Defensive Security Project
by: Room 3 Cybergoons

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- JobeCorp has targeted VSI’s Windows and Apache servers!! (NOT GOOD)
- These attacks have taken down critical systems! (EVEN WORSE)
- Lucky for VSI having monitoring systems that quickly identified the attack. (THIS IS GOOD)
- Along with these monitoring systems, management provided us with additional logs to look over and help determine the severity of the attack. (AWW MORE WORK)
- Let’s work together and see if these monitoring solutions even works. (I REALLY HOPE THEY DO)

Website Monitoring App

Website Monitoring App

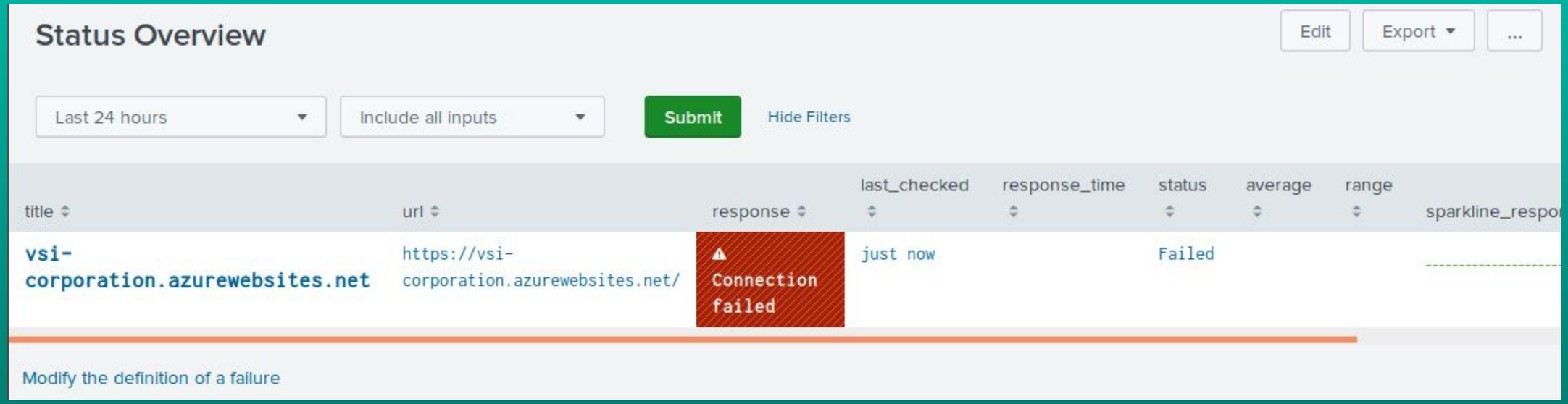
1. Large companies like Amazon are so large that they hire multiple third-party services to manage different aspects of their website.
2. This tends to make the companies web architecture complex and a pain to manage and troubleshoot.
3. Add-On Apps plus monitoring tools allows the company to better monitor any web architectures to minimize potential threats and ensure websites run smoothly.

Website Monitoring

The Website Monitoring App for Splunk was designed to monitor performance and availability of websites. Here are some of its features:

1. Allows users to track website metrics in real-time.
2. Customisable alarms and dashboards.
3. Along with Splunk’s analytics platform, this app allows users to correlate website performance data with other system data for a better insight of website and system performance.

Website Monitoring App



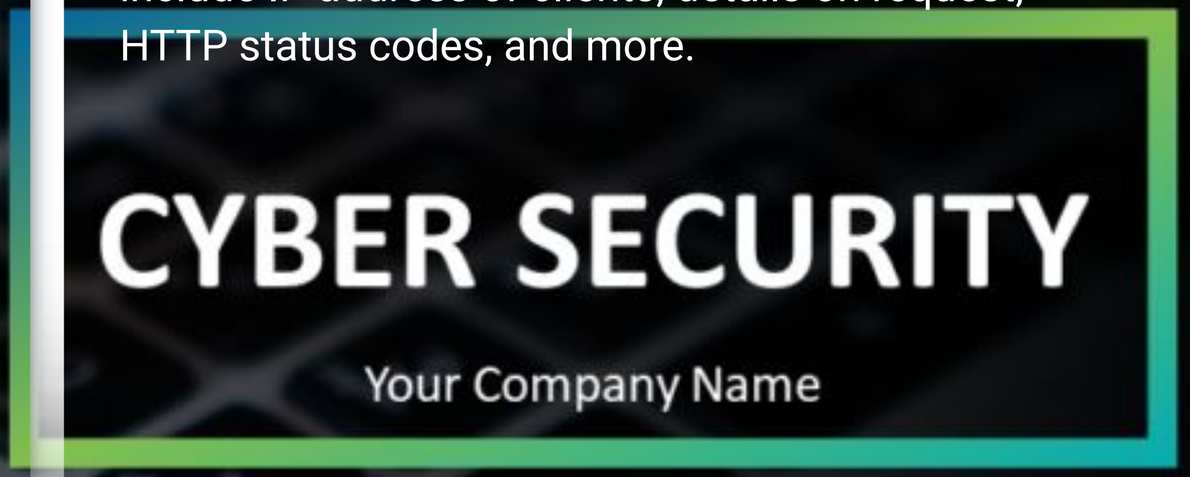
Logs Analyzed

1 Windows Logs

This Server Contains intellectual property of VSI's next-generation virtual reality programs. Logs include hardware components, Security events, system errors , and more.

2 Apache Logs

This server is used for VSI's main public-facing website vsi-company.com. Logs include IP address of clients, details on request, HTTP status codes, and more.



