Defensive Security - Project 3

Marko Jovanovic

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- We are a team working at a small company called **Virtual Space Industries (VSI)**
- We are working as SOC analysts
- **JobeCorp**, their competitor, may launch cyberattacks to disrupt business
- Our main goal is to monitor for potential attacks using Splunk
  - Monitoring includes: an Apache web server and a Windows operating system
- Using past logs we need to develop baselines, look for patterns and create reports

[“Add-On” App]

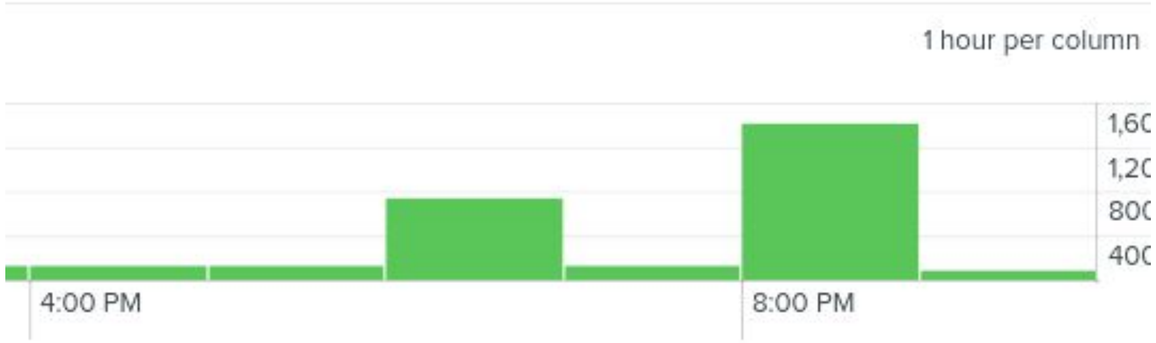
Whois XML IP Geolocation API

Whois XML IP Geolocation API is an API service which allows a us to identify our web visitors and their geographic location

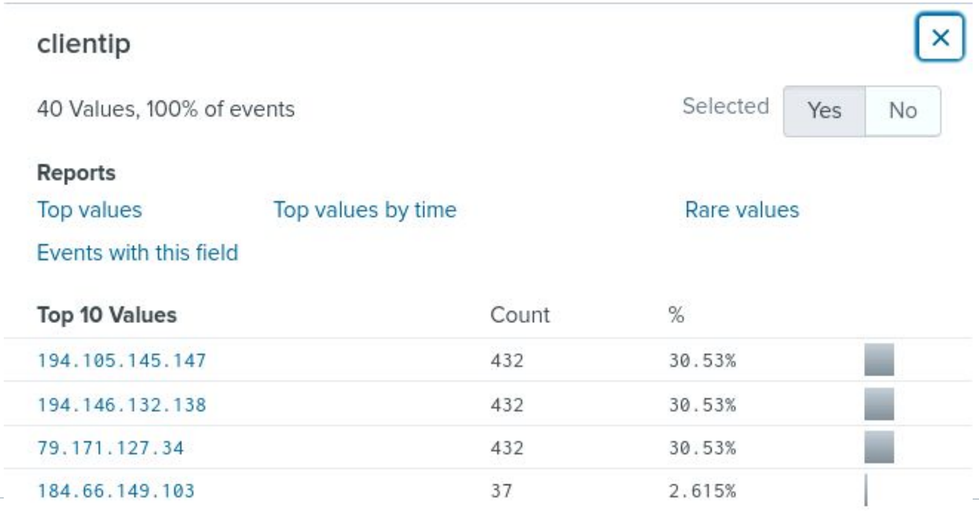
This should allow us to better identify where attacks are originating, which in turn will allow us to configure our Firewalls more accurately and will allow us to monitor our traffic better

Geolocation - Scenario

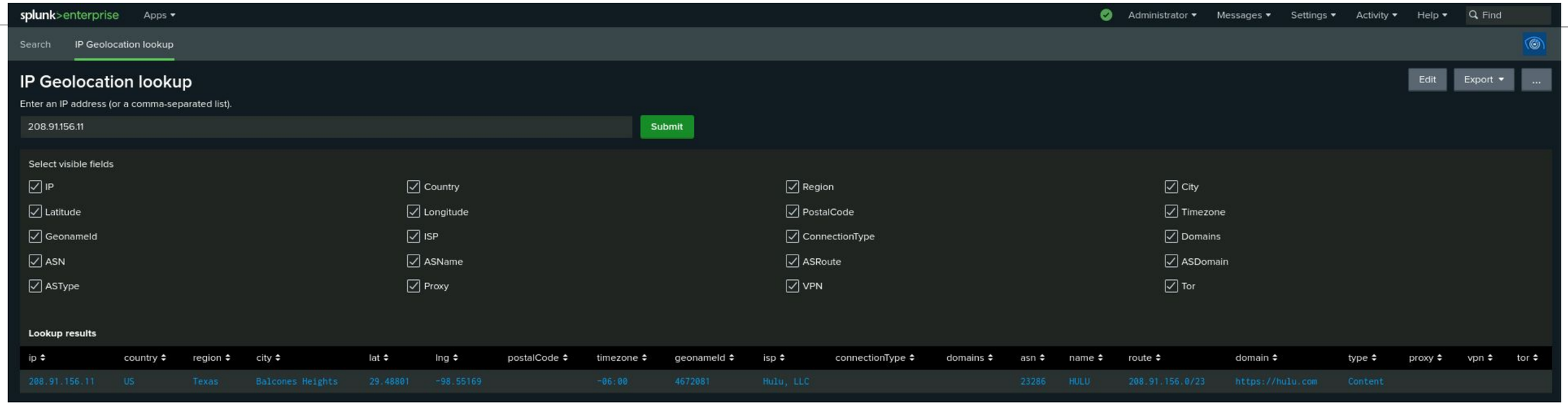
While analyzing the attacked apache server data, we found a suspicious spike in web traffic at 6:00 PM and 8:00 PM

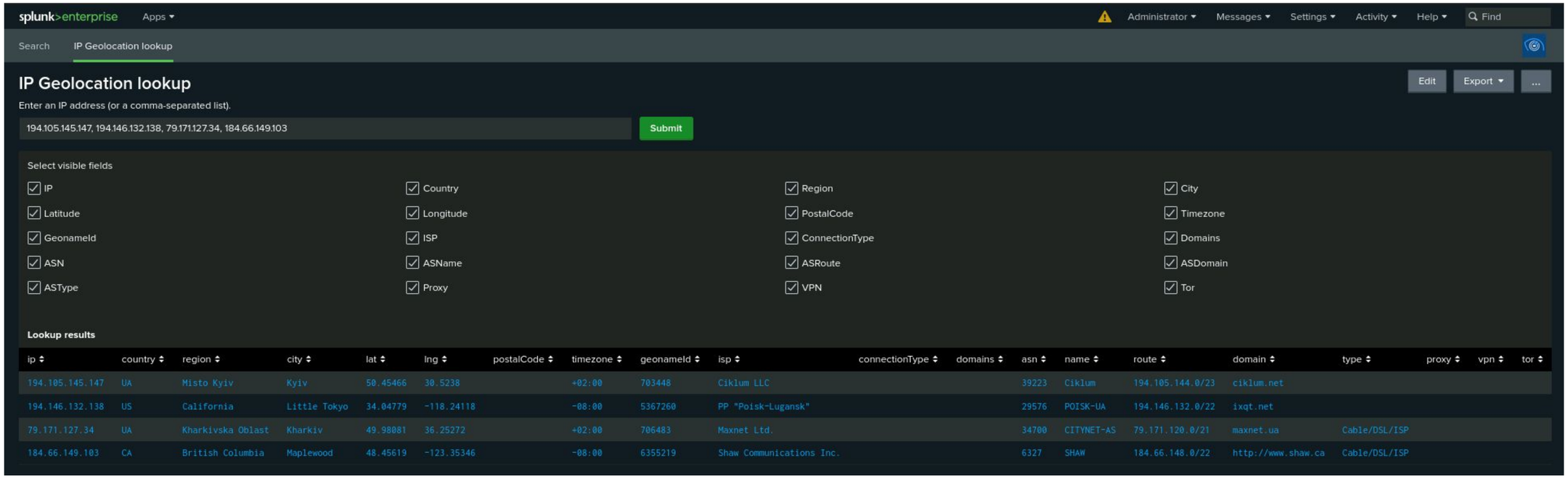


Knowing this, we can choose to analyse the IPs with the most events at those time periods



Geolocation - Results





Logs Analyzed

1 Windows Logs

These logs contain the intellectual property of VSI's next generation virtual reality programs.

- User Information
- Login Data
- Command signatures

2 Apache Logs

These logs contain the event data of VSI's main public-facing website, vsi-company.com. Data includes:

- HTTP method request information
- HTTP response codes
- user IPs and location
- URIs (Uniform Resource Identifiers)

Windows Logs

Windows Reports

Designed the following reports:

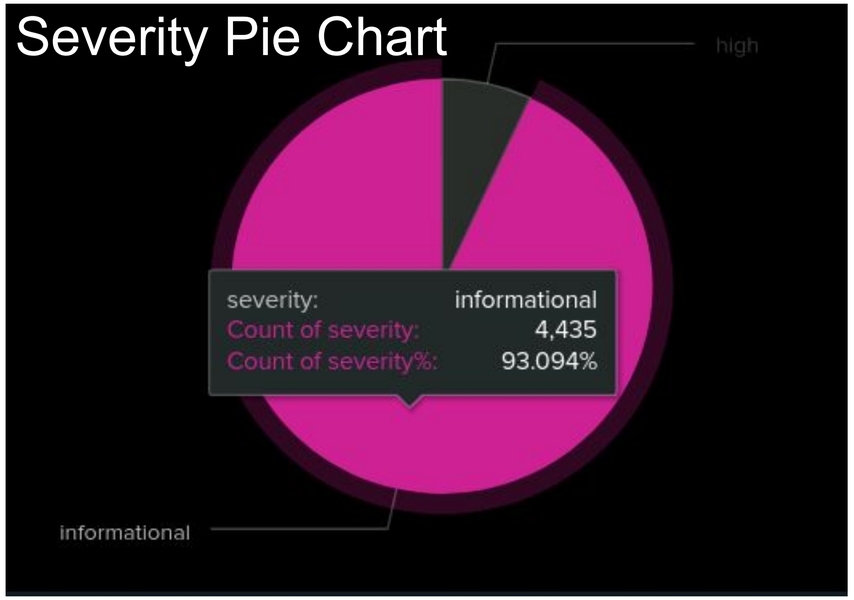
Report Name	Report Description
Signatures & Associated Signature ID’s	shows ID number associated with the specific signatures for Windows activity
Severity Levels	displays severity levels, count and percentage of each for Windows logs being viewed.
Success & Failure levels	comparison between the success and failure of Windows activities. Helps to point out suspicious levels of failed activities on the server.

Images of Windows Reports

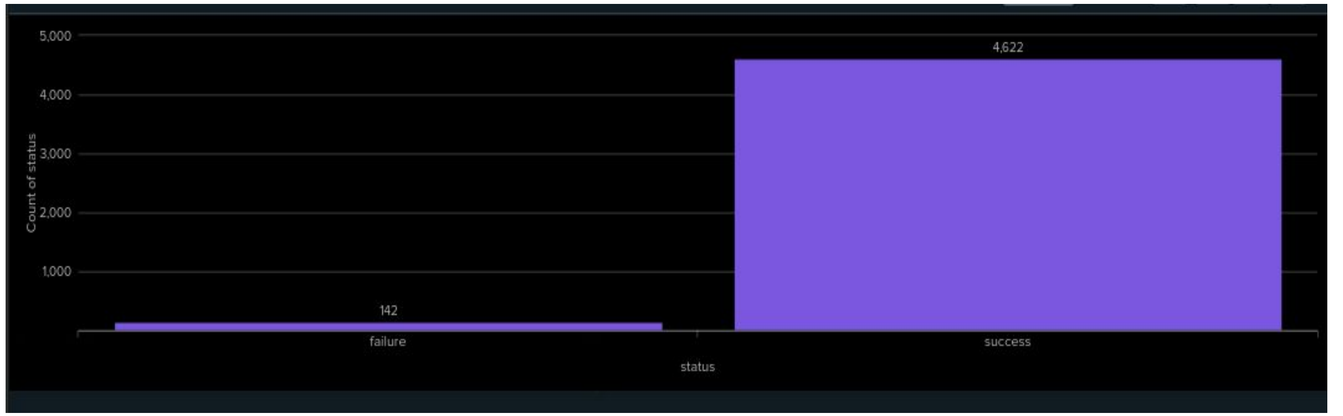
Signatures & ID’s

i	_time	signature	signature_id
›	3/24/20 11:46:27.000 PM	The audit log was cleared	1102
›	3/24/20 11:45:38.000 PM	System security access was removed from an account	4718
›	3/24/20 11:56:40.000 PM	System security access was granted to an account	4717
›	3/24/20 11:57:51.000 PM	Special privileges assigned to new logon	4672
›	3/24/20 11:54:25.000 PM	Domain Policy was changed	4739
›	3/24/20 11:56:41.000 PM	An attempt was made to reset an accounts password	4724
›	3/24/20 11:57:54.000 PM	An account was successfully logged on	4624
›	3/24/20 11:54:39.000 PM	A user account was locked out	4740
›	3/24/20 11:59:54.000 PM	A user account was deleted	4726
›	3/24/20 11:59:53.000 PM	A user account was created	4720
›	3/24/20 11:50:07.000 PM	A user account was changed	4738
›	3/24/20 11:48:36.000 PM	A process has exited	4689
›	3/24/20 11:54:46.000 PM	A privileged service was called	4673
›	3/24/20 11:54:42.000 PM	A logon was attempted using explicit credentials	4648
›	3/24/20 11:59:31.000 PM	A computer account was deleted	4743

Severity Pie Chart



Success & Failure Status

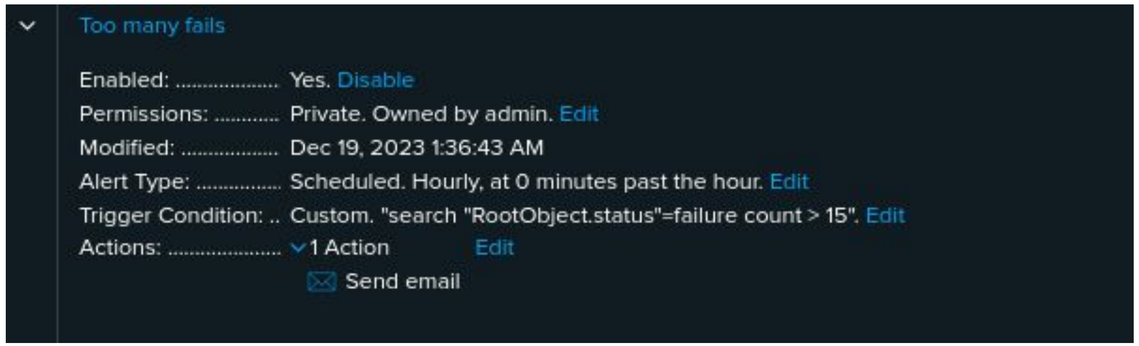


Windows Alert 1

Design the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	alerts when the hourly threshold for failed suspicious activity has been reached	2-9	failure count over 15

JUSTIFICATION: Failed hourly windows activity typically stays within the range of 2-9, peaking at 9. We felt that 15 was a good number for being overly suspicious and out of range.

