Defensive Security Project
by: Hack Overflow

Hackoverflow

Hackoverflow

Table of Contents

This document contains the following resources:

01 Monitoring Environment

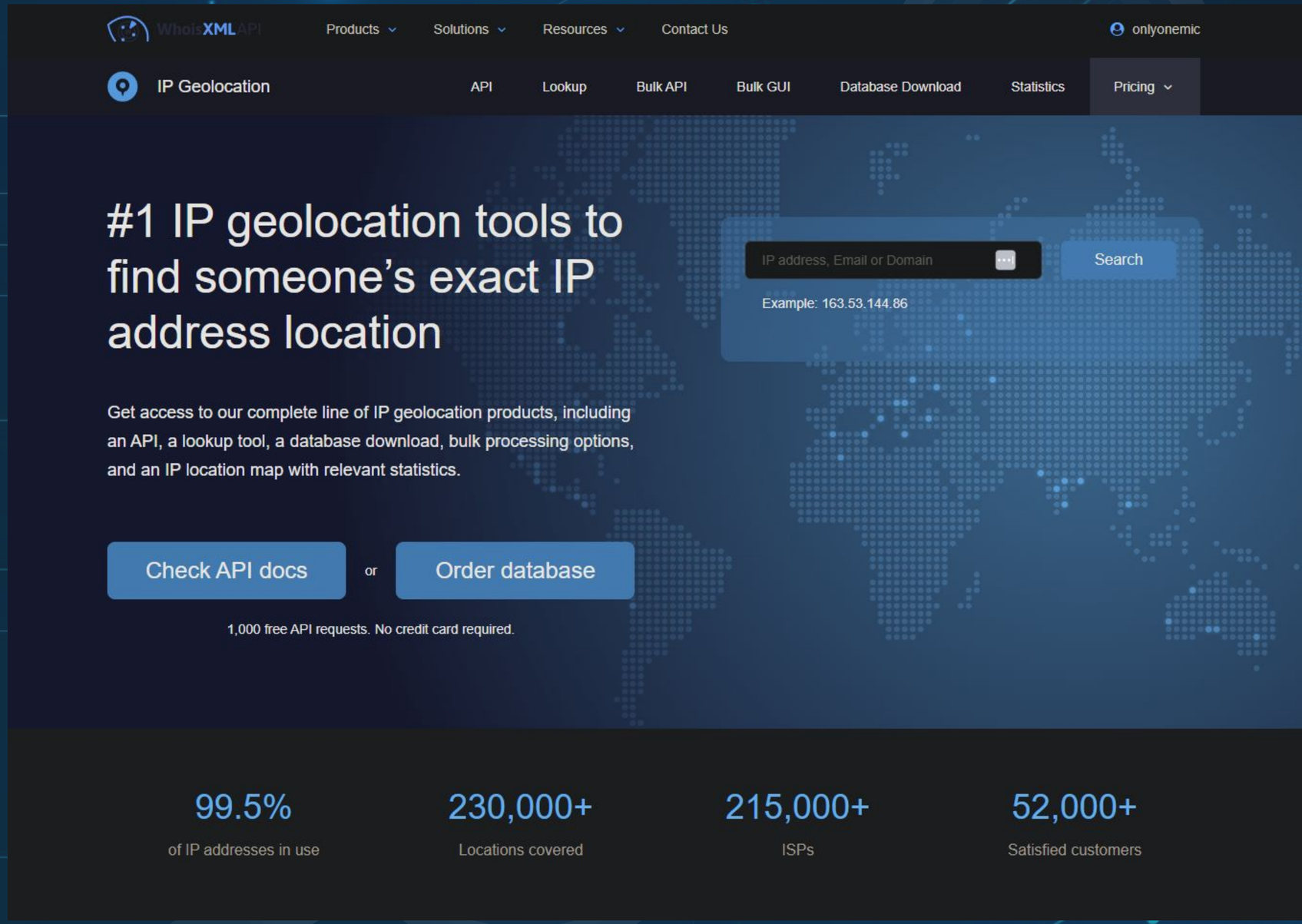
02 Attack Analysis

03 Project Summary & Future Mitigations

Monitoring Environment

Whois XML IP Geolocation API

identifies the physical locations and attributes associated with source IP addresses



Whois XML IP Geolocation API

As part of our Splunk SIEM implementation, the team opted to incorporate the WHOIS XML IP Geolocation API.

This tool Identifies the physical locations and attributes associated with source IP addresses logged by the monitoring environment.

=

We can Identify the physical origin of malicious IP connections to the organisation.

Hack Overflow were able to use this data to create filters which should minimise malicious activity from these IP locations in the future.

Whois XML IP Geolocation API

Not only can this tool be used in defending against malicious actors.
It can provide valuable data into user behaviour for marketing purposes.

Hackoverflow

Logs Analyzed

1 Windows Logs

Contains event information of VSI's back end systems such as access data, user logs and system events.

2 Apache Logs

Contains event data of the server which hosts the VSI web application such as client IPs, HTTP data and error logs

Windows Logs

Hackoverflow

Reports—Windows

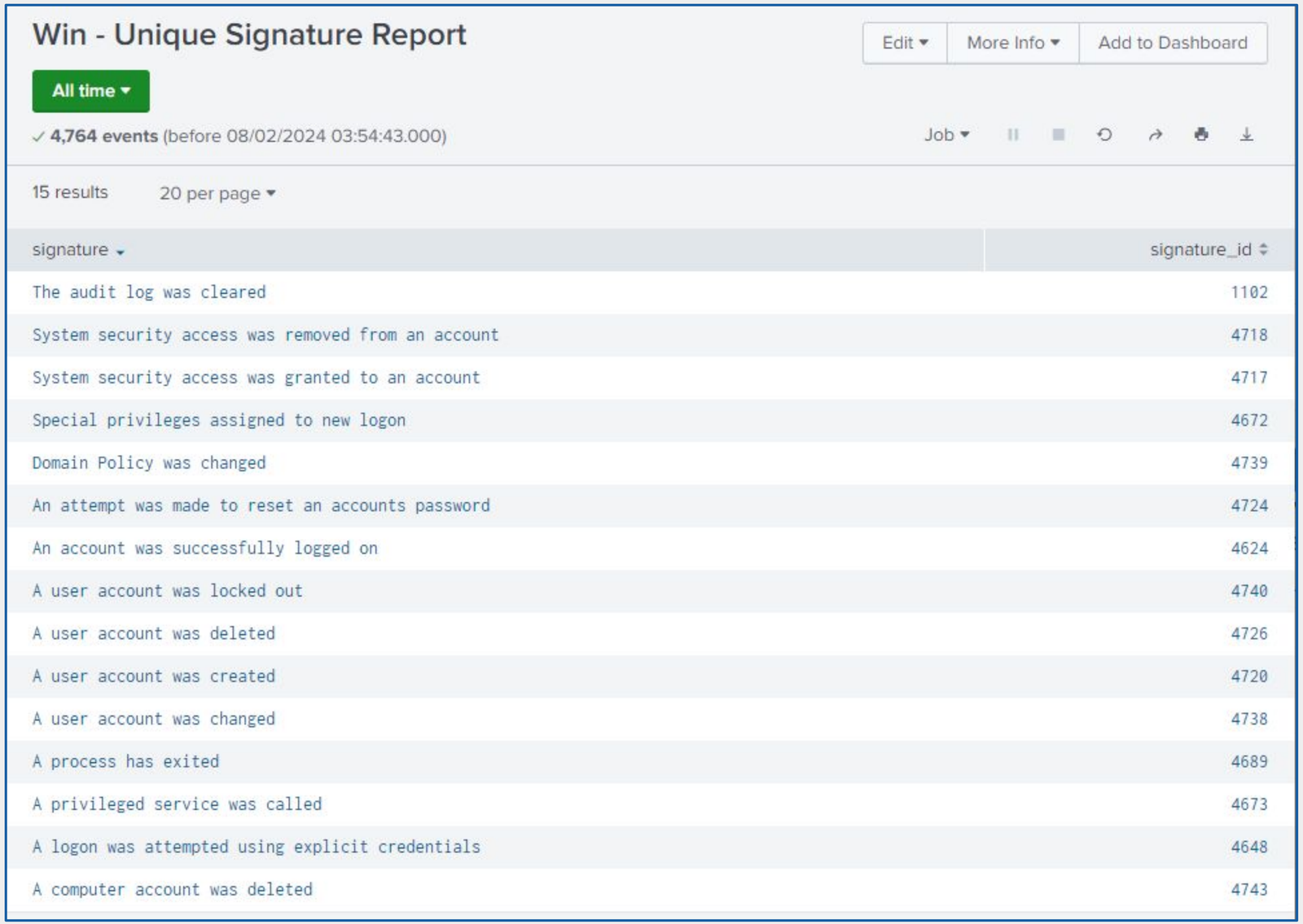
Report Name	Report Description
Win - Unique Signatures & IDs Report	Shows VSI the ID number associated with the specific signature for Windows activity.
Win - Activity Severity Level Report	Allows VSI to quickly understand the severity levels of the Windows logs being viewed.
Win - Success/Failure Activity Status Report	Shows VSI if there is a suspicious level of failed activities on their server.

