SIEM Environment Simulation

Robert Russell

Table of Contents

Monitoring Environment

Scenario

- SOC analyst for **Virtual Space Industries (VSI)**
  - a software company that designs virtual-reality programs for businesses.

- Rumors of a competitor (**JobeCorp)** will possibly launch cyberattacks to disrupt VSI.

- the SOC analysts have been tasked with monitoring for the potential disruptions
  - Logs include:
    - An Apache web server for VSI's administrative webpage
    - A Windows operating system used for back-end operations

- Our networking team has past logs to help develop baselines to create reports, alerts, dashboards.

- We are tasked with analyzing these "attack logs" with your monitoring solution to determine the efficacy of our solution.

Logs Analyzed

1 Windows Logs

Analyzed Windows Server user account for suspicious activity by comparing them to a baseline.

- Monitored account creations
- Identified failed user activities such as:
  - Failed logins
  - Account Deletions

2 Apache Logs

Analyzed VSI’s website traffic for suspicious activity by comparing them to a baseline.

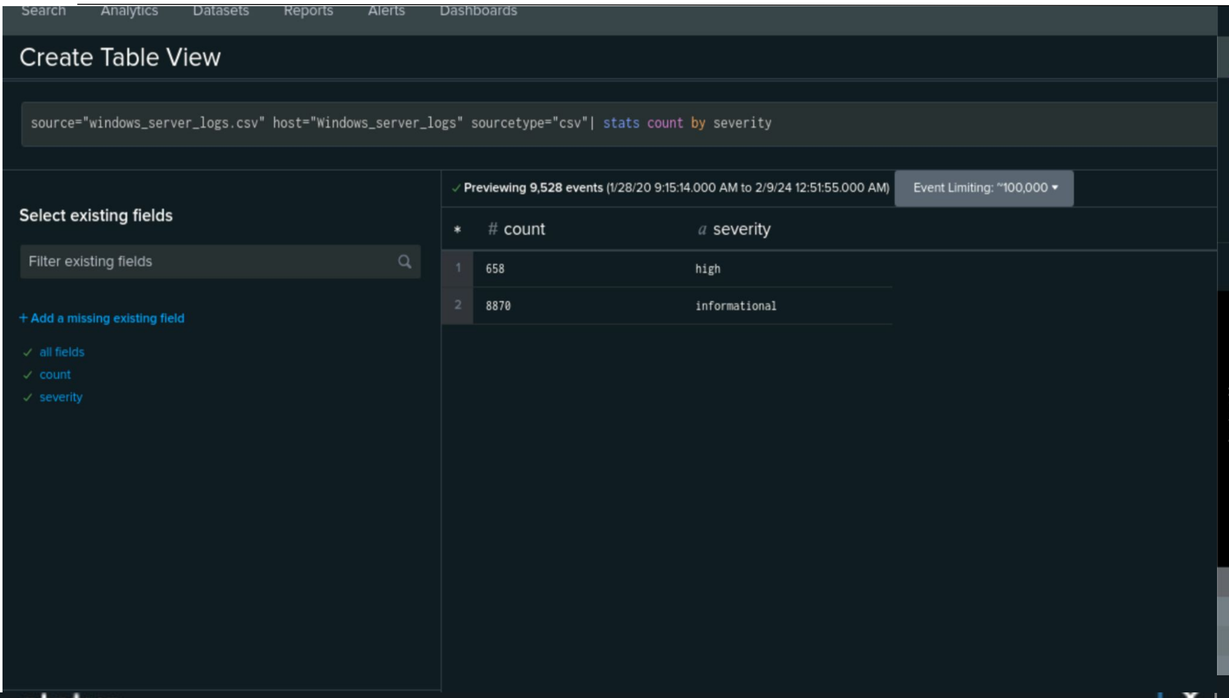
- HTTP requested activity
  - Success vs Failure as well
- Patterns from requesting domains

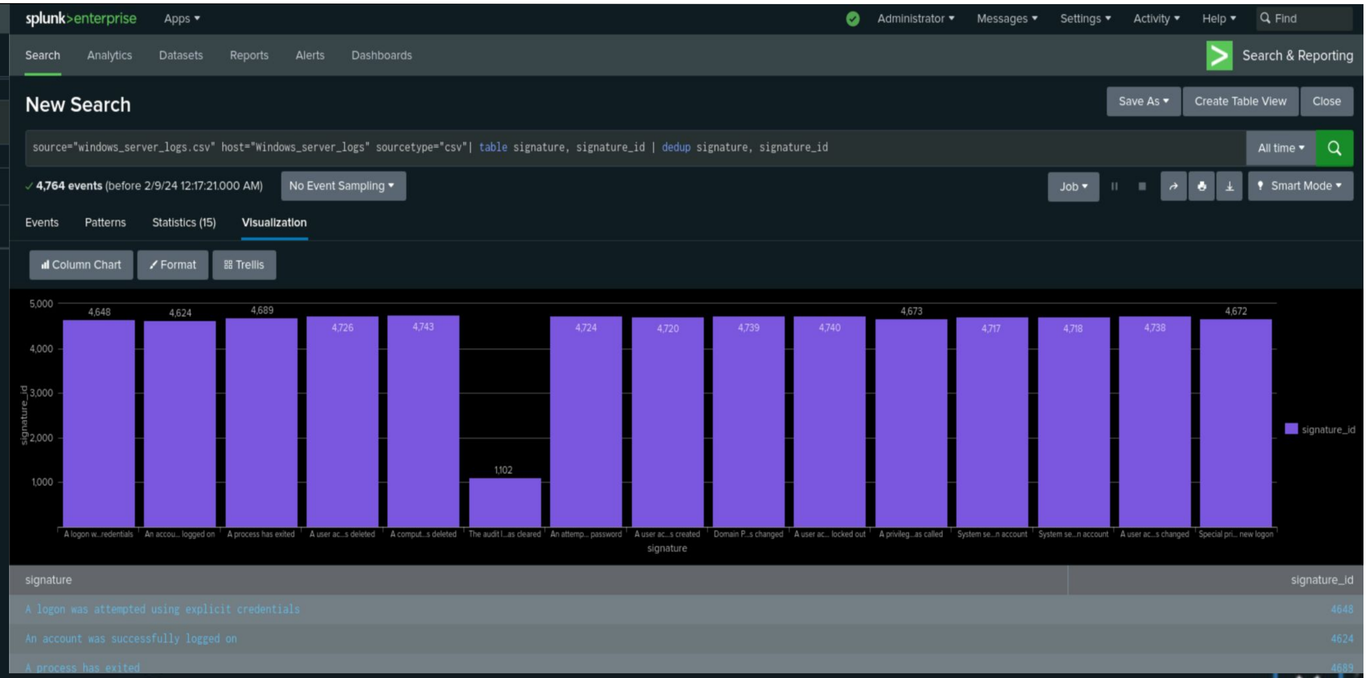
Windows Logs

Reports - Windows Servers

Report Name	Report Description
Signatures	Plain text description of an event that happened. • Special privilege assigned, account created/deleted, domain policy changed, etc..
Severity	Amount and variety of severity levels tracked (high vs informational)
Status	Success or failure of an attempted action
Users	Connecting WHO to WHAT

Reports - Windows





Alerts — Windows - Successful Logins

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Server Hourly Successful Logins Exceeded	>45 successful logins occurred within an hour	27/hr	45/hr

JUSTIFICATION:

- Successful logins are ~650 in 24hrs with spikes at the beginning and middle of the workday. The higher threshold is close enough to the spikes for no trigger, but low enough to alert unusual behavior without false positives.

Alerts — Windows - User Accounts Deleted

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alarming amount of User Accounts Deleted	>40 User Accounts have been deleted within the hour	27/hr	>40/hr

JUSTIFICATION:

- The data illustrated a range of 18 - 44 user accounts deleted per hour within 24hrs. There is room for calibration as it’s currently set a little under the found max.

Alerts — Windows - Failed Event

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Event Activity Has Exceeded Threshold	Failed Windows Activity Exceeded Threshold. Check: Signature	12/hr	25/hr

JUSTIFICATION: The events spanned a wide range, but 25 is still low for hourly login attempts failures.