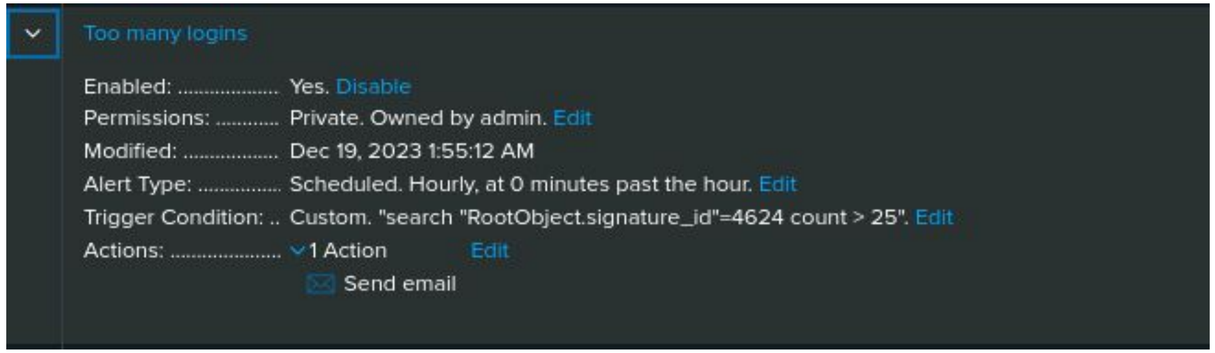


Windows Alert 2

We created the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Too many successful logins	alerts when the threshold of too many hourly successful logins have been reached	12-21	“an account was successfully logged on” > 25

JUSTIFICATION: Average successful logins range from 12-21 hourly, so we thought that 25 would be a good number to deem as suspicious but not too far from the peak of 21.

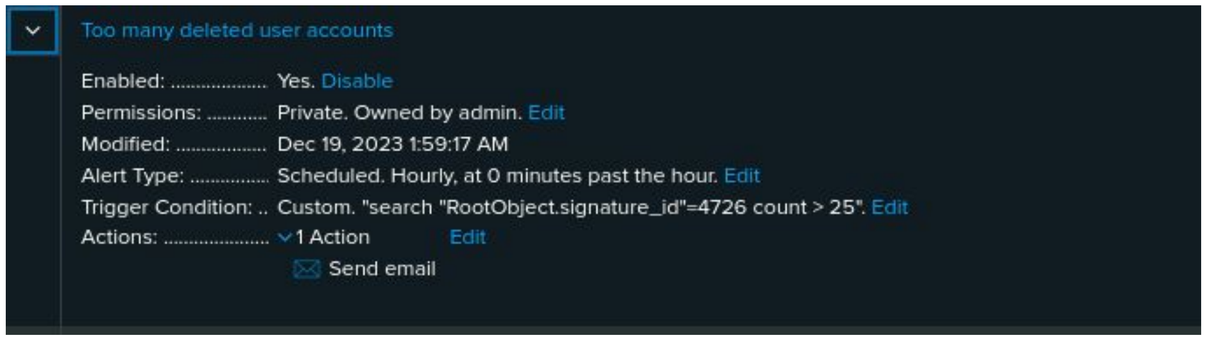


Windows Alert 3

Designed this following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Too many user accounts deleted	alerts when a suspicious amount of accounts have been deleted within an hour	7-22	“a user account was deleted” > 25

JUSTIFICATION: Within an hour we observed 7-22 user accounts get deleted. We set a threshold of 25 because too many deleted accounts is suspicious and should be flagged.



Windows Dashboard

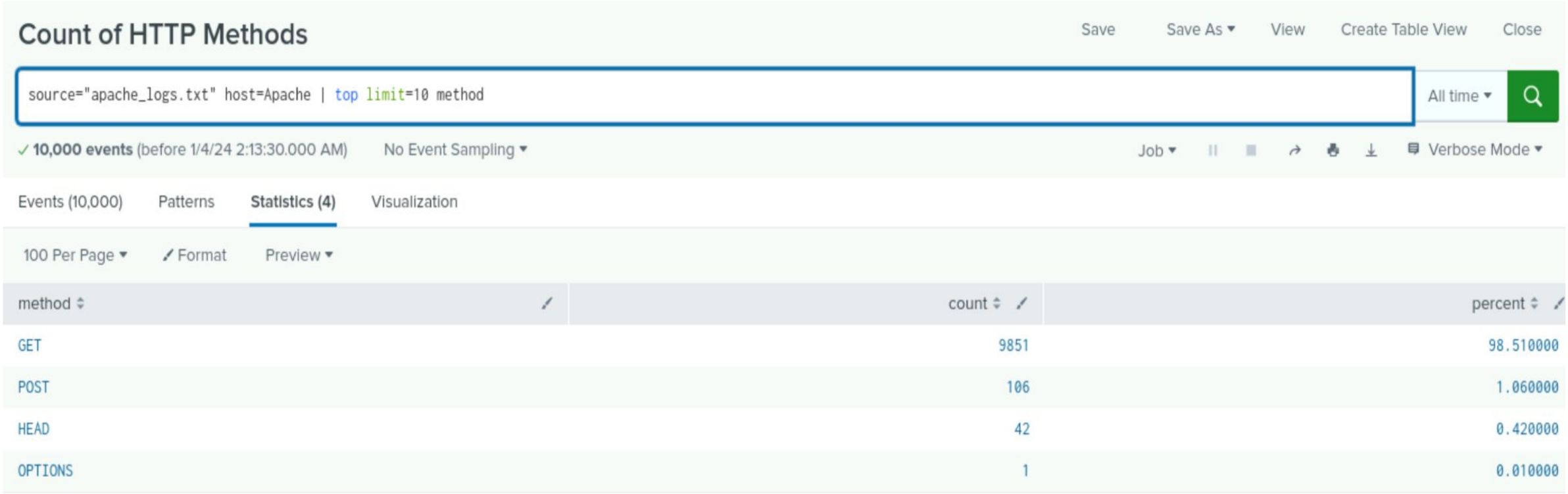
Apache Logs

Apache Reports

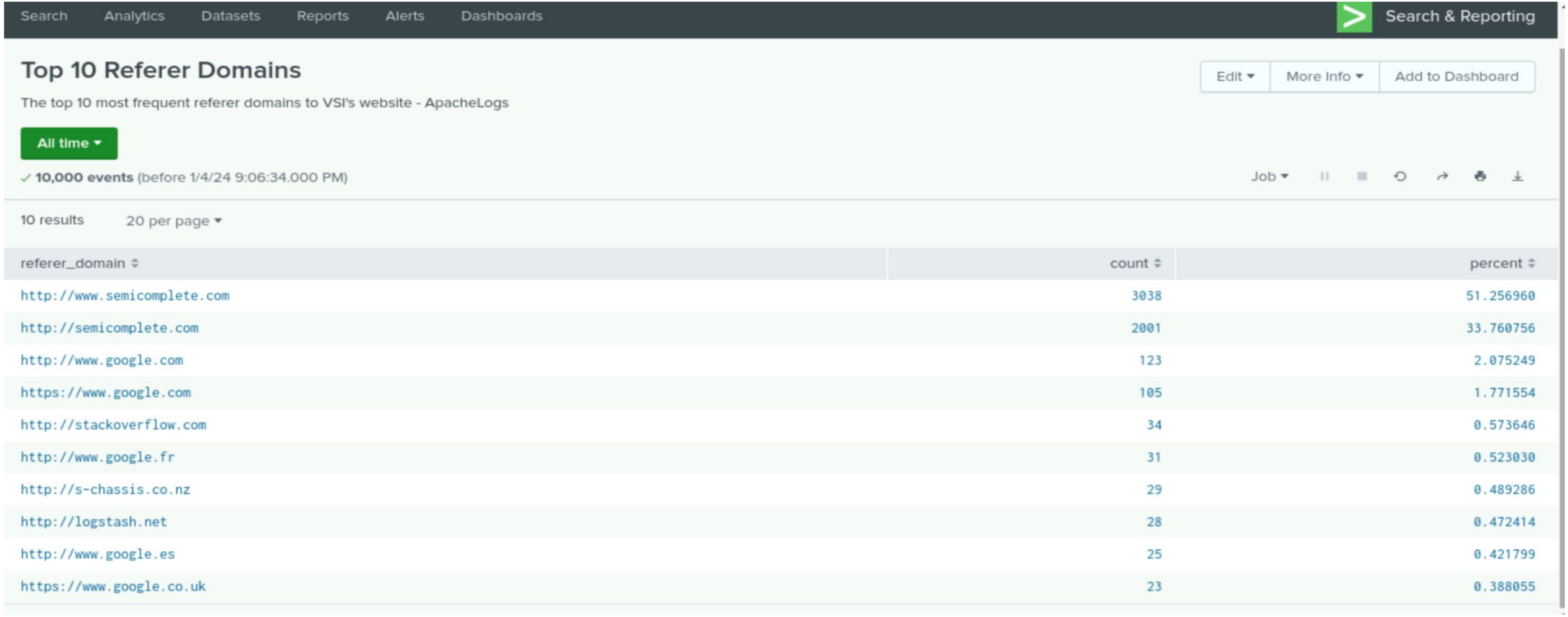
Designed the following reports:

Report Name	Report Description
Count of HTTP Methods	Displays a statistical count of different HTTP methods and how frequently they are used
HTTP Status	A count of each HTTP response code
Top 10 Referer Domain	The top 10 most used referrer domains to the VSI’s website

Report - HTTP Method Count

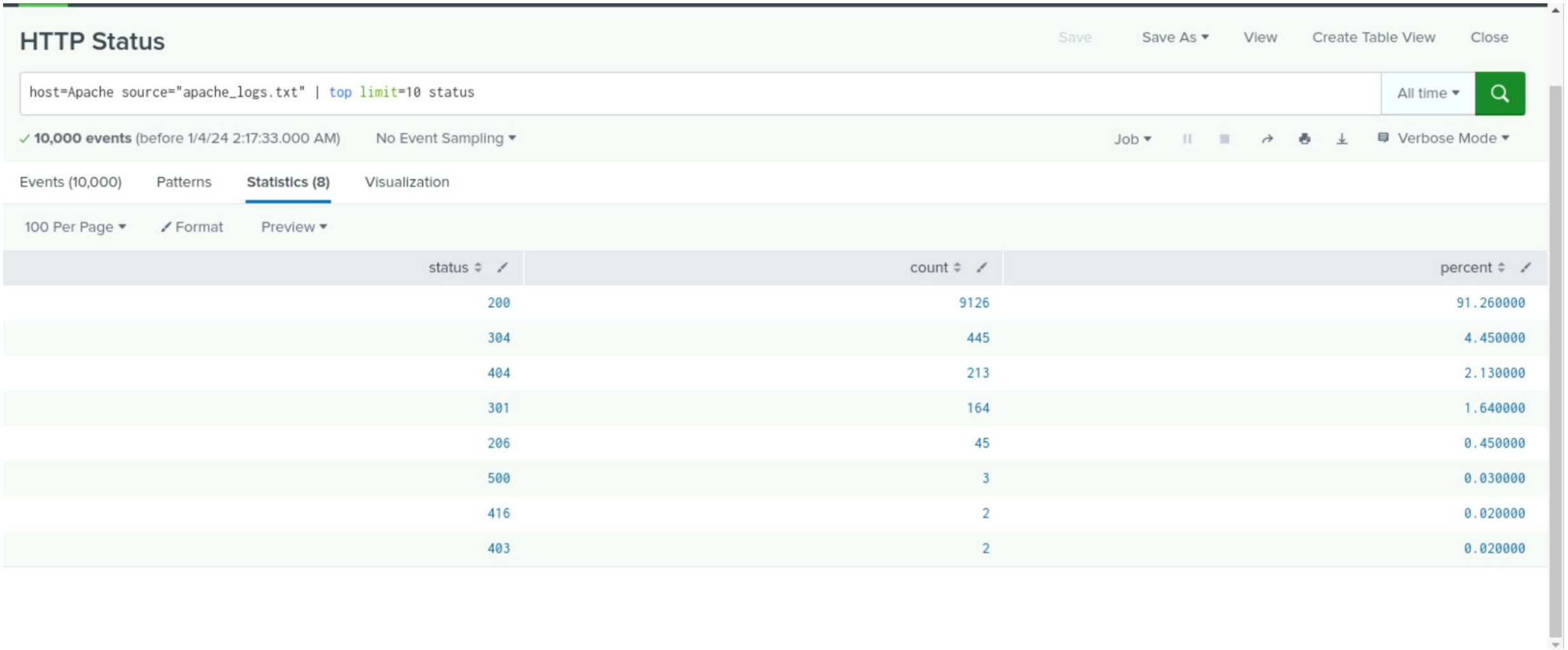


Report - Top 10 Referrer Domains



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



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

Apache Alert 1

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Alert	alert for hourly activity of HTTP POST requests that exceeds the threshold	74-136	160

JUSTIFICATION: Hourly HTTP POST requests range from 74-136. We decided to add the median of the baseline to the top end, which results in a threshold of 160. This leaves room for increased POST activity (to avoid false positives), while establishing a threshold for suspiciously high activity that could be potentially be malicious.