Hackoverflow

Reports—Windows

Win - Unique Signatures & IDs Report

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



Win - Unique Signature Report

Edit | More Info | Add to Dashboard

All time

✓ 4,764 events (before 08/02/2024 03:54:43.000)

Job

15 results 20 per page

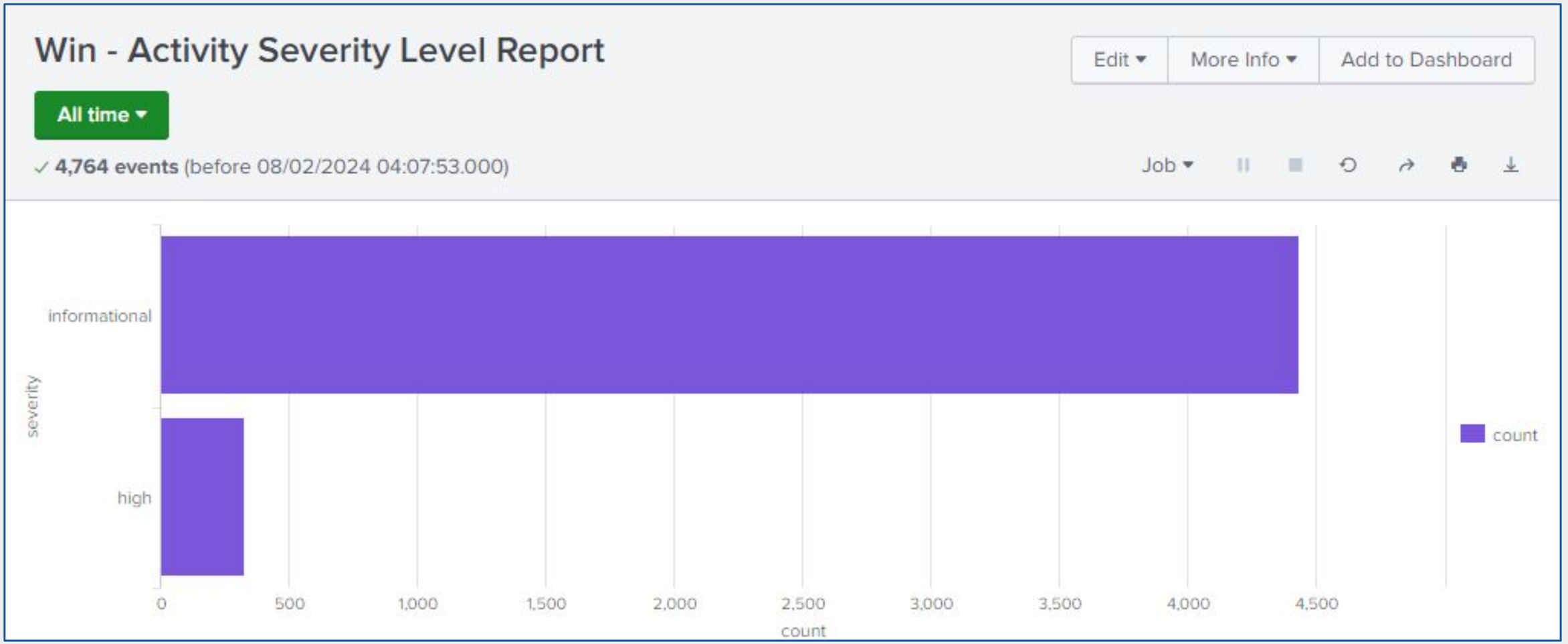
signature	signature_id
The audit log was cleared	1102
System security access was removed from an account	4718
System security access was granted to an account	4717
Special privileges assigned to new logon	4672
Domain Policy was changed	4739
An attempt was made to reset an accounts password	4724
An account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

Hackoverflow

Reports—Windows

Win - Activity Severity Level Report

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

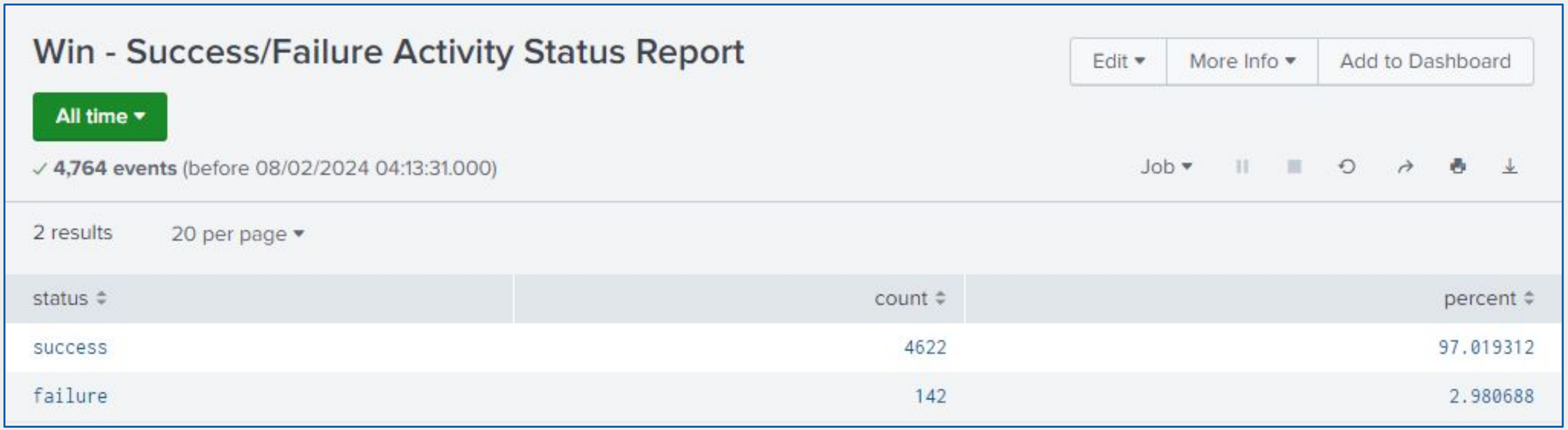


Hackoverflow

Reports—Windows

Win - Success/Failure Activity Status Report

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



Hackoverflow

Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Win - Failed Attempt Status	Windows activity returned the status failed	8	16
Justification	With the data set provided it was observed that the regular average was just under 8 events. 16 is 200% of the observed baseline.		

Hackoverflow

Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Win - Successful Log on Alert	The hourly number of successful logs on has exceeded the threshold	12	35
Justification	With the data set provided it was observed that the regular average was around 12 events. 35 is just over 200% of the observed baseline		

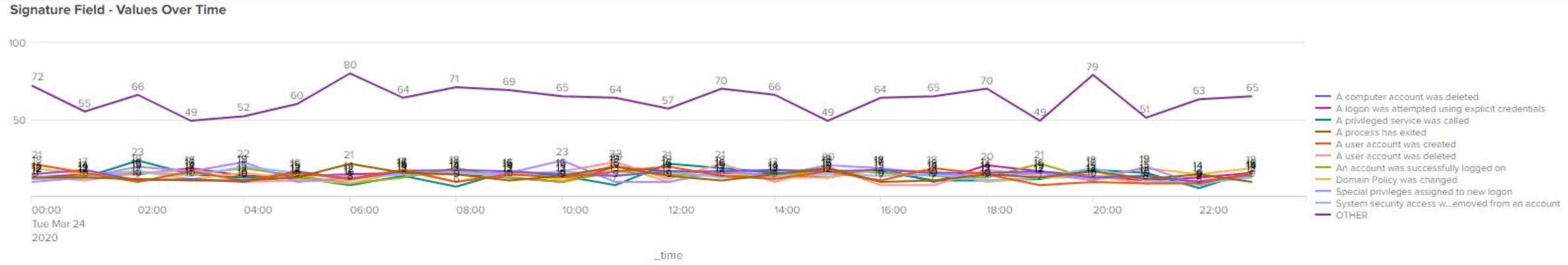
Hackoverflow

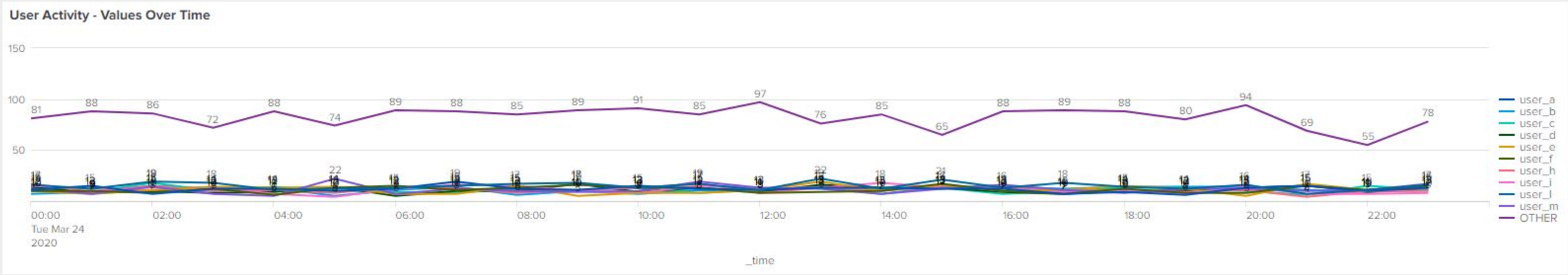
Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Win - User Accounts Deleted	The hourly threshold of user accounts being deleted has been met	16	40
Justification	With the data set provided it was observed that the regular average was around 16 events. 40 is around 200% of the observed baseline. With the amount of increase and decrease it was justifiable to increase the threshold above 200% of the baseline.		