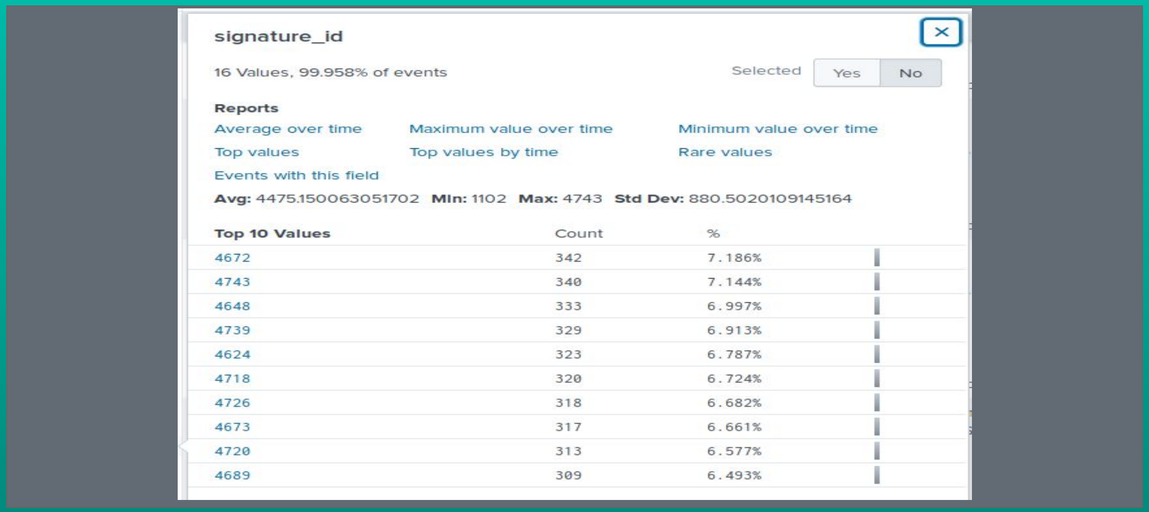
Windows Logs

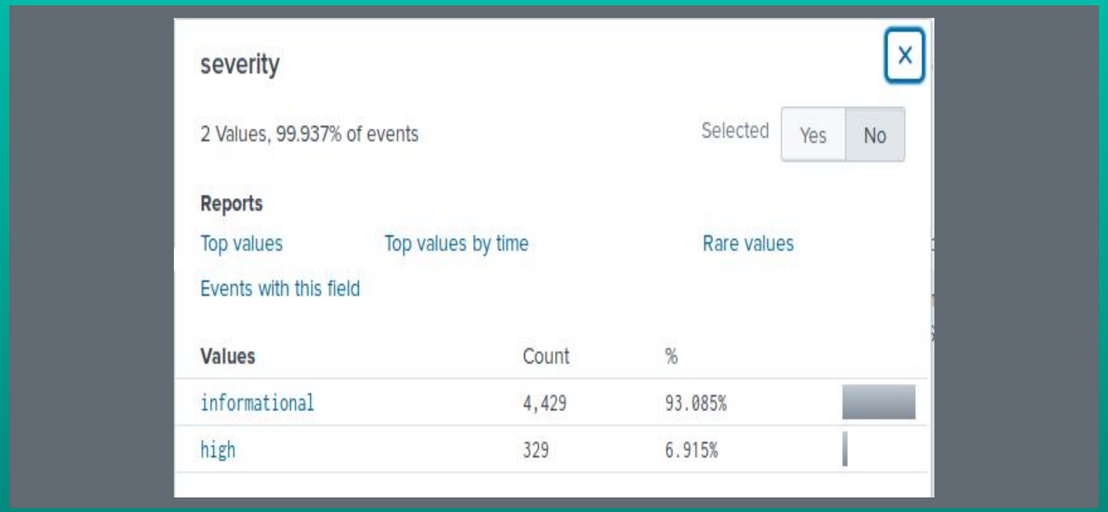
Reports—Windows

Designed the following reports:

Report Name	Report Description
Signiture_ID	This allows VSI to view reports that show the ID number with a specific signature of the Activity in Windows.
Severity	This allows VSI to know the severity levels of the Windows logs being viewed
Status (Success and Failures)	This allows VSI to see if there is a suspicious level of failed activities in their servers
Users	This allows VSI to view its top Users

Images of Reports—Windows

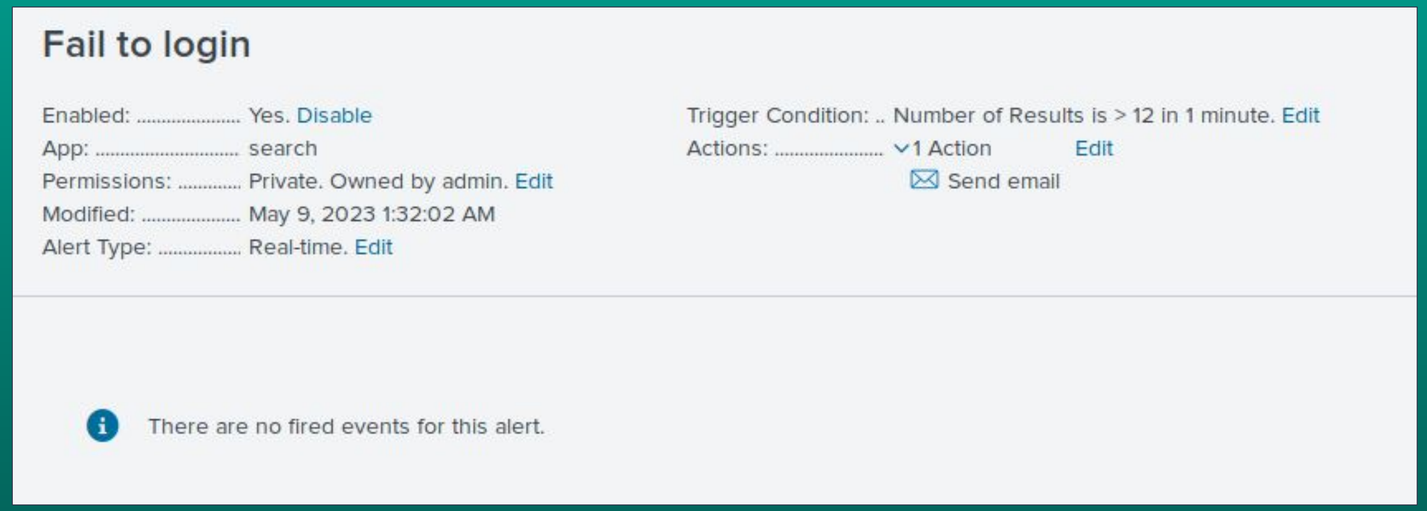




Alerts—Windows

Designed the following alert:

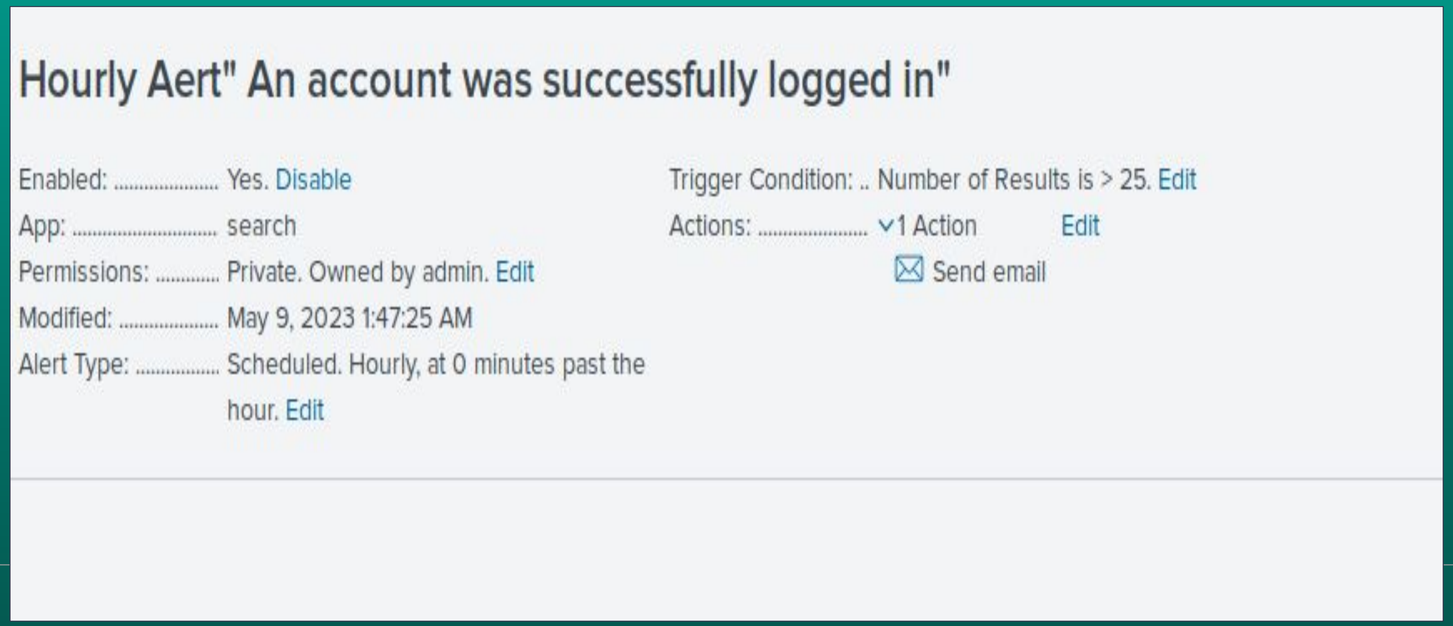
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Fail to Login	Hourly level of failed Windows activity	5	12



Alerts—Windows

Designed the following alert:

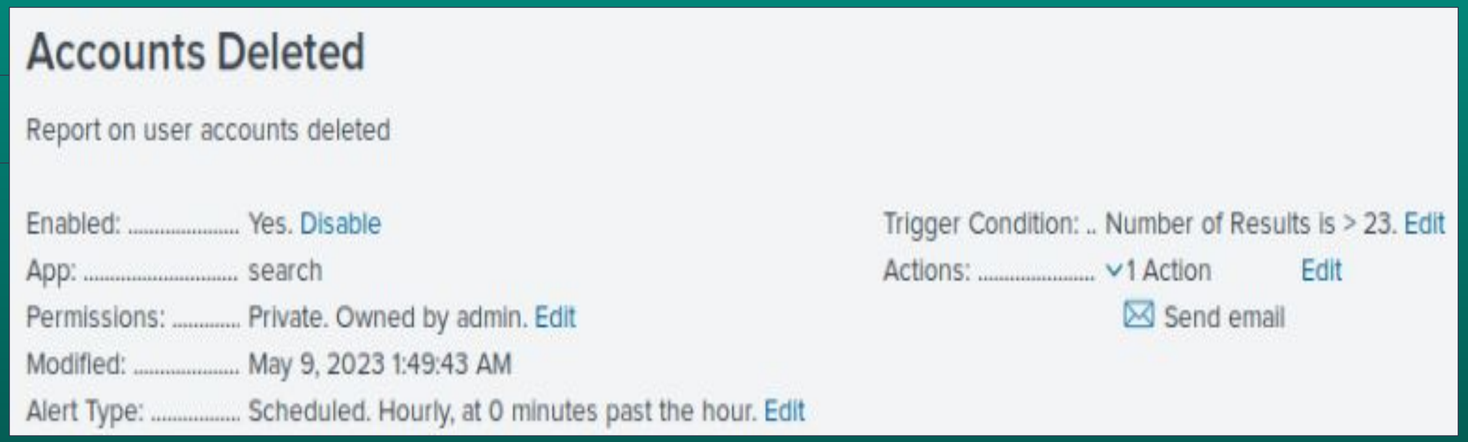
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful logins	Hourly count of the signature: logged in successfully	10	25



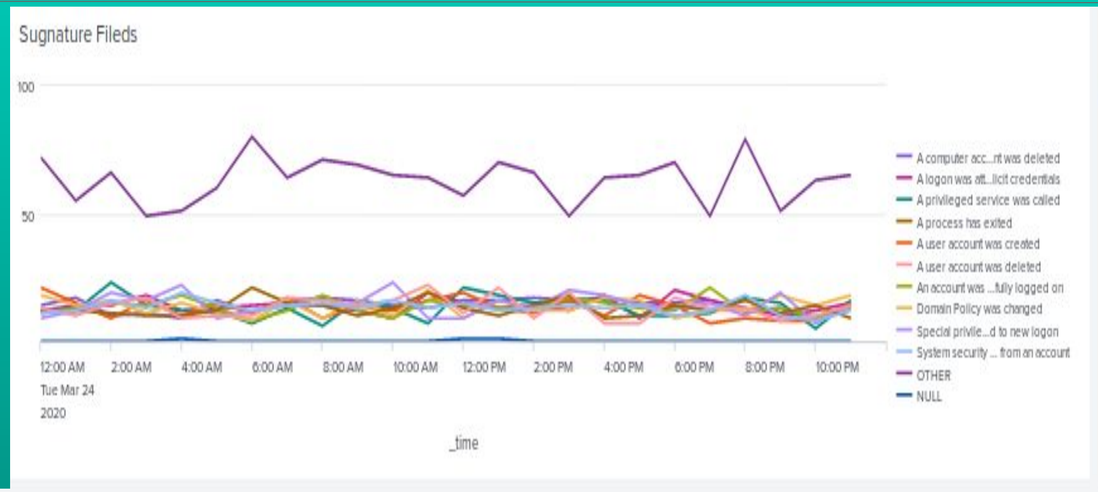
Alerts—Windows

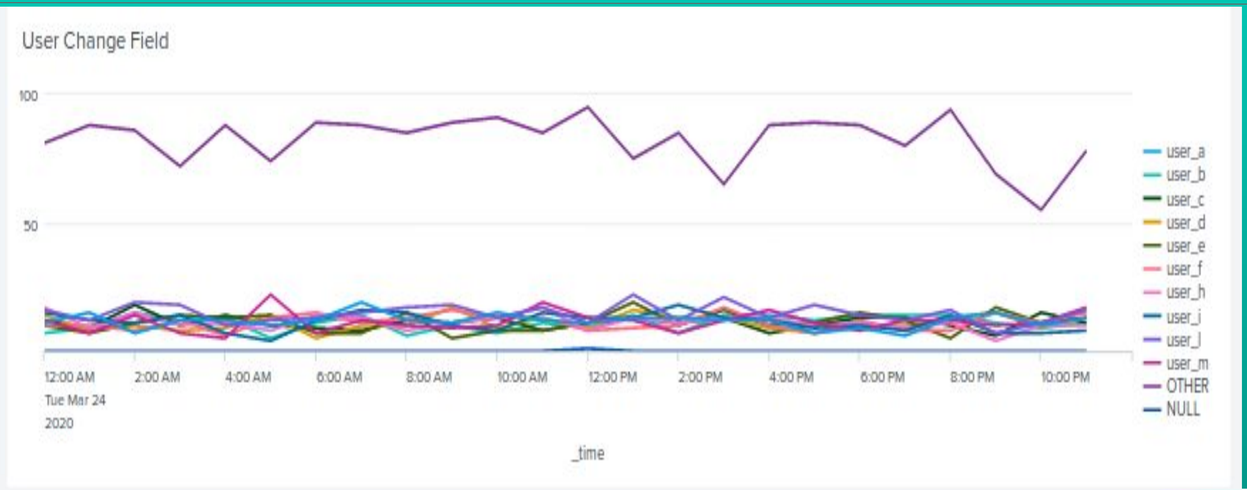
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Accounts Deleted	Alerts VSI when an id signature of: “account deleted” is detected.	7	23