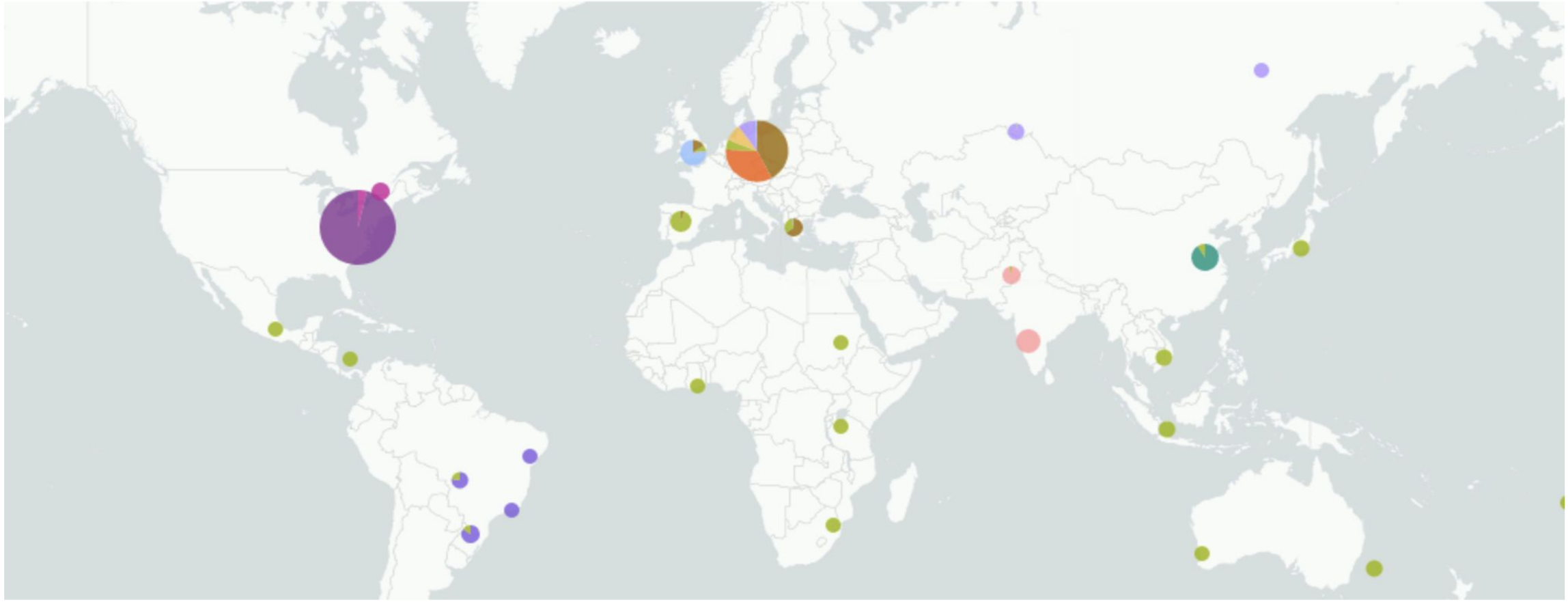
Apache Alert 2

Designed the following alerts:

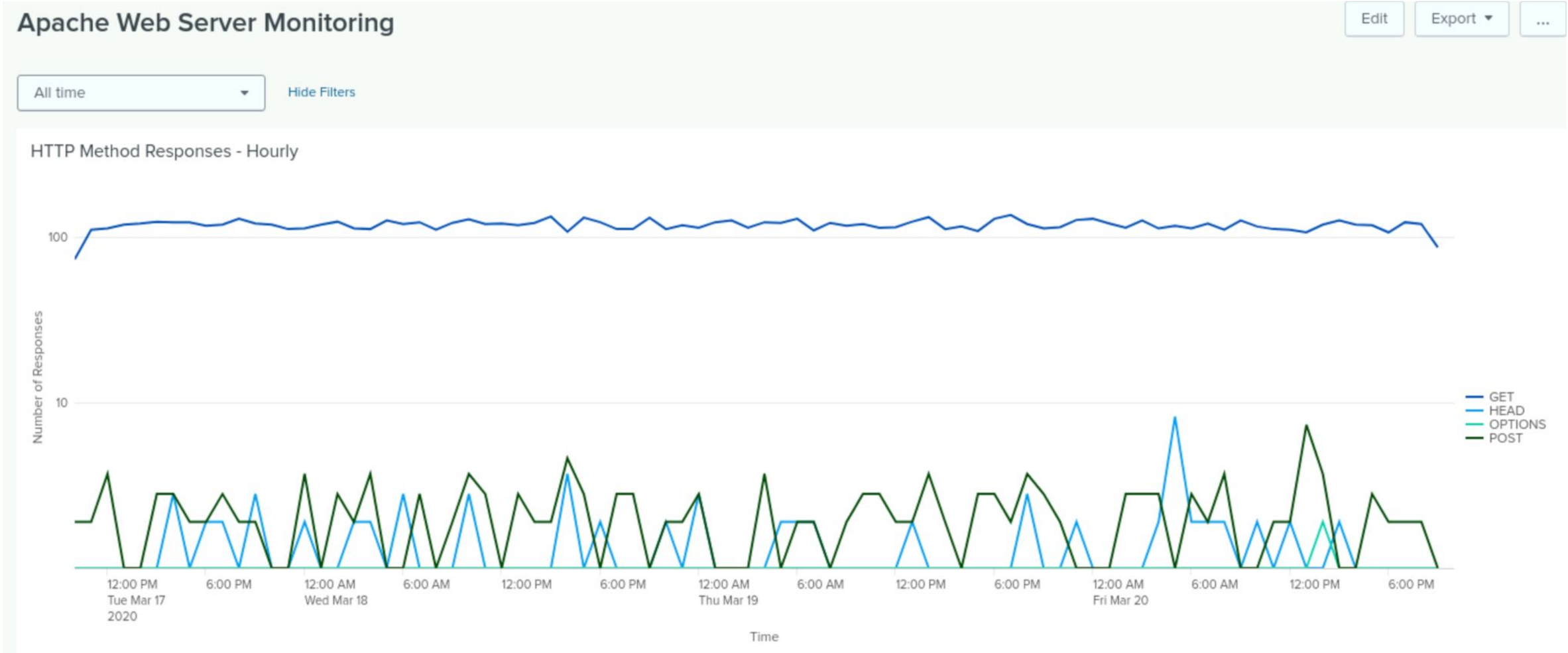
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity Alert (Excluding United States)	Every hour there is a report notifying the activity levels	1-120	160

JUSTIFICATION: Hourly activity ranges from 1-120. We added approximately 1.5 standard deviations to the top end of the baseline, which results in a threshold of 160. This leaves room for some increased international activity (to avoid false positives), while establishing a threshold for suspiciously high activity that could potentially be malicious.

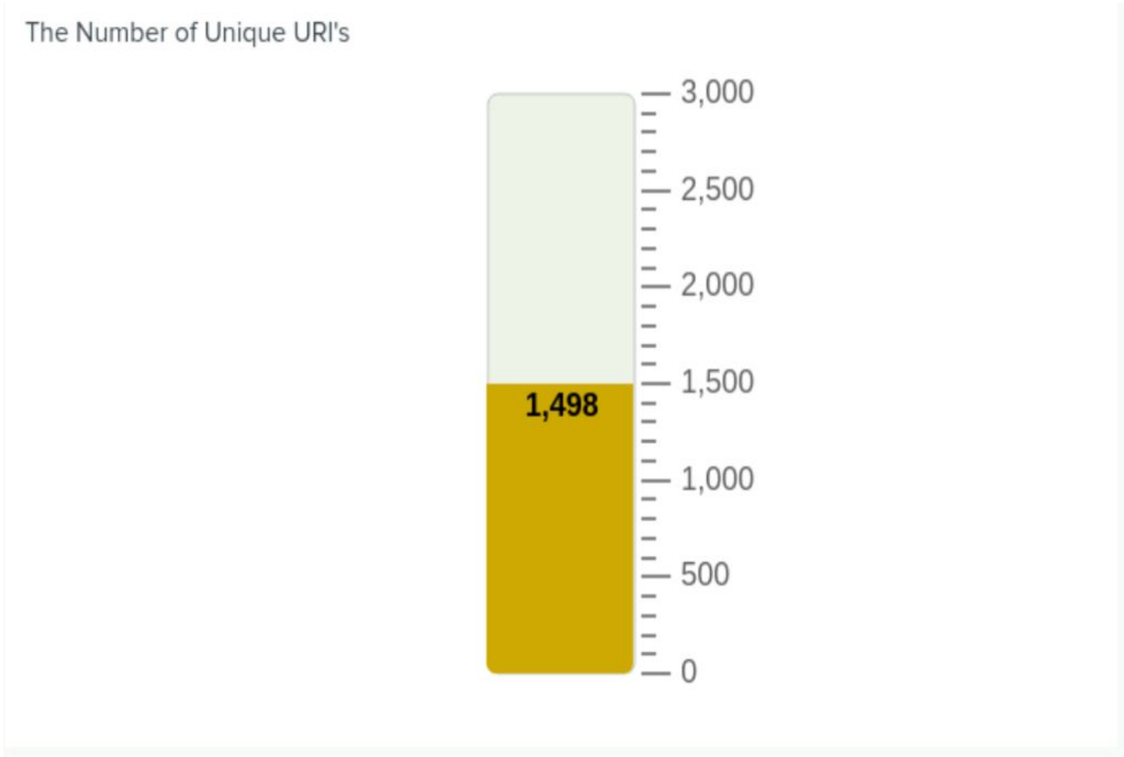
Apache Dashboard - Cluster Map

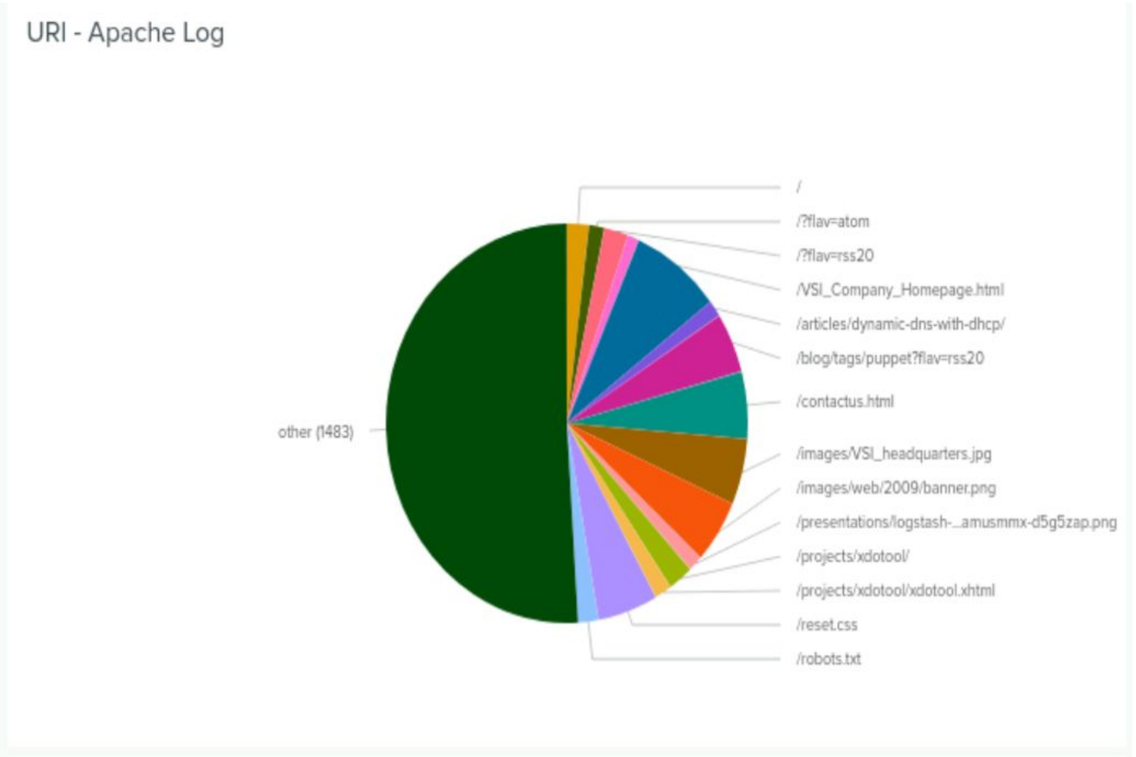


Apache Dashboard - HTTP Method Responses



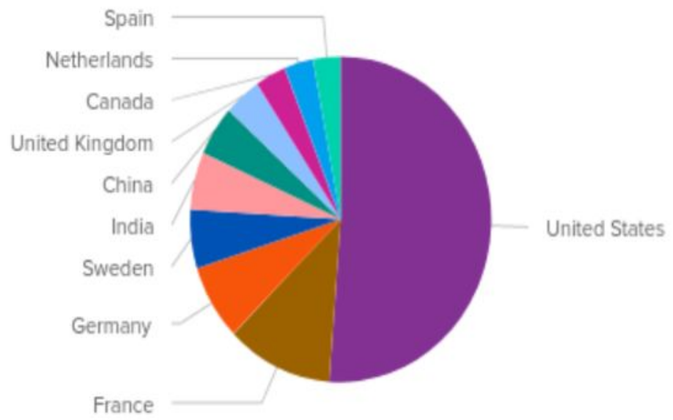
Apache Dashboard - URIs





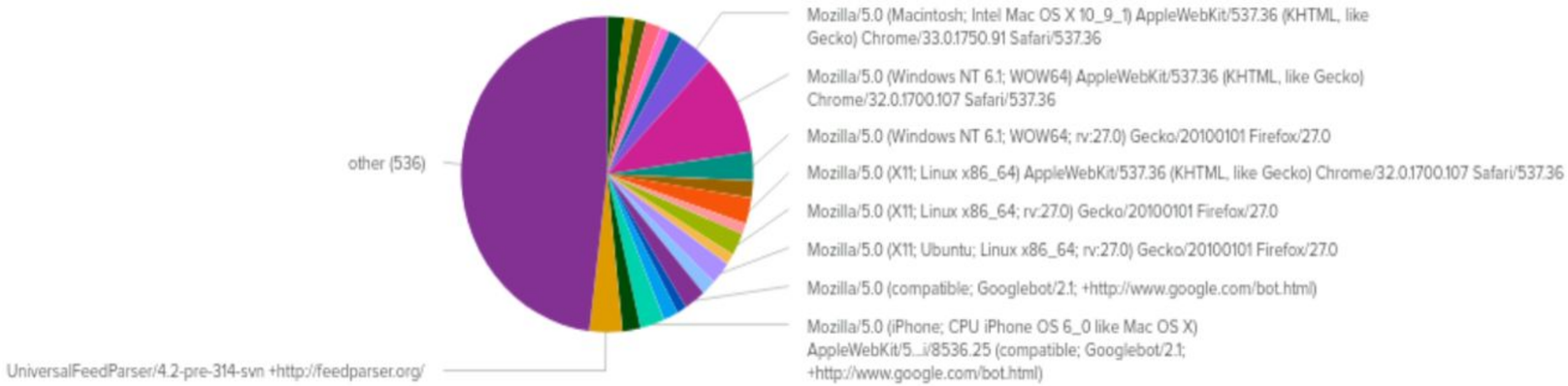
Dashboard - Miscellaneous

Top 10 Countries in Log



Number of POST Requests

Count of Different User Agents



Windows Attack Summary

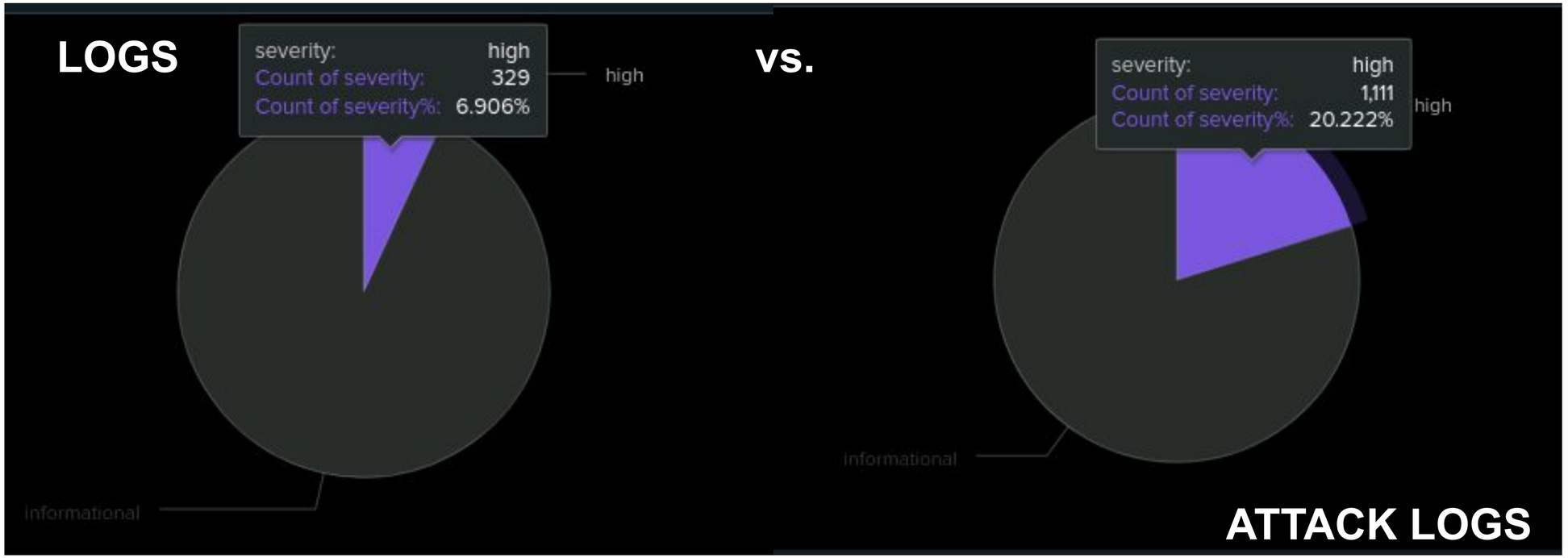
Windows Attack Summary

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

compared to the previous logs, the attack logs have a higher percentage of high severity.