Baseline Dashboards - Windows - Users

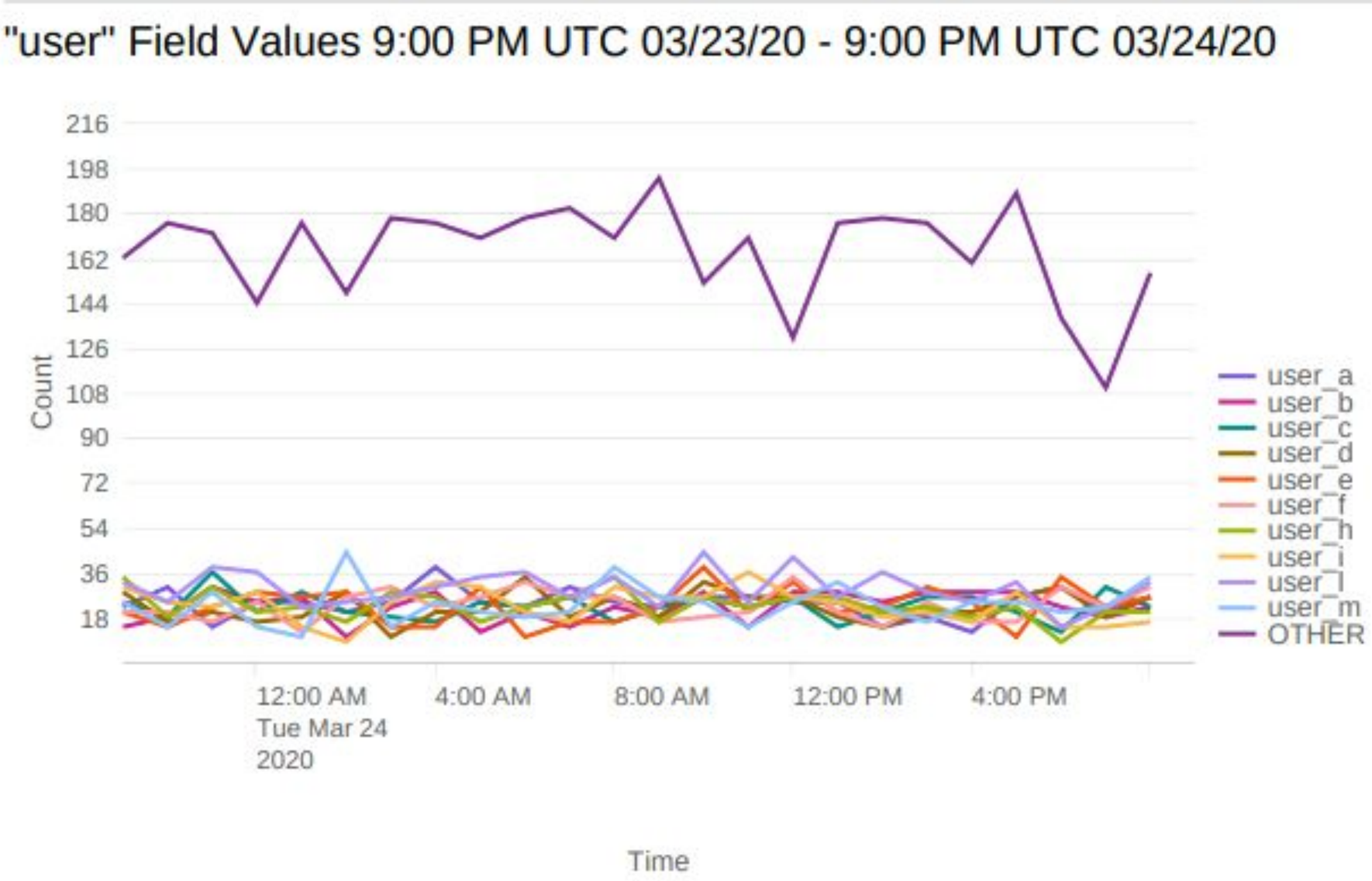


Fig 2: User activity over 24 hours

Baseline Dashboards — Windows - Amount of User Logins

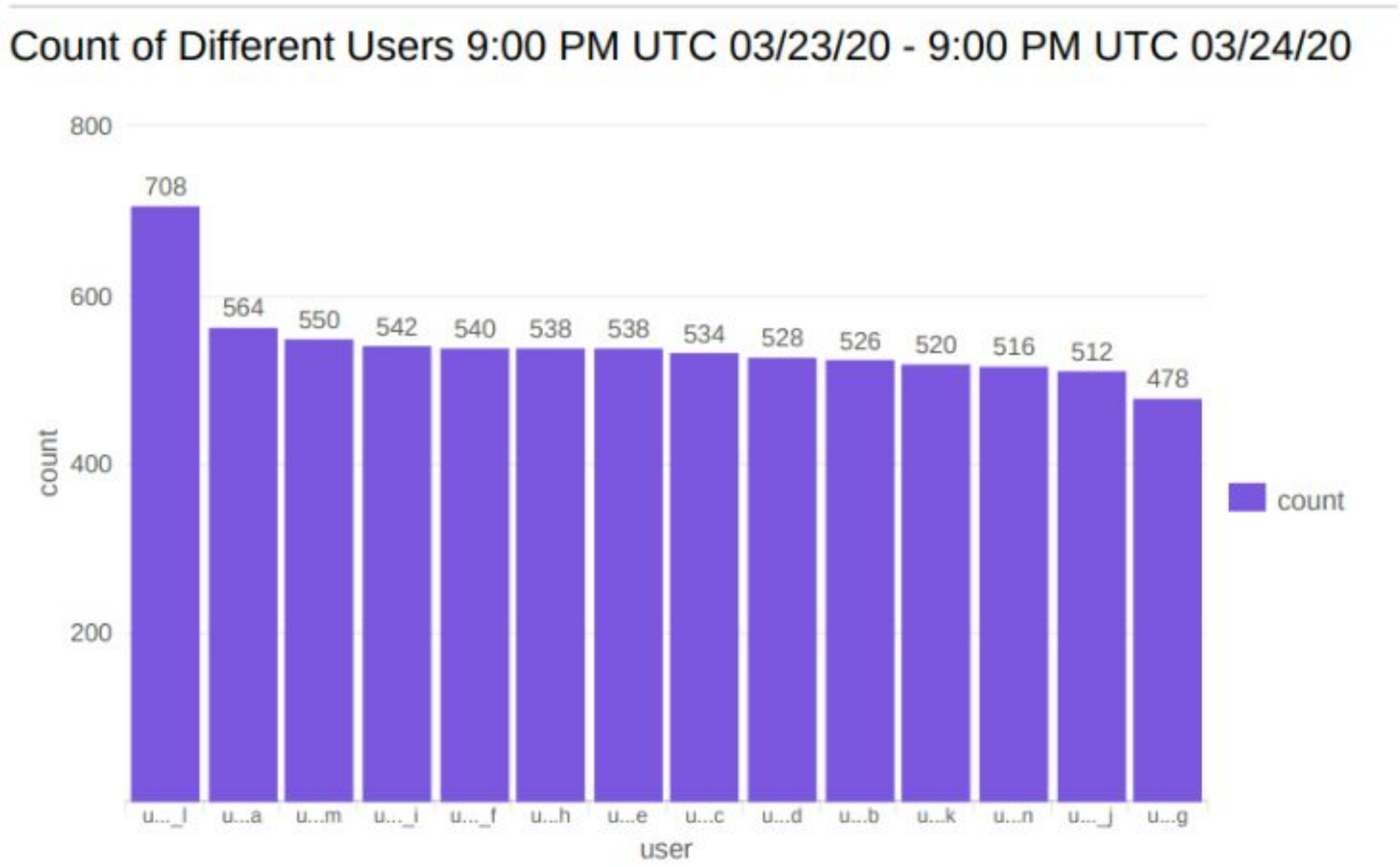


Fig 1: Baseline of the Top 14 active users in a 24 hour period

Baseline Dashboards - Windows - Signature Event Count

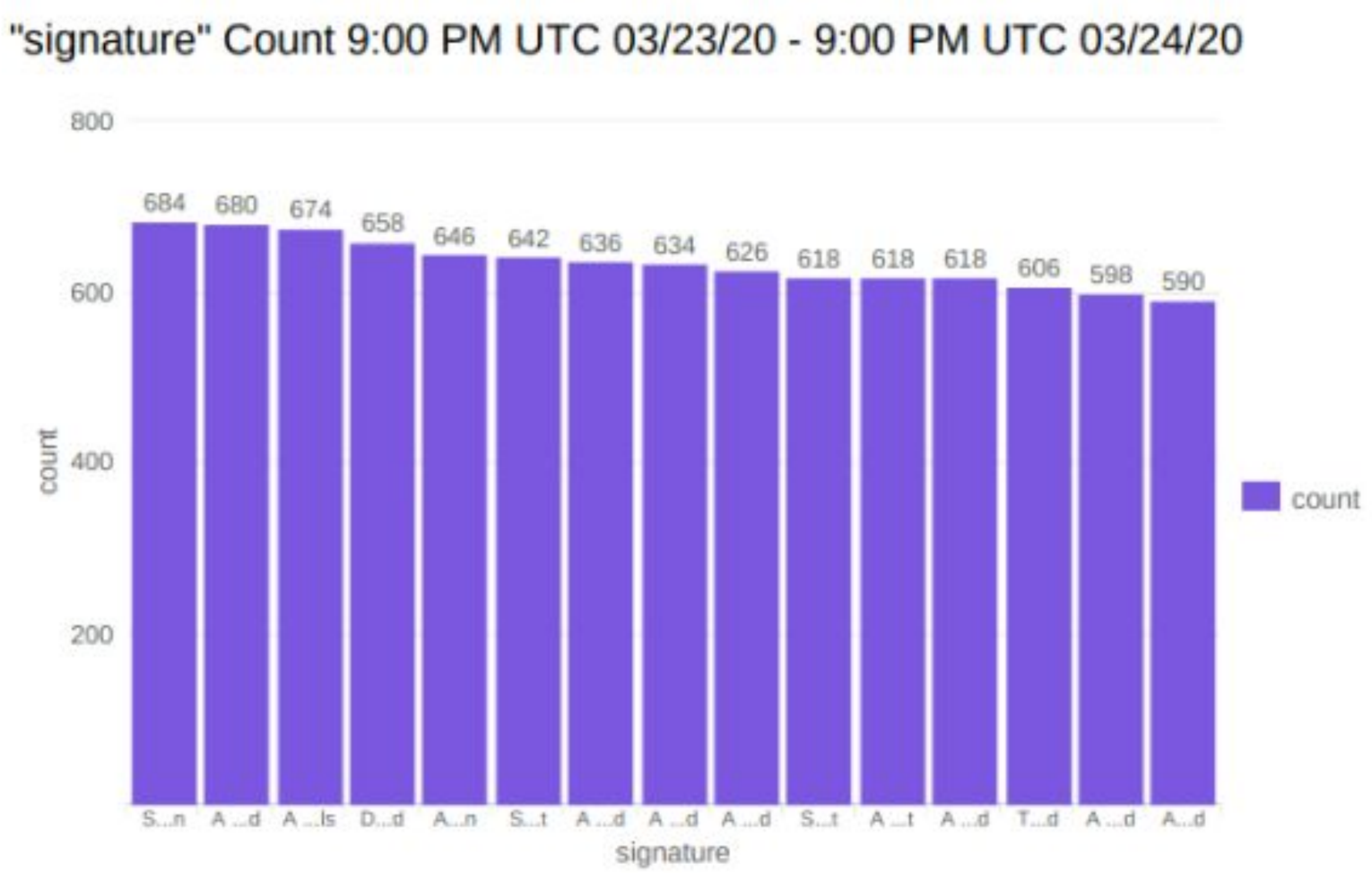


Fig 3: Counts of specific event names that were logged

1	Special Privilege assigned to new logon
2	A computer account was deleted
3	A logon was attempted using explicit credentials
4	Domain Policy was changed
5	An Account was successfully logged on
6	System security access was removed from an account
7	A user account was deleted
8	A privileged service was called
9	A user account was created
10	System security access was granted to an account
11	A user account was locked out
12	A process has exited
13	The audit log was cleared

