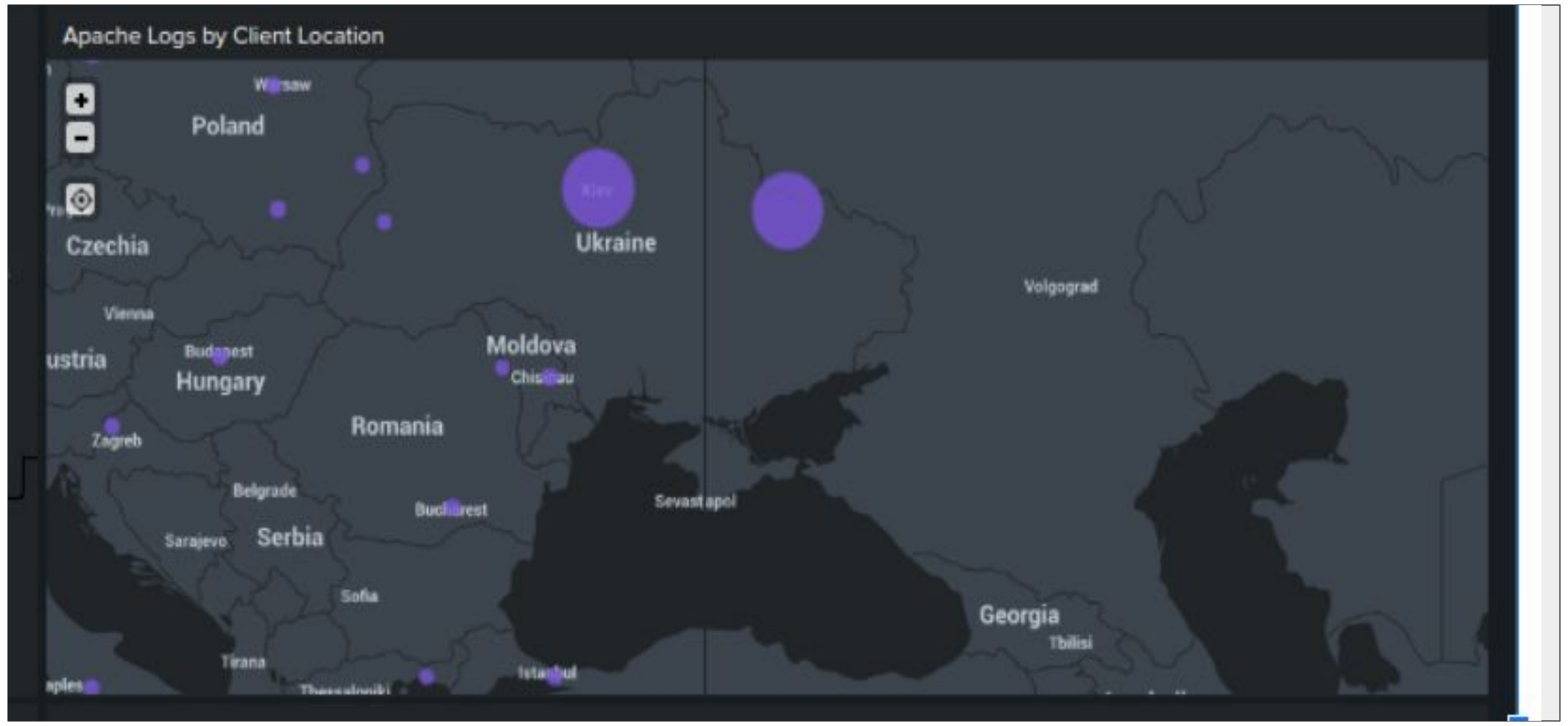
Designed the following alerts:

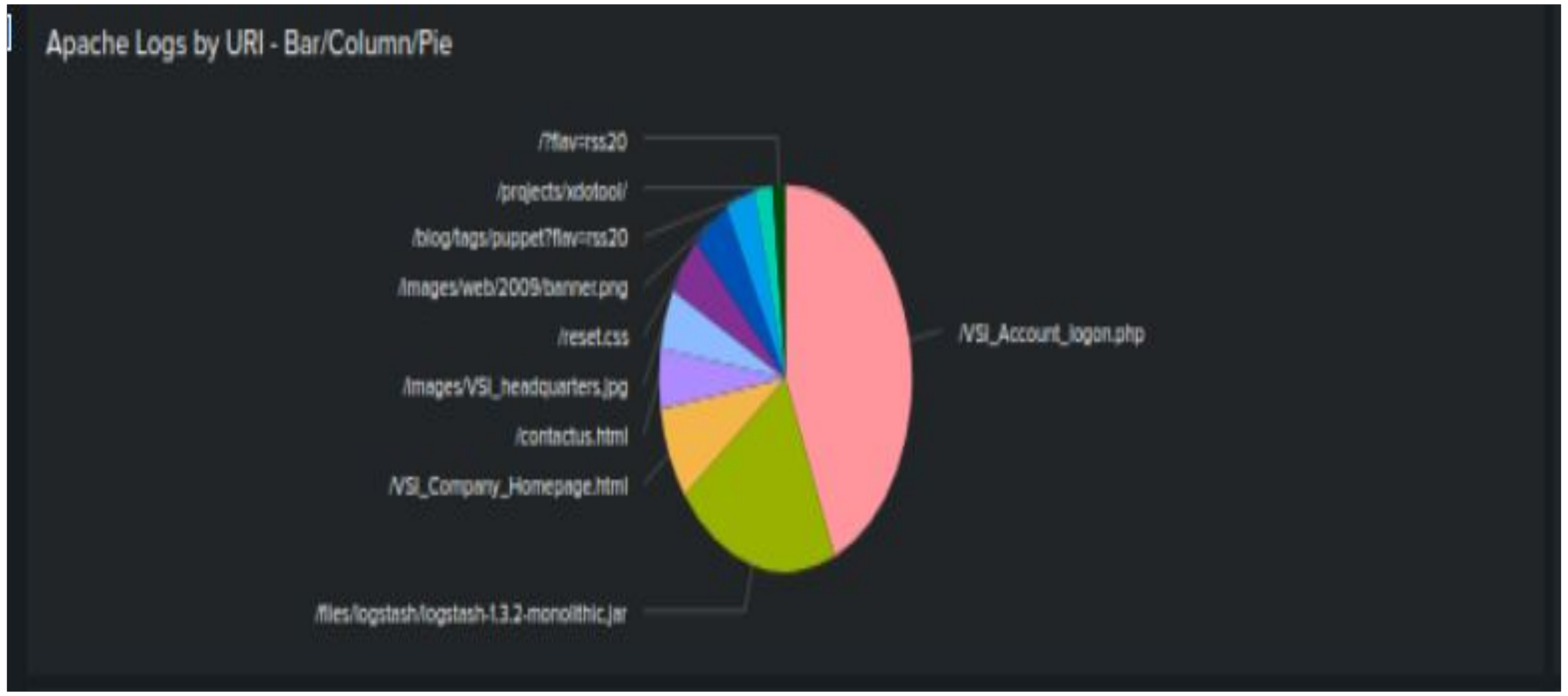
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache HTTP Post Alert	A baseline and threshold for hourly count of HTTP POST methods to trigger an email above normal activity	Around 1.5-2	9