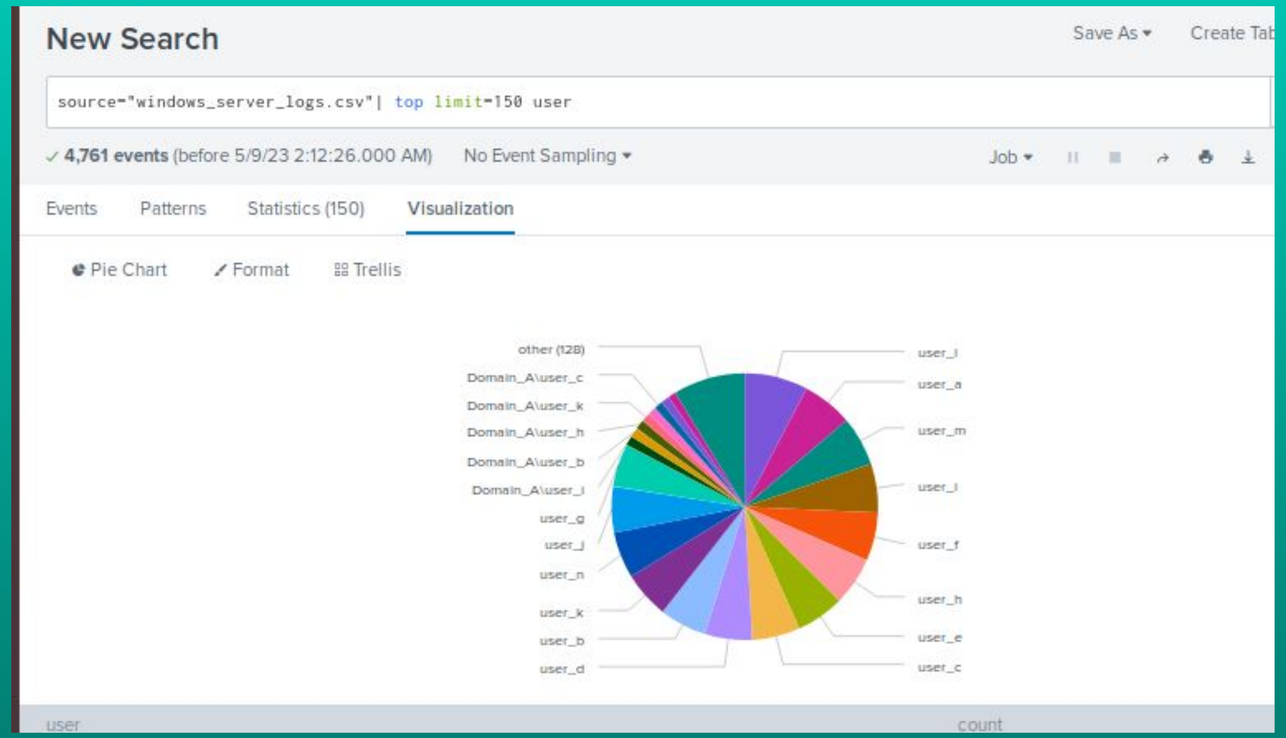


Dashboards—Windows





Dashboards—Windows



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP methods	The different type of HTTP activity being requested against VSI's web server
Top 10 domains	The top domains that referred to VSI's website. Help identify suspicious referrers.
HTTP response codes	Identifying the most common used HTTP response codes. Help to see suspicious levels of the codes.

Images of Reports—Apache

New Search

Save As ▾ Create Table View Close

source="apache_logs.txt"| top limit=20 method

All time ▾

✓ **10,000 events** (before 5/9/23 2:50:55.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (4)** Visualization

20 Per Page ▾ Format Preview ▾

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

New Search

Save As ▾ Create Table View Close

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

All time ▾

✓ **10,000 events** (before 5/9/23 3:18:27.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (10)** Visualization

20 Per Page ▾ Format Preview ▾

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

New Search

Save As ▾ Create Table View Close

source="apache_logs.txt" | top status

All time ▾

✓ **10,000 events** (before 5/9/23 3:19:05.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (8)** Visualization

20 Per Page ▾ Format Preview ▾

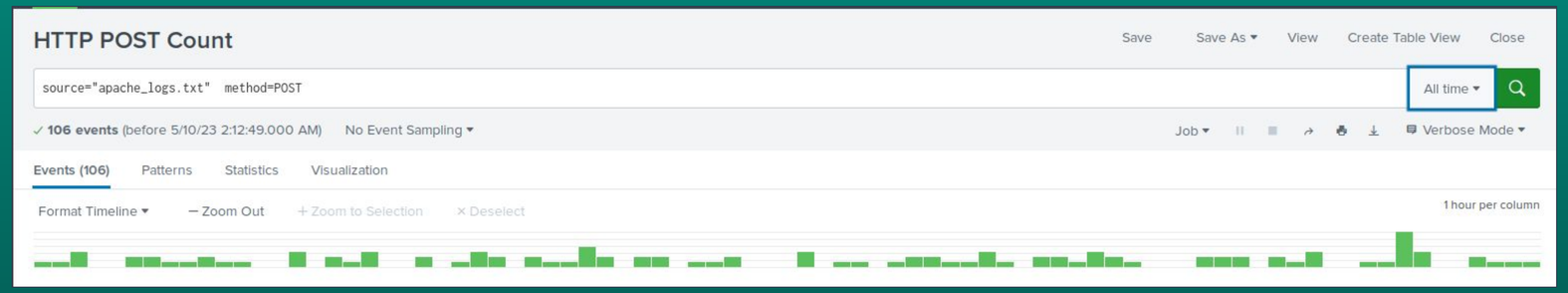
status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST	Hourly count of the HTTP POST method	2	10

JUSTIFICATION: The baseline for HTTP POST was 2 because that was close to the average per hour. The threshold was put at 10 because the highest spike for an hour was 7.

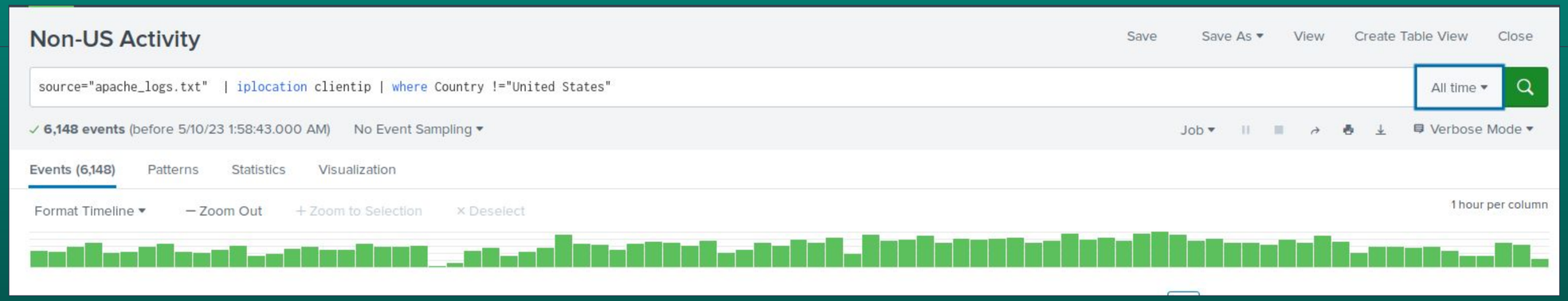


Alerts—Apache

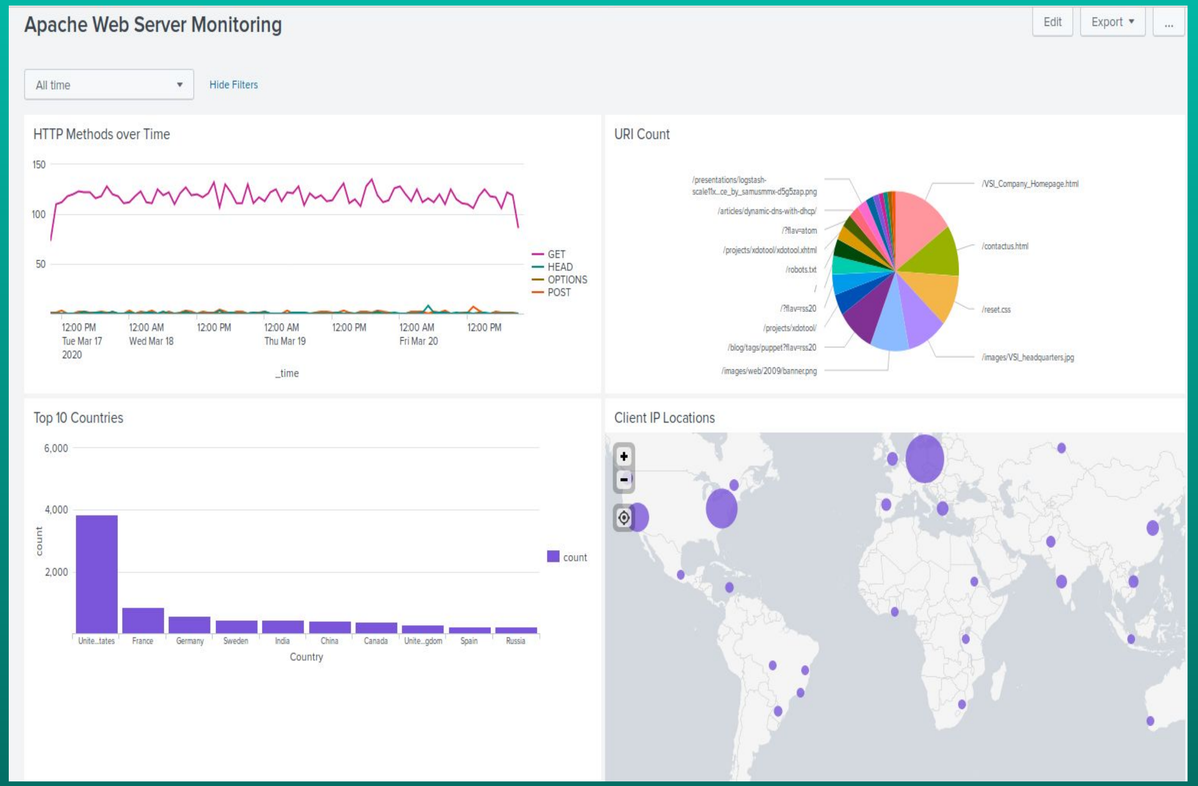
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US activity	Hourly activity from any country besides the United States	80	140

JUSTIFICATION: For the baseline we decided to do 80 because that was close to the average events per hour. The threshold was put at 140 because the biggest spike for any hour was 120.