Hackoverflow

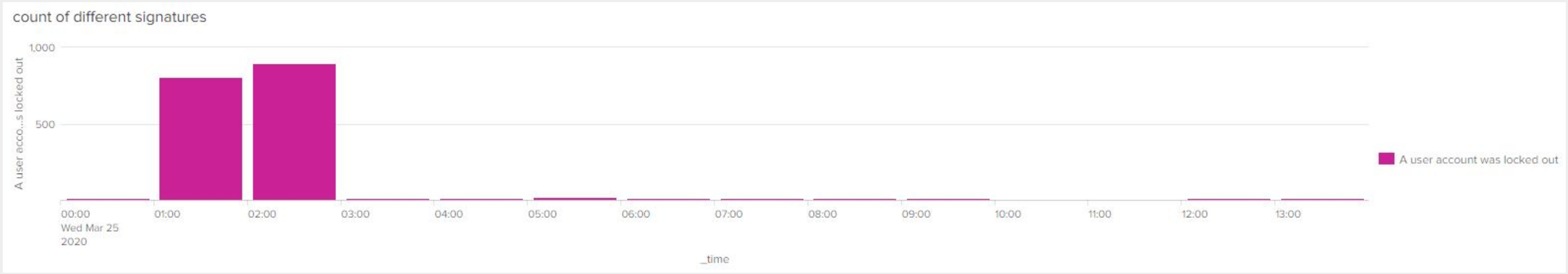
Dashboards—Windows

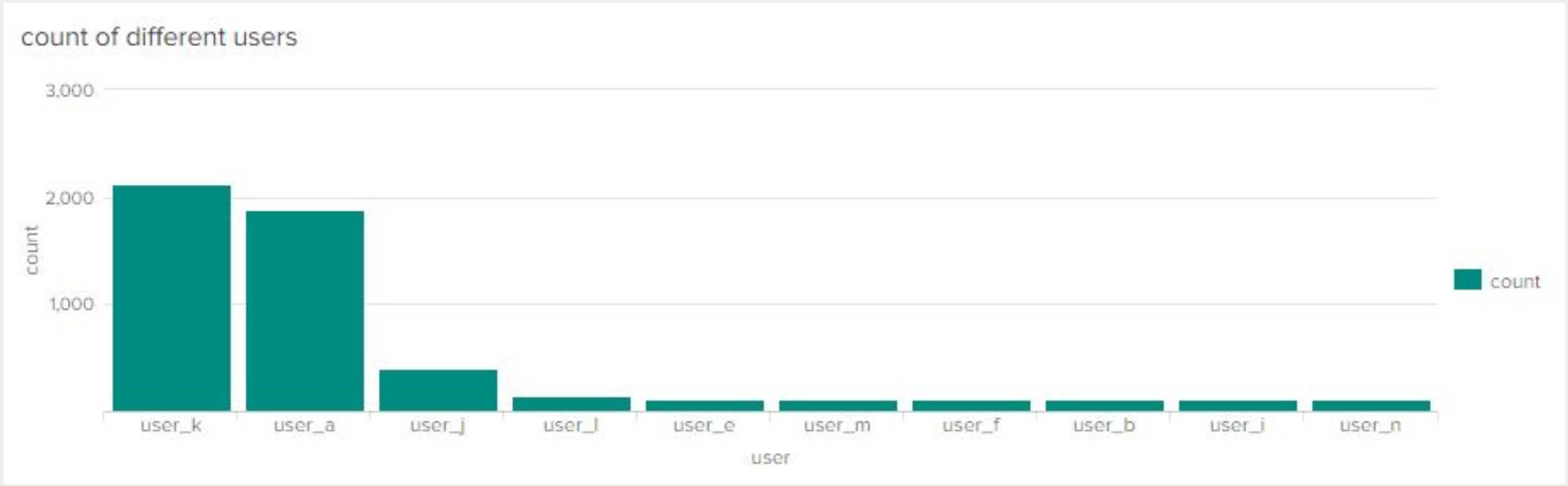




Hackoverflow

Dashboards—Windows





Hackoverflow

Dashboards—Windows

count of different users

user	count	percent
user_l	354	7.430730
user_a	282	5.919395
user_m	275	5.772460
user_i	271	5.688497
user_f	270	5.667506
user_h	269	5.646516
user_e	269	5.646516
user_c	267	5.604534
user_d	264	5.541562
user_b	263	5.520571

all signature id's over time

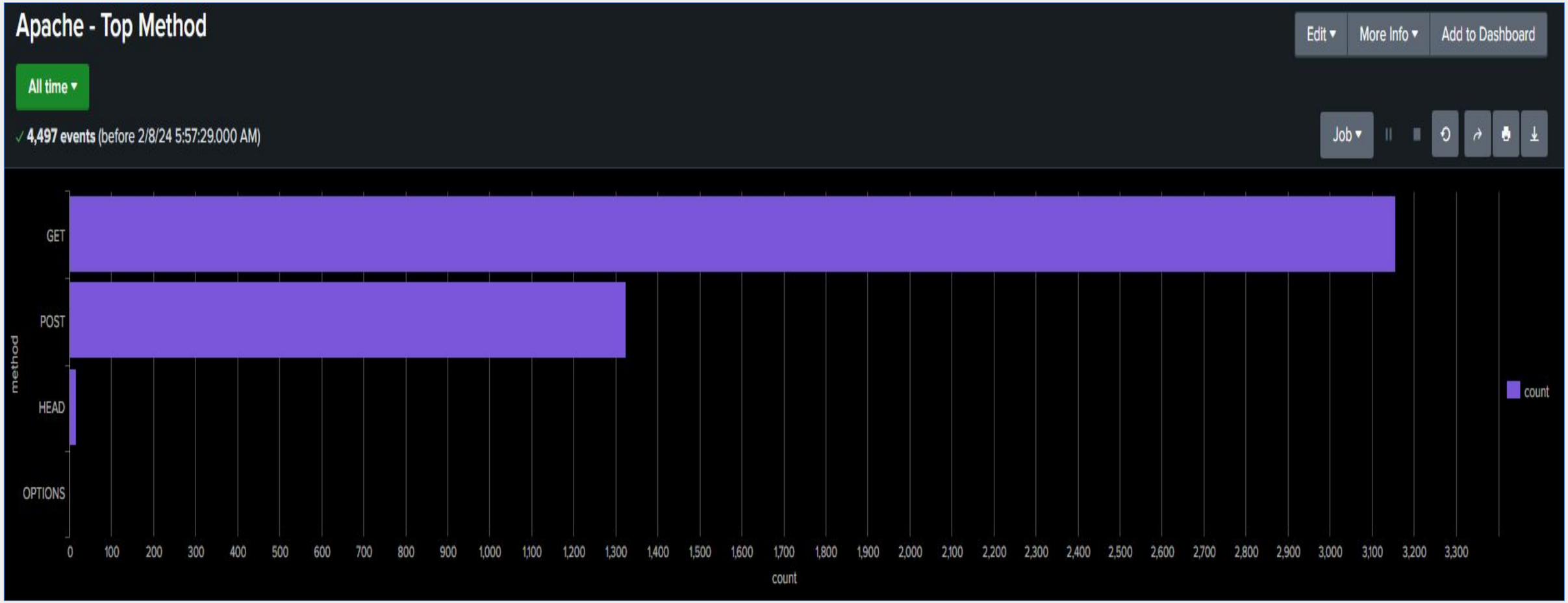
Apache Logs

Hackoverflow

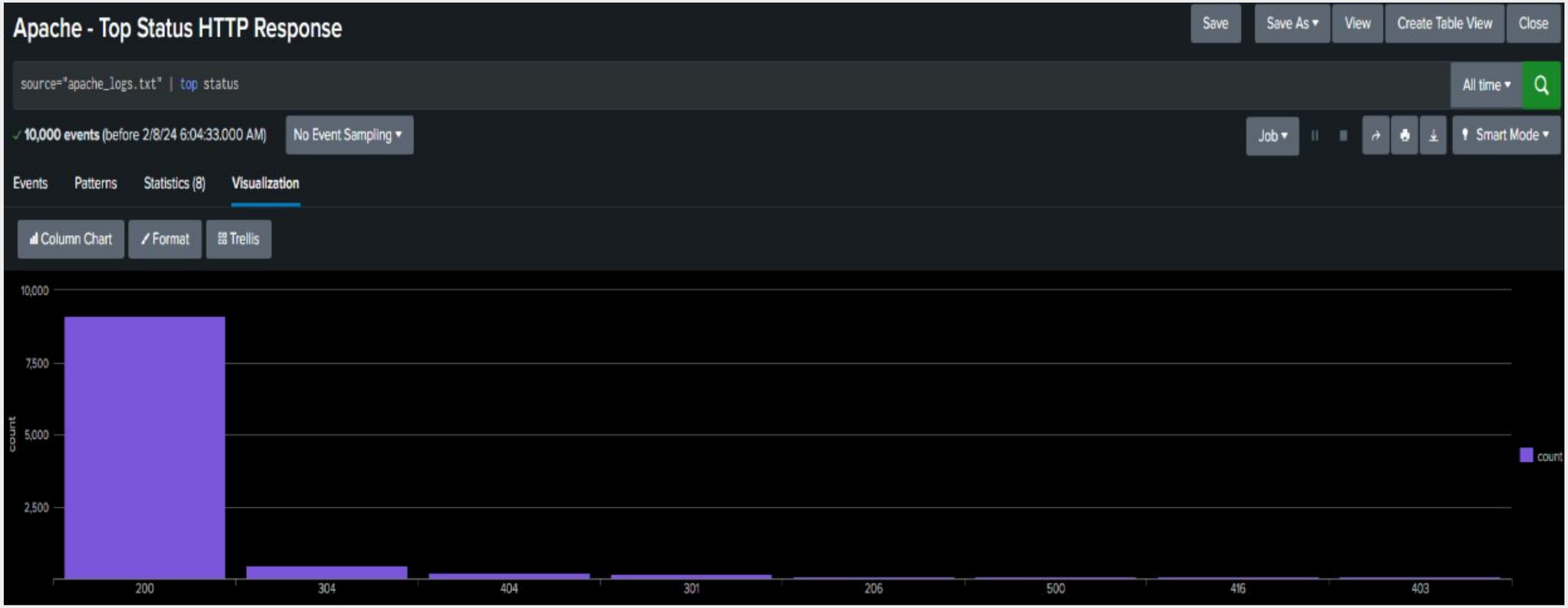
Apache - Report

Report Name	Report Description
Method Report	The most frequently used HTTP methods found in those logs. such as GET, POST, PUT ect.
Top Status HTTP Response	Most frequently encountered HTTP status codes found in those logs.
Top referrer domain	The top 10 referrer domains from those logs
Top 10 countries report	Report that shows the countries that visited VSI’s website.