Dashboards — Windows - Severity

Low amount of High Severity logs

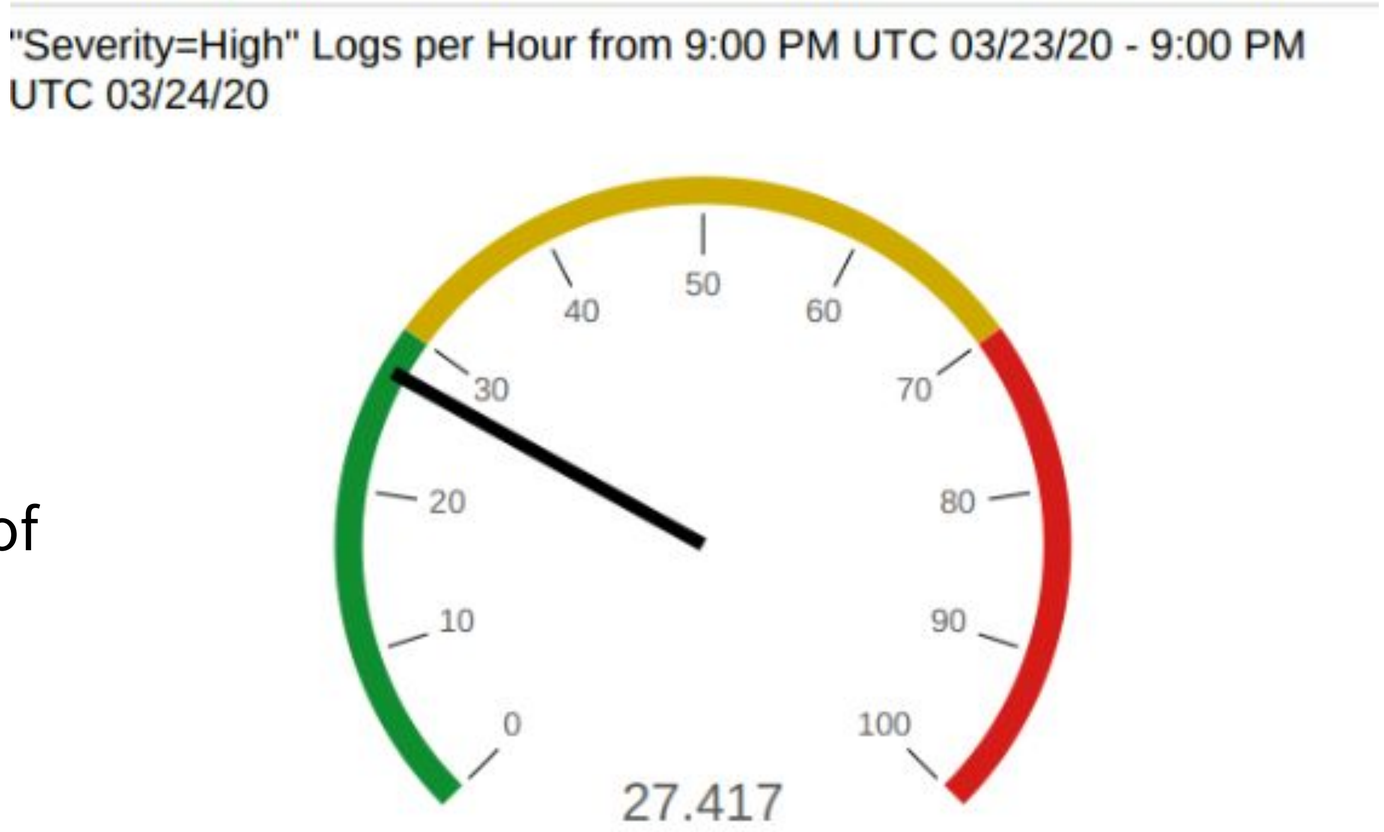


Fig 5: Baseline indicator of high severity events per hour. Green=Good

Apache Logs

Reports — Apache

Report Name	Report Description
Apache Server HTTP Methods	To identify the count and percent of HTTP methods (GET, POST, HEAD, OPTIONS)
Apache Server HTTP Response Codes	To identity suspicious levels of HTTP responses.
Top 10 URI’s to VSI’s website	To identify suspicious referrers to VSI’s website.

Images of Reports—Apache

Report for HTTP Methods Used in Apache

Edit ▾ | More Info ▾ | Add to Dashboard

ranges from 7:00 AM UTC 03/17/20 - 7:00PM UTC 03/20/20

All time ▾

✓ **10,000 events** (before 2/11/24 5:19:34.000 PM)

Job ▾

4 results 20 per page ▾

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

Report: Top 10 Referrer Domains to VSI's Website

Edit ▾ | More Info ▾ | Add to Dashboard

7:00AM UTC 03/17/20 - 7:00 PM UTC 03/20/20

All time ▾

✓ **10,000 events** (before 2/11/24 5:24:49.000 PM)

Job ▾

10 results 20 per page ▾

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

Report: HTTP Response Codes

Save | Save As ▾ | View | Create Table View | Close

source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" status="*"| top limit=0 status

All time ▾

✓ **10,000 events** (before 2/12/24 10:04:47.000 PM) No Event Sampling ▾

Job ▾ Verbose Mode ▾

Events (10,000) Patterns **Statistics (8)** Visualization

20 Per Page ▾ Format Preview ▾

status	count	percent
200	9126	91.26
304	445	4.45
404	213	2.13
301	164	1.64
206	45	0.45
500	3	0.03
416	2	0.02

Alerts — Apache - International

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Activity (Hourly)	Alert: an IP	60 hit/hr	120 hits/hr

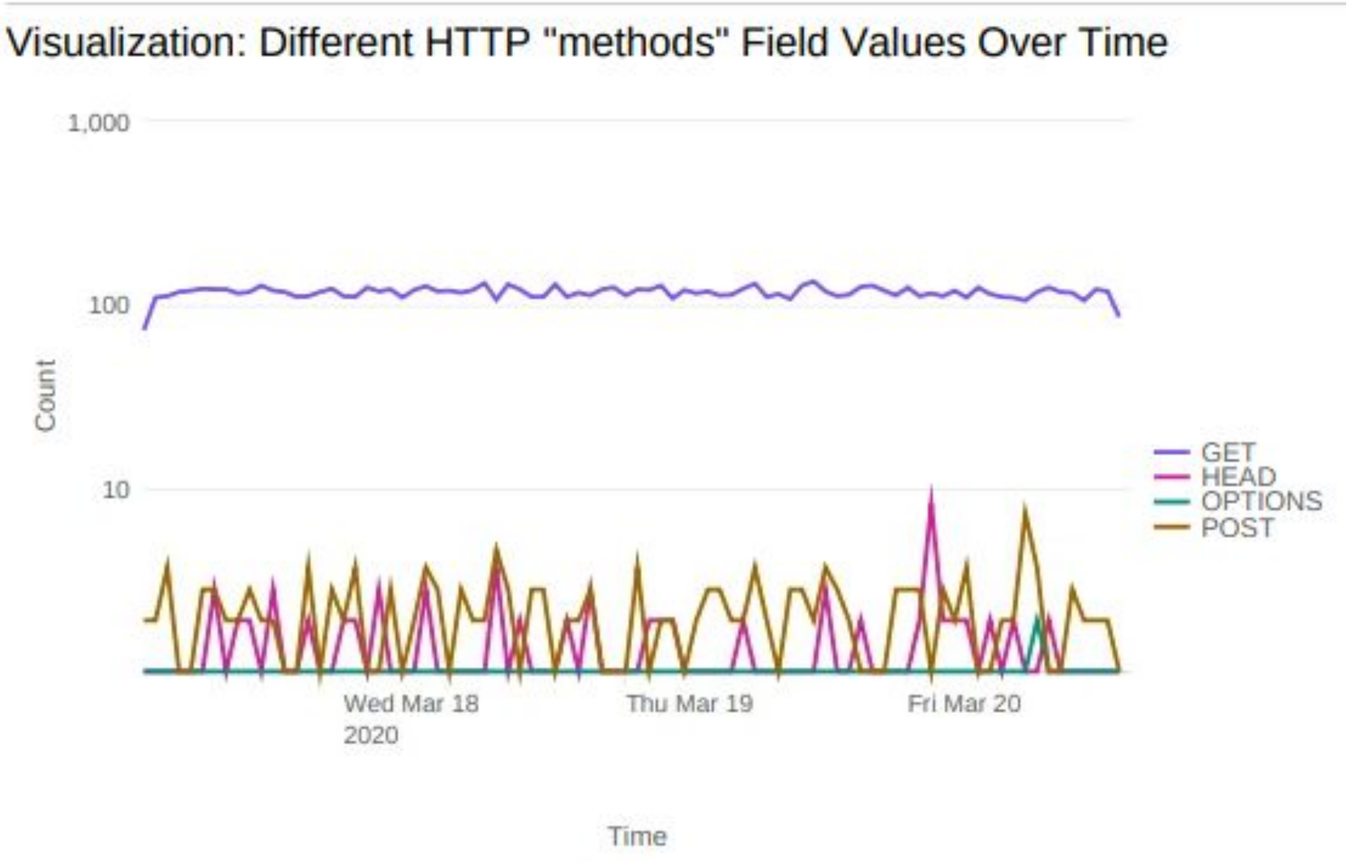
JUSTIFICATION: We observed the baseline of 60hits/hr as the avg number of hits of hourly activity. While 120hits/hr allows for legitimate activity seen from outside the US.

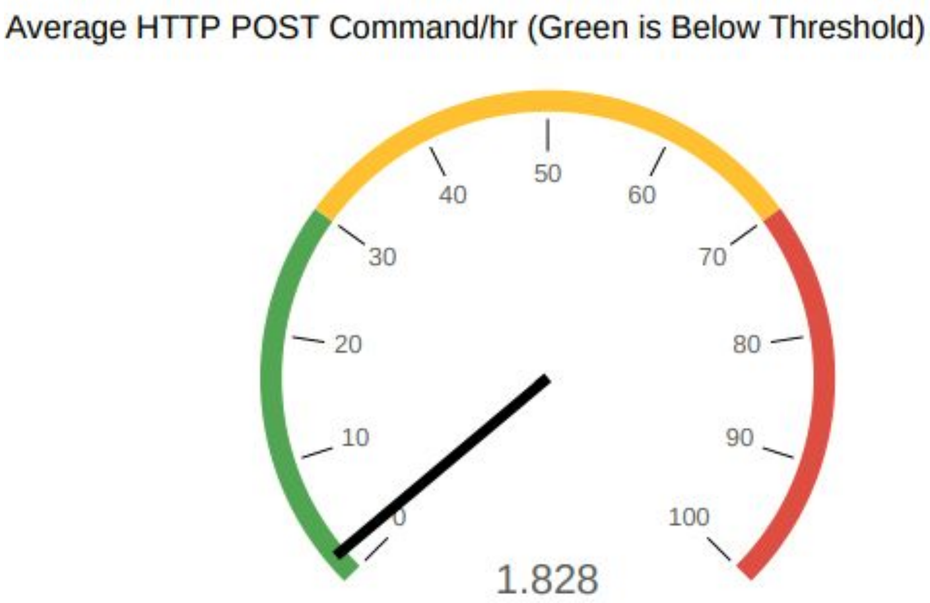
Alerts — Apache - POST

Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST Requests Exceeded Threshold	The hourly HTML POST requests has exceeded the normal rate	2/hr	5/hr

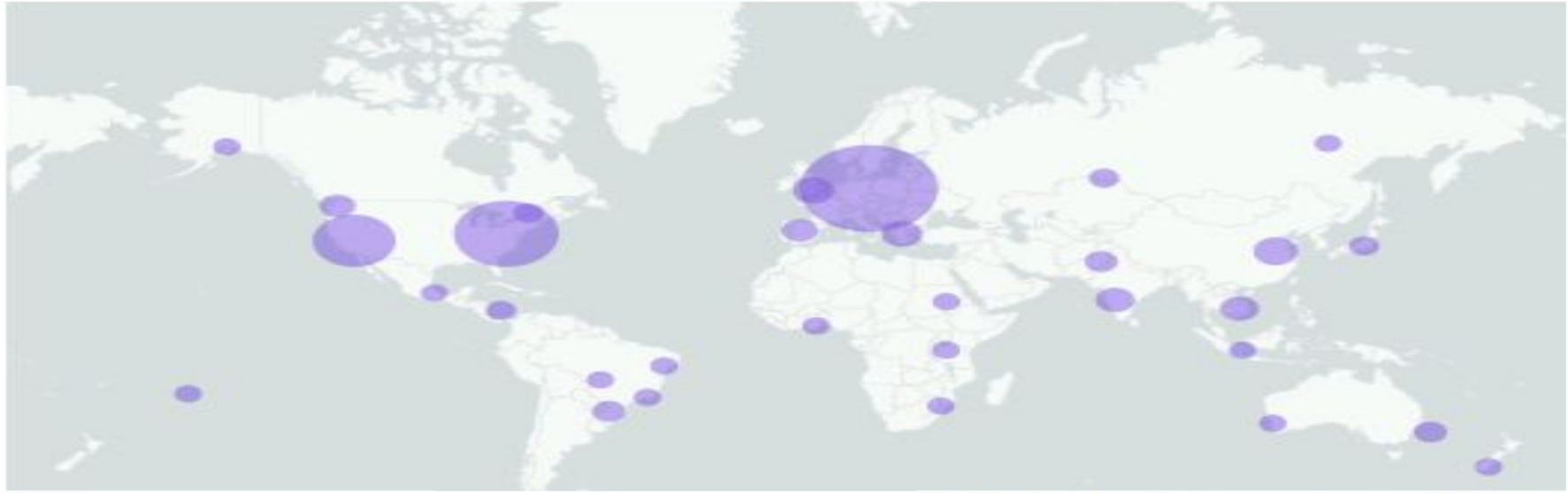
JUSTIFICATION: Over the 84 hours of logs, only once did the POST requests exceed 5 within an hour.