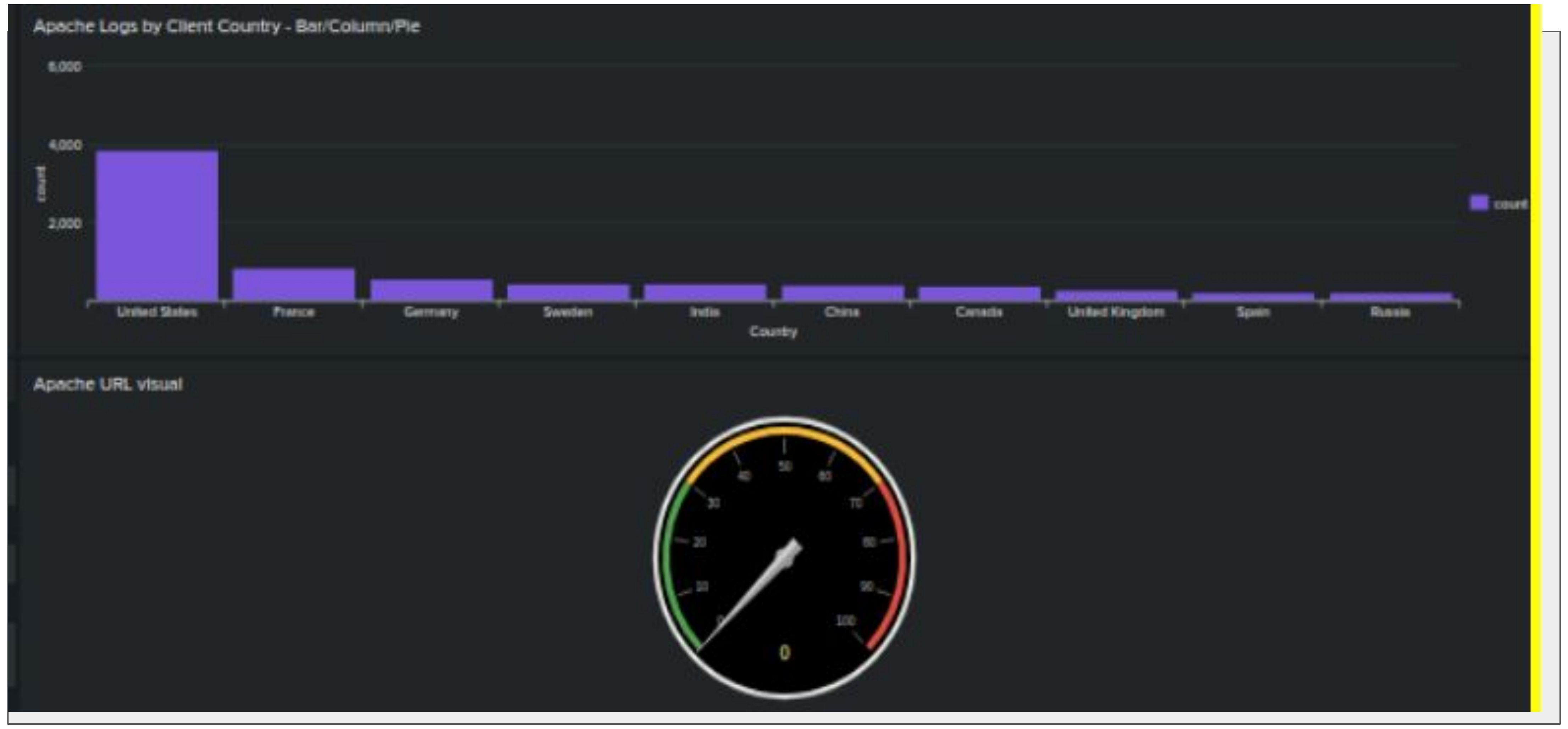
JUSTIFICATION: The majority of hourly activities didn’t hit more than 4 or 5 but it did have a spike of 7 so 9 gave us some room for irregularity that may be in play.

Dashboards—Apache






Apache Logs by URI - Bar/Column/Pie
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Company_Homepage.html
/files/logstash/logstash-1.3.2-monolithic.jar
/VSI_Account_logon.php



Supplemental Dashboard APACHE

Apache WebServer Monitoring
Edit
Export ▾
All time ▾
Hide Filters
Apache Logs by Method
150
100
50
Mar 17, 2020 9:00 PM
HEAD: 2
Terminal
Tue Mar 17
2020
6:00 PM
12:00 AM
Wed Mar 18
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Thu Mar 19
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Fri Mar 20
6:00 AM
12:00 PM
6:00 PM
_time
GET
HEAD
OPTIONS
POST
1m ago
Apache Logs by Client Location
Apache Logs by URI - Bar/Column/Pie
/robots.txt
/
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/images/VSI_headquarters.jpg
/VSI_Company_Homepage.html
/contactus.html
/reset.css
Apache Logs by Client Country - Bar/Column/Pie
6,000
4,000
2,000
count
United States
France
Germany
Sweden
India
China
Canada
United Kingdom
Spain
Russia
Country
count
Apache Logs by UserAgent - Table
Apache URL visual
10
20
30
40
50
60
70
80
90
100
0

useragent ⇕	count ⇕	percent ⇕
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1044	10.441044
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	369	3.690369
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364	3.640364
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	296	2.960296
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)	271	2.710271
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268	2.680268
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237	2.370237
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	236	2.360236
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	229	2.290229
Tiny Tiny RSS/1.11 (http://tt-rss.org/)	198	1.980198

Attack Analysis

Attack Summary—Windows

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

- There were suspicious changes in severity which showed that the high increased from 6.9% to 20.22% and the informational decreased from 93.08% to 79.77%.
- As for the failed activities. They did not change much, the count decreased on the attack log to 93 from 142. Percentage changed from success: 97% /failure: 3% to success: 98.5%/failure: 1.5%.

Attack Summary—Windows

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

- For the failed activity there were excess events on Wednesday March 25, 2020 at 8am on the attack log file, up to 35 events and the most on a typically log file was 10 so this showed an increase in failures. The threshold was certainly set low enough to trigger the alert as it was set to 15 and this point in time hit 35.
- As for the successful logins, the attack file increased massively from 21 to 196 by the primary User J at 11am on Wednesday March 25, 2020. Yes the threshold of 33 would certainly catch this attack for review.
- During the time of the attack, it appears that the deleted accounts showed a large decrease in the number of deleted accounts. Although nothing could be concluded with this information. This threshold would have been better suited to trigger at a lower threshold under the trigger condition to trigger when **less than rather than greater than.**