Apache - Top Method Report



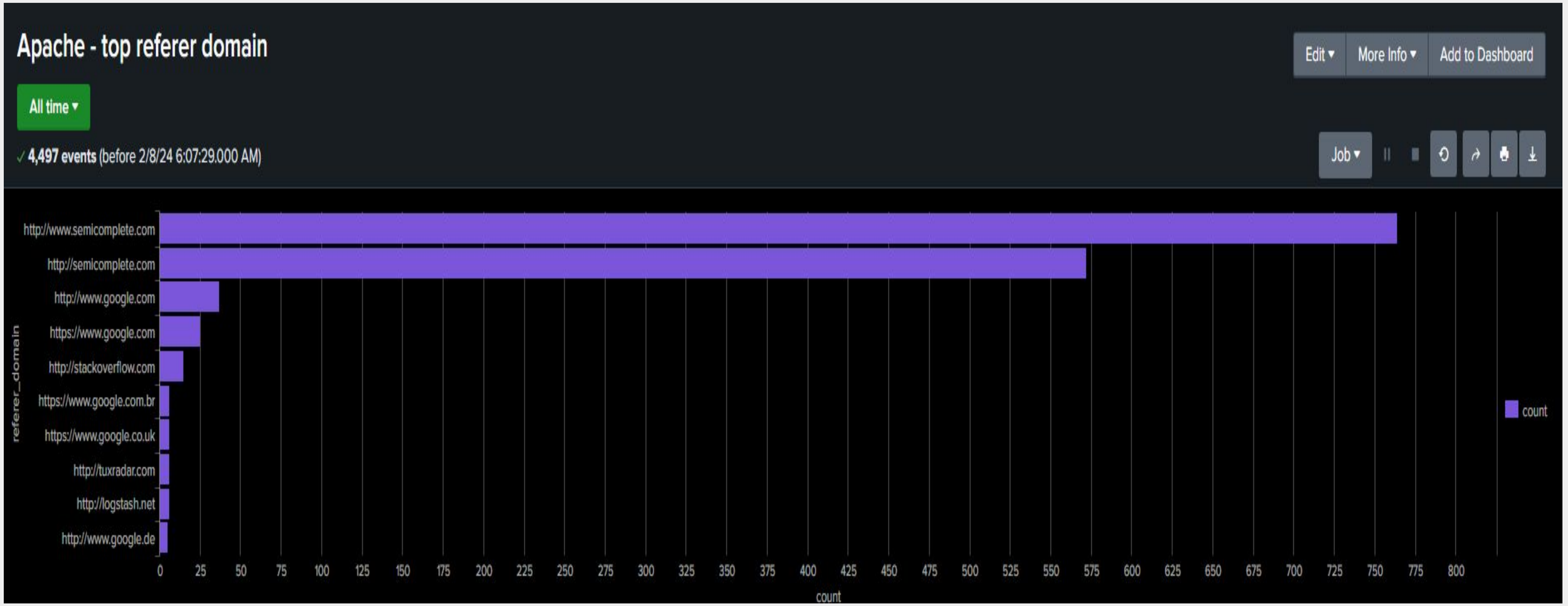
Apache - HTTP Response



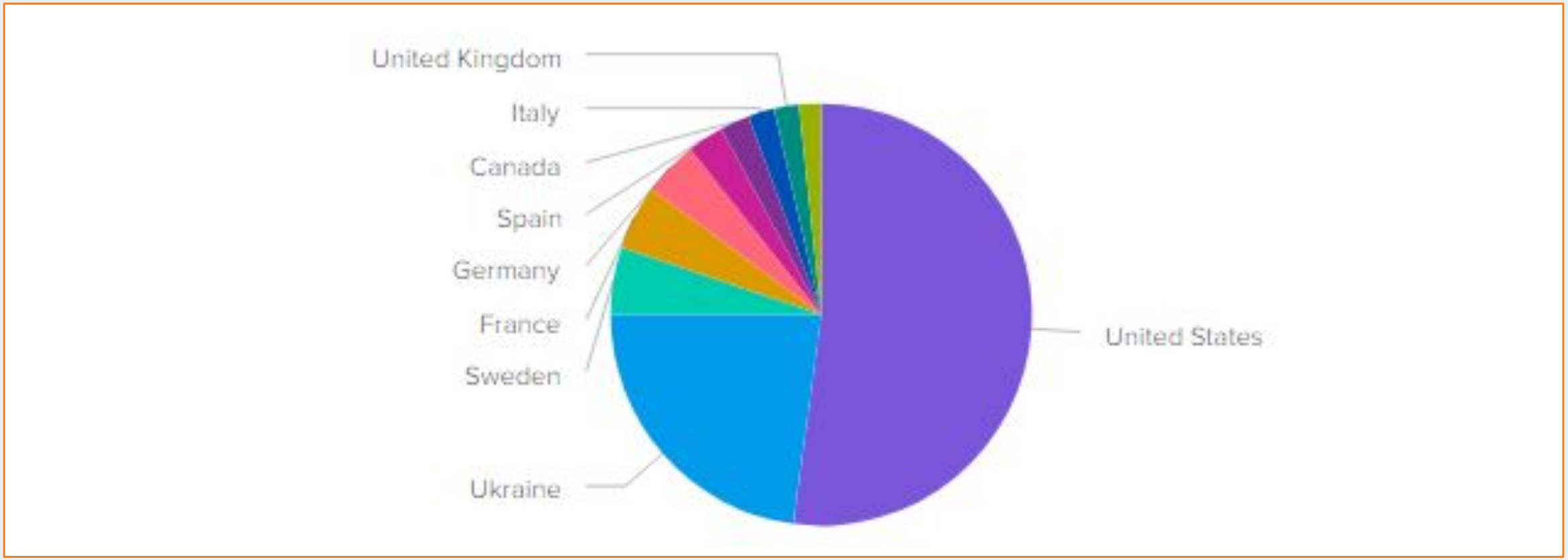
Hackoverflow

Apache - Report

Apache - Top referrer domain

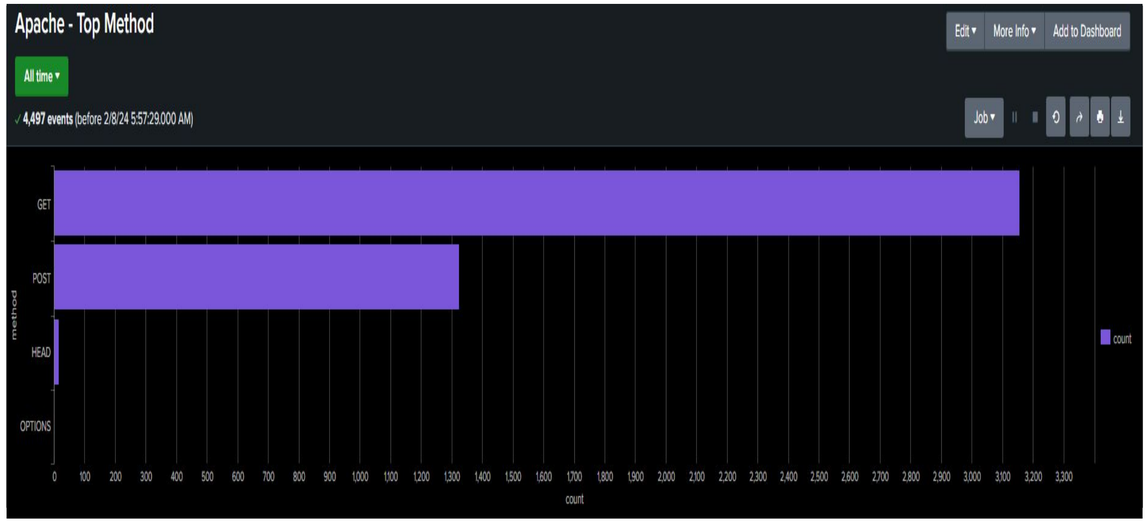


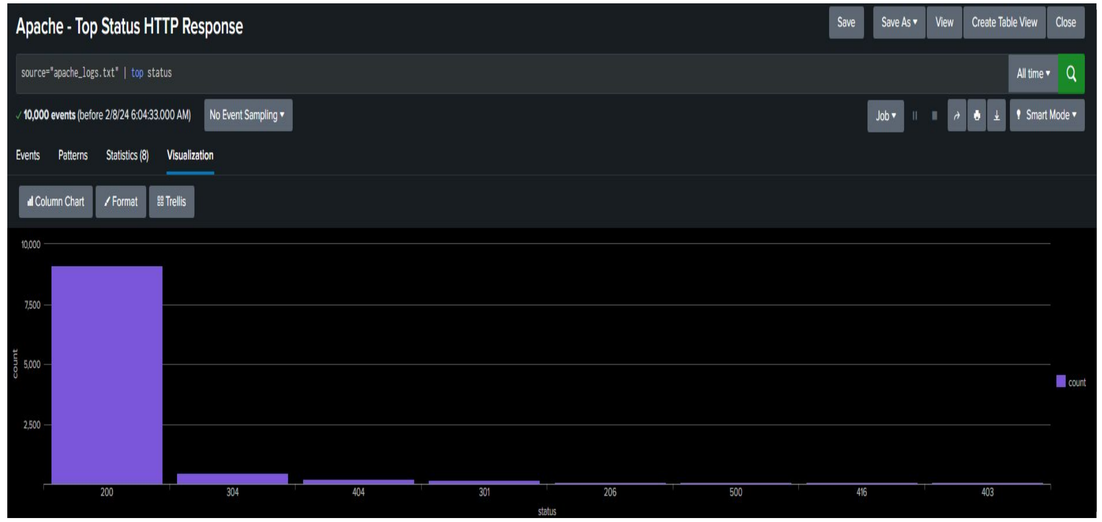
Apache - Top 10 Countries visiting

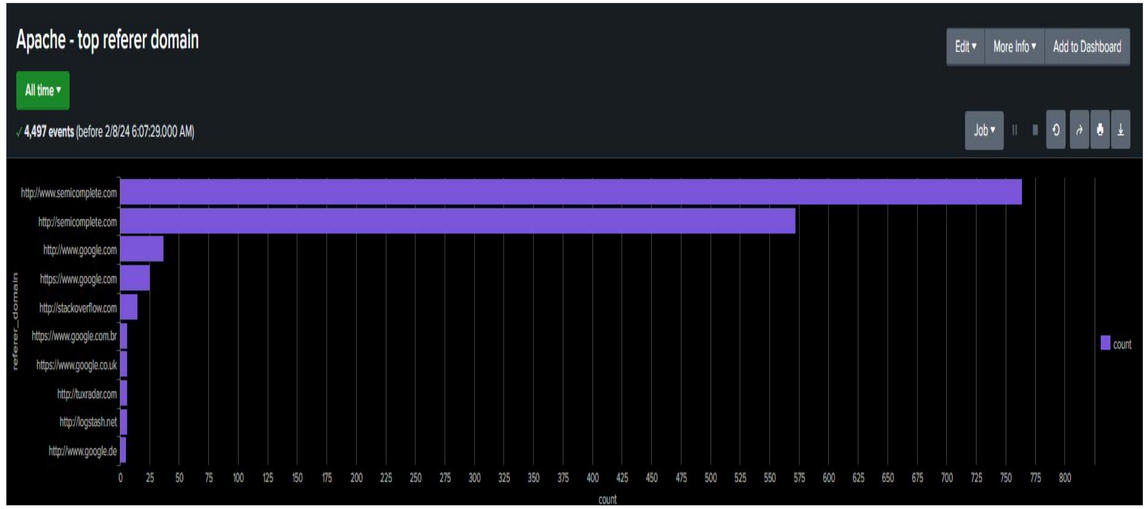


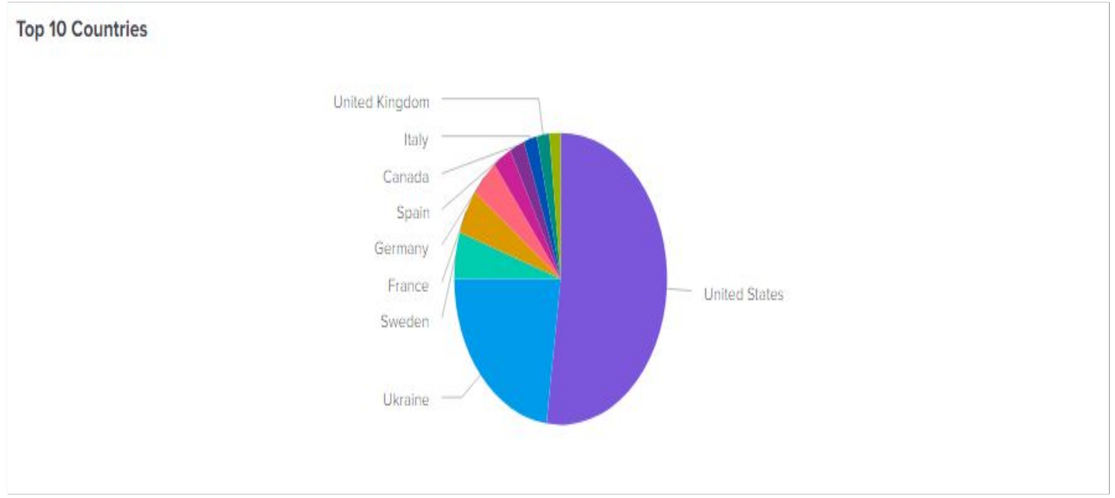
Hackoverflow

Apache - Report









Hackoverflow

Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST method	Hourly threshold for POST HTTP method reached	2	12
Justification	Threshold was set to 12 as the peaks would only reach an average of 7. Leaving 12 as a good area for a threshold.		

Hackoverflow

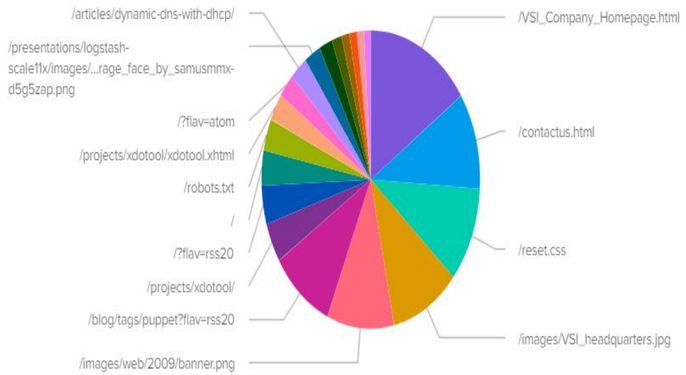
Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Outside US Activity alert	Hourly activity not from US reaches threshold	70	150
Justification	The peaks of the day on average reached 120 and the average baseline was 70. Therefore leaving 150 as a safe area for the threshold.		