Baseline Dashboards — Apache

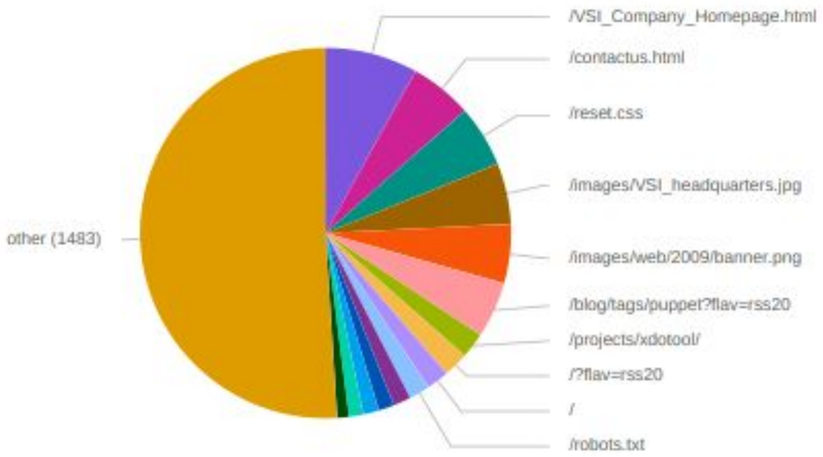




Baseline Dashboards - Apache - IP Location Pings

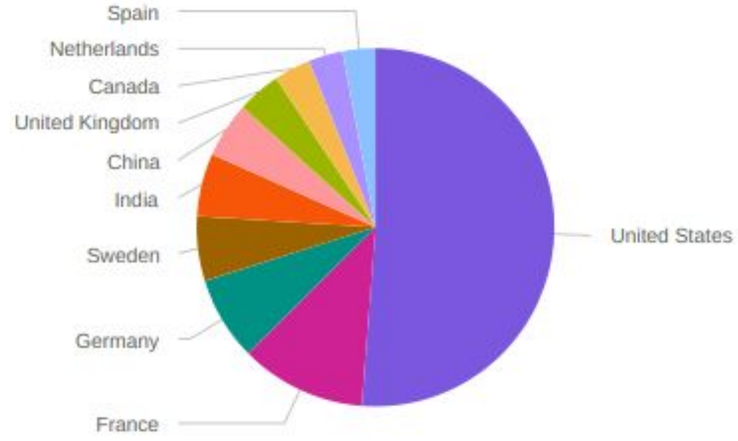


The Number of Different URIs

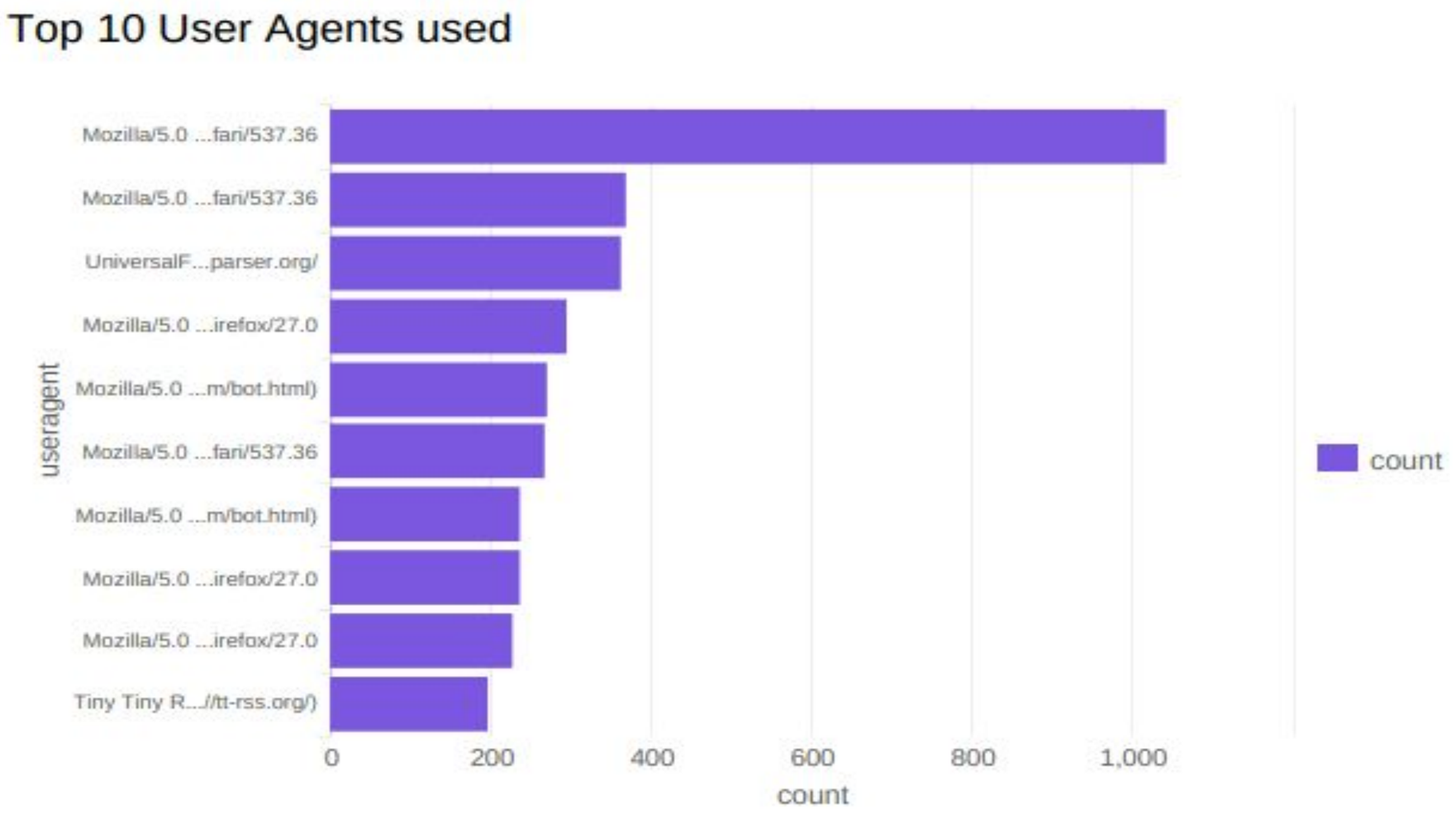


“Other” comprises 50.99%. 1,485 unique URIs

VIsualization of The Top 10 Countries Who Appeared in The Baseline Log



Dashboards - Apache - URIs



1	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2	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
3	UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
4	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
5	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)
6	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
7	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
8	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
9	Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
10	Tiny Tiny RSS/1.11 (http://tt-rss.org/)

Attack Analysis

Attack Summary — Windows

When Analyzing the 14-hour span of Attack Logs, We Found:

- 192% Increase in high severity reports compared to a 24 hour baseline
- Brute Force Attacks started ~10:00PM UTC
- Infiltration occurred ~5:00AM UTC
- Successful Logins Occurred ~6:00AM UTC
- 2 users were identified
  - user_a
  - user_k

Top 10 Values	Count	%
An attempt was made to reset an accounts password	64	68.817%
A user account was created	5	5.376%
A user account was deleted	3	3.226%
An account was successfully logged on	3	3.226%
Special privileges assigned to new logon	3	3.226%
A computer account was deleted	2	2.15%
A user account was changed	2	2.15%
Domain Policy was changed	2	2.15%
System security access was removed from an account	2	2.15%
The audit log was cleared	2	2.15%