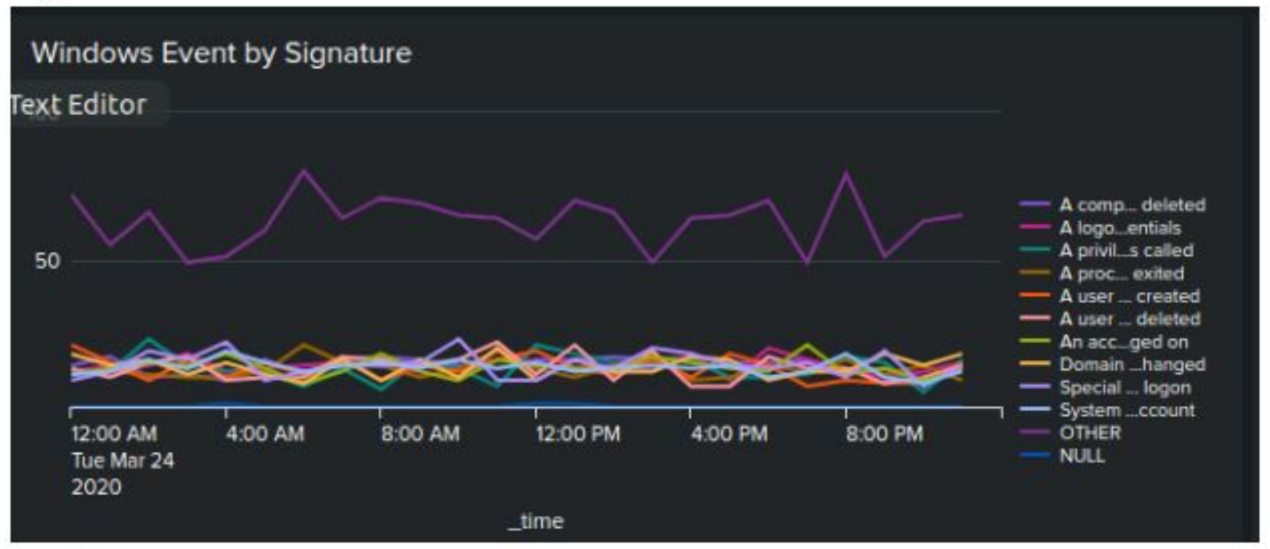
Attack Summary—Windows

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

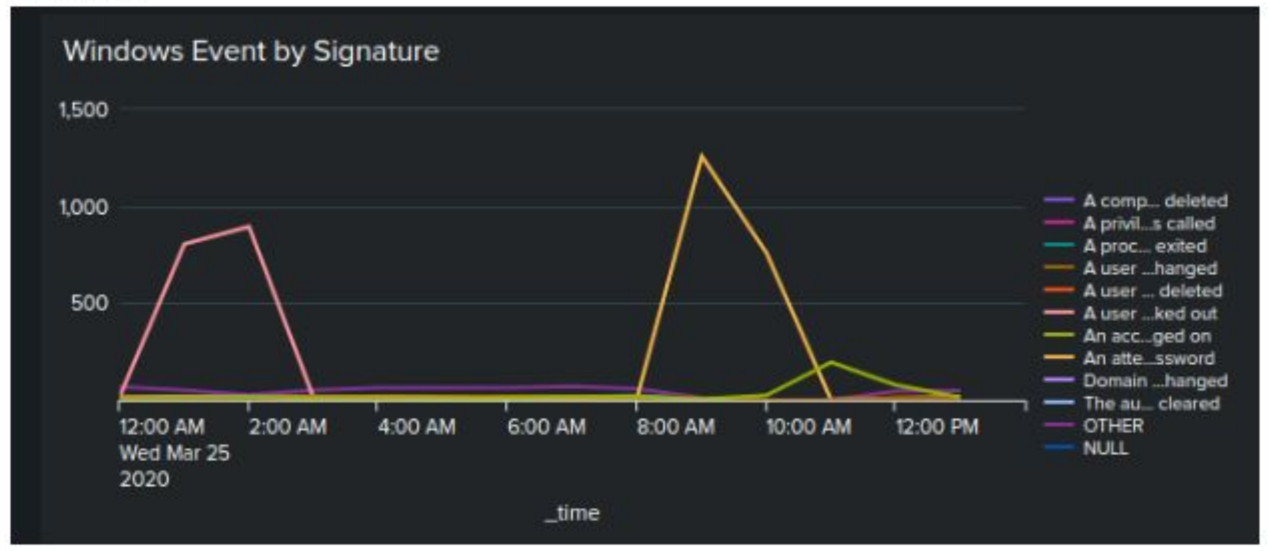
- When viewing the events by signature with the windows log file alongside the attack log file, there is an obvious spike and you can clearly see the irregular activity in plain view (see image 1 below)
- Large amounts of attempts were made to log in from the time of 8 am to 11am. An attempt was made to reset the password. Large amounts of attempts were made from 12am to 3 am March 25th, where user accounts were locked out. Possible DDoS/brute force attack. Normal activity doesn't occur during these hours typically
- Users A, K and J all displayed excess activity out of the normal scope on a typical day. (see image 2 below)
- There was a slight increase in the accounts logged on so it appears that they were successful but there was a huge increase in the attempts to reset passwords and accounts getting locked out (see image 3 below)
- See also Dashboard Analysis for Users with Stats added for reference (see image 4 below)

Screenshots of Attack Logs (v.s. normal logs)

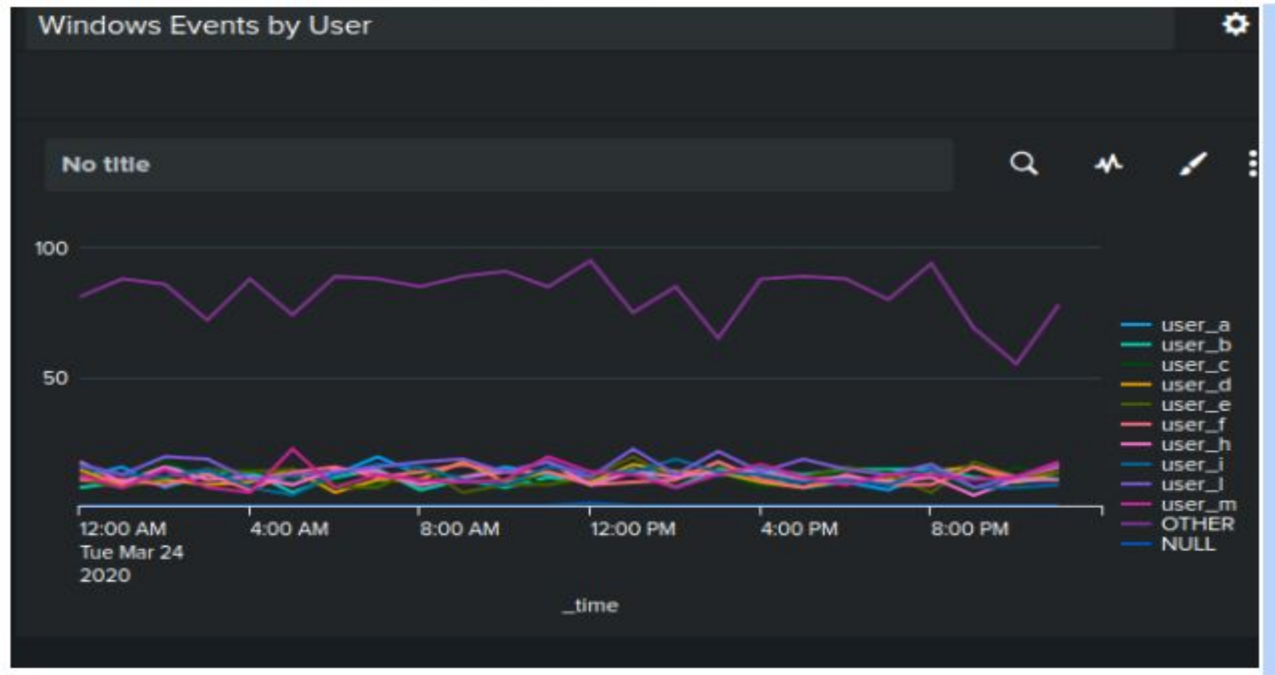
Dashboard Analysis for Time Chart of Signatures regular