Dashboards—Apache



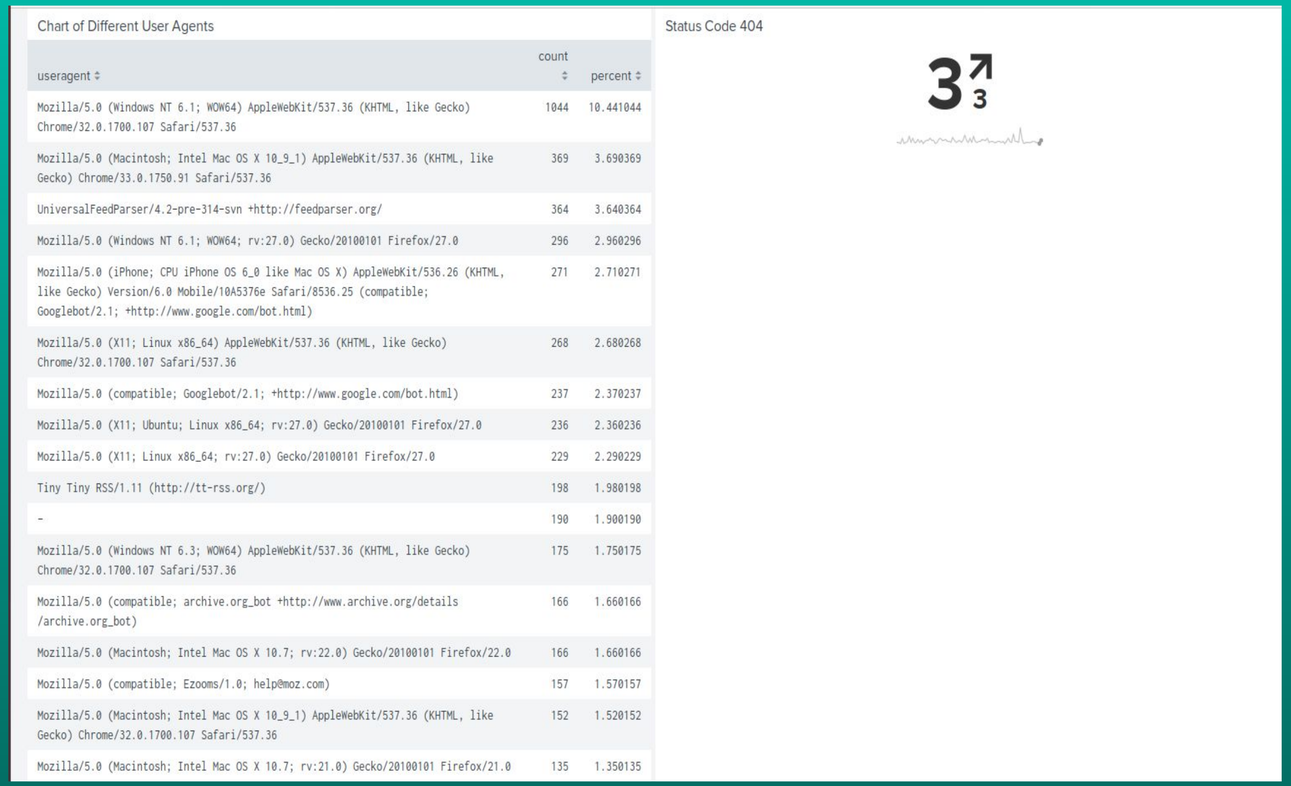


Chart of Different User Agents

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
-	190	1.900190
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	175	1.750175
Mozilla/5.0 (compatible; archive.org_bot +http://www.archive.org/details /archive.org_bot)	166	1.660166
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0	166	1.660166
Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)	157	1.570157
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	152	1.520152
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:21.0) Gecko/20100101 Firefox/21.0	135	1.350135

Status Code 404

3
3

Attack Analysis

Attack Summary—Windows

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

- Severity Report: Showed increase in high severity events.
- Failed Attempts Report: Showed us number of failed logins went down and successful logins went up. Indicating the attack was successful and critical information was exposed.

Attack Summary—Windows

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

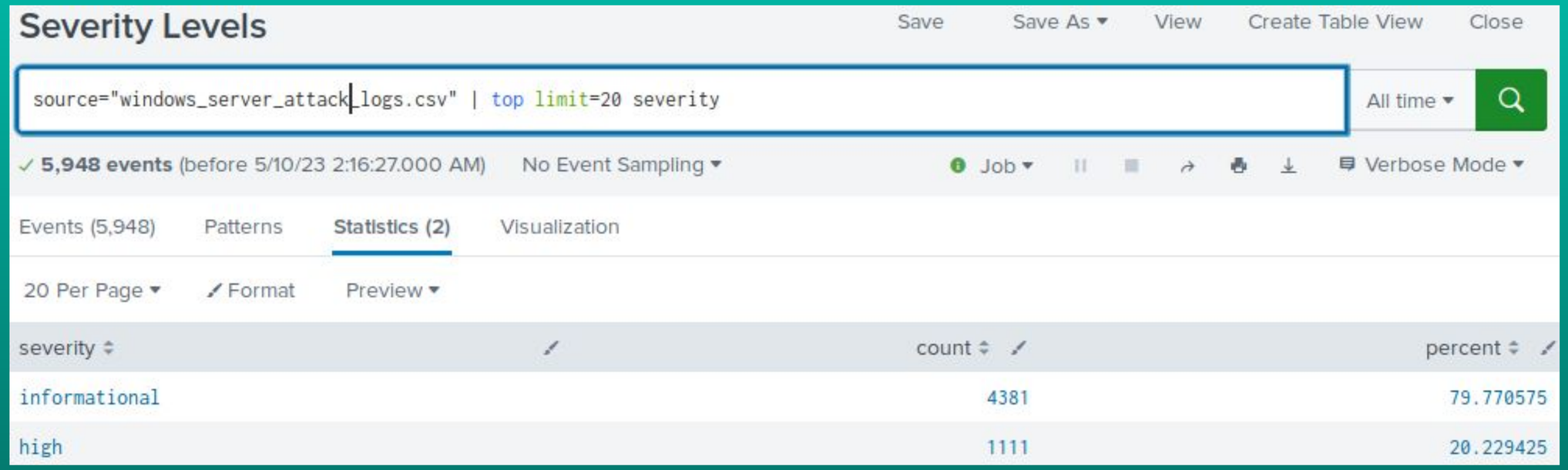
- Failed Windows Activity Alert: Showed the number of failed login events went down indicating attack was successful and system was compromised.
- Successful Logins Alert: Showed the number of successful login events went up, meaning the attackers got into system.
- Deleted Accounts Alert: Showed the number of accounts being deleted