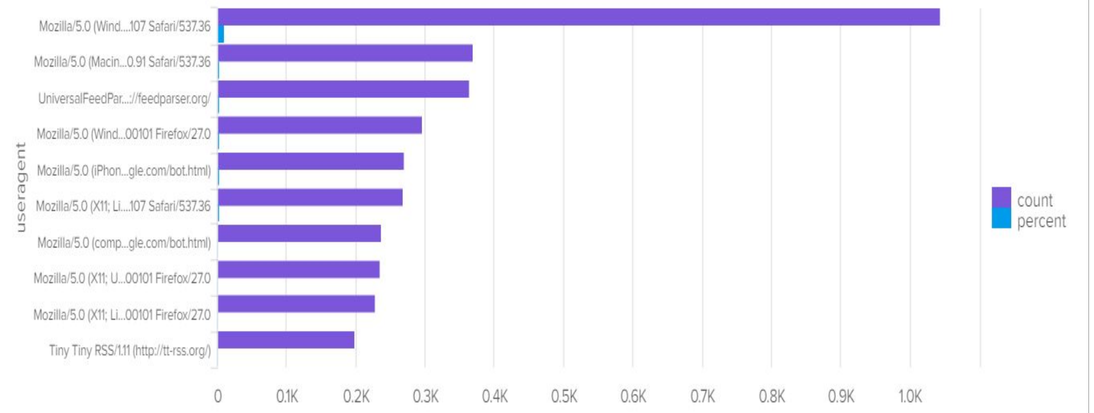
Hackoverflow

Dashboards—Apache

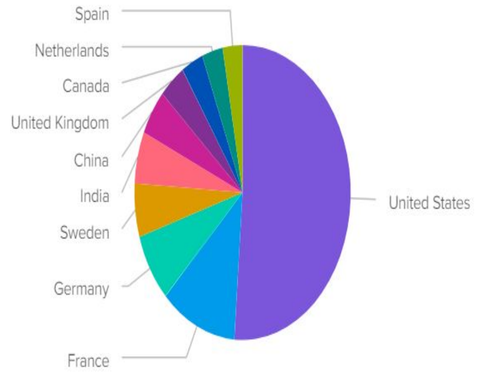
URI Interactions



Top User Agents



Top 10 Countries



Denial of Service - Error 500

Attack Analysis

Attack Summary—Windows

Report Analysis - Log Severity Records

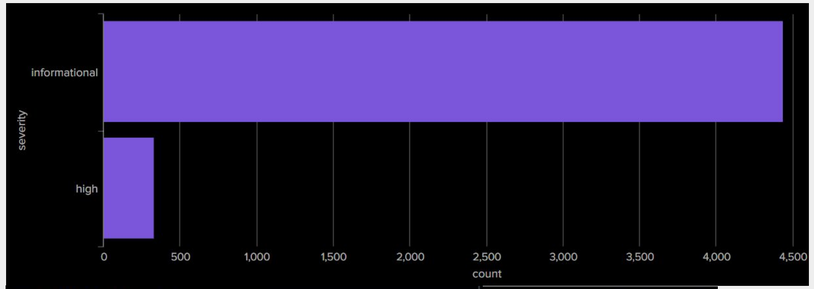
Significant change detected in proportions between ‘Informational’ and ‘High’ severity classes.

Informational: 93% down to 80%

High: 7% up to 20%

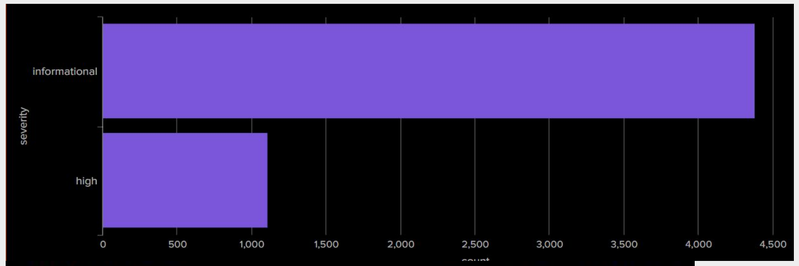
High Severity Records Tripled

Pre Attack Statistics - Baseline



severity	count	percent
informational	4435	93.094039
high	329	6.905961

Post Attack Statistics



severity	count	percent
informational	4383	79.777940
high	1111	20.222060

200% increase

Attack Summary—Windows

Report Analysis - Success / Failure Logs

Insignificant change in proportions

Pre attack

4622 - Success 97.01%

142 - Failure 2.98

Post attack

5856 - Success 98.43 %

93 - Failure 1.56%

There was a 24.8% increase in total activity.