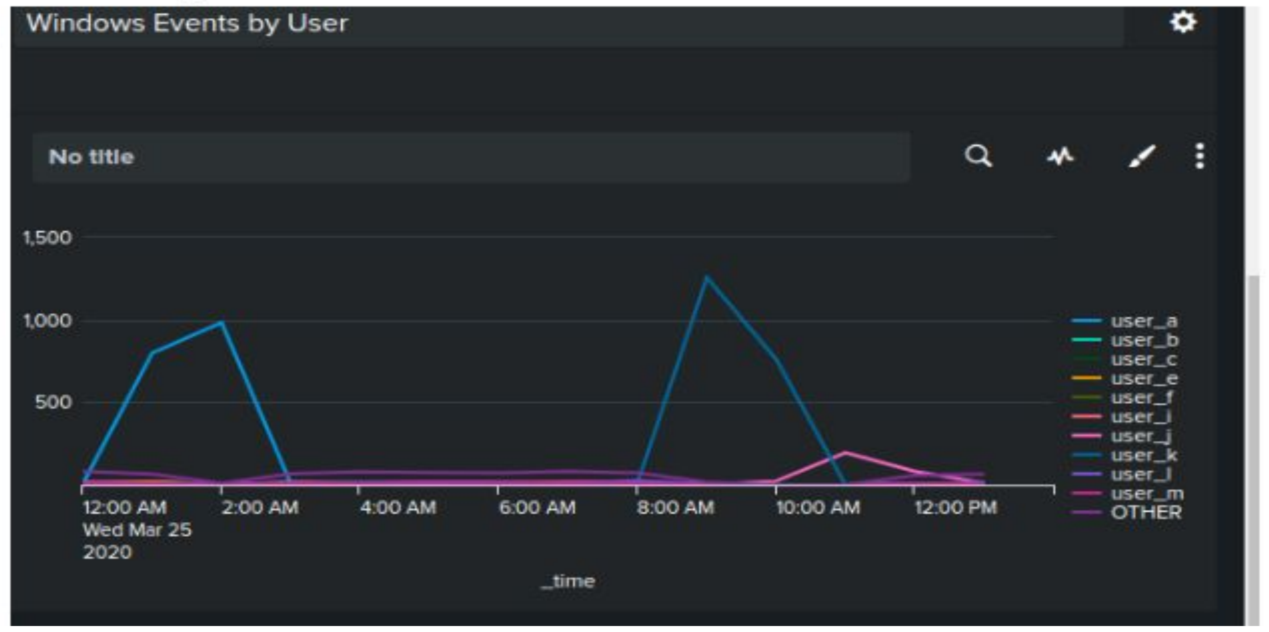
vs attack

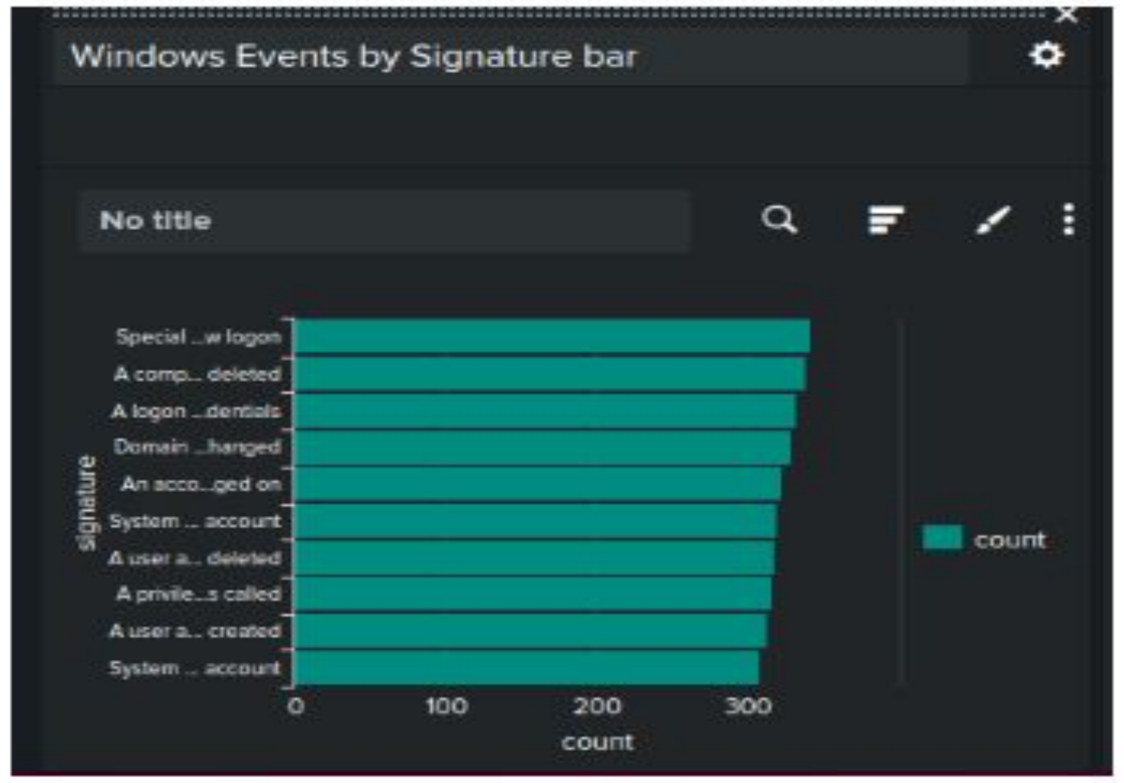


Dashboard Analysis for Users - regular log

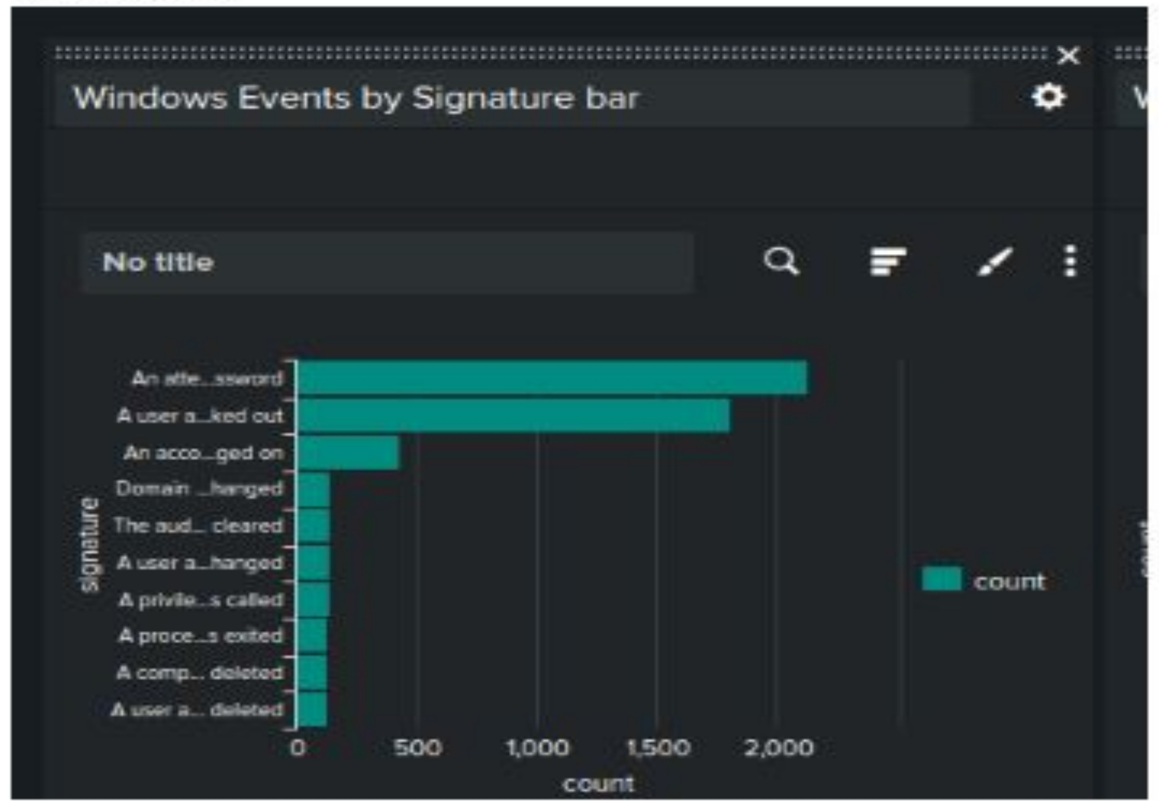


vs attack log





vs attack log



Dashboard Analysis for Users with Statistical Charts - regular

Windows Events by User - Table

No title

user	count	percent
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

vs attack logs

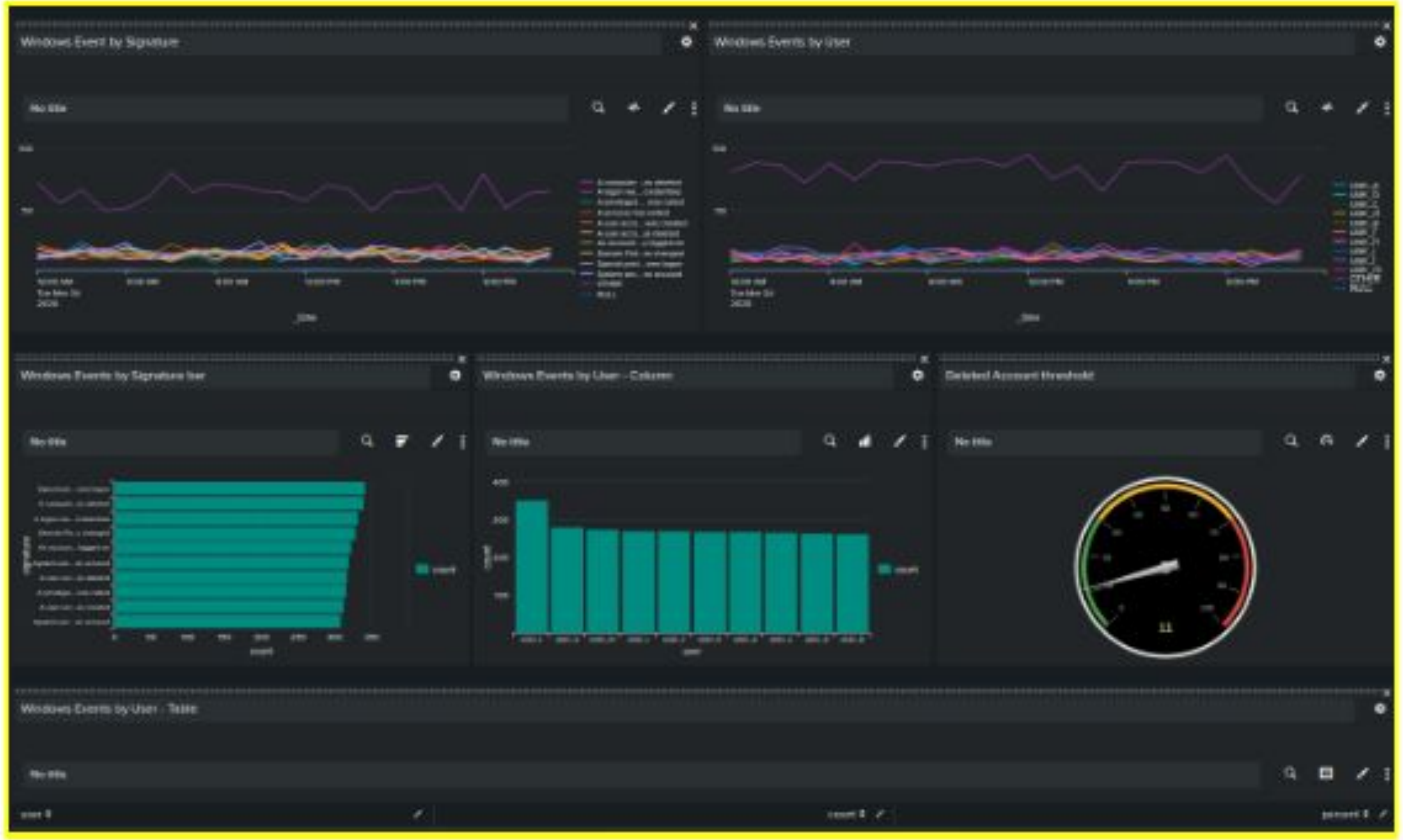
Windows Events by User - Table

No title

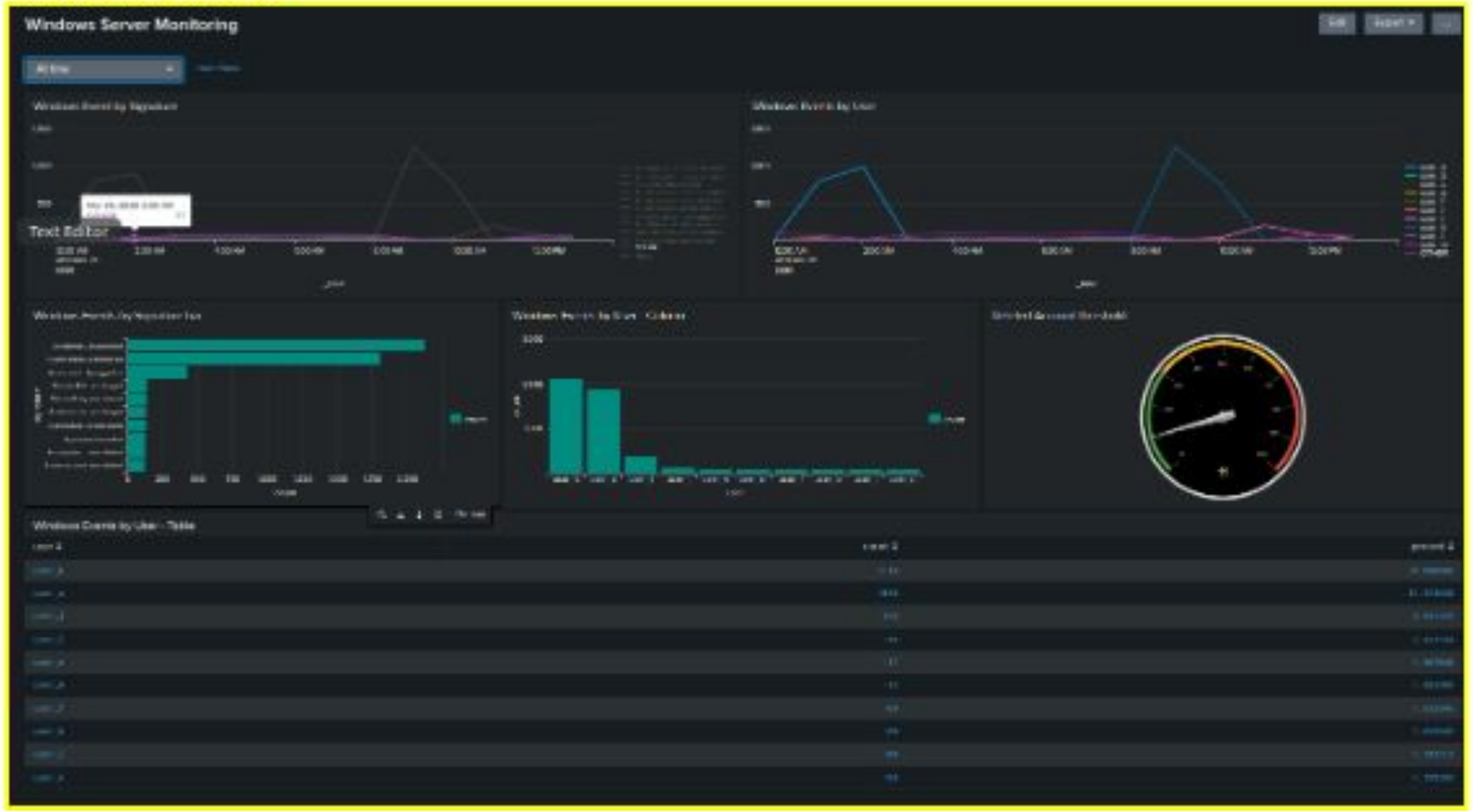
user	count	percent
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	145	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

Windows log vs Windows Attack Log Supplemental Slide

windows regular dashboard


Windows Event by Signature
Windows Events by User
No title
Windows Events by Signature bar
Windows Events by User - Column
Deleted Account threshold
11
Windows Events by User - Table
user
count
percent

vs attack dashboard


Windows Server Monitoring
All time
Windows Event by Signature
Windows Events by User
Text Editor
Windows Events by Signature bar
Windows Events by User - Column
Deleted Account threshold
Windows Events by User - Table
user
count
percent

Attack Summary—Apache

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

- The report for the different HTTP methods show that the GET requests decreased from 98% to 70% and increased the amount of POST requests from 1% to 29% on the attack logs
- The report for the top 10 domains referred to VSI’s website didn’t show anything suspicious or out of the ordinary
- However, the report analysis for HTTP response codes did come back with suspicious activity. The percentage of 404 error status increased from 2% to 15% so the site was having trouble during this time. Also the percentage of 200 successful codes decreased from 91% to 83%