Windows Attack Summary

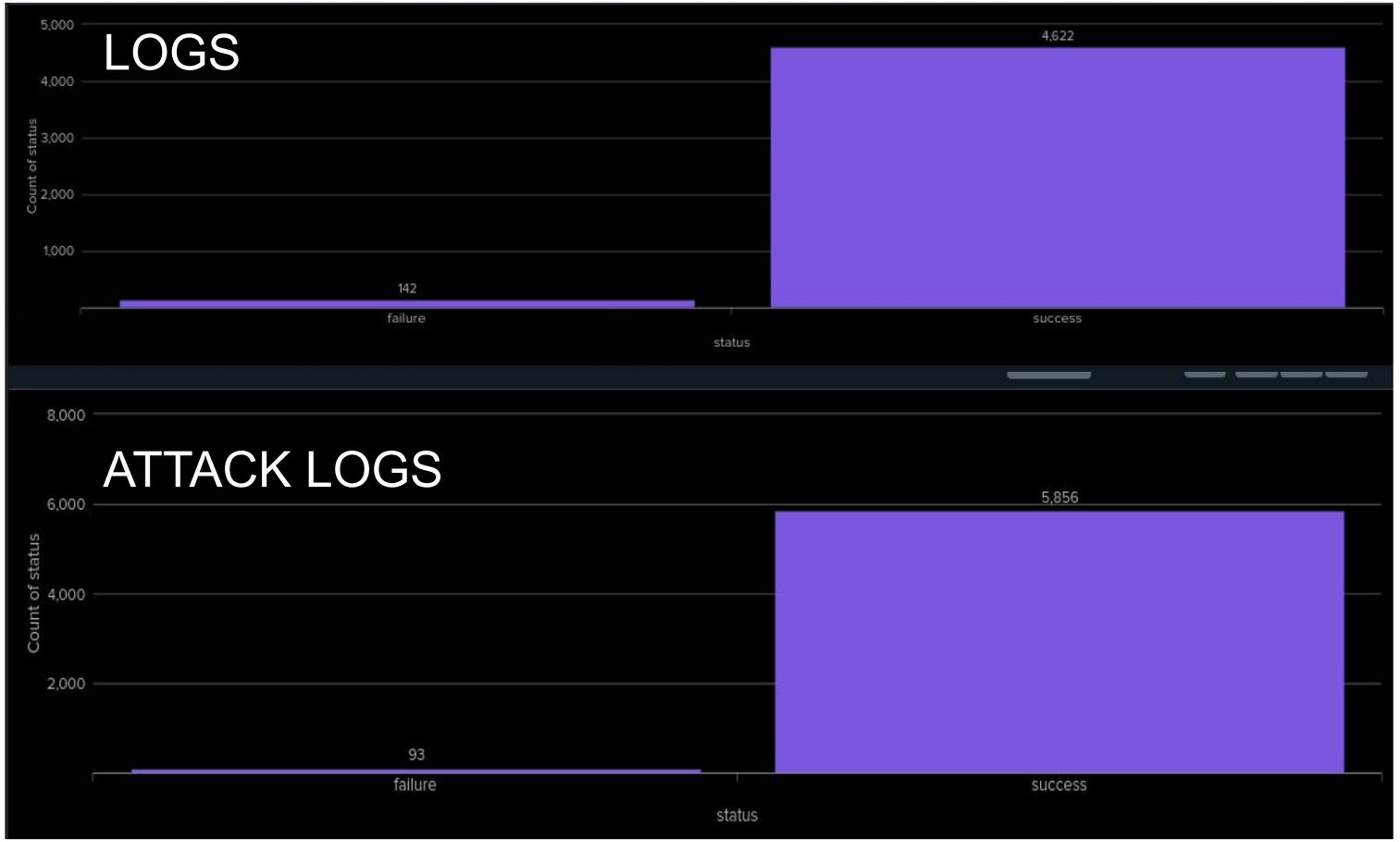
- Summarize your findings from your reports when analyzing the attack logs.



compared to the previous logs, the attack logs have a higher percentage of high severity.

Windows Attack Summary

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



compared to the previous logs, the attack logs have increased counts of success, by around a thousand.

This can indicate that there were higher amounts of attackers accessing the server.

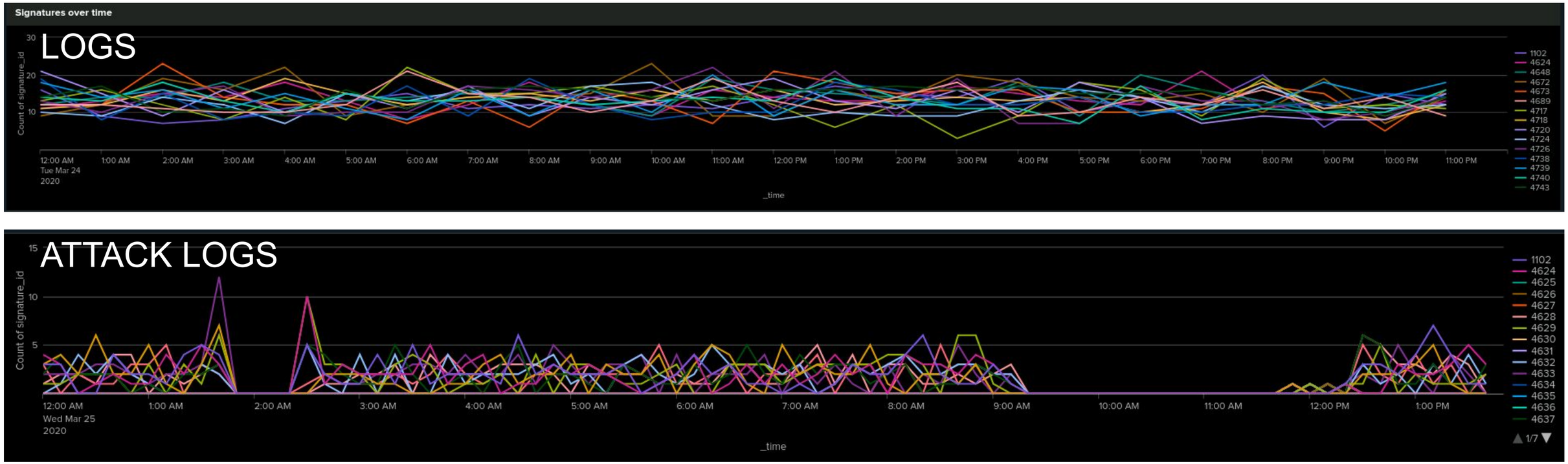
Windows Attack Summary

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

- No, because none of our alerts were triggered.
  - Our thresholds were too high
  - Will lower thresholds for future threats

Windows Attack Summary

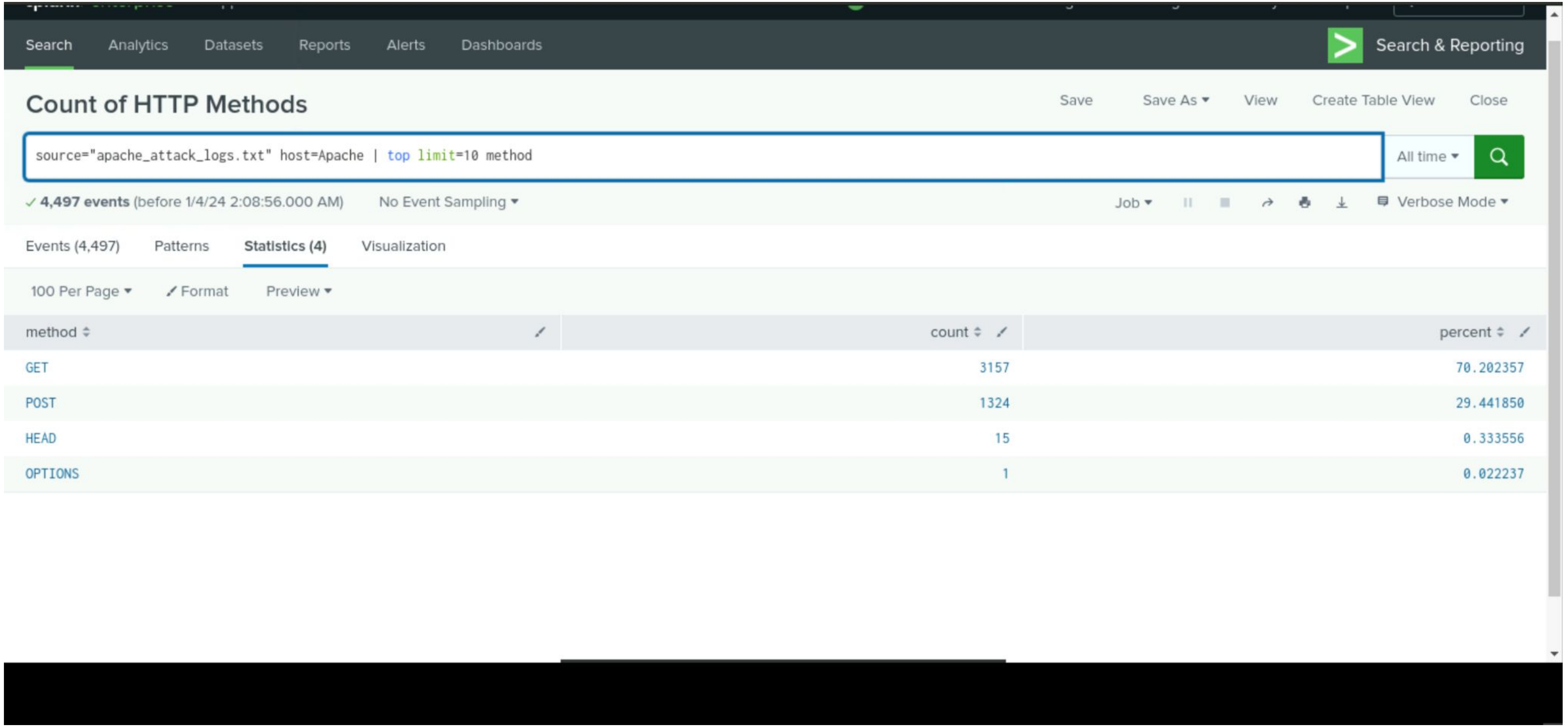
Summarize your findings from your dashboards when analyzing the attack logs.



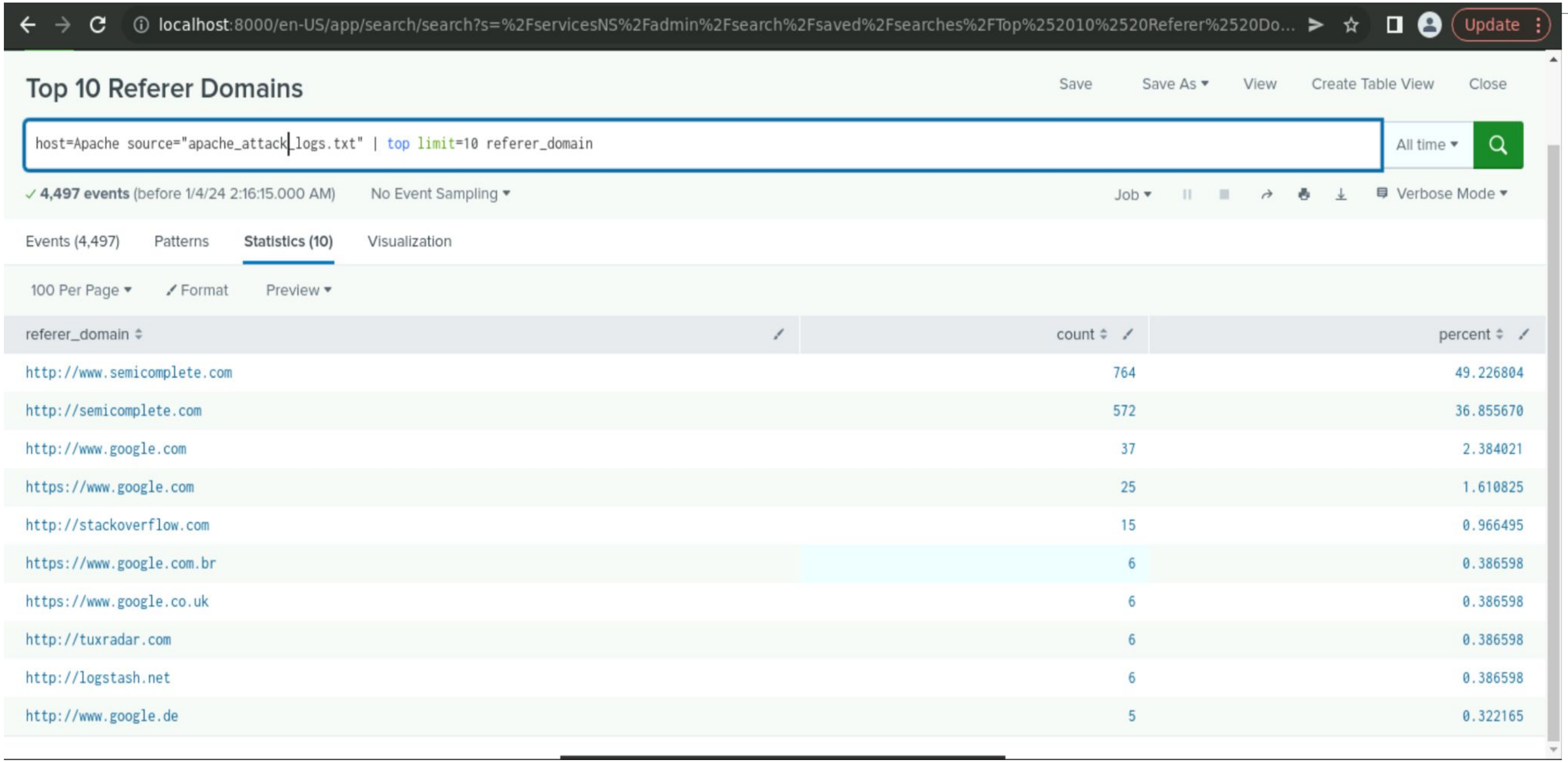
compared to the previous logs, the attack logs indicate spaces of no activity, due to denial of service attack - preventing users from logging in.