26.6% increase in successes

34.5% decrease in failures

Pre Attack Statistics - Baseline

status	count	percent
success	4622	97.019312
failure	142	2.980688

Post Attack Statistics

status	count	percent
success	5856	98.436712
failure	93	1.563288

Attack Summary—Windows

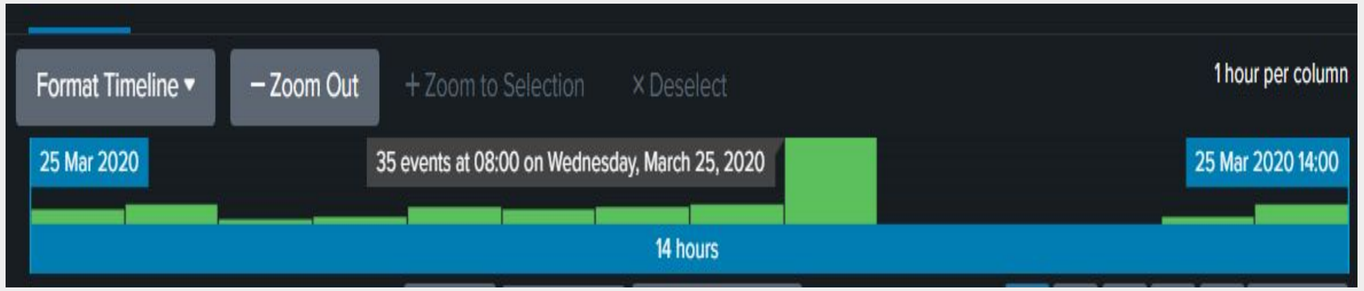
Alert Analysis Summary

Alert for Failed activity

Baseline: 10 per hour

Suspicious Activity Threshold: >19

Alert Triggered with 35 events

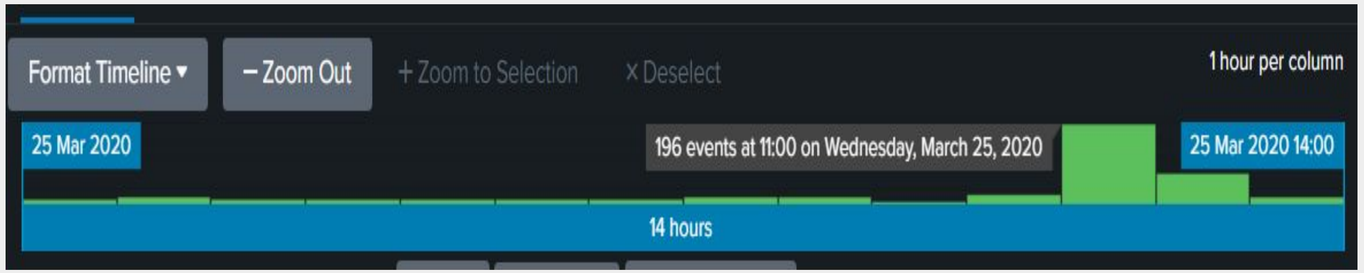


Alert for Successful Logins

Baseline: 15 per hour

Suspicious Activity Threshold: >35

Alert Triggered with 196 events



Attack Summary—Windows

Dashboard Analysis - Signatures

Signature=Account Lockouts

Baseline Avg: 15 per hour

During Attack: Peak 896 @ 02:00

Duration: 00:00 - 03:00 25/03/2020 (3 hours)

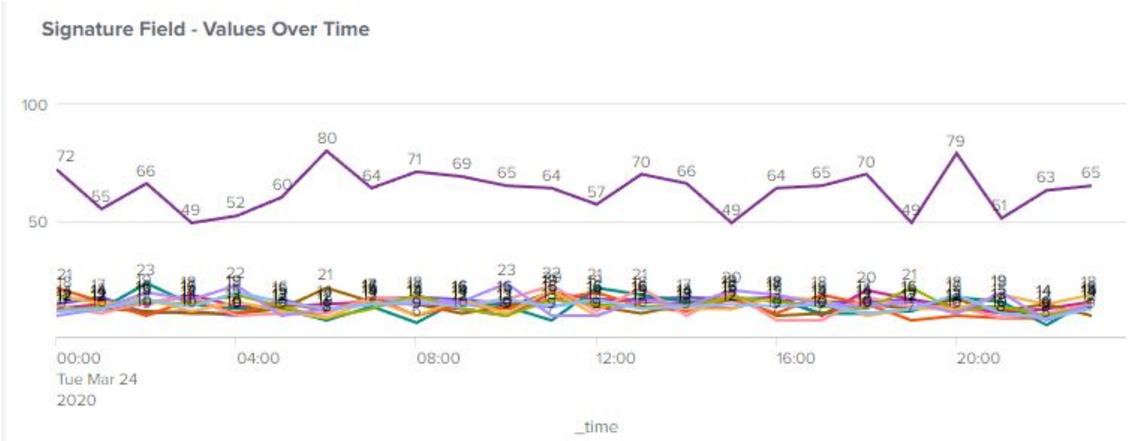
Signature=Password Reset Attempt

Baseline Avg: 15 per hour

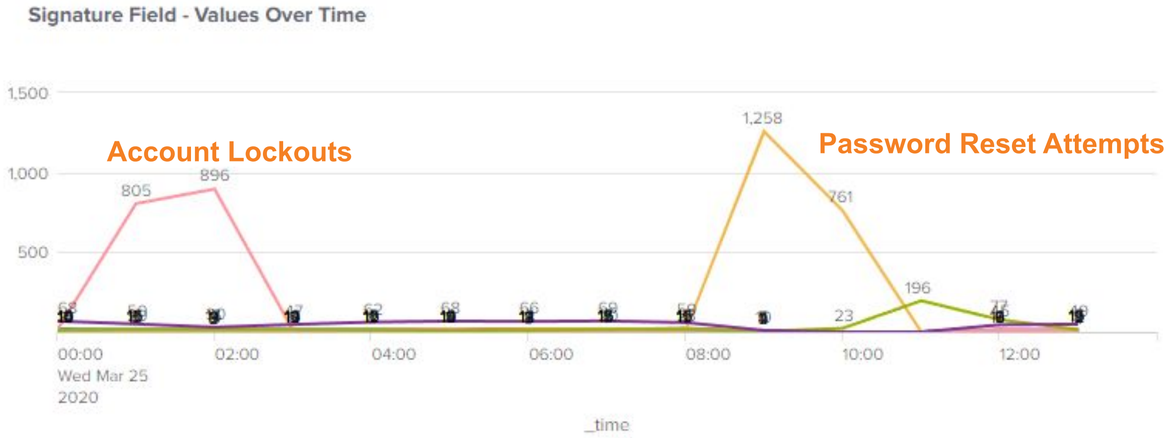
During Attack: Peak 1258 @ 09:00

Duration: 08:00 - 11:00 25/03/2020 (3 hours)

Pre Attack Statistics - Baseline



Post Attack Statistics



Hackoverflow

Attack Summary—Windows

Dashboard Analysis - User Activity

User_a

Baseline: 7 actions per hour

During Attack: Peak 984 @ 02:00

Duration: 00:00 - 03:00 25/03/2020 (3 hours)

User_k

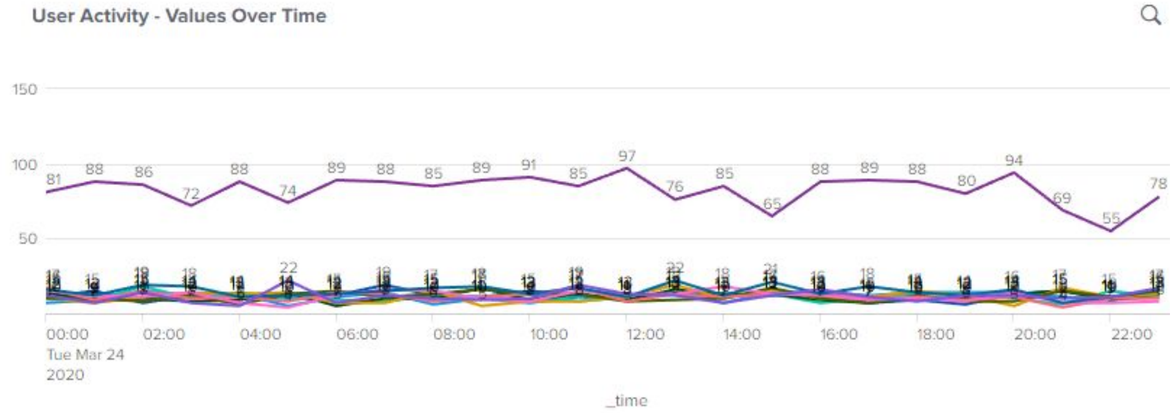
Baseline: <7 per hour

During Attack: Peak 1256 @ 09:00

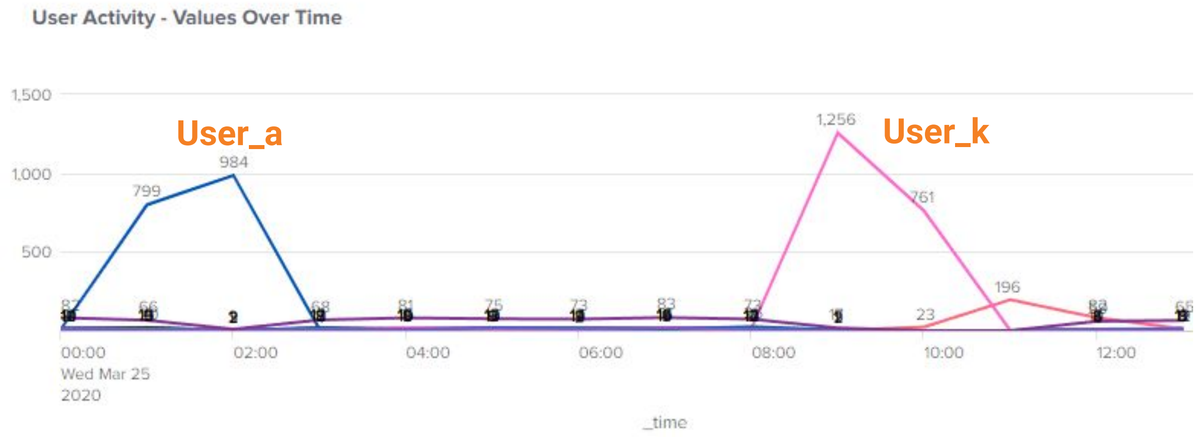
Duration: 08:00 - 11:00 25/03/2020 (3 hours)

Activity of these users directly match the signature activity shown in the previous slide.