Attack Summary—Windows

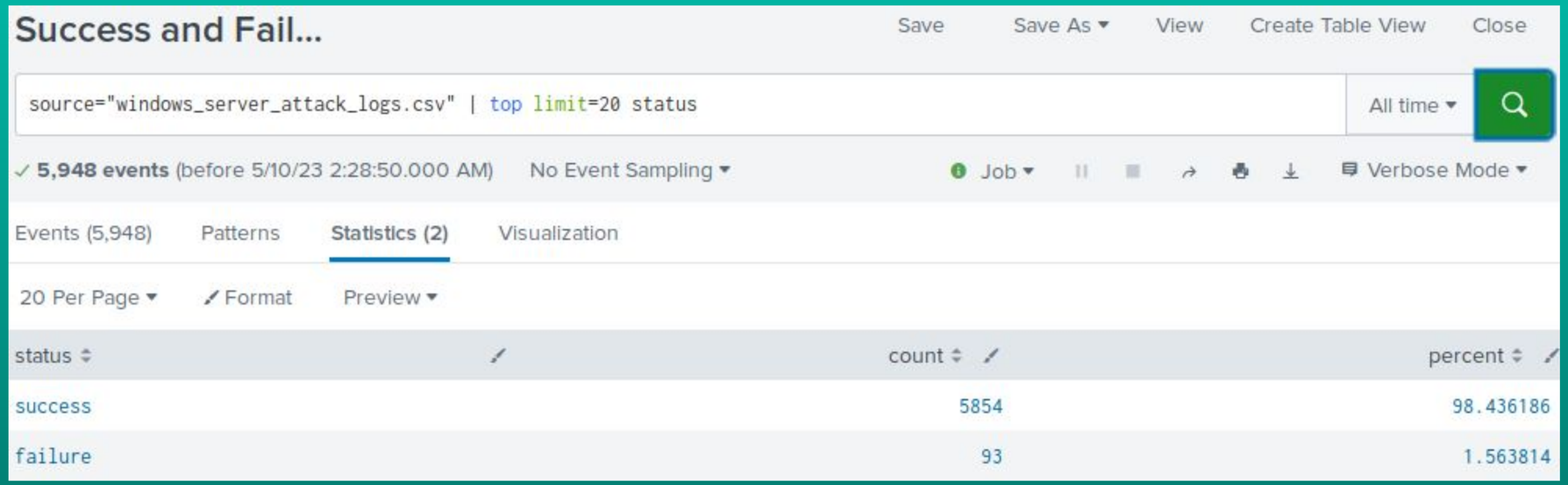
Summarize your findings from your dashboards when analyzing the attack logs.

- Signature Values Over Time Chart: Revealed a brute force attack occurred between 12am-3am on March 25th, 2020. Which lead to the conclusion that attack was successful because the number of successful logins went up from 8am-11am. The two signatures that stand out are “An attempt was made to reset an account password” and “A user account was locked out”
- User Analysis Chart: Revealed to us the users behind the attack by showing us time of their activity and number of events. The users are user_k and user_a.

Screenshots of Attack Logs

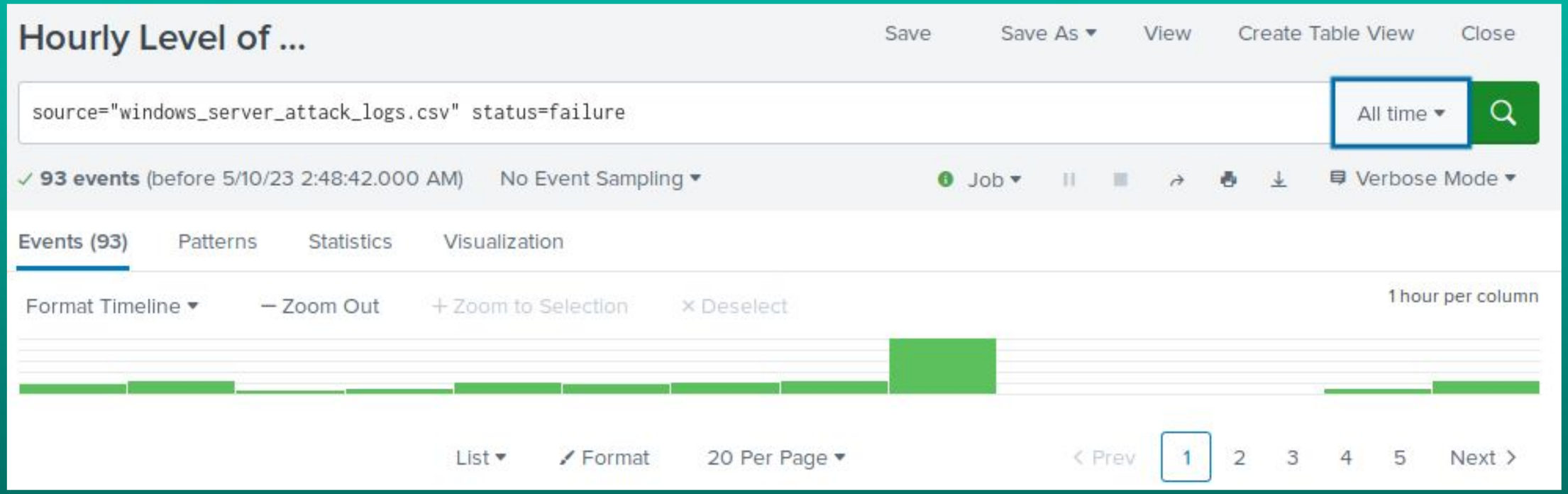


Screenshots of Attack Logs



status	count	percent
success	5854	98.436186
failure	93	1.563814

Screenshots of Attack Logs

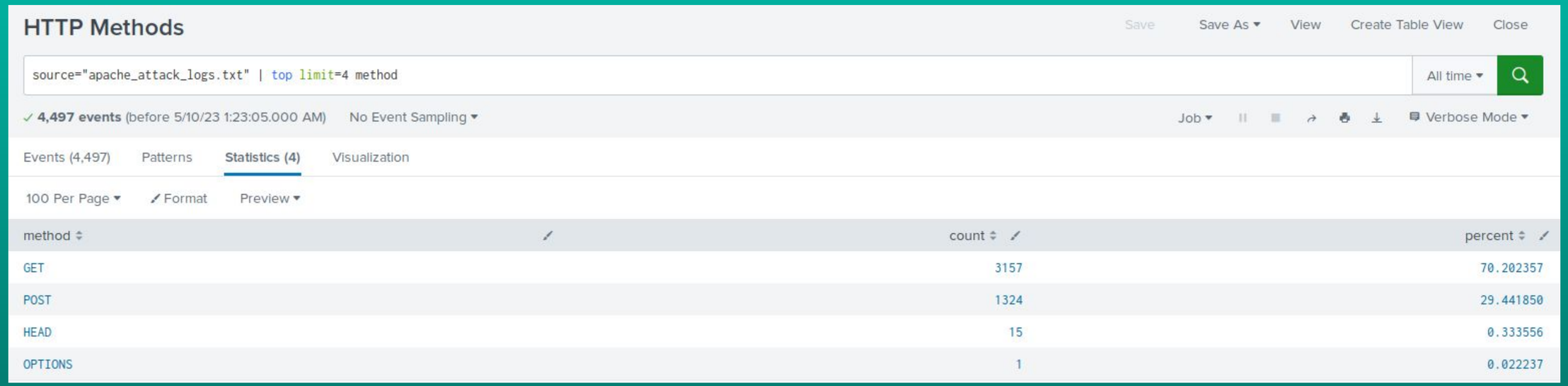


Attack Summary—Apache

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

- From the HTTP methods report there was a decrease in GET activity by about 28% and an increase in POST activity by about 28%.
- From the top 10 domains report there was no suspicious activity because the percent of the referred domains were similar in both logs.
- From the HTTP response codes report there was suspicious activity with code 404 with an increase of 13%.