Apache Attack Logs

Screenshots of Attack Logs - HTTP Methods

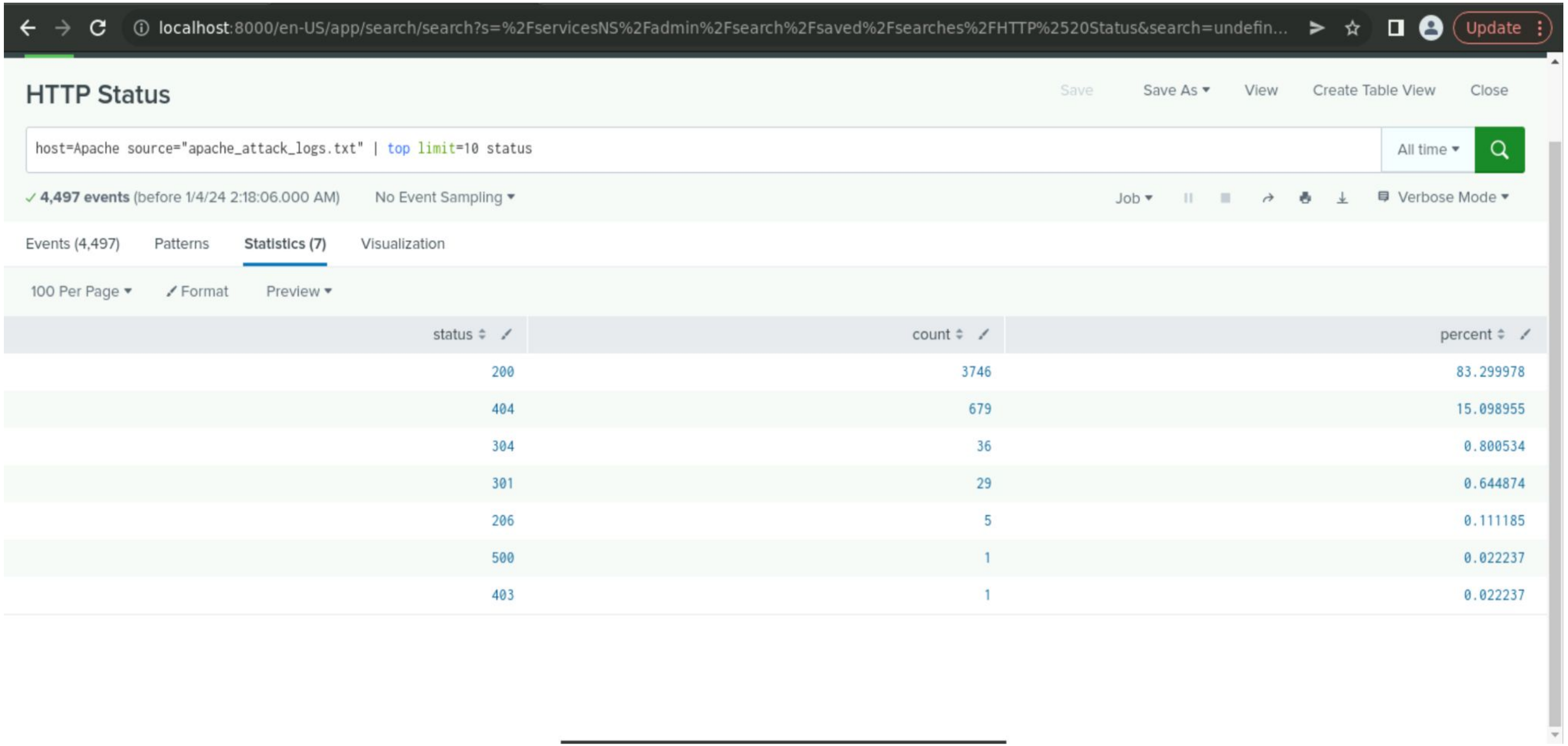


Referrer Domains



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

HTTP Response Codes



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

Apache Attack Summary

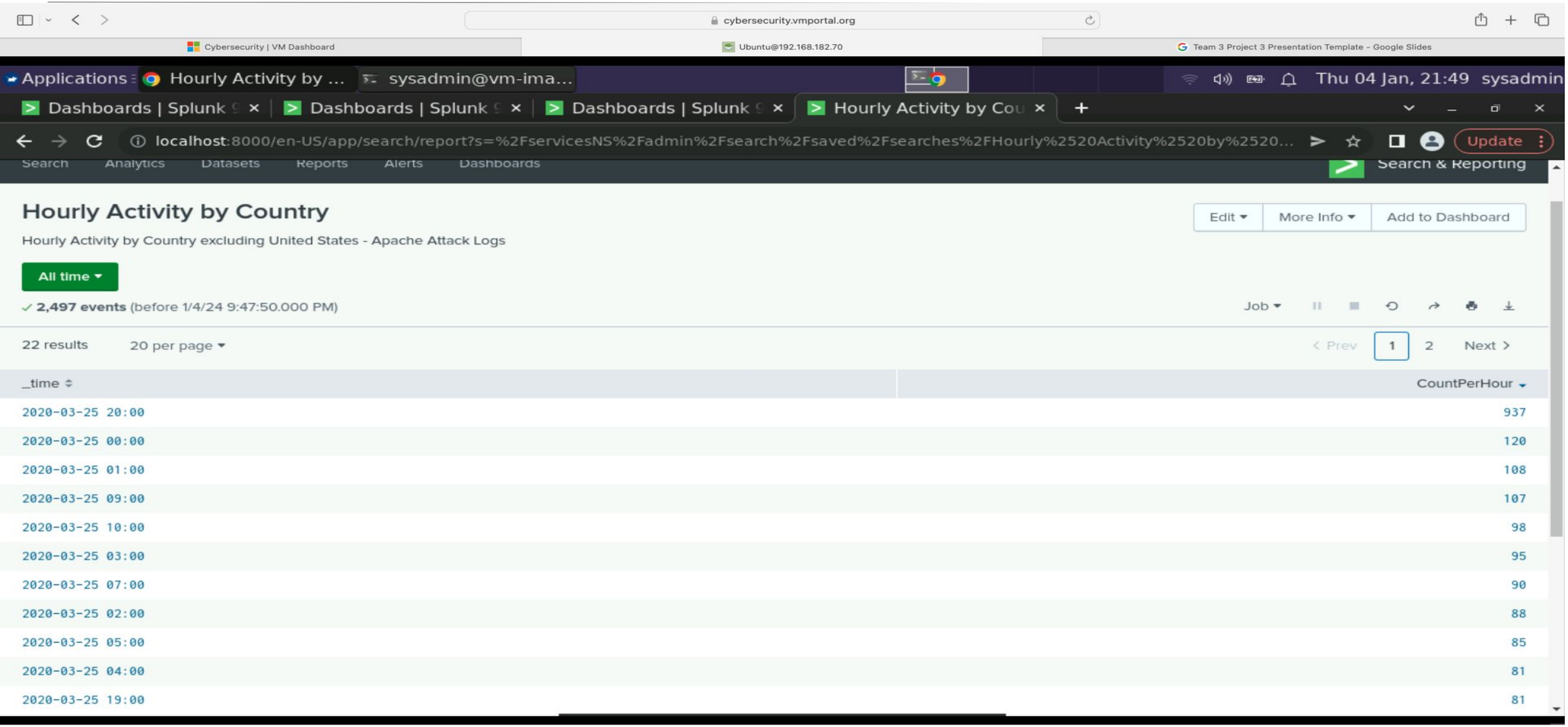
Summarize your findings from your reports when analyzing the attack logs.

- We witnessed a massive increase in the amount of POST requests, indicating some sort of attack (potentially DOS, brute force, injection attacks, cross-site scripting)

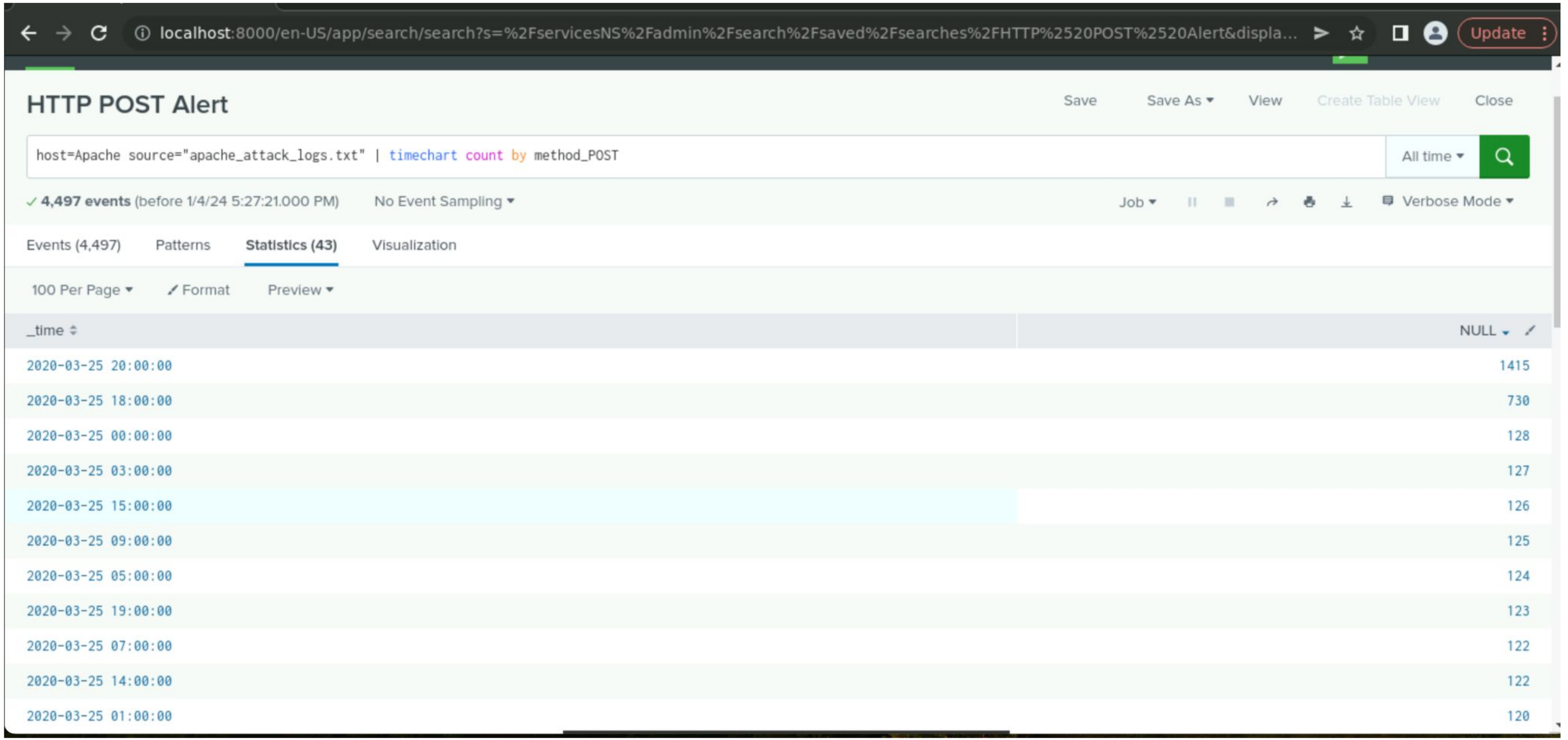
- Referrer domains don’t look suspicious at first glance (at least the top 2 results). Further investigation is required to locate anything suspicious.

- Drastic spike of 404 http error codes (from about 2.13% to over 15% of the time). Could be marker of DOS/DDOS attack as resources come offline.