Pre Attack Statistics - Baseline

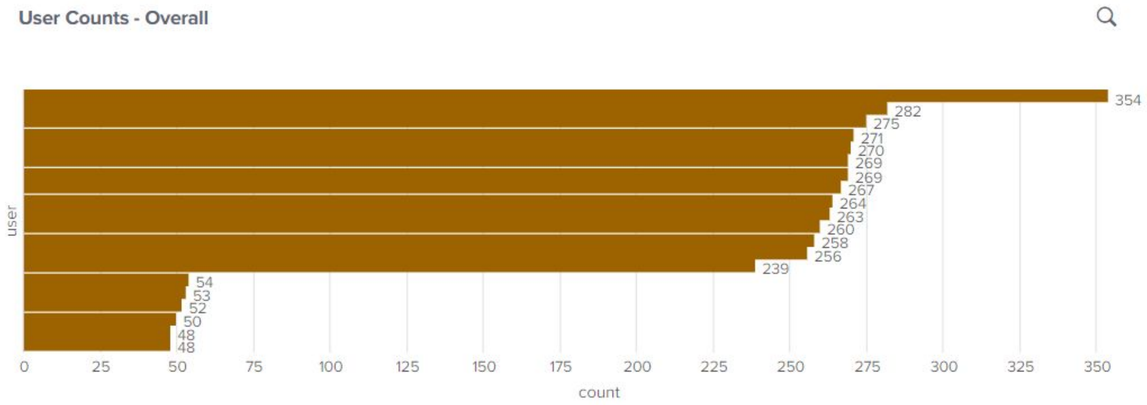


Post Attack Statistics

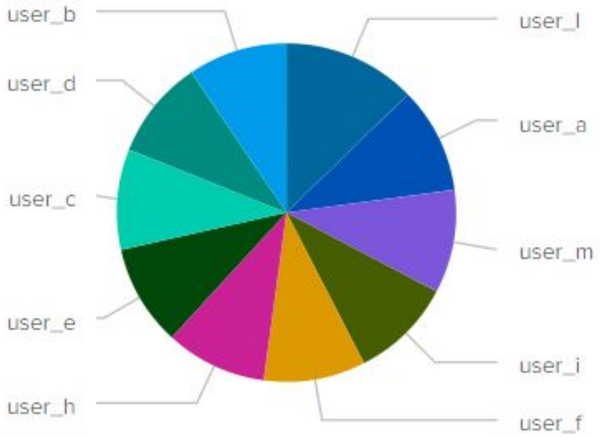


Attack Summary—Windows

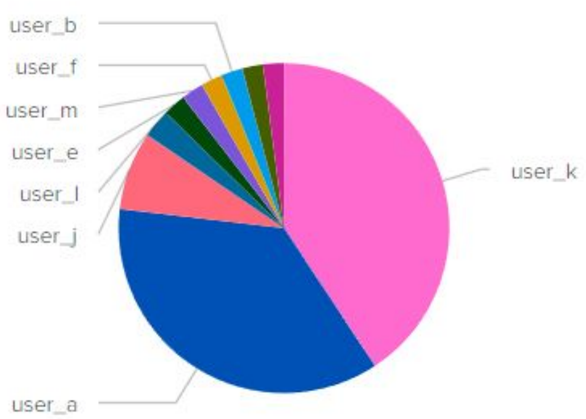
Pre Attack



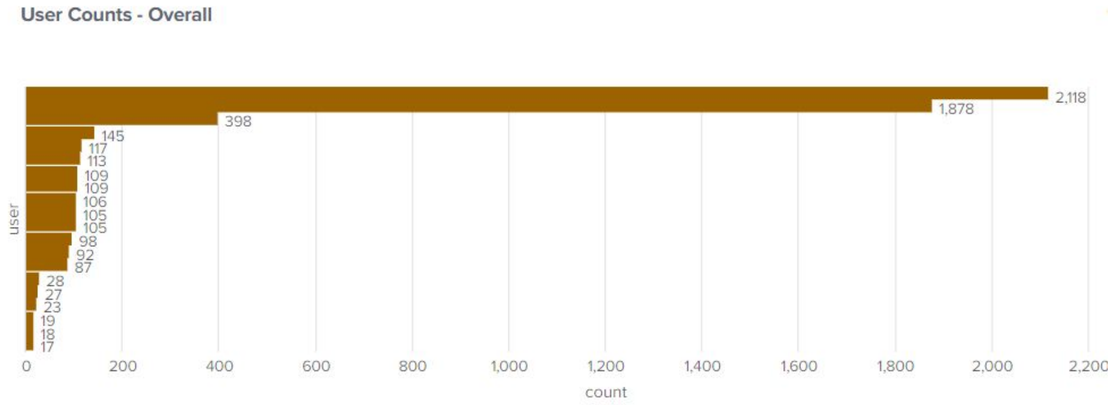
Pre Attack



Post Attack



Post Attack



Bar graphs and pie charts tracking user activity were also found to correlate with the previous dashboard charts depicting severity, signature and user activities.

Values	Count	%
An attempt was made to reset an accounts password	610	54.905%
An account was successfully logged on	278	25.022%
Domain Policy was changed	143	12.871%
A user account was locked out	80	7.201%

Above: Events categorised as ‘High’ Severity

Hackoverflow

Attack Summary - Apache

Report Analysis - HTTP Method Records

Significant change detected in proportions of HTTP GET & POST Methods recorded.

HTTP GET: 99% decreased to 70%

HTTP POST: 1% increased to 29%

Investigation into web server integrity is highly recommended.

Pre Attack Statistics - Baseline

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

Post Attack Statistics

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

Hackoverflow

Attack Summary—Apache

Report Analysis - Referrer Domains

Pre Attack Statistics - Baseline

referer_domain	count	percent
http://www.semicomplete.cor	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

Post Attack Statistics

referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Significant reduction in count - Denial of Service

Overall count of referrals decreased, indicating a denial of service, however no significant changes in referrer domains identities and proportions were observed.

