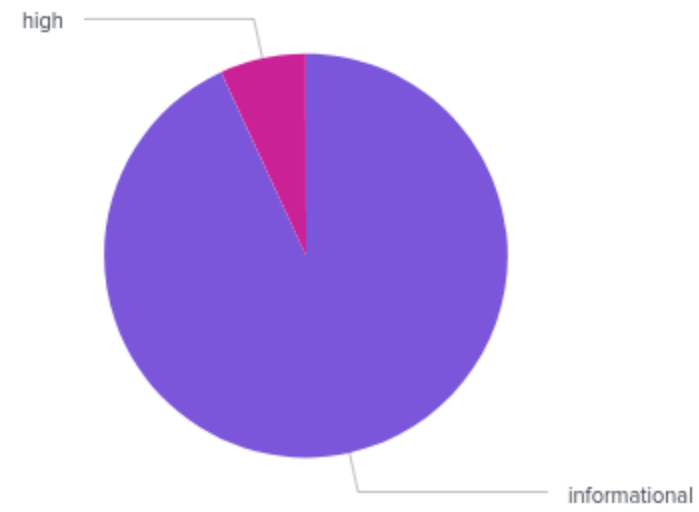
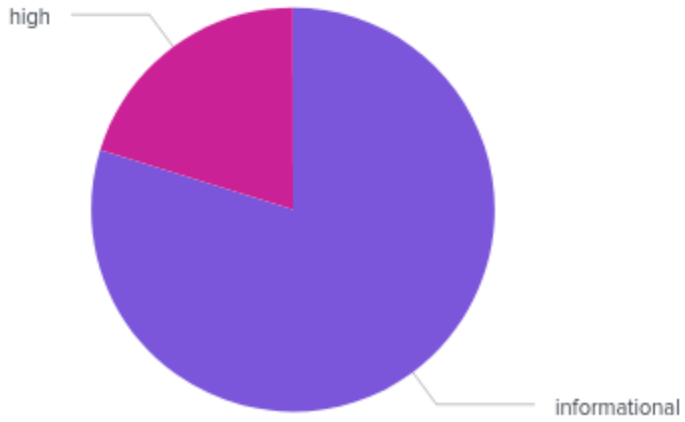
Part 2:

Severity Logs Comparison Report

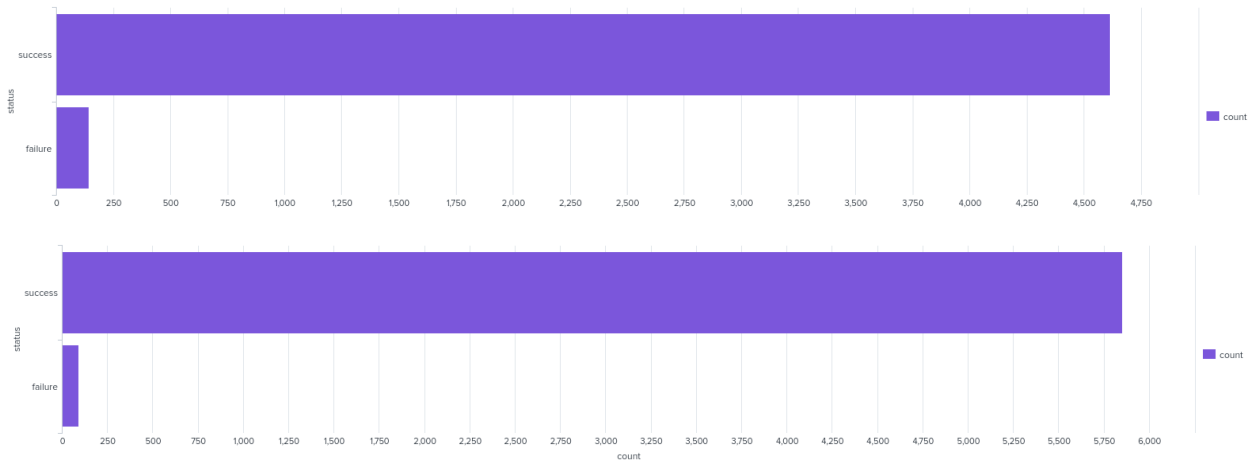


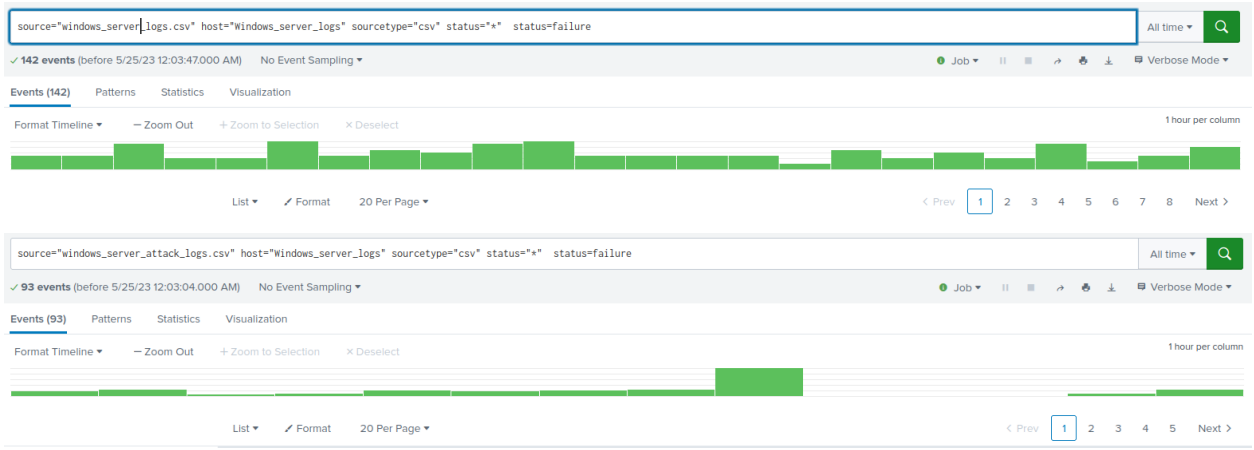


Percentage Change from 6.9% on normal logs -> 20.2% on the attack logs

---

Success vs Failure Report





Despite there being less attacks on the attack logs; there is a spike at 8 am which then dips to 0 after.

Failure Alert

On a normal day the number of failures never exceed 10, on the attack logs there is a major spike at 8 pm with a number of 35 failures.

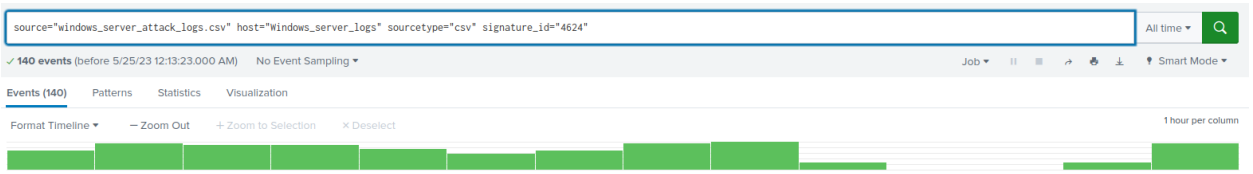
- Did you detect a suspicious volume of failed activity? yes
- If so, what was the count of events in the hour(s) it occurred? 35
- When did it occur? 0800
- Would your alert be triggered for this activity? yes
- After reviewing, would you change your threshold from what you previously selected? no

---

Success Alert

Before

After



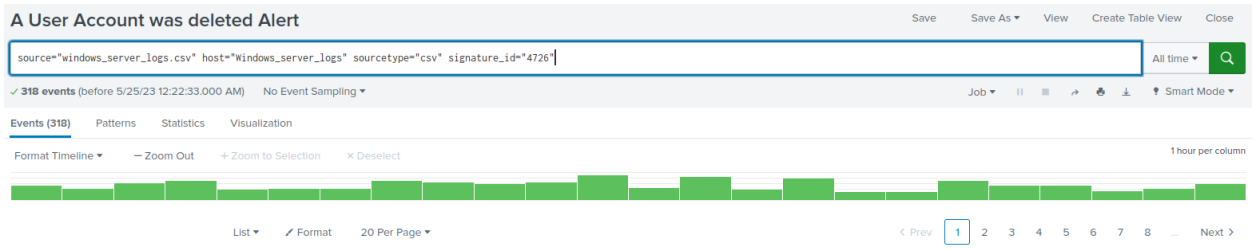
Despite there being no spike, there are 0 logins from the times of 10 and 11 PM.

- Did you detect a suspicious volume of successful logins? yes
- If so, what was the count of events in the hour(s) it occurred? 15, 16
- Who is the primary user logging in? User c
- When did it occur? 0800 04/25/2020
- Would your alert be triggered for this activity? yes
- After reviewing, would you change your threshold from what you previously selected? no

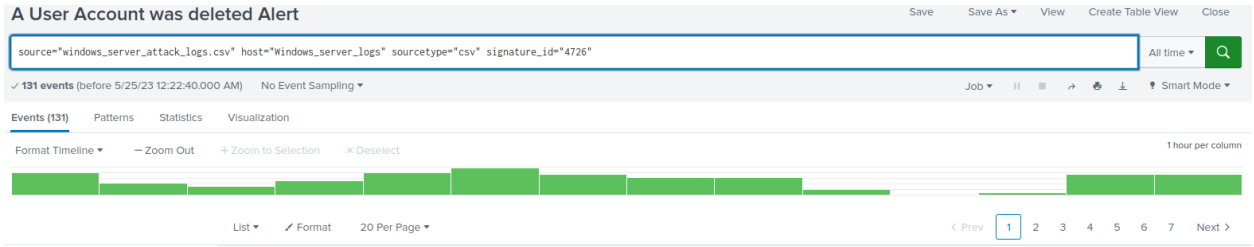
---

Deleted Accounts Alert

Before