Hourly Activity Alert - Countries excl. United States



HTTP POST Alert



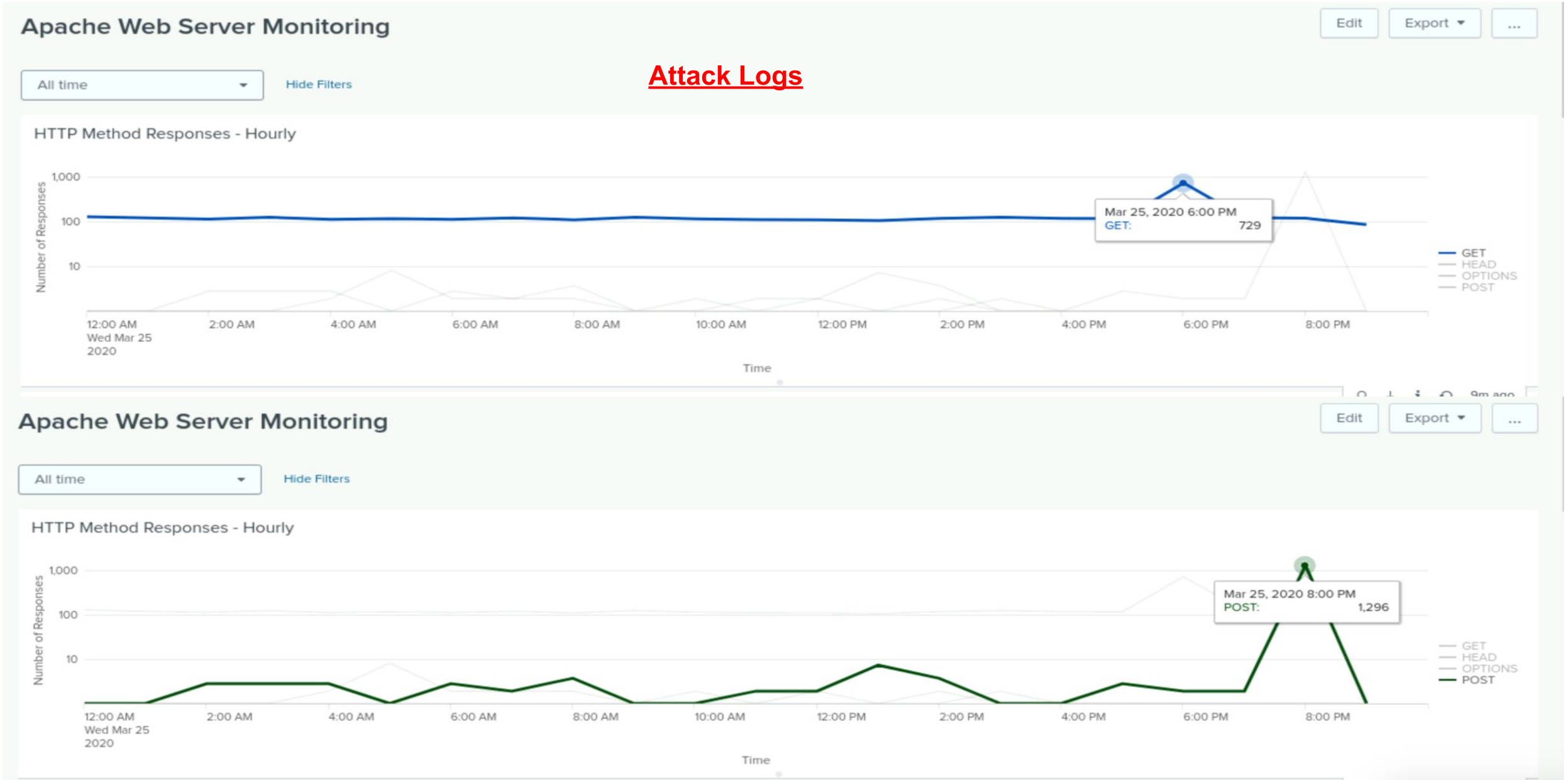
Apache Attack Summary

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

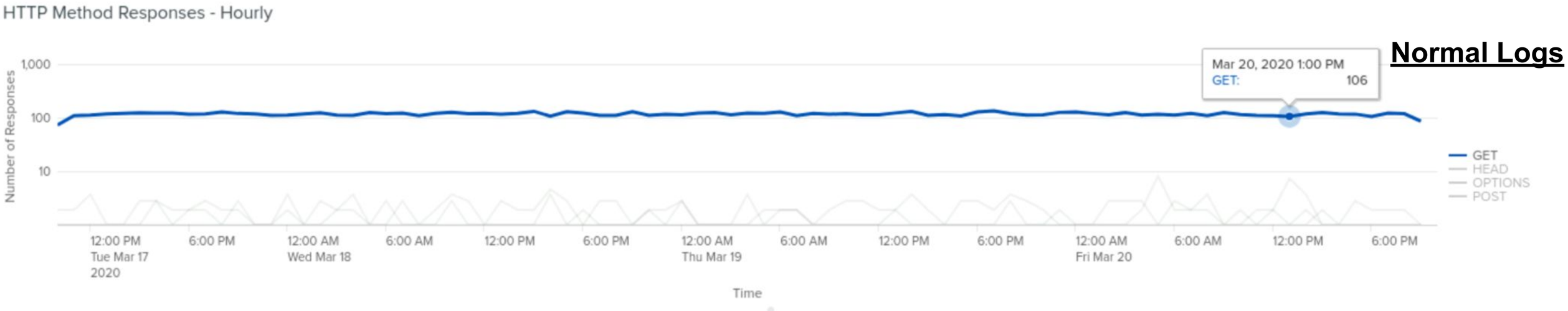
- Hourly Activity - we noticed a significant jump in hourly activity on March 25, 2020 at 8 PM. 937 is the count that was logged, which drastically breached the alert threshold of 160. For now, we will keep this alert, as the next highest count was within the original baseline.

- HTTP POST - beginning at 6 PM on the same date, we witnessed a huge increase in POST requests (730). At 8 PM, we noticed an even steeper spike in POST requests (1415). It also breached our threshold and triggered an alert. The 3rd count value down (128) fell within the baseline, so it seems our threshold is appropriately placed, for the time being.

Dashboard Analysis - HTTP Methods

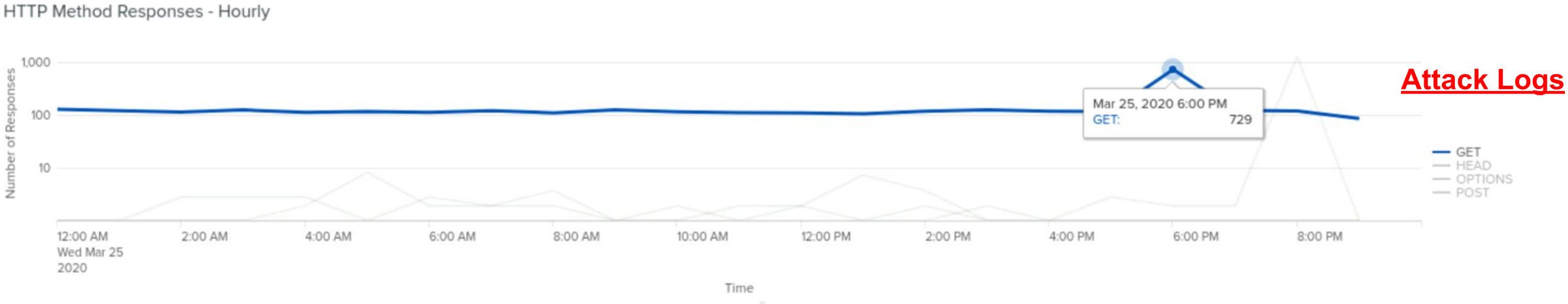


Dashboard Analysis - HTTP GET Request Comparison



Normal Logs

GET requests see a significant spike at 6 PM, from an average of just over 100 all the way up to 729

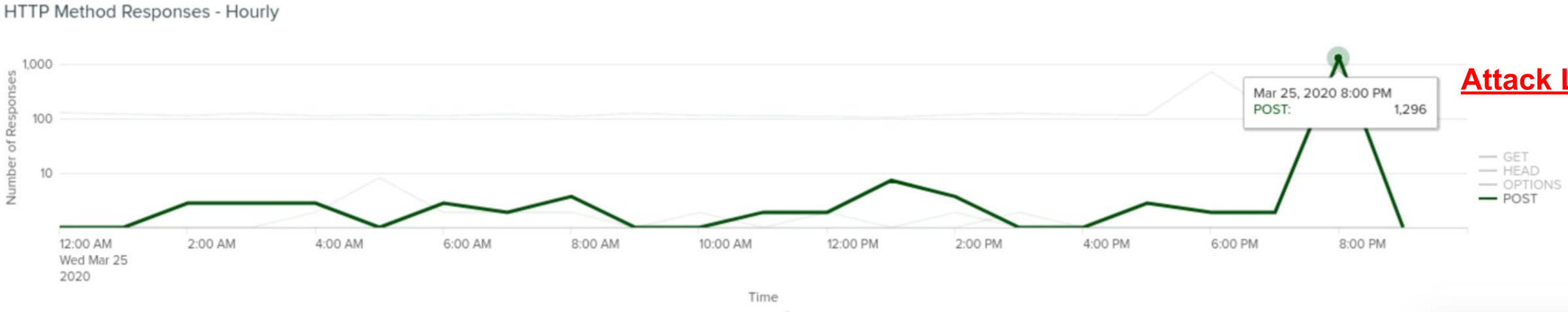


Attack Logs

Dashboard Analysis - HTTP POST Request Comparison

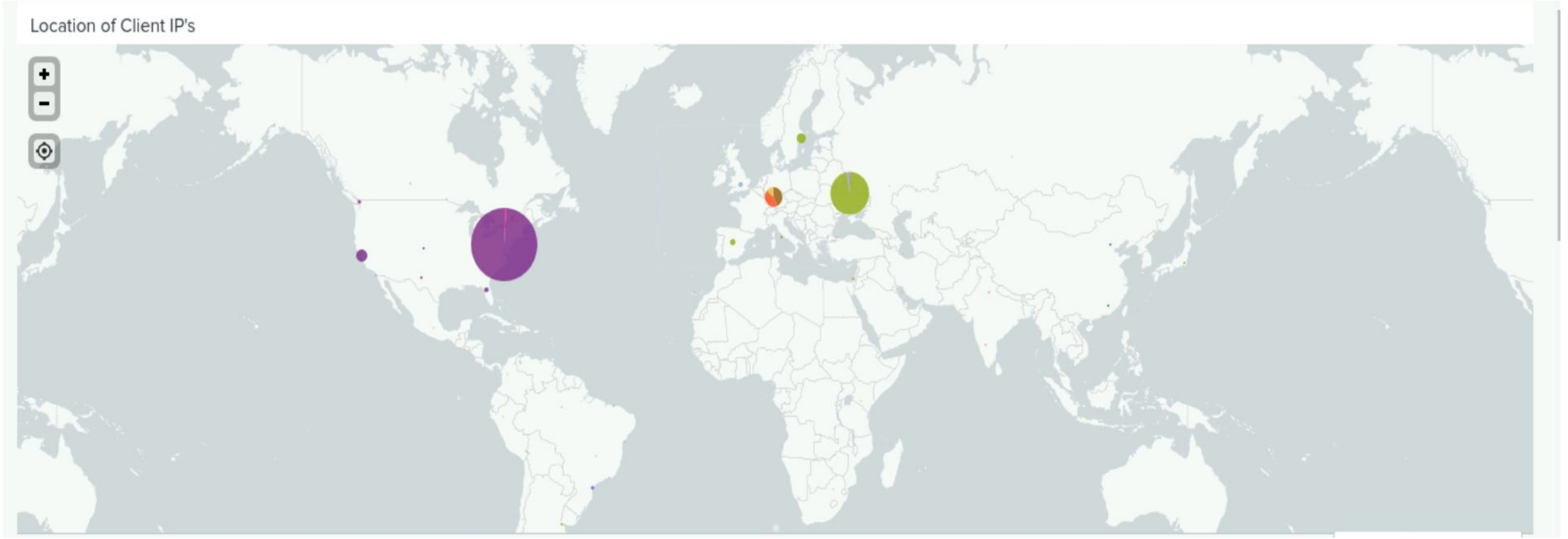
Normal Logs

POST requests see a drastic spike at 8 PM, from an average of below 10 all the way up to 1296