Windows Attack Logs - Severity Level

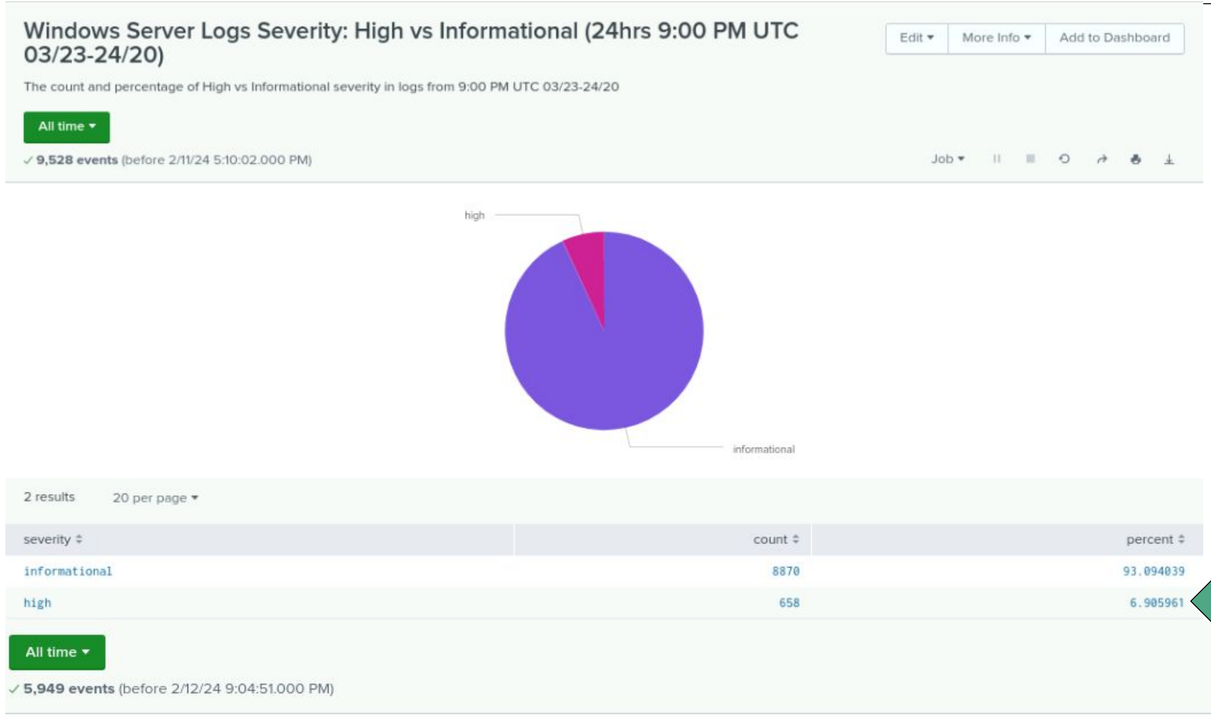


Figure 1: Baseline of High Severity Logs

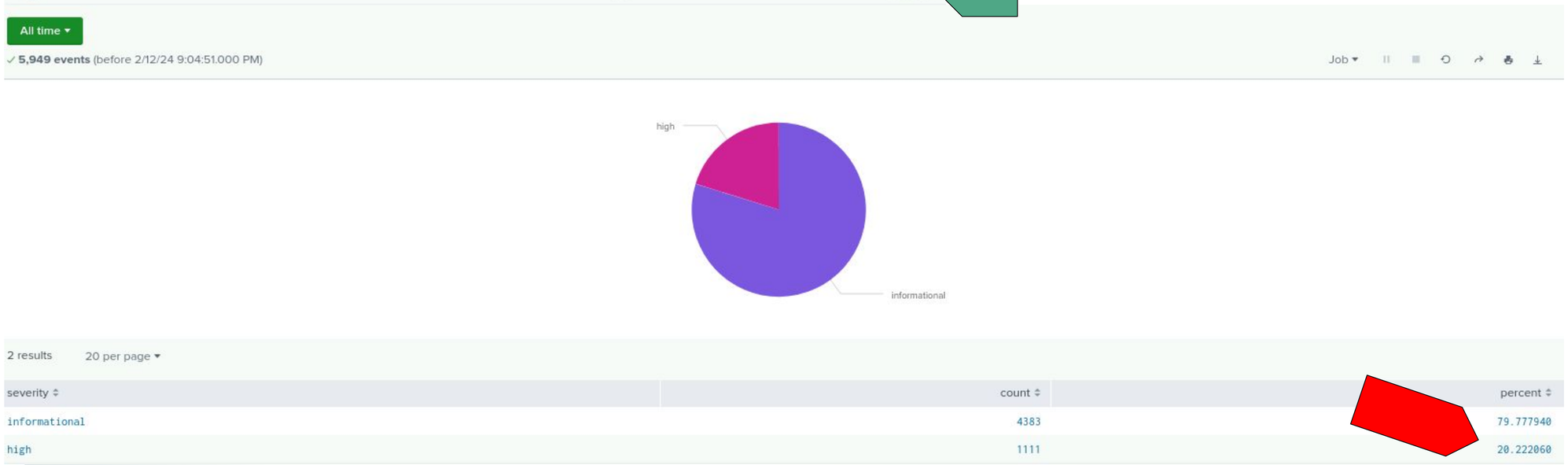


Figure 2: High Severity Logs During Attack

Windows Attack Logs - Success + Failed Activities

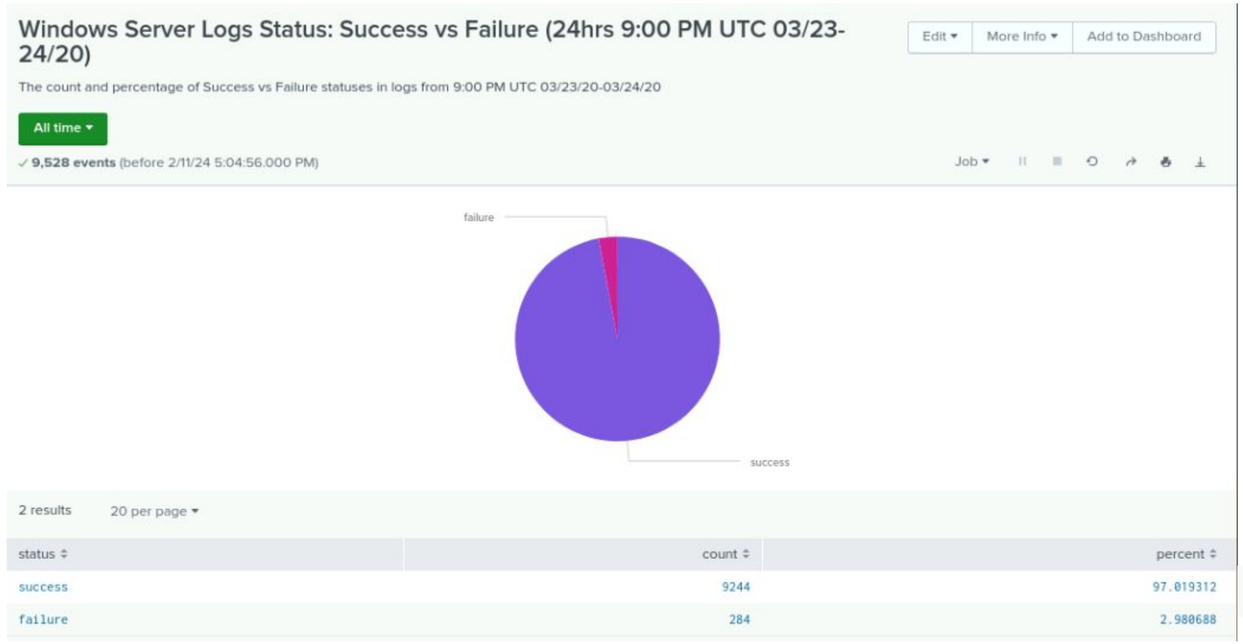


Figure 3:
Baseline is 397 events/hr

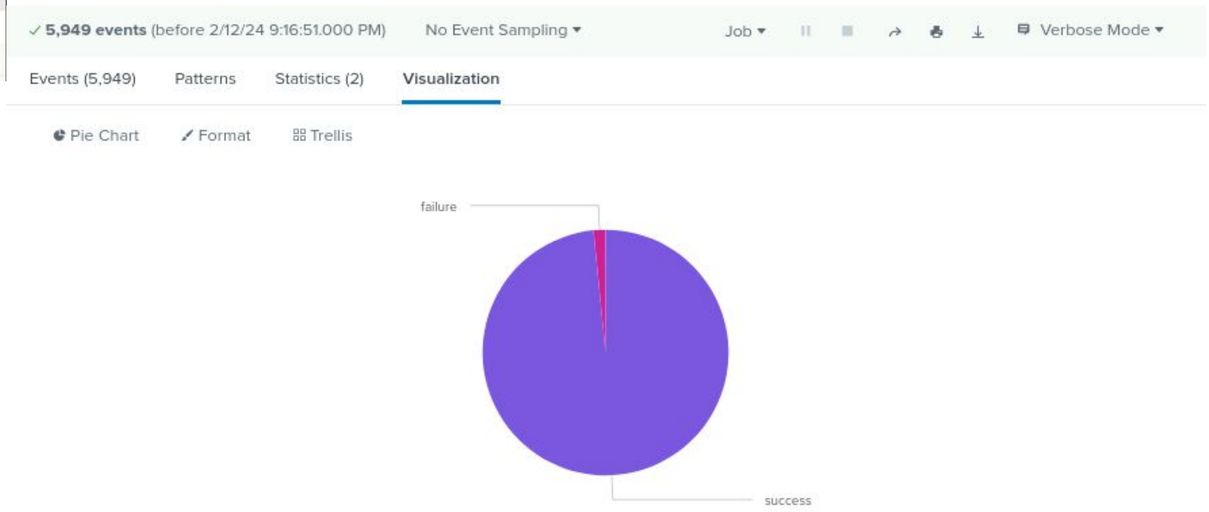


Figure 4: Attack is 424 events/hr

Windows Attack Logs - Alert for Failed Activities

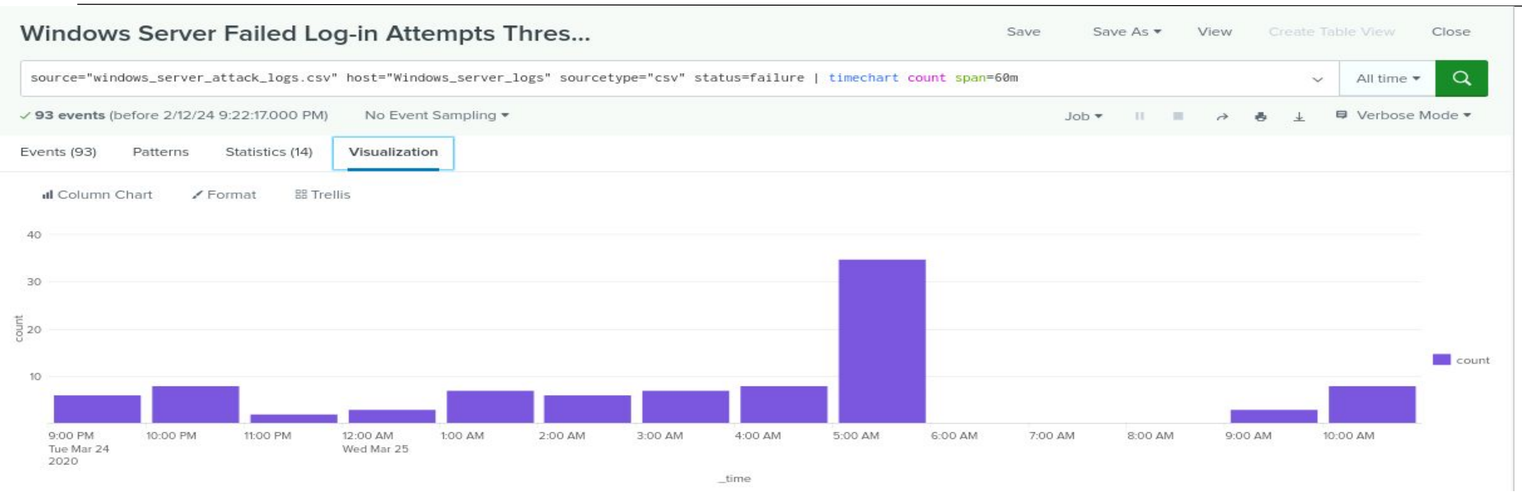


Figure 5: suspicious amount of failed login attempts at 5:00AM UTC

#	signature	count
1	An attempt was made to reset an accounts password	6
2	A user account was created	5
3	Special privileges assigned to new logon	3
4	An account was successfully logged on	3
5	A user account was deleted	3
6	The audit log was cleared	2
7	System security access was removed from an account	2
8	Domain Policy was changed	2
9	A user account was changed	2
10	A computer account was deleted	2
11	System security access was granted to an account	1
12	A user account was locked out	1
13	A process has exited	1
14	A privileged service was called	1
15	A logon was attempted using explicit credentials	1