Screenshot of HTTP Methods report attack log



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

Screenshot of Top Domains Referred report attack log

Top Domains Referred

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

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

All time

✓ **4,497 events** (before 5/10/23 1:35:29.000 AM) No Event Sampling

Job | Verbose Mode

Events (4,497) | Patterns | **Statistics (10)** | Visualization

100 Per Page | Format | Preview

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

Screenshot of HTTP Response Code report attack log

HTTP Response Codes

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

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

All time

✓ **4,497 events** (before 5/10/23 1:37:56.000 AM) No Event Sampling

Job | Verbose Mode

Events (4,497) | Patterns | **Statistics (7)** | Visualization

100 Per Page | Format | Preview

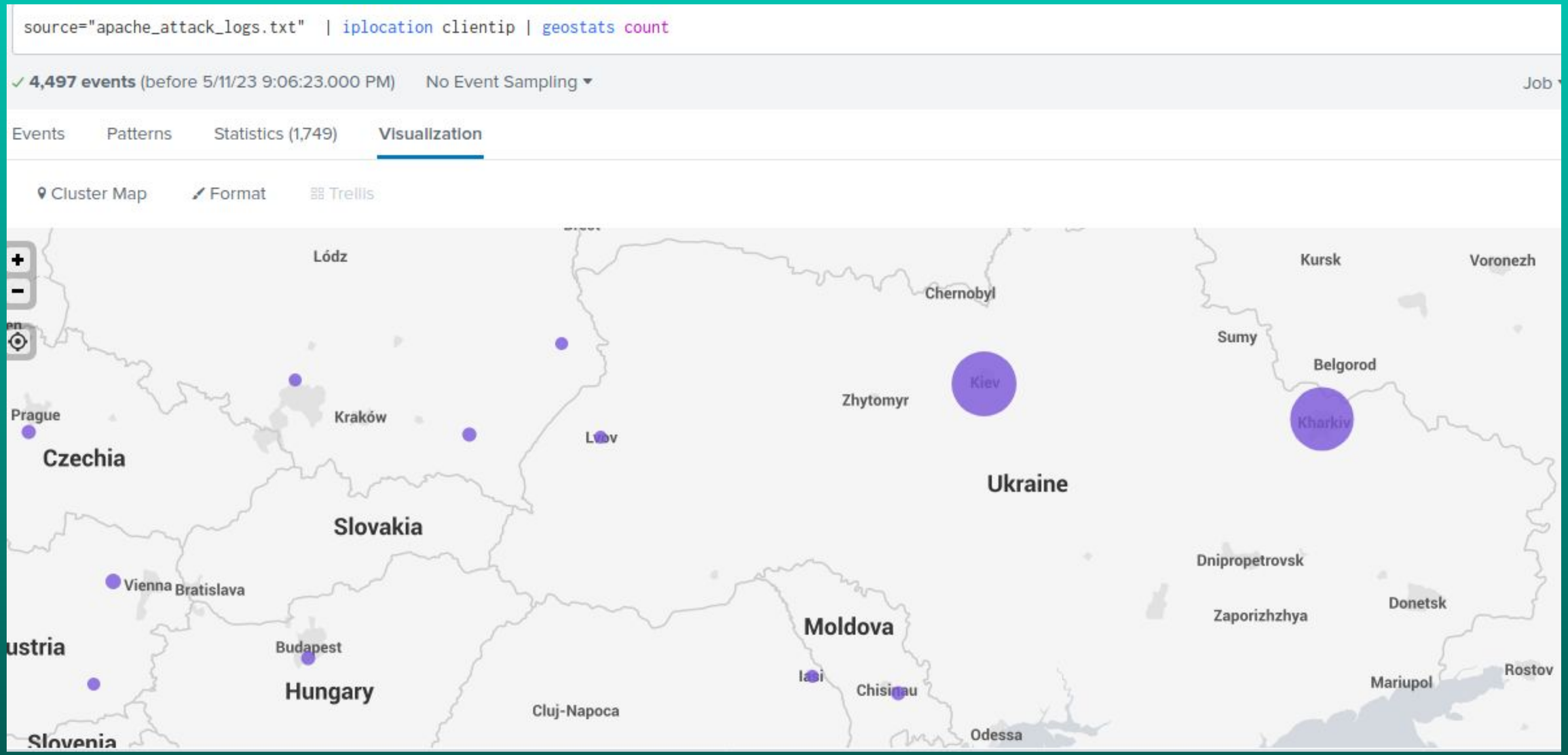
status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Attack Summary—Apache

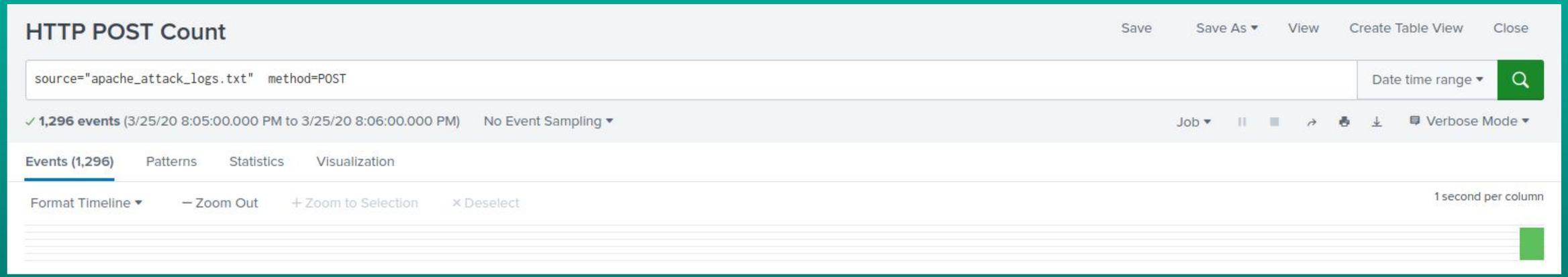
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- From the Non-US activity alert there was suspicious activity coming from Ukraine. In the first log there was a count of 88 events coming from Ukraine, and in the attack log there was a count of 877 events from Ukraine. The two cities in Ukraine that had most of the events were in Kiev with a count of 439 and Kharkiv with a count of 433. 864 of the events in Ukraine occurred at 8:05 p.m. on Wednesday, March 25, 2020.
- From the HTTP POST Activity alert there was a count of 1,296 events that occurred at 8:05 p.m. on Wednesday, March 25, 2020.