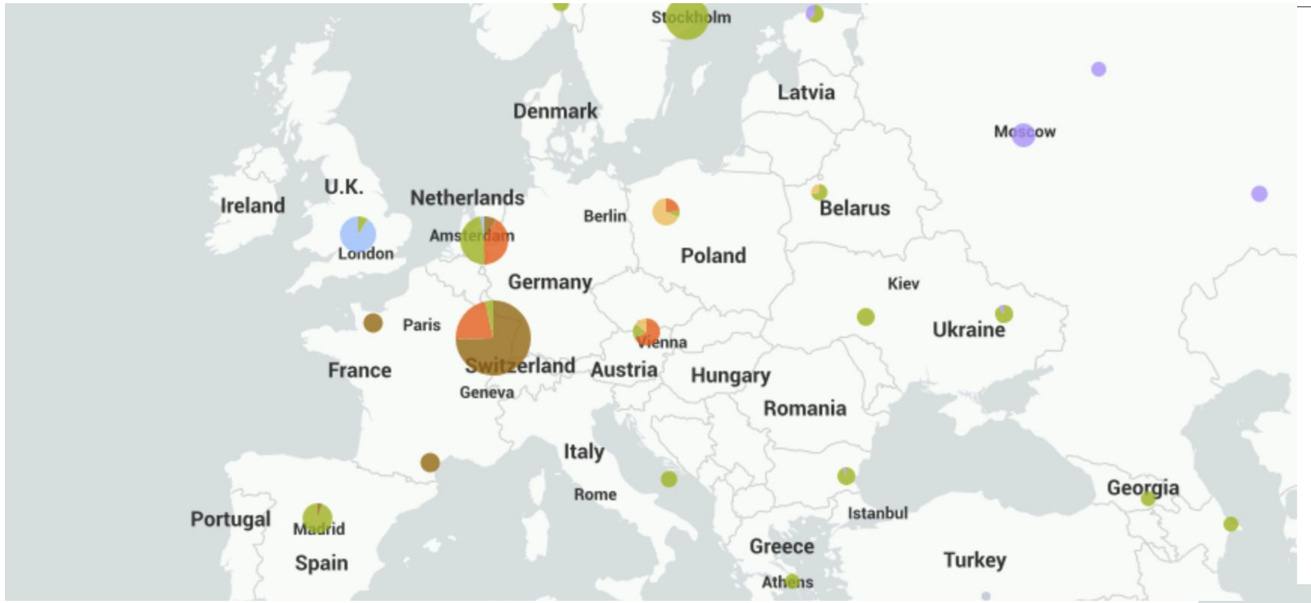


Attack Logs

Dashboard Analysis - Cluster Map



Dashboard Analysis - Cluster Map Europe

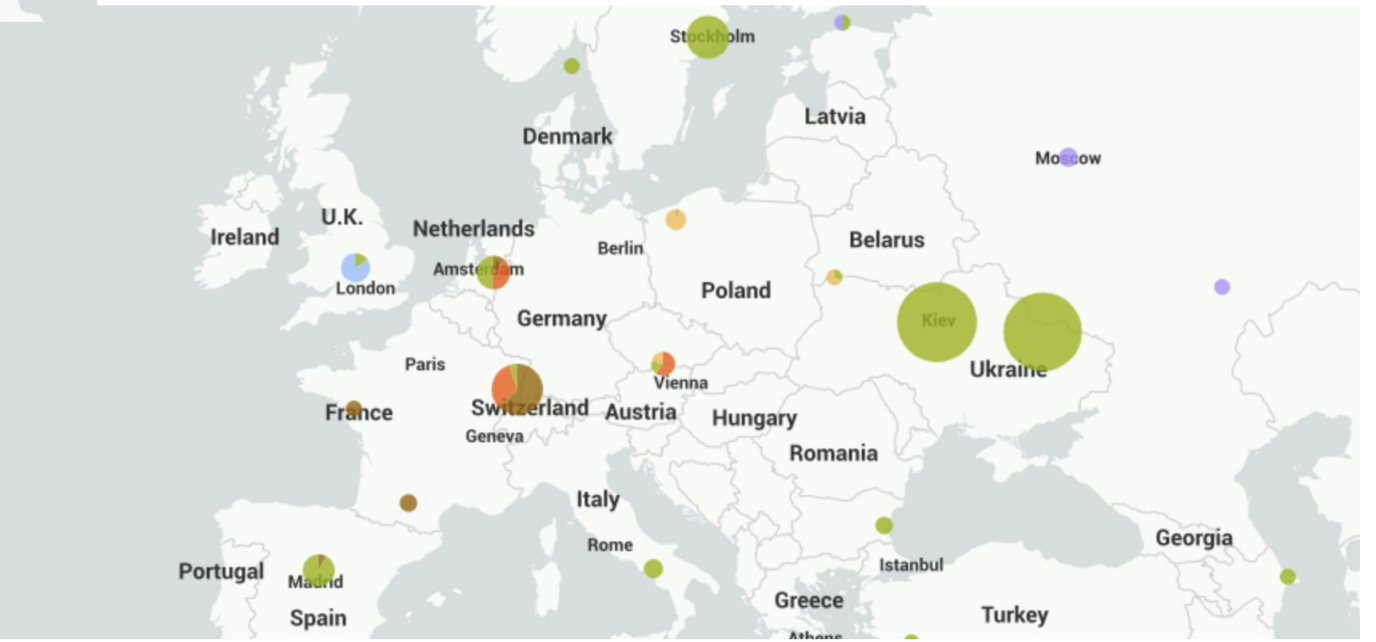


Normal Logs

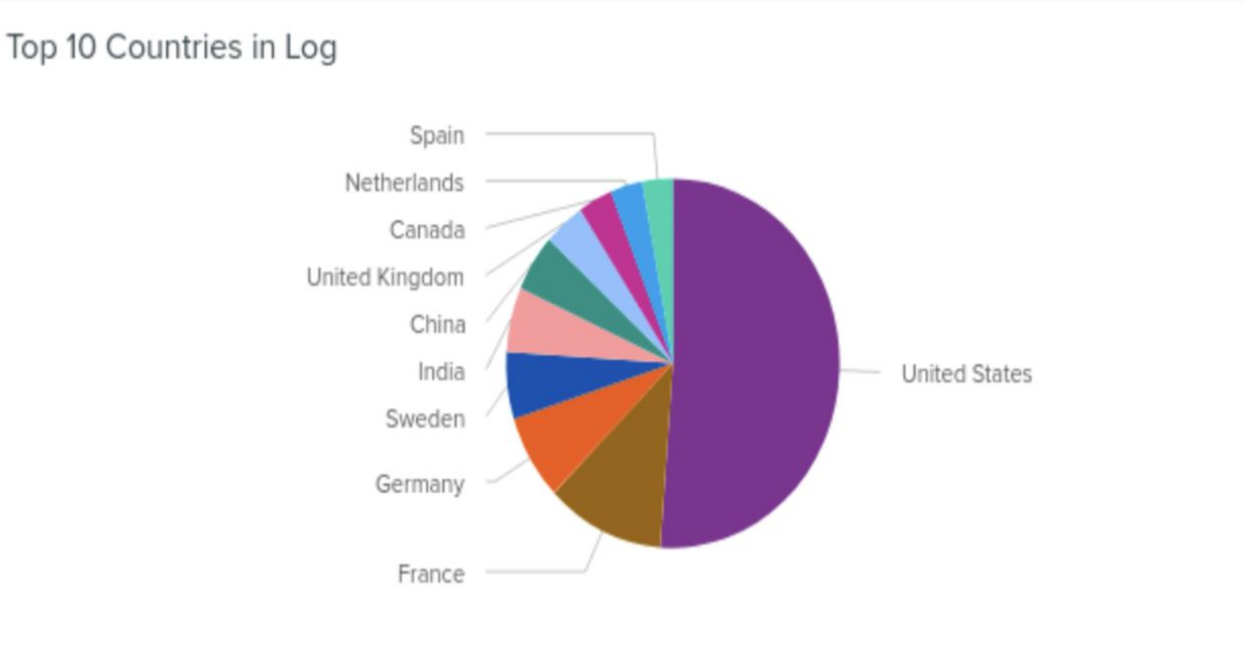
We simultaneously see an unusually significant drop in activity from most other regions within Europe.

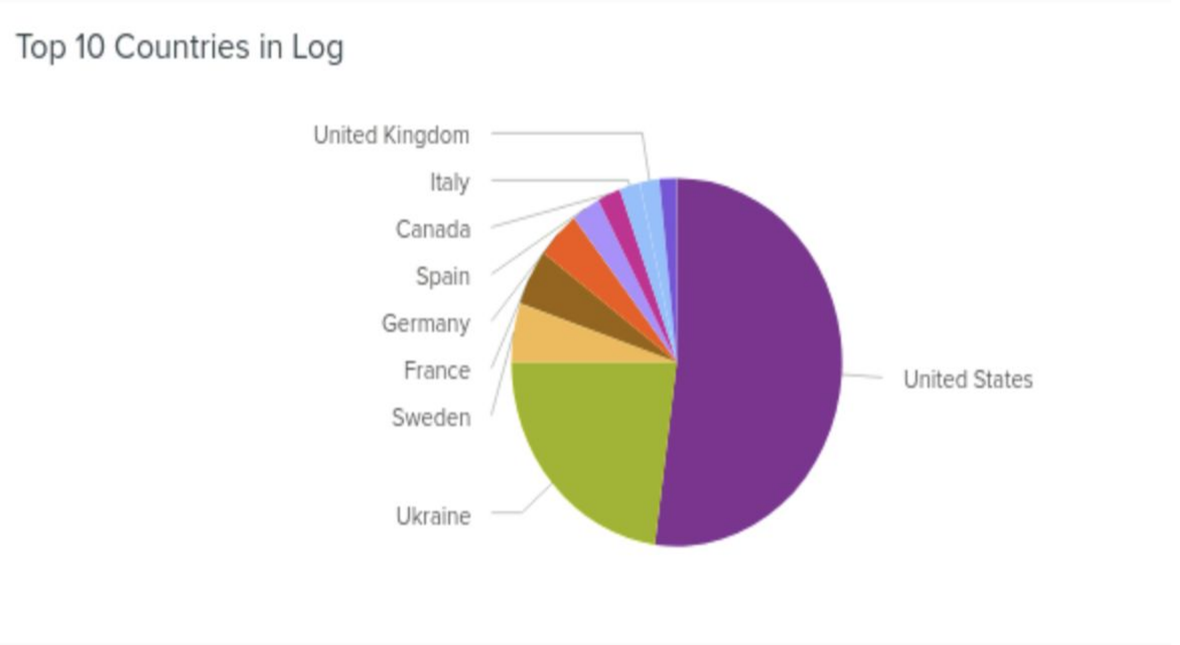
Upon closer examination, the suspicious increased level of hourly activity is coming from Ukraine. Specifically from two cites: Kyiv (Solom'yans'kyi district) and Kharkiv (Shevchenkivs'kyi district).

Attack Logs



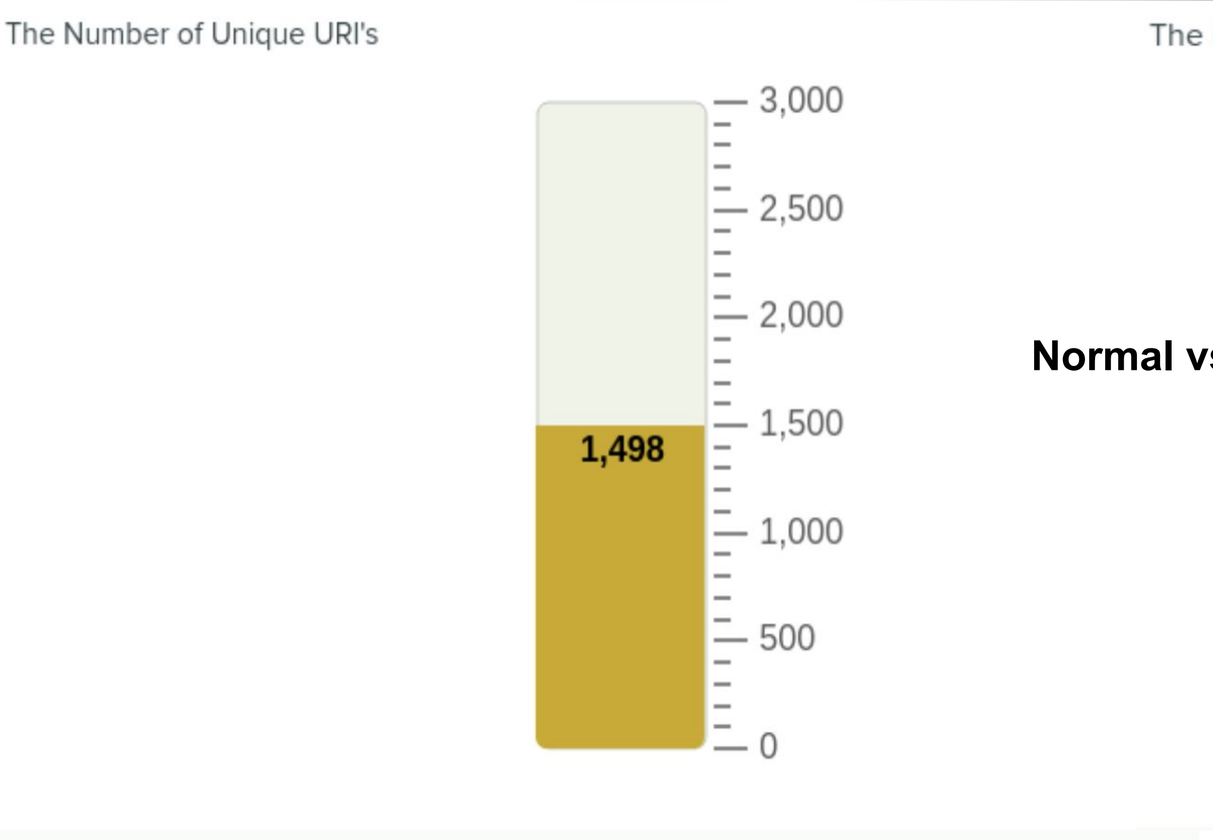
Dashboard Analysis - Top Countries Comparison



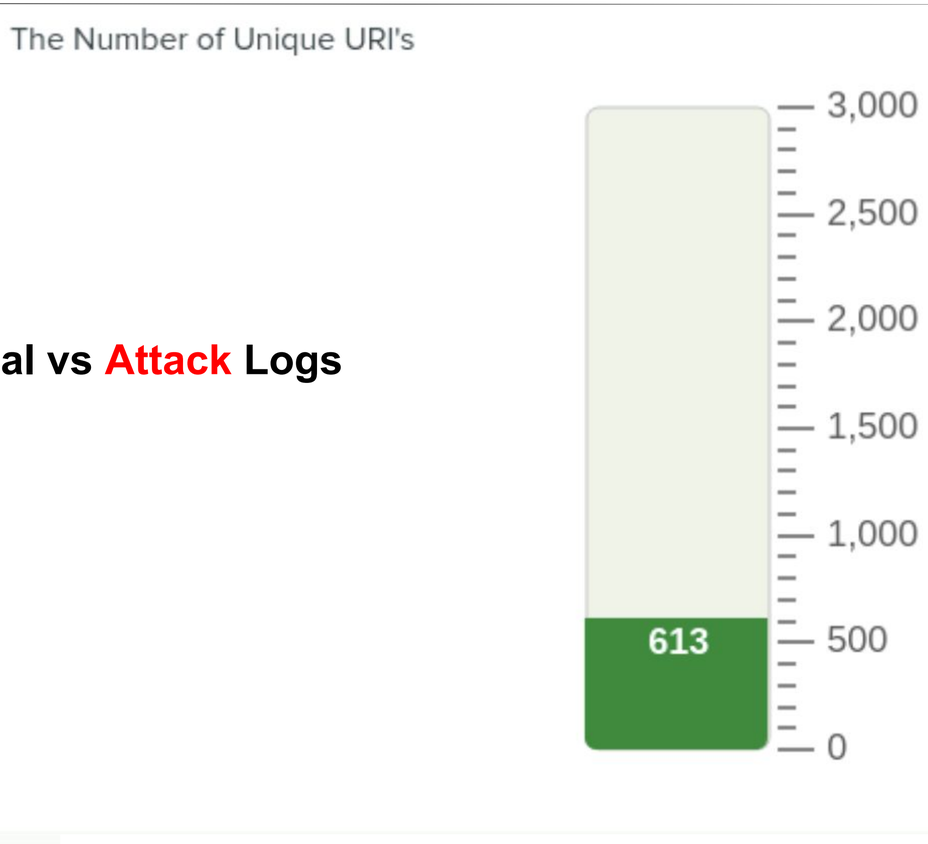


While hourly activity from the United States remained relatively constant, it appears that the spike in activity from Ukraine came at the expense of the other top nations, specifically major European ones, along with China and India. This could be indicative of a Denial of Service attack.