Table 1: Failed Events logged during 5:00AM UTC

The only baseline Failed Events were “An attempt was made to reset an accounts password”

Windows Attack Logs - Alert - Successful Logins

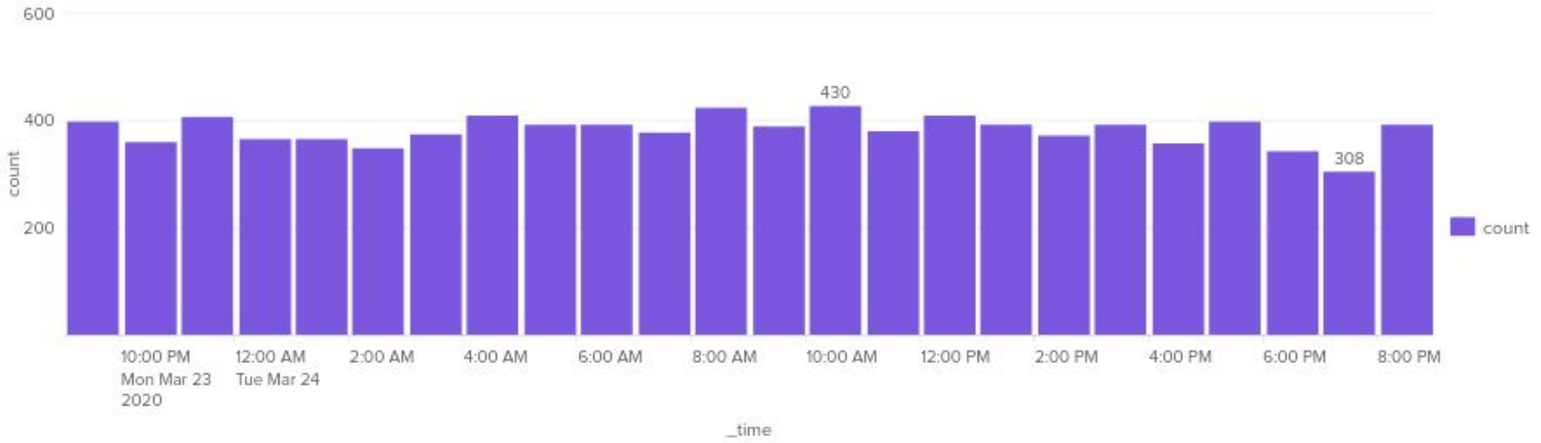


Figure 5: Baseline Successful Login Activity

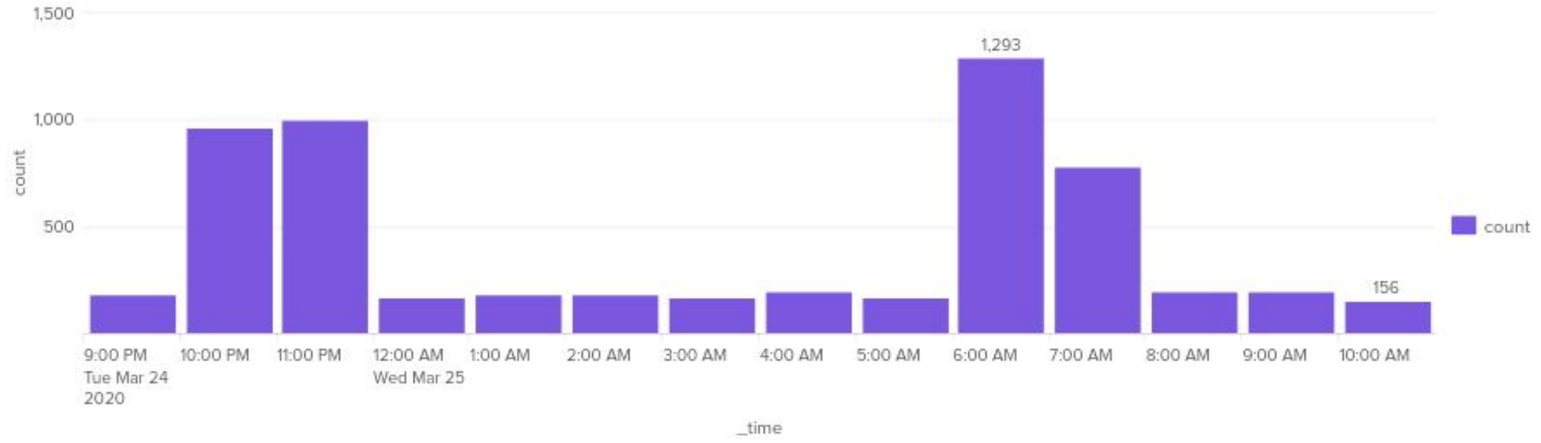


Figure 6: Attack. Alarming amount of successful logins at 6:00AM UTC into 7:00AM UTC

Windows Attack Logs - Alert - Deleted Accounts

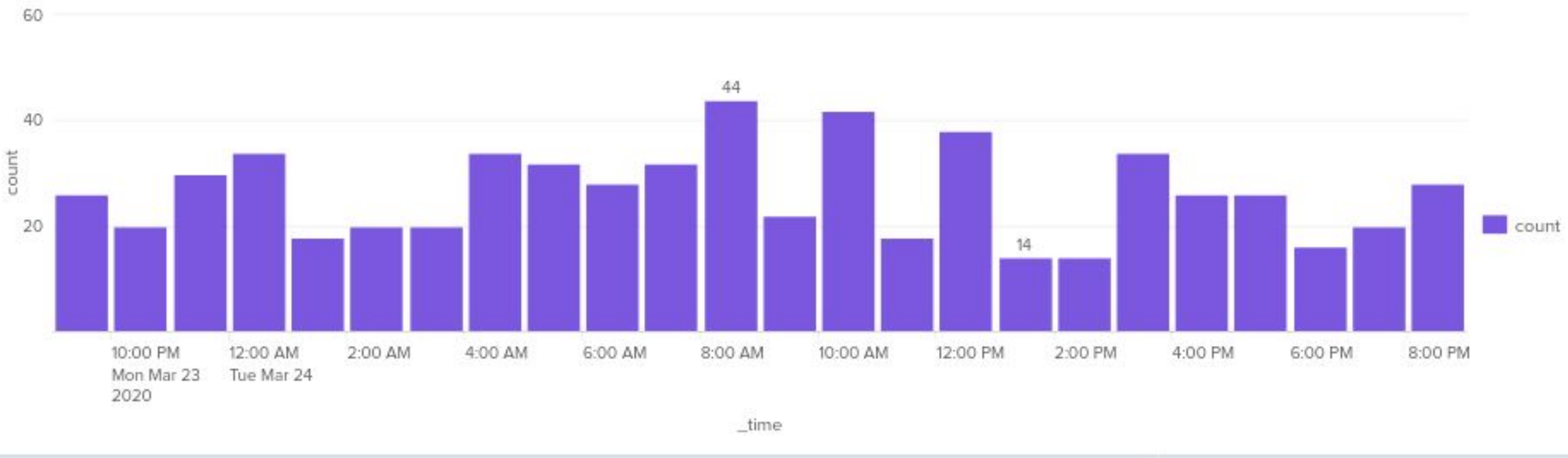


Figure 7: Baseline detected accounts activity

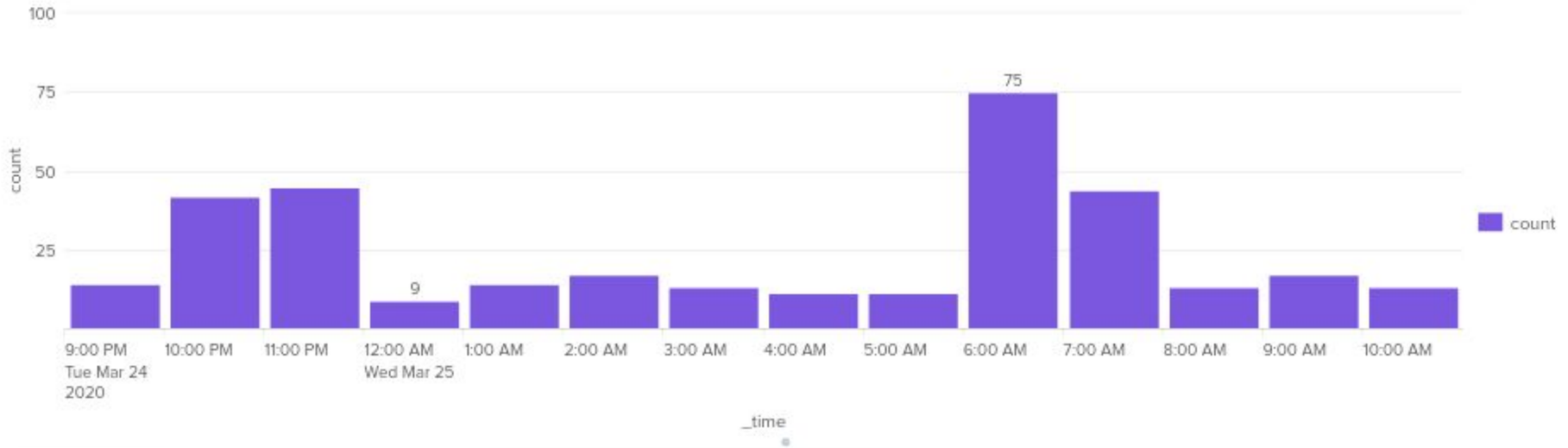


Figure 8: Deleted Account spiked during the attack

Windows Attack Logs - Severity Indicator

Figure 9: Baseline radial gauge for the amount of logs reported with a high severity

Figure 10: High severity logs per hour during the attack

Windows Attack Logs - Event Signature

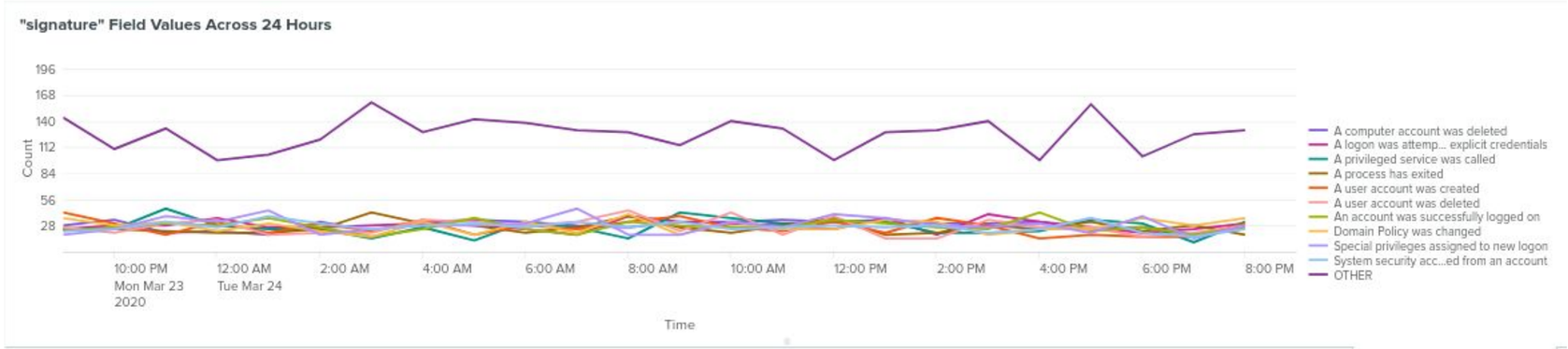


Figure 11: Baseline Signatures.