Attack Summary—Apache

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

- The alert analysis for International Activity did come back with some location data of where the attack may have stemmed from. There was activity from Ukraine at 8 p.m. on Weds, March 25th, with a count of 939 events. Since our threshold was set to 143 we would have been in line for triggering the alert during the attack
- The alert analysis for HTTP POST activity indicated a spike in the POST and GET methods. During the attack The POST method was used, starting after 7 PM and ending by 9 PM. The peak count was 1,296. The GET method was used, starting after 5 PM and ending by 7 PM. The peak count was 729. The threshold was set within the specifications necessary to trigger the alert during the attack

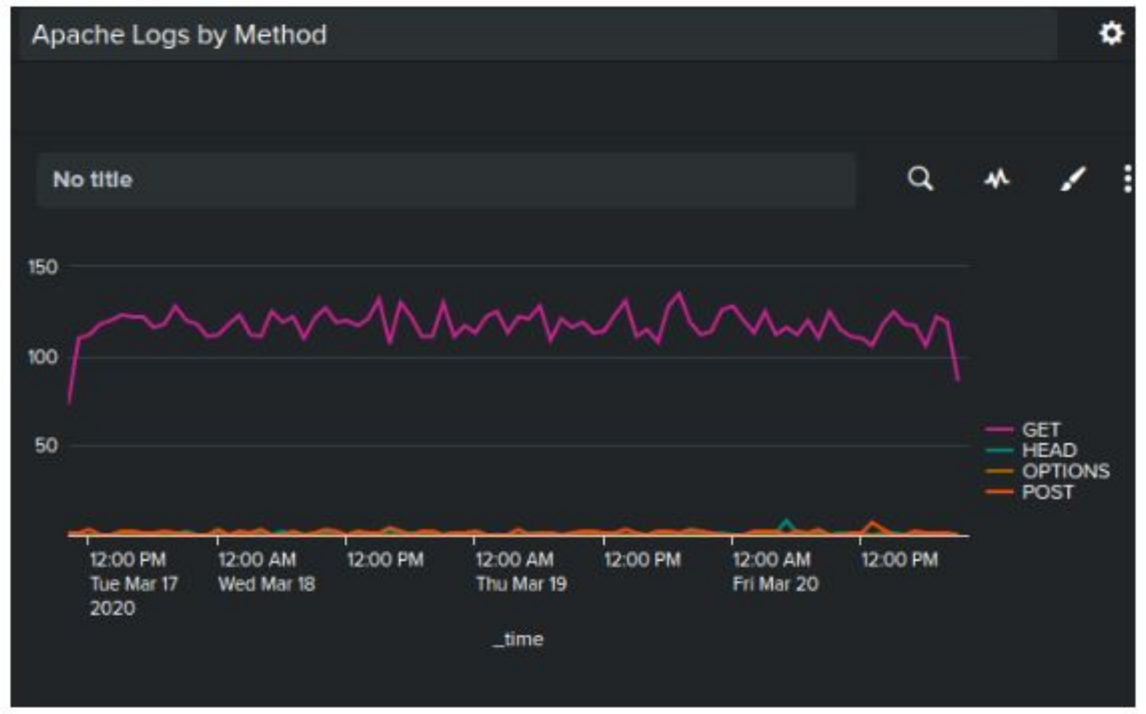
Attack Summary—Apache

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

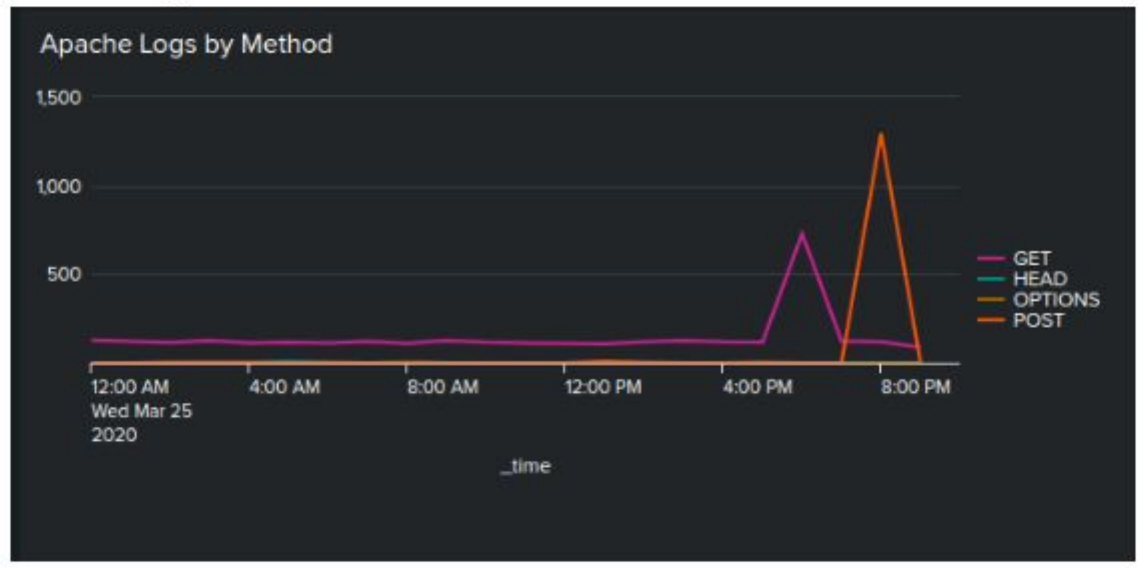
- Analysis of the Time Chart of HTTP methods shows suspicious activity from Ukraine with the POST and GET method. Possibly a DDoS with POST and GET methods. The POST method was used, starting after 7 PM and ending by 9 PM. The peak count was 1,296. The GET method was used, starting after 5 PM and ending by 7 PM. The peak count was 729 (see image 1)
- Analysis of the Cluster Map also demonstrated suspicious activity coming from the Ukraine. In particular, the count and locations were as follows: Kyiv(formerly Kiev): Count of 439; Kharkiv: Count of 433 (see image 2)
- The analysis for URI data show that there was some activity against the main VSI logon page: /VSI_Account_logon.php which showed a large increase in the logon page which could indicate a brute force or password spraying attack (see image 3)