Screenshot of Non-US Activity alert attack log



Screenshot of HTTP POST Activity alert attack log

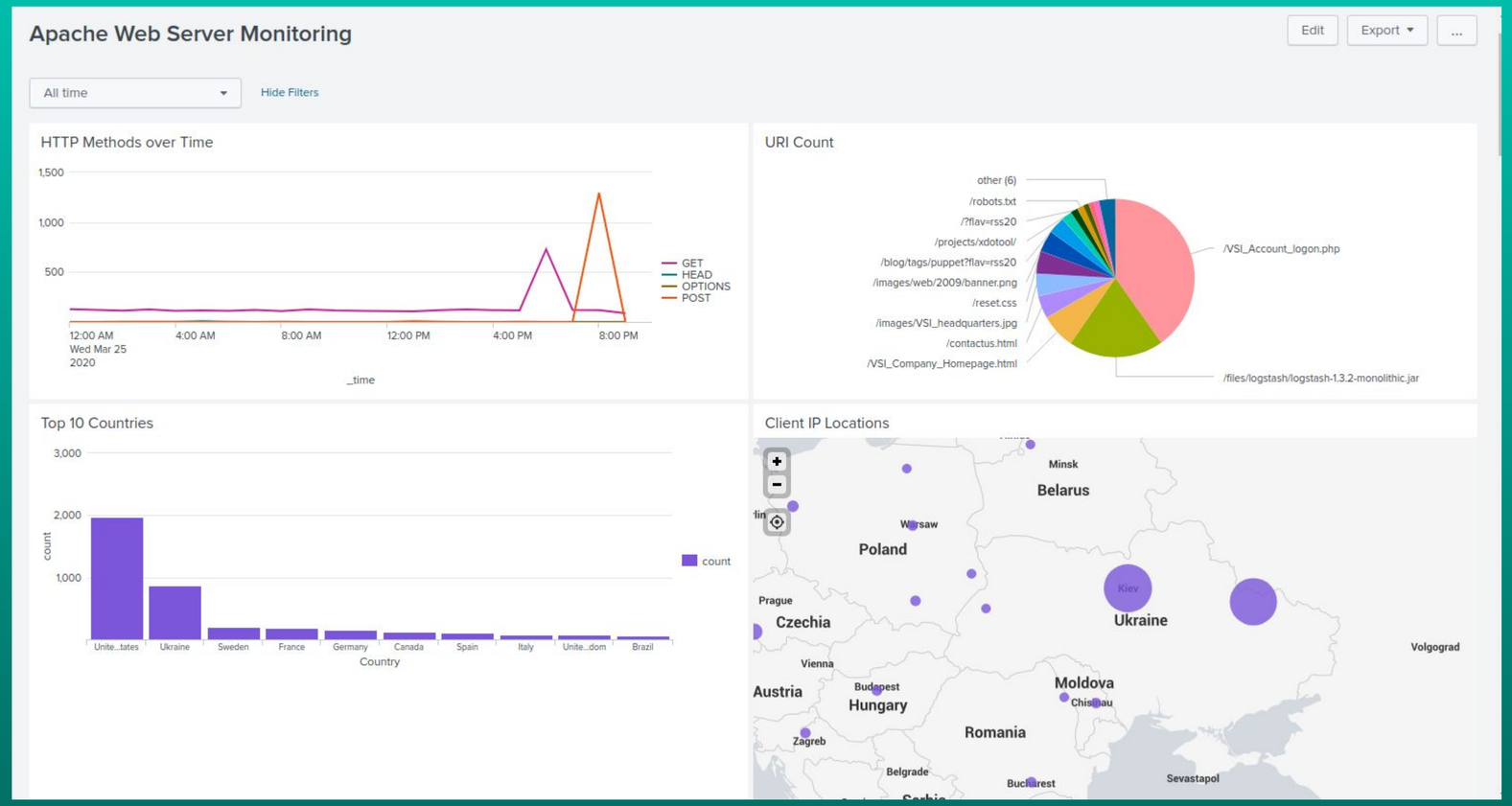


Attack Summary—Apache

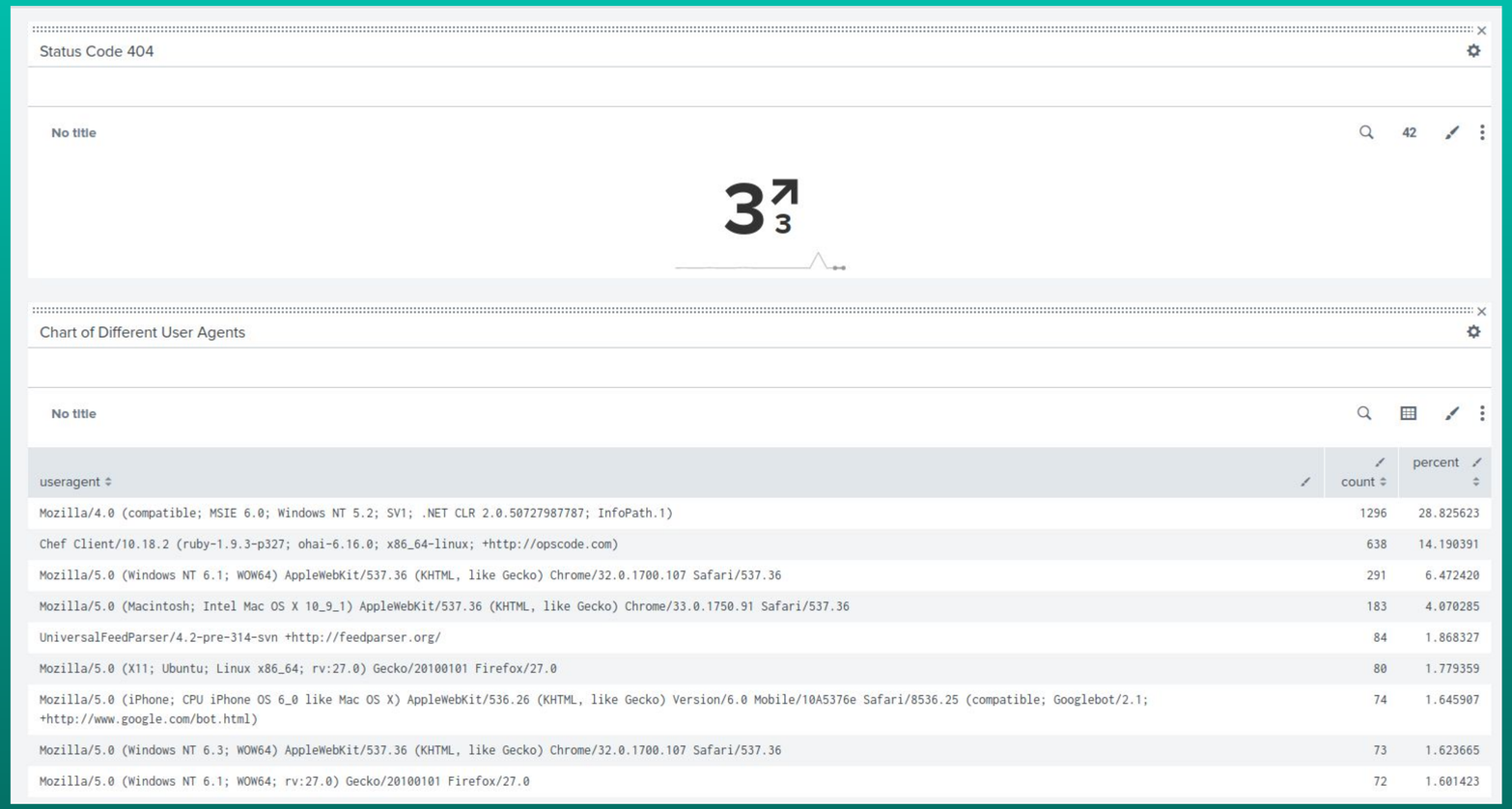
Summarize your findings from your dashboards when analyzing the attack logs.

- The HTTP dashboard has uncovered that the attacker leveraged both Get and Post methods during attack.
- During the Cluster Map analysis, we observed an increase in activity in Ukraine. Our analysis also identified two new cities, Kiev and Kharkiv, where this activity was observed.
- URI Data dashboard revealed that there was high activity on /VSI_Account_logon.php and /files/logstash/lo_3.2-monolithic.jar. Additionally, it was discovered that a brute force attack had taken place.

Screenshot of Apache Web Server Monitoring Dashboard Attack Log



Screenshot of Apache Web Server Monitoring Dashboard Attack Log



useragent	count	percent
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)	1296	28.825623
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)	638	14.190391
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	291	6.472420
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	183	4.070285
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	84	1.868327
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	80	1.779359
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)	74	1.645907
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	73	1.623665
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	72	1.601423

Summary and Future Mitigations

Project 3 Summary

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

  Our overall findings found that on March 25th, 2020 VSI experienced multiple attacks on both their Windows and Apache servers. There was a brute force attack and suspicious activity coming from Ukraine.

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

  - Limit the number of login attempts to protect from a brute force attack
  - Authenticate Users
  - Input Validation