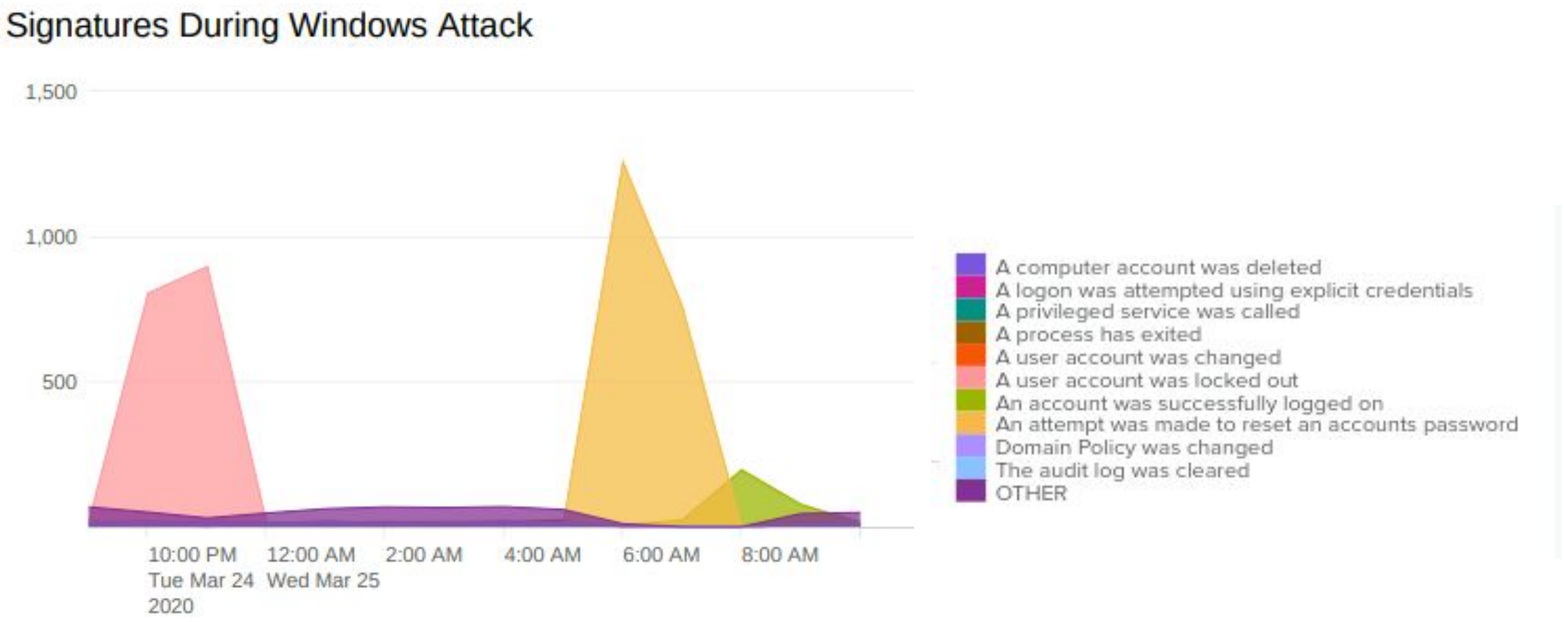


Figure 12: Attack. Spike in User Accounts locked out. Then later, spike in password resents at the same time the abnormal logins were successful

Windows Attack Logs - Users

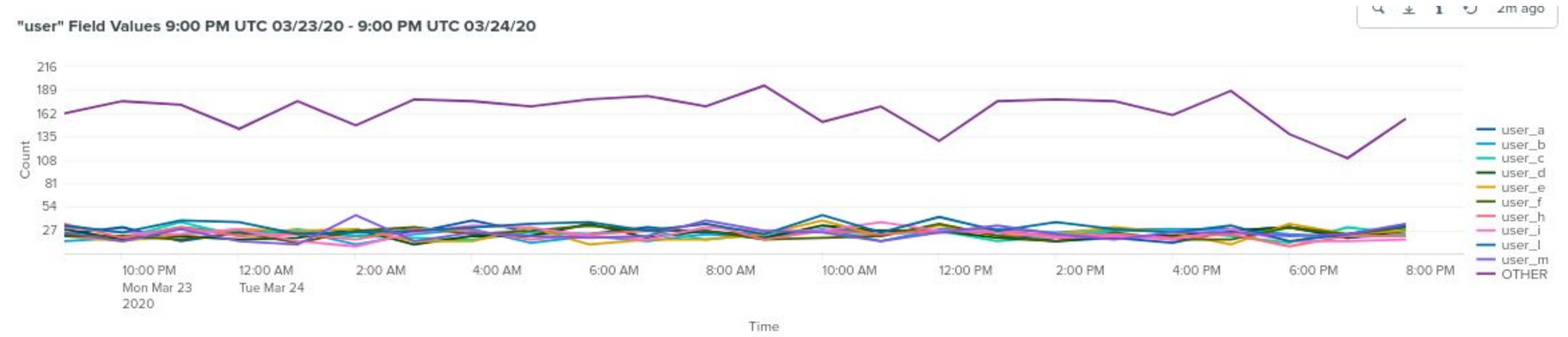


Figure 12: Baseline. Top line is “OTHER”

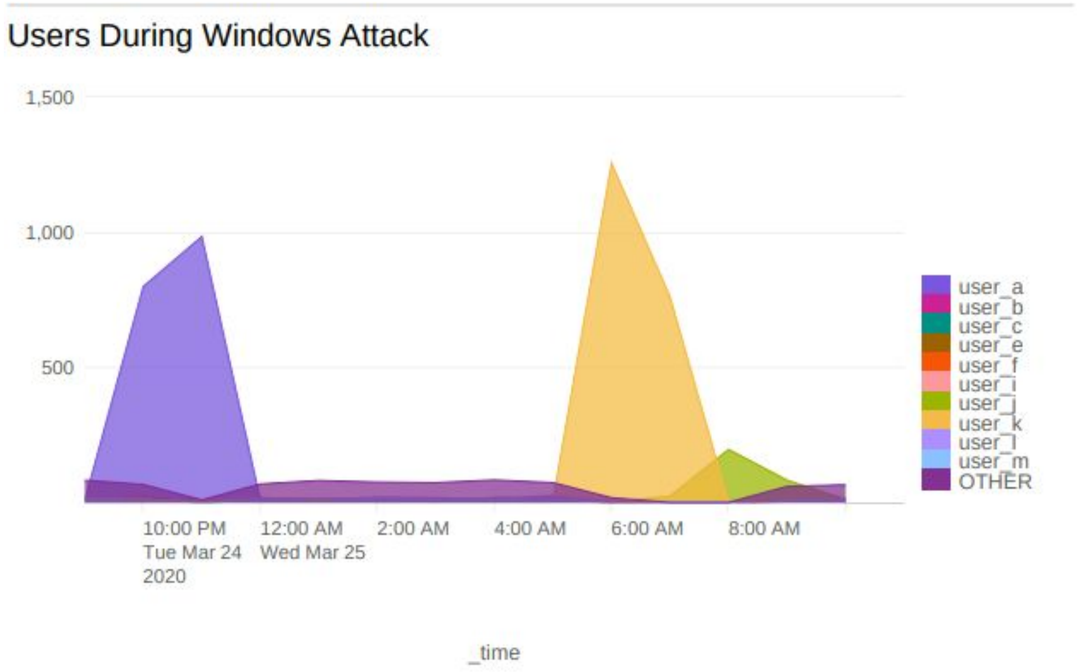


Figure 13: Attack. User spikes correlate with abnormal event signatures.

Windows Attack Logs - Different Users

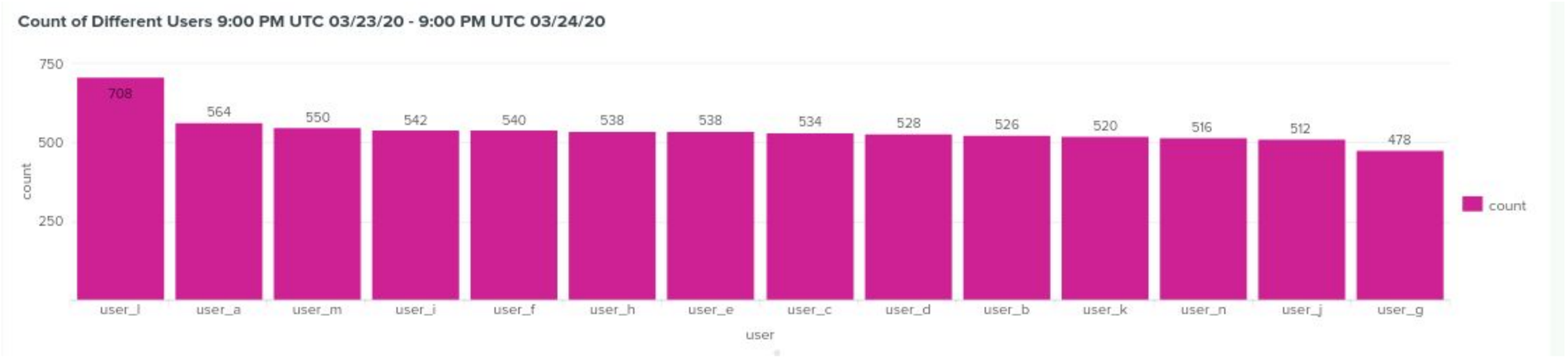


Figure 15: Baseline Bar Chart Count of user log-ins.