Screenshots of Attack Logs

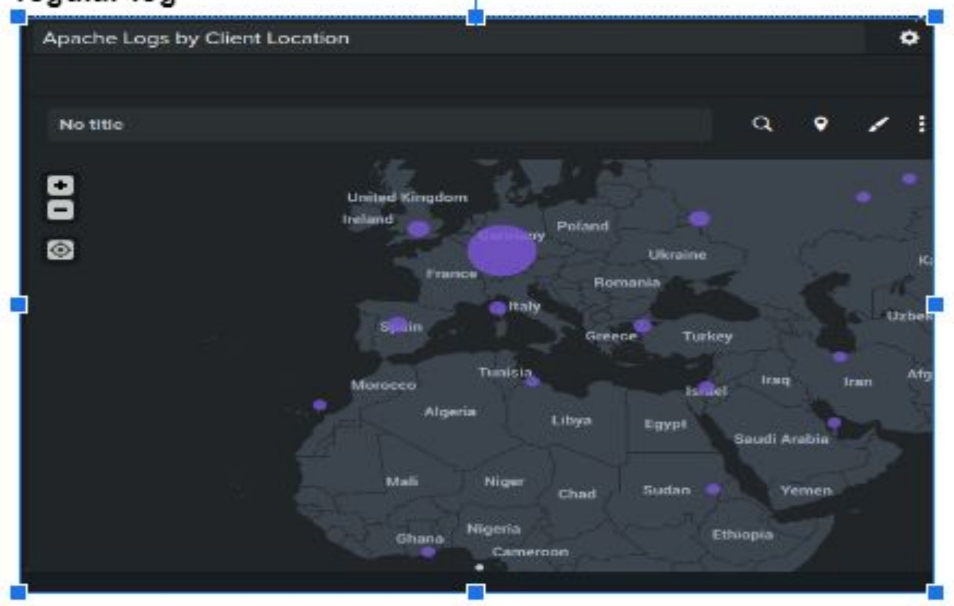
regular log

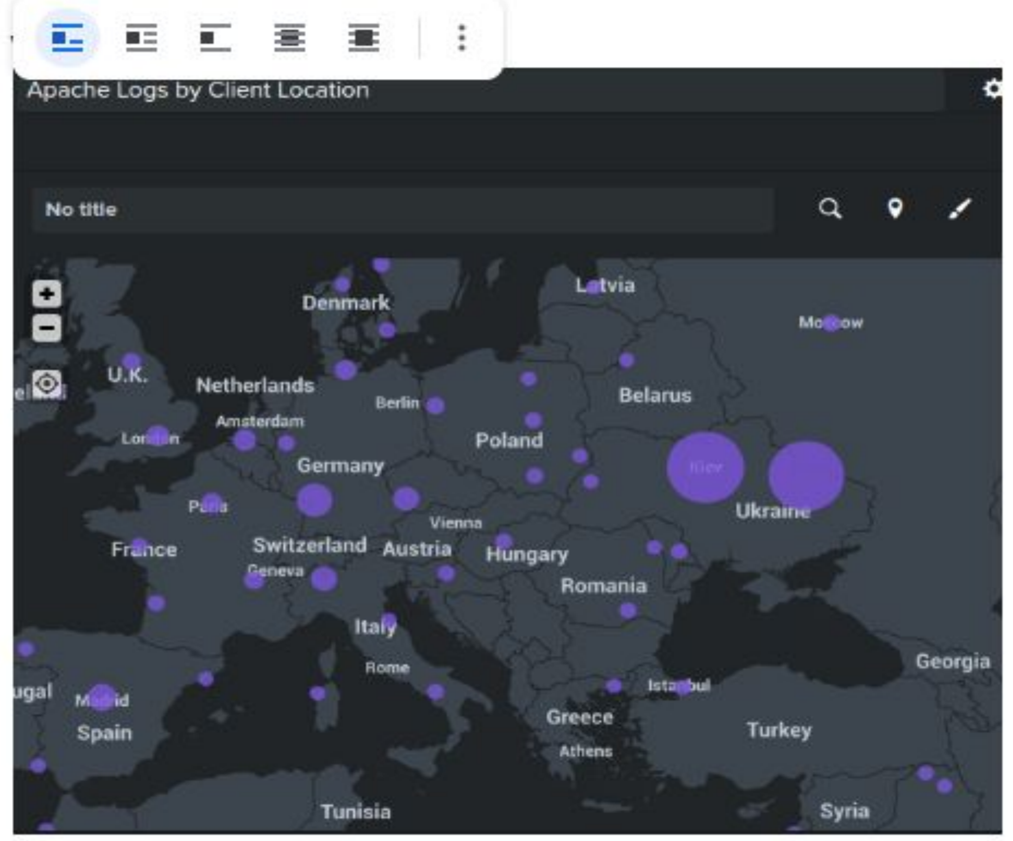


vs Attack log

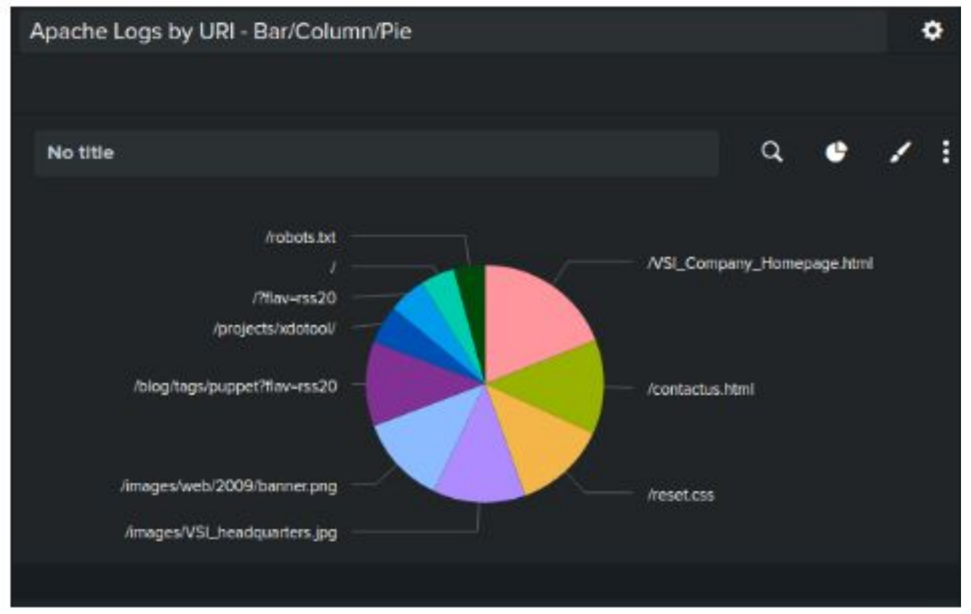


regular log

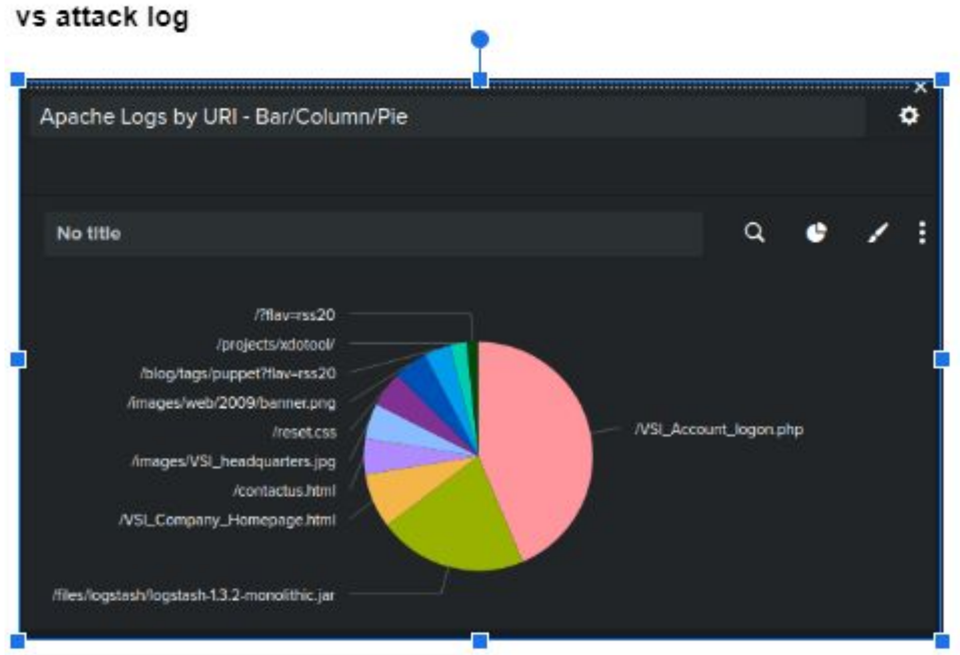




regular log

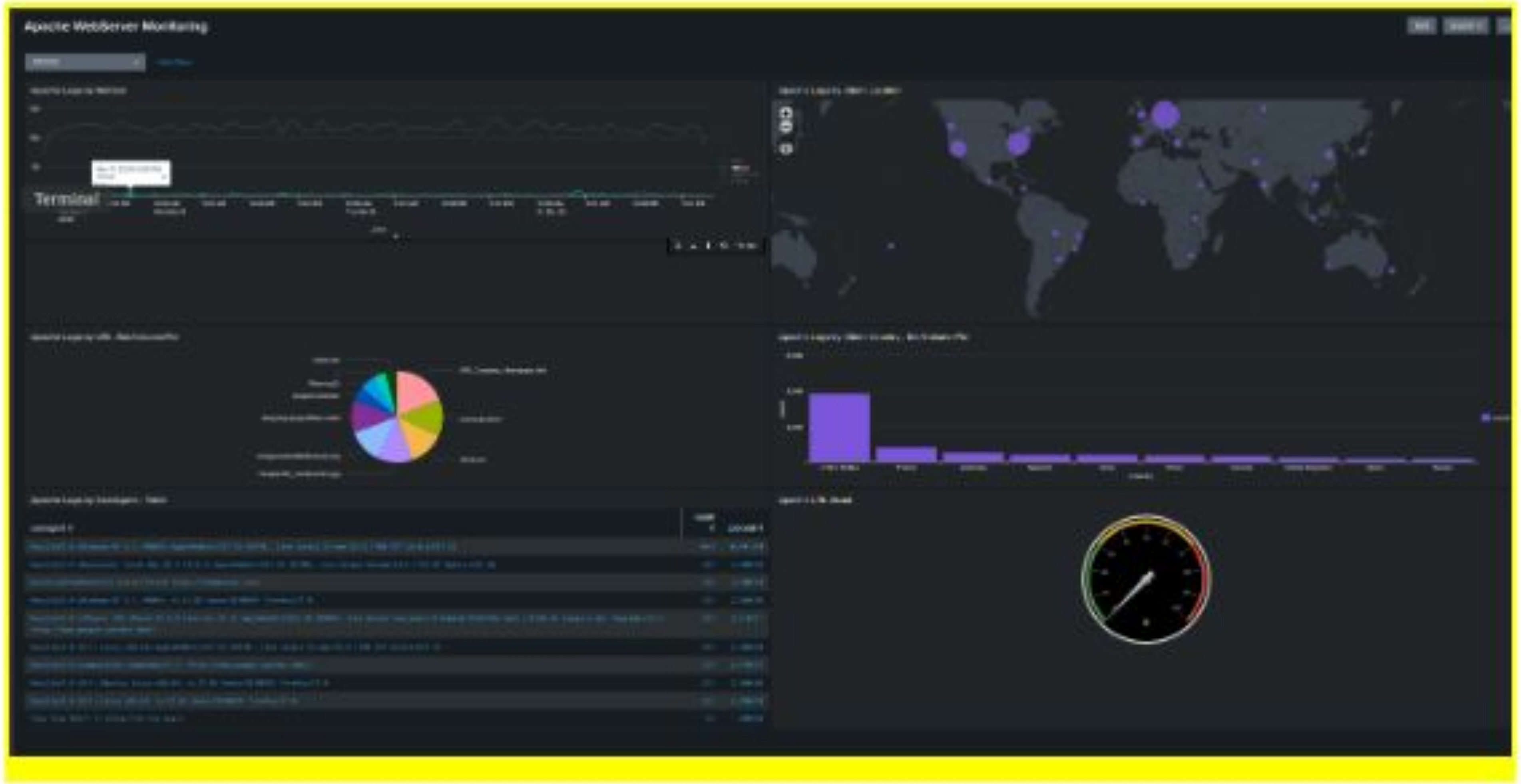


vs attack log

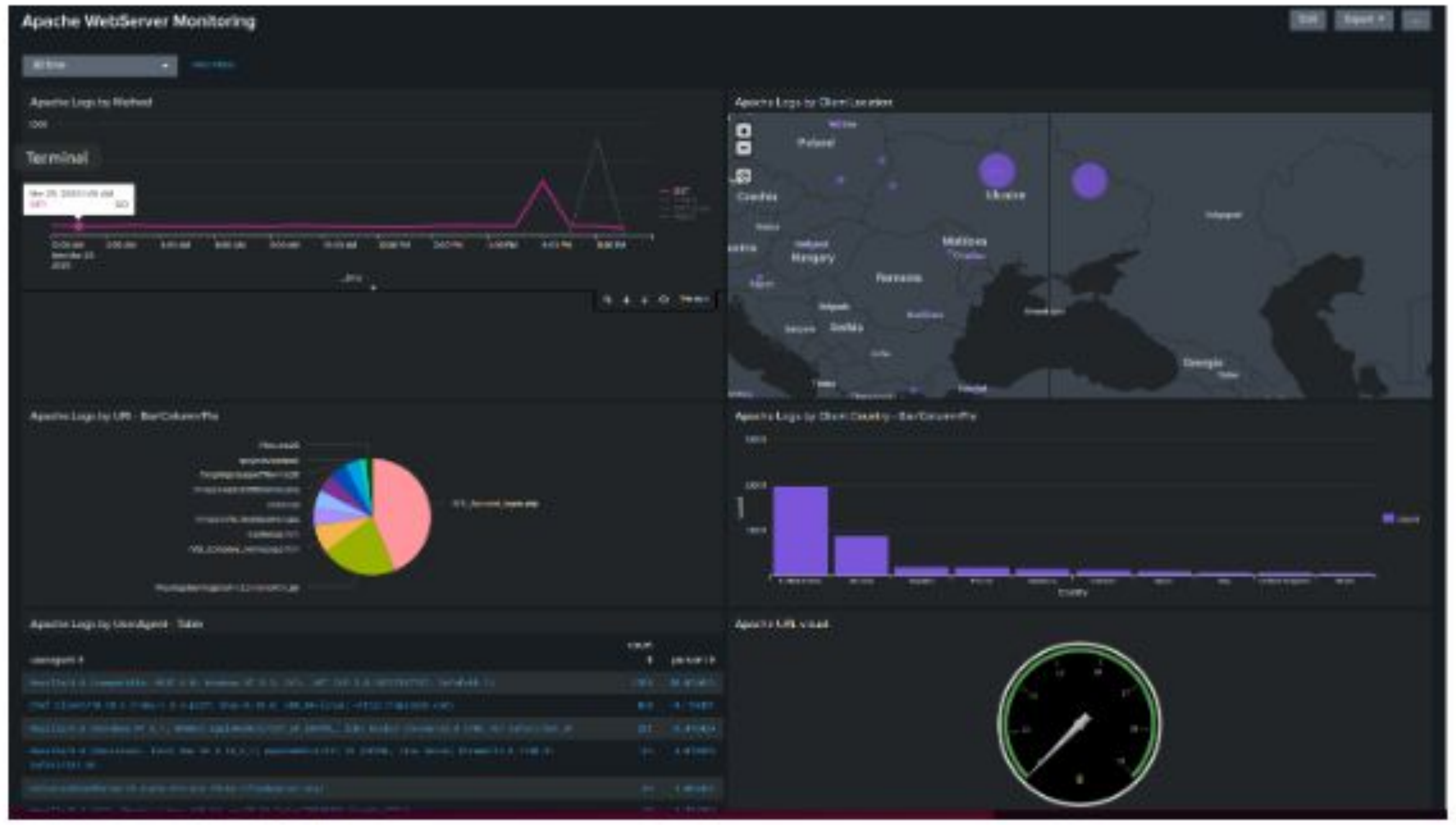


Apache logs vs Apache attack logs Supplemental Slide

regular dashboard Apache



vs attack dashboard Apache


Apache WebServer Monitoring
Apache Logs by Method
Terminal
Apache Logs by Client Location
Poland
Ukraine
Czechia
Hungary
Moldova
Romania
Sofia
Georgia
Apache Logs by URI - Bar/Column/Pie
Apache Logs by Client Country - Bar/Column/Pie
Apache Logs by UserAgent - Table
Apache URL visual

Summary and Future Mitigations

Project 3 Summary

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

  Overall, the attack findings led our team to determine the user accounts that were used during this attack appear to be Users A/K/J. They used off hours on the windows server to brute force it so that the large amount of attempts to log in and get locked out were not done while most people are in the office. We found that this activity from these users occurred in two main cities in the Ukraine, Kiev and Kharkiv. Appears they were successful at deleting accounts and most likely gained unauthorized access to accounts as well.

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

  The alert threshold we set up would certainly help the team get to issue at hand much quicker once these excess activities are discovered and reported. One quick resolution to the accounts that were attacked would be to set up a more strict protocol for attempted logins and stronger password security measures overall. If malicious activity from this region is still making the site vulnerable then setting limitations from the Ukraine IPs could be another alternative if these other measure don’t help.