Hackoverflow

Attack Summary—Apache

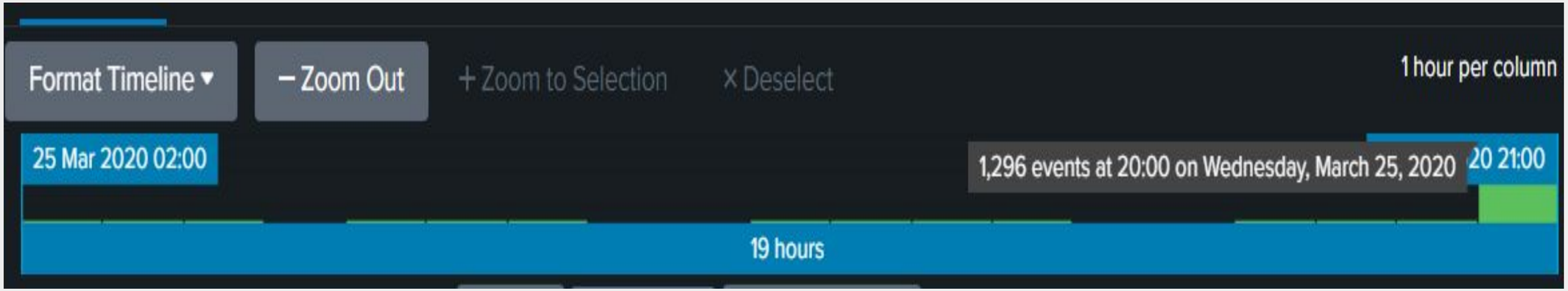
Alert Analysis Summary

Alert for HTTP POST activity

Baseline: 4 per hour

Suspicious Activity Threshold: >12

Alert Triggered with 1296 events



Attack Summary—Windows

Dashboard Analysis - HTTP Method

HTTP GET

Baseline: 110 per hour

During Attack: Peak 729 @ 18:00

Duration: 1 hour

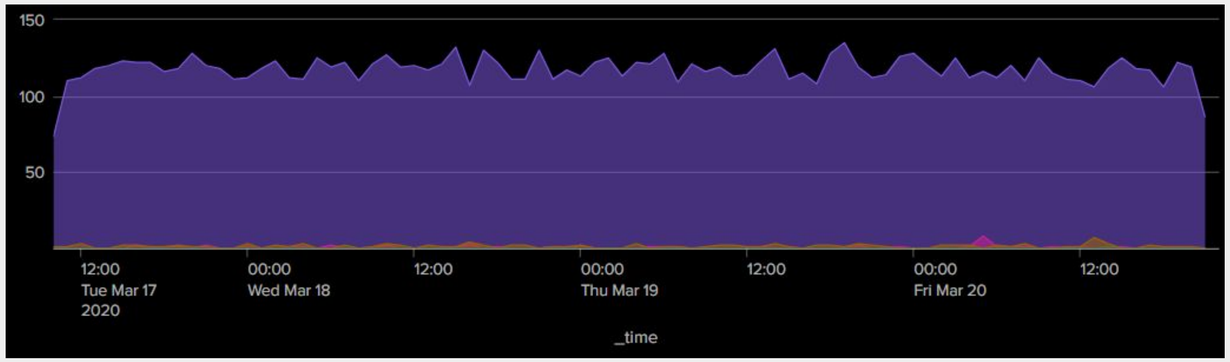
HTTP POST

Baseline: 2 per hour

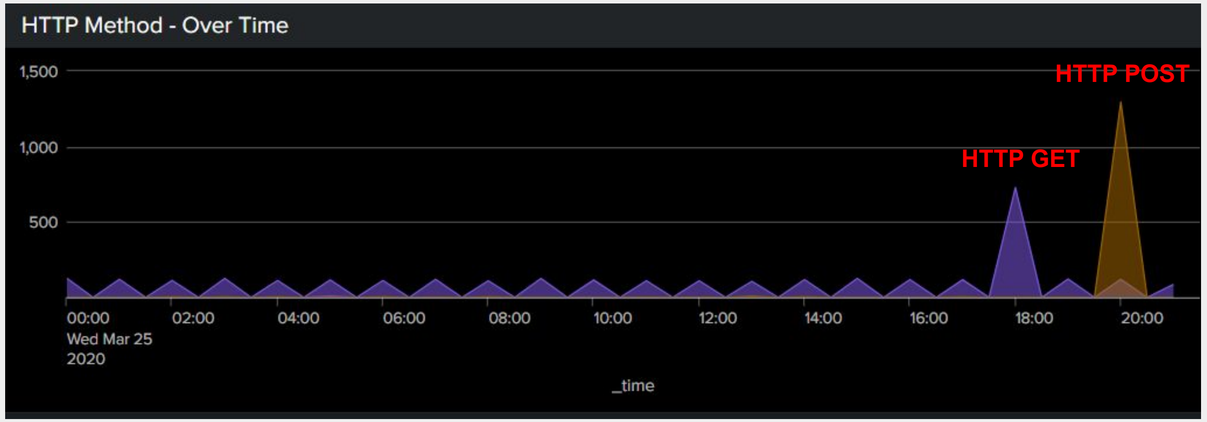
During Attack: Peak 1296 @ 20:00

Duration: 1 hour

Pre Attack Statistics - Baseline



Post Attack Statistics

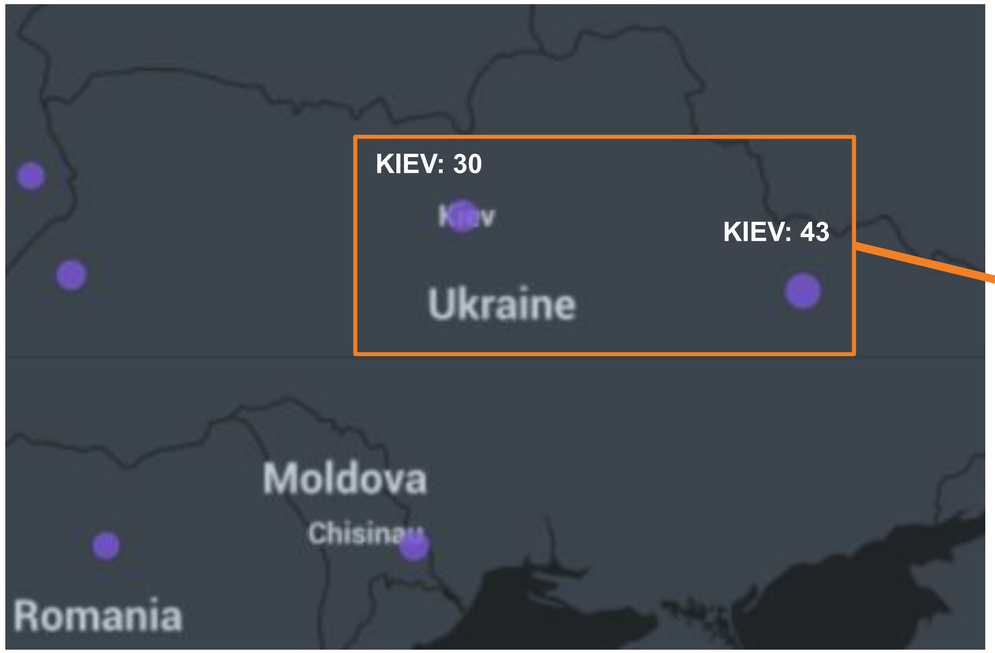


Hackoverflow

Attack Summary—Windows

Dashboard Analysis - Location Statistics

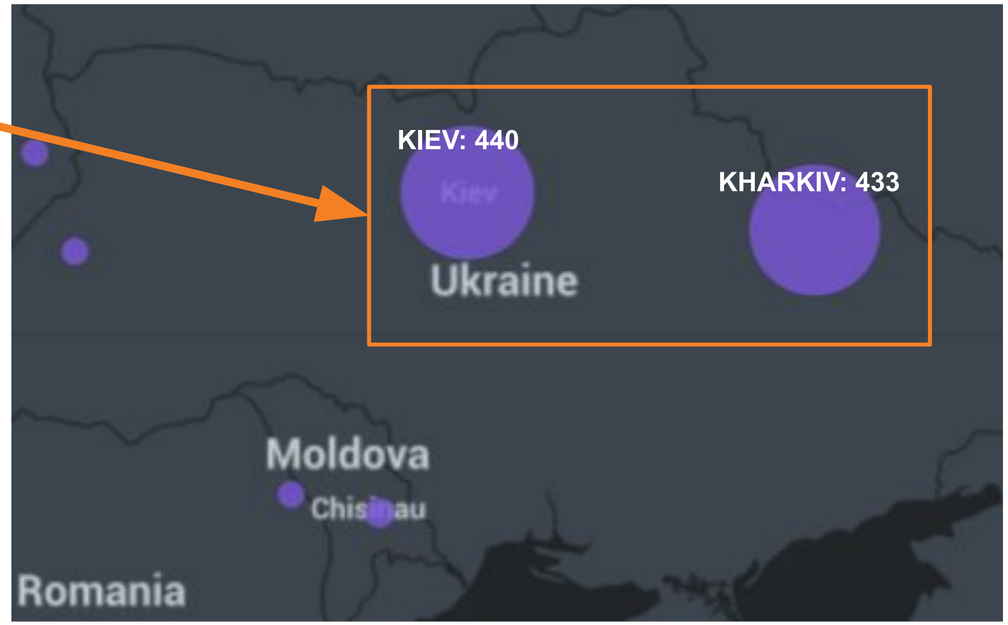
Pre Attack Statistics



Analysis identified attack to have originated from Ukrainian Cities Kiev and Kharkiv.

Volume from these locations exceeded 10x baseline levels.

Post Attack Statistics



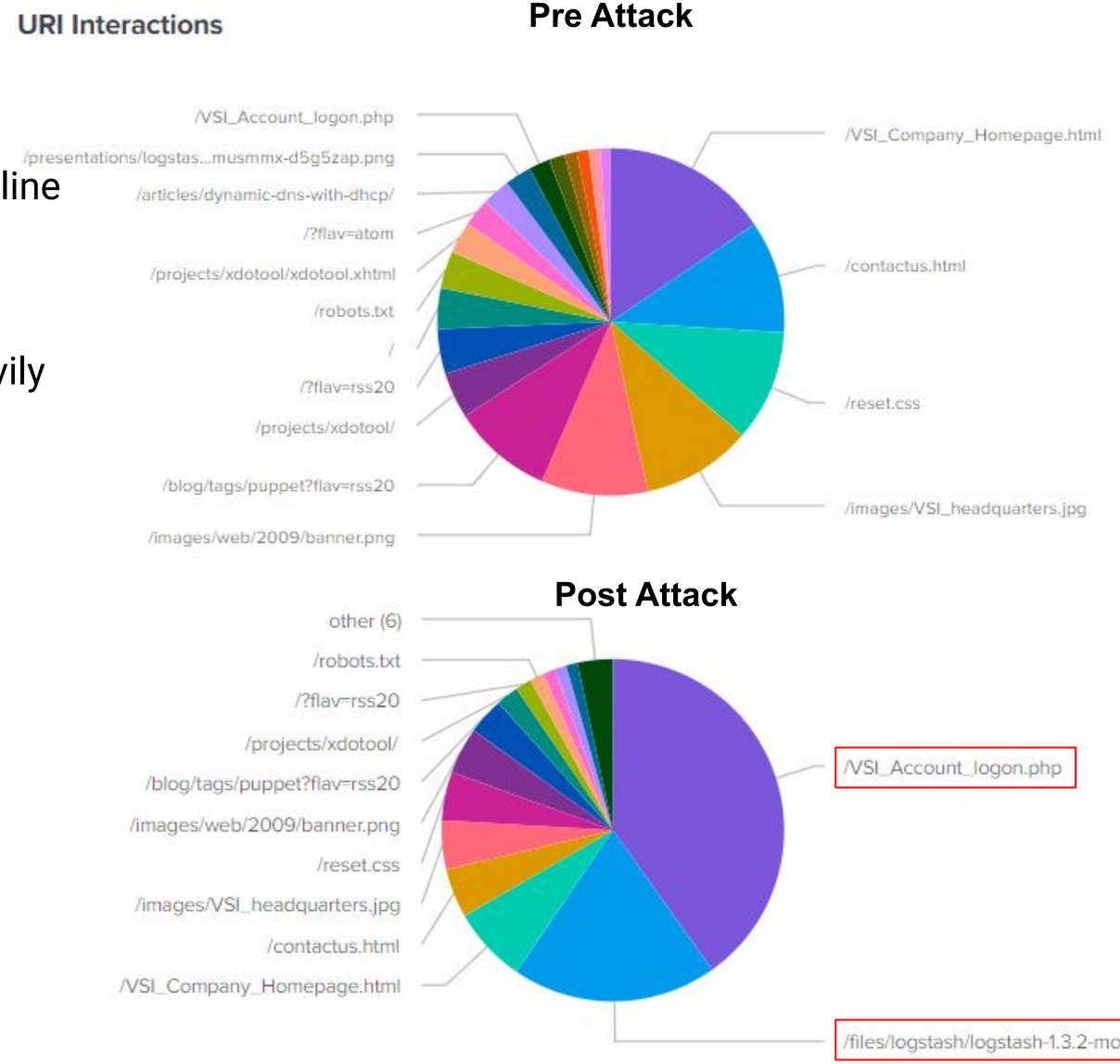
HTTPGET HTTP POST

Hackoverflow

Attack Summary—Windows

Pre Attack: URI requests are in line with expectations.

Post Attack:
- VSI_Account_logon.php heavily targeted
- logstash-1.3.2-monolithic.jar heavily targeted



URI targets indicate attempts to exfiltrate data and/or sabotage systems and intellectual property

Data supports the rumours that the attack was launched by a corporate adversary

Summary & Future Mitigations

Hackoverflow

Project 3 Summary

Overall Findings

- Attack occurred on the 25/03/2020
- Attacks were spread out over the course of the day
- Adversary employed a multi pronged approach disrupting web and backend services
- Attacks originated from Ukraine
- Adversary attempted to exfiltrate data and/or sabotage systems and intellectual property

Hackoverflow

Project 3 Summary

Mitigations & Recommendations

- Comprehensively investigate data and system integrity of Apache and Windows Servers
- Conduct a security review of all user accounts and reset passwords
- Consider moving sensitive files and applications such as Logstash into a more secure location
- Blacklist malicious IP locations based on the parameters given by the Whois XML Geolocation API
- Review web host traffic filtering capability and consider migrating web application to prevent future DoS attacks
- If resources permit, assert market dominance by launching a counteroffensive against Jobecorp