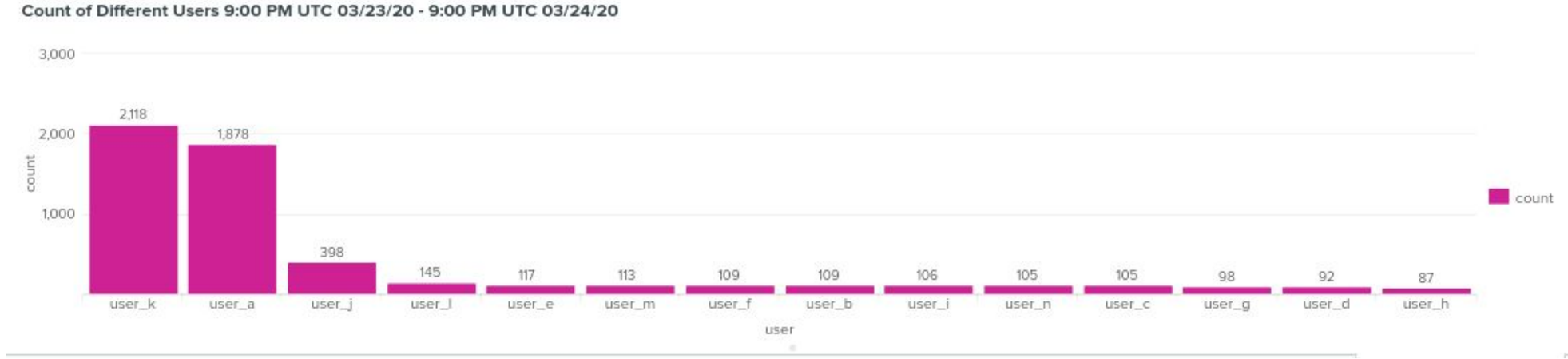


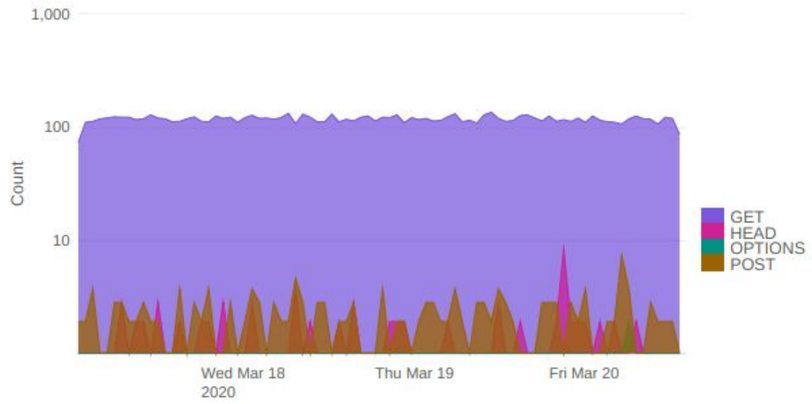
Figure 16: user_k and user_a stand out during the attack.

Attack Summary — Apache

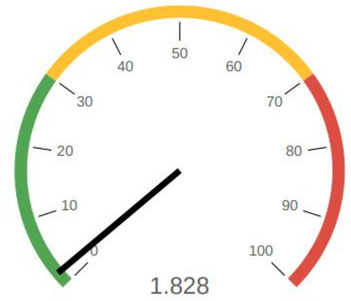
- POST alerts threshold did work
- Spike in activity from Ukraine
- In the recent data analysis, there was a notable rise in POST HTTP methods usage which can be because of a denial of service attack.
- no suspicious activity was found in referrer domains.
- However, it's acknowledged that there may be gaps in the reporting system, warranting further investigation.
- the report highlighted a significant surge in the occurrence of "404" HTTP response codes, escalating from 2% to approximately 15%.

Apache Attack Logs — HTTP Methods

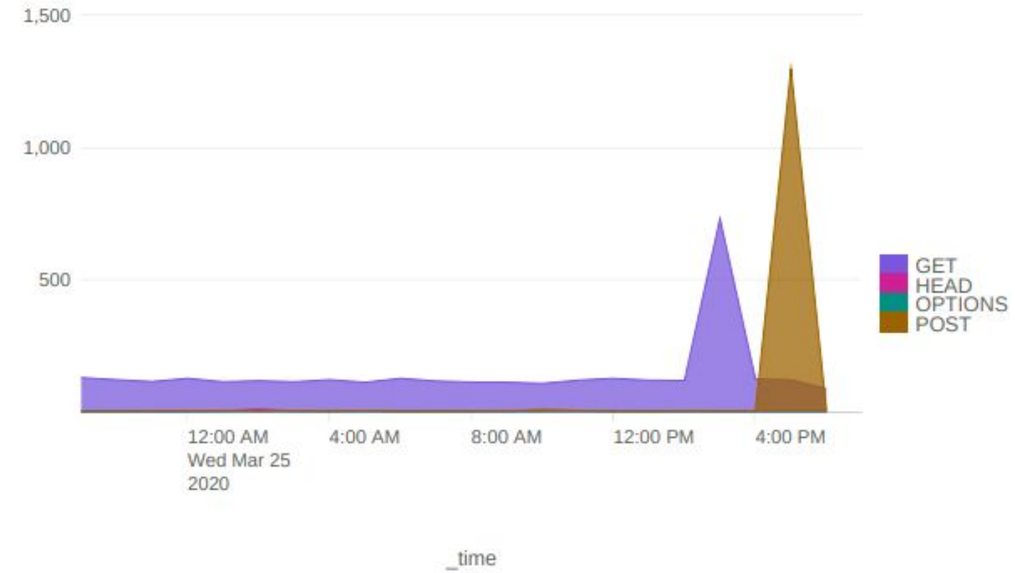
Visualization: Different HTTP "methods" Field Values Over Time



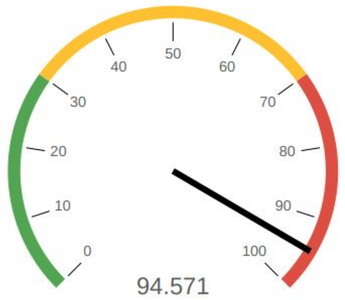
Average HTTP POST Command/hr (Green is Below Threshold)



HTTP Methods During Attack over time



Radial Gauge of HTTP POST commands/hour



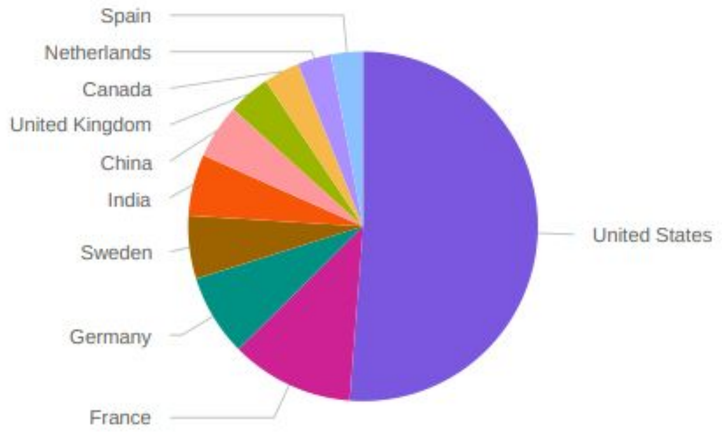
Apache Attack Logs — Client IP Locations

Geolocation of Client IPs

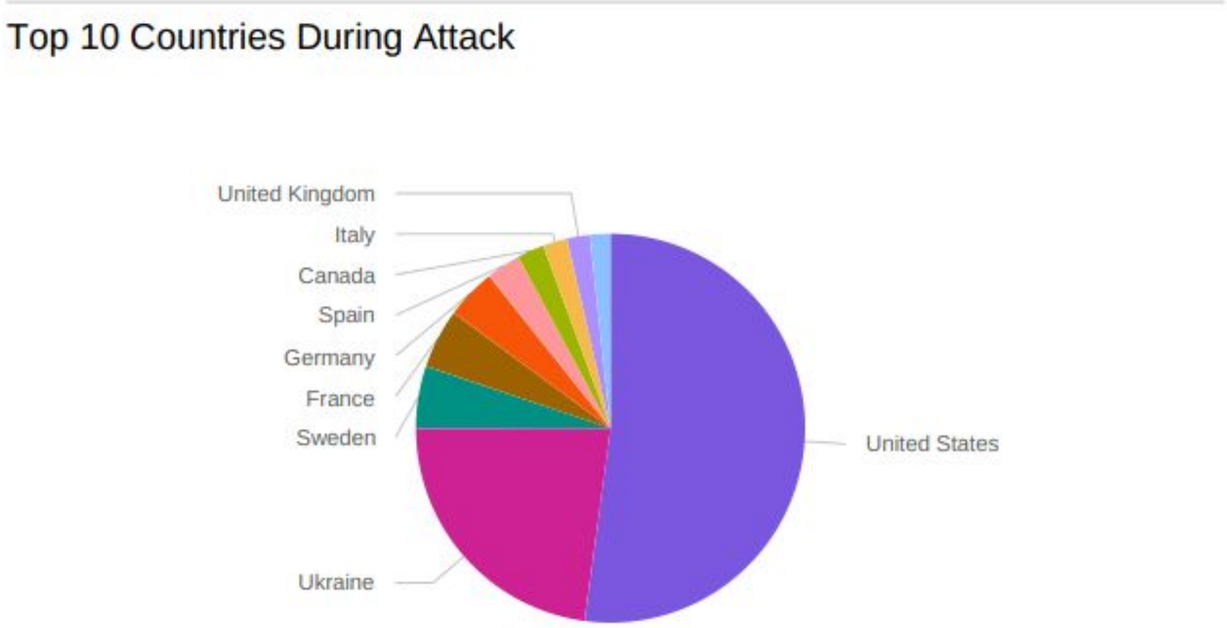
Cluster Map of Attacks

Apache Attack Logs — Top 10 Countries

VIsualization of The Top 10 Countries Who Appeared in The Baseline Log

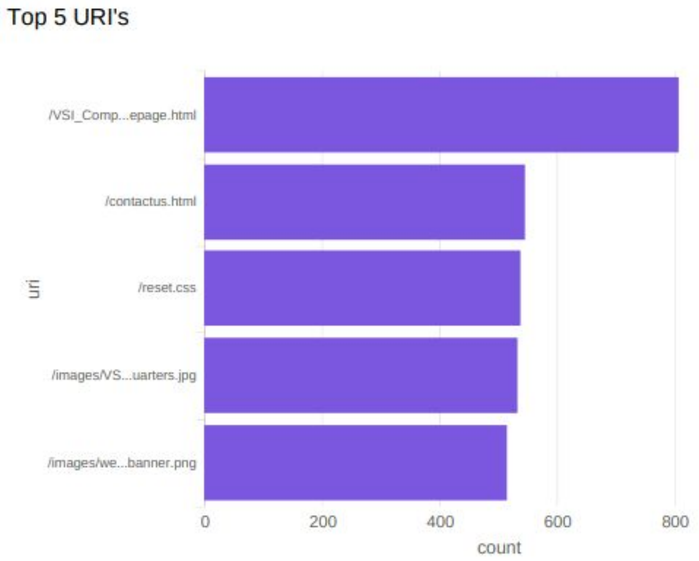


Baseline



Attack

Apache Attack Logs — Top 10 Countries



Baseline:
/VSI_Company_Home
page.html

count

/VSI_Account_logon.php

Summary and Future Mitigations

Findings Summary

Findings from the Attack:

- Our competition collaborated to crash our systems utilizing a DDOS attack as well as overloading us with HTTP POST requests.
  - To protect VSI from future attacks is to address the flood of HTTP POST requests and prevent any from coming in once a new threshold has been reached based on this attack.
  - Another measure is remediation through workshops to teach users how to deal with failed login attempts or issues with account management.
  - Implement a firewall policy to stop unwanted traffic from foreign locations

THANK YOU!