Dashboard Analysis - Unique URI Comparison

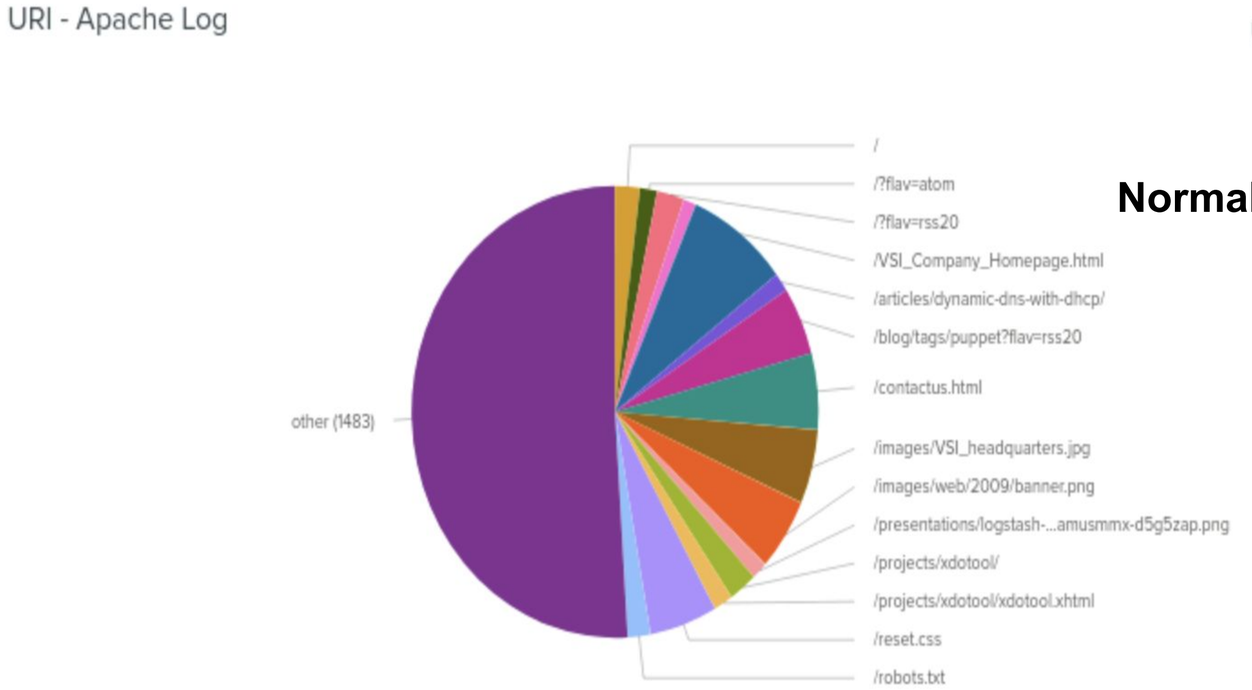


Normal vs Attack Logs

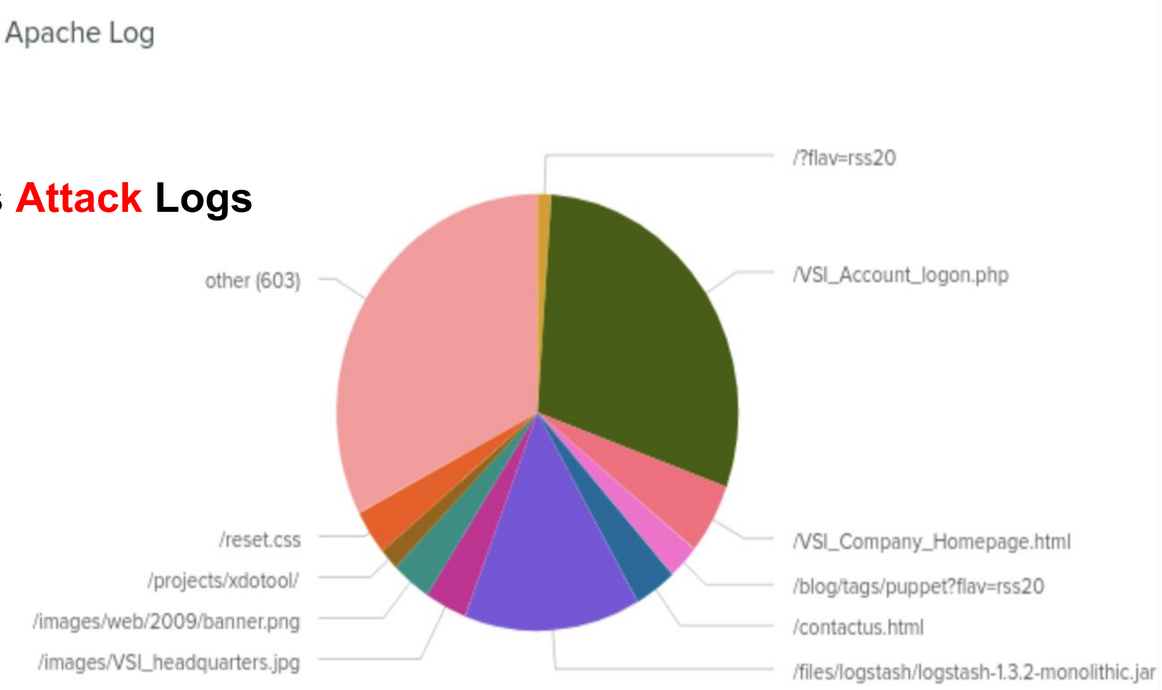


Significantly fewer unique resources being accessed potentially supports the theory of a Denial of Service attack.

Dashboard Analysis - URI Comparison



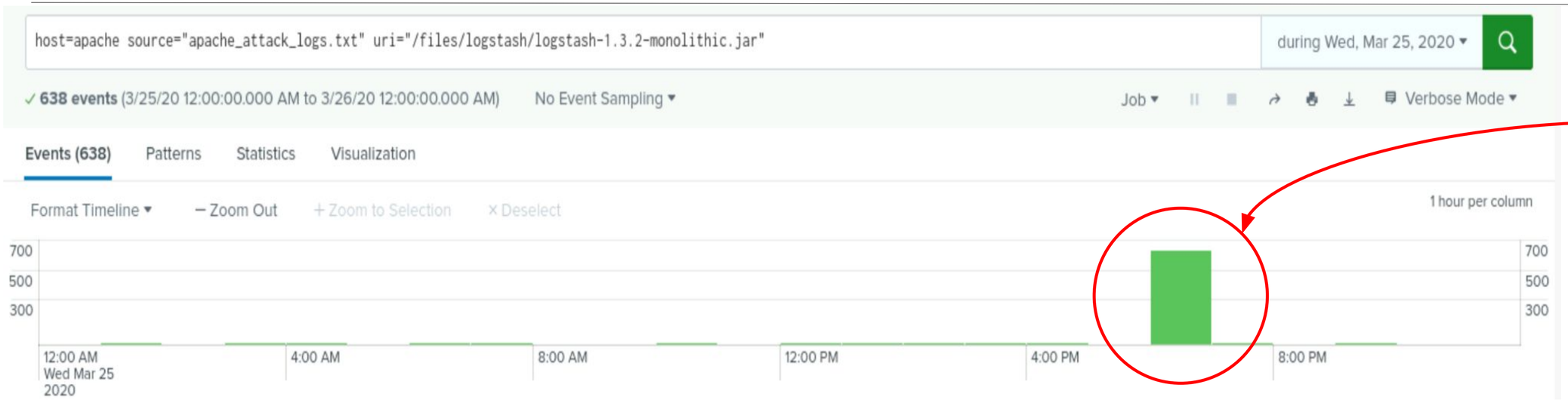
Normal vs Attack Logs



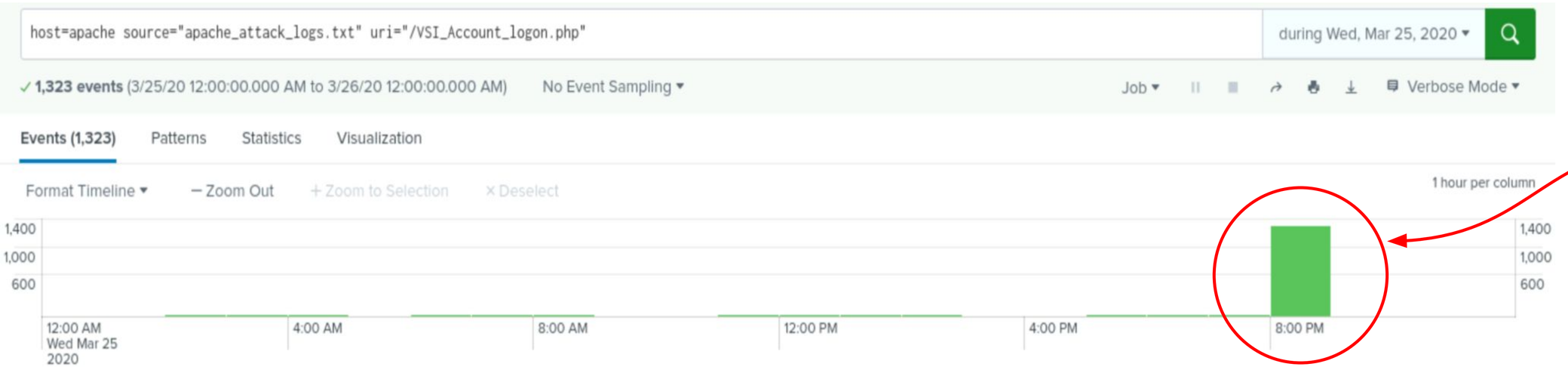
The most commonly accessed URIs evident in the normal logs seem ordinary: the VSI Company Homepage and the Contact Us page.

Interestingly, the most accessed URIs during the attack, by a relatively much larger amount, include the VSI Account Log-on page, followed by a zipped file that appears to contain log data: logstash-1.3.2.monolithic.jar.
This points to a potential Brute Force attack.

URI - Resources Accessed at Specific Times



A spike in access to this file suspiciously occurs at the same time that we have a spike in GET requests - 6 PM on March 25, 2020.



We subsequently observed a massive spike in the VSI Account Logon page at the same time that we have a spike in POST requests - 8 PM on March 25, 2020.

Dashboard Analysis - Total Post Request Count

Number of POST Requests

Normal vs Attack

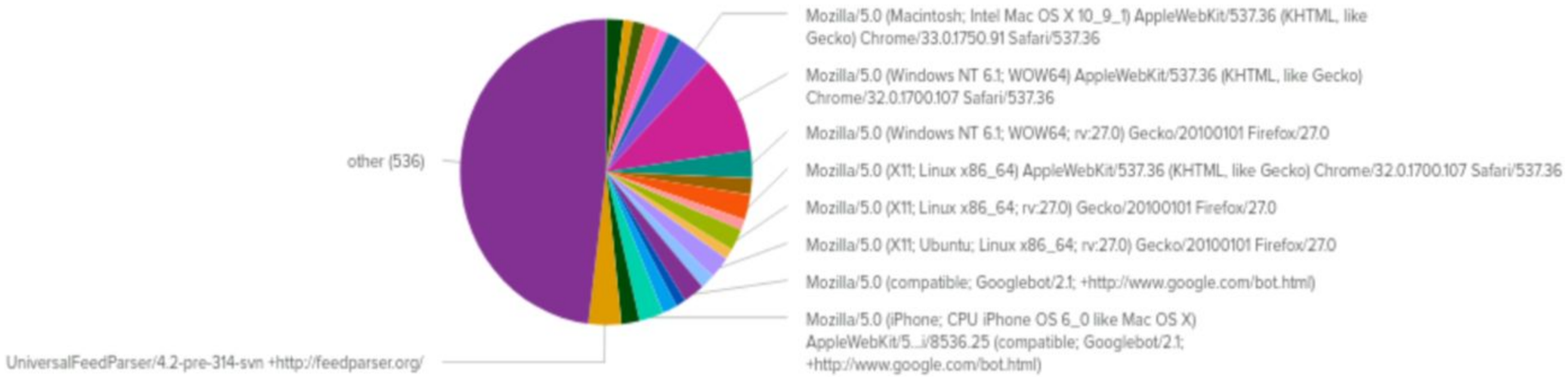
Number of POST Requests

The POST request gauge is literally off the scale!

Dashboard Analysis - User Agent Comparison

Count of Different User Agents

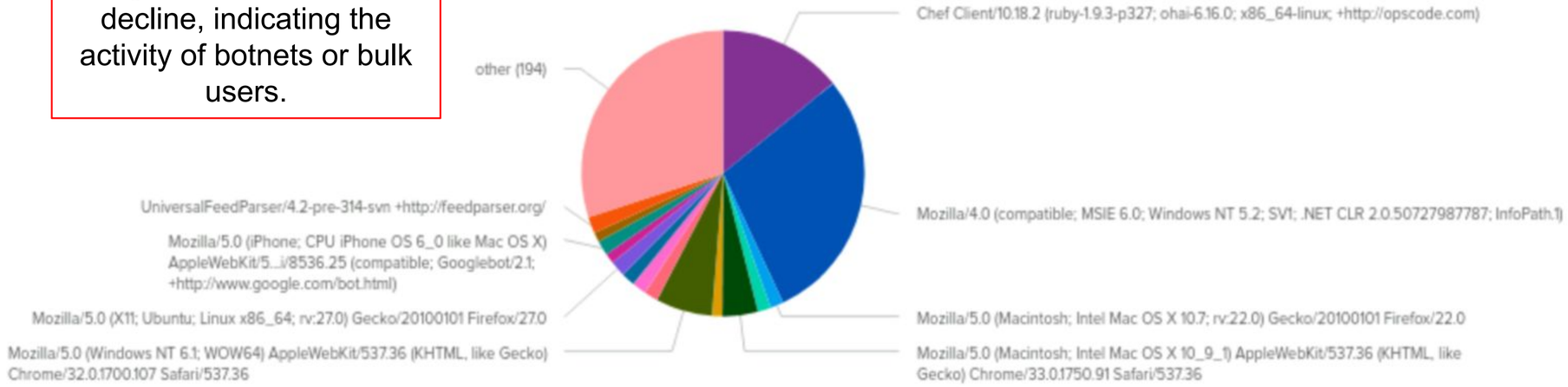
Normal Logs



Count of Different User Agents

The number of unique user agents sees a steep decline, indicating the activity of botnets or bulk users.

Attack Logs



Apache Attack Summary

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

- HTTP Methods - the attacks seems to have begun at 6 pm with a huge increase in GET requests (requesting info from the server). As these came down (back to normal levels by 7 pm), a massive increase in POST requests was detected at 6 and 8 pm.

- URI Data - two specific pages stick out as having suspiciously high levels of activity: the VSI account logon page and zipped file that appears to contain log data. These point to potential Brute Force or Credential Stuffing Attacks. Less likely would be some form of inclusion attack.

Apache Attack Summary

- Our findings point towards a two stage attack: the attacker first requests data from the server (i.e. the logstash file). Using the information from the file, the attacker proceeds to send a huge amount of requests (i.e. brute force attack, credential stuffing) in an attempt to logon with a VSI employee’s credentials.

- The attack appears to originate out of Ukraine, specifically the cities of Kyiv and Kharkiv. Simultaneously, there is a significant drop in activity from other major countries, as well as in the total number of unique URIs being accessed. This could indicate a DOS component to the attack.

Summary and Future Mitigations

Project 3 Summary

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

- For the Windows attack logs, we found that the count of signatures severely reduced except for peak moments
- The nature of most signatures after the attack are mostly accounts being locked
- This lead us to believe that the attack was most likely a brute force attack that caused denial of service
- Special privileges were assigned to new logons so this lead us to believe that either higher privilege users are not implementing secure passwords or that the principle of least privilege was not being adequately applied

Project 3 Summary

- From the Apache log side, we witnessed suspicious levels of activity from a typically low activity region (Ukraine). Additionally, the reduced number of unique user agents might be indicative of a botnet operating, or some other method of bulk users.

- This coincided with massive spikes in the number of GET and then POST requests. The attackers most likely extracted information from the servers, likely reconnaissance information as well as log information from the logstash file URI (logstash-1.3.2.monolithic.jar) that had unusually high levels of access to it.

- The attackers proceeded to send a large amount of POST requests, which we determined to be reflective of a Brute Force attack (potentially using info/credentials from the logstash file), while simultaneously causing a Denial of Service for many other users, specifically from European Union countries, China and India.

Project 3 Summary

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

- Setting up and configuring Intrusion Prevention System (IPS) and firewall rules to halt future DOS attacks. Implement critical alerts for detection of botnets and bulk users.
- Block or limit activity from IP's located in countries where the attacks originate (in this case, Ukraine). Whois XML IP Geolocation API will be useful here. Ensure to monitor the baselines of countries and respond quickly to any suspicious spikes, especially from typically low-activity regions.
- Set up a lock out policy; implement a form(s) of multi-factor authentication; institute password hygiene.
- Employ the "Concept of Least Privilege" to limit fallout from potential future breaches.
- Input Validation to reduce the likelihood of SQL and cross-scripting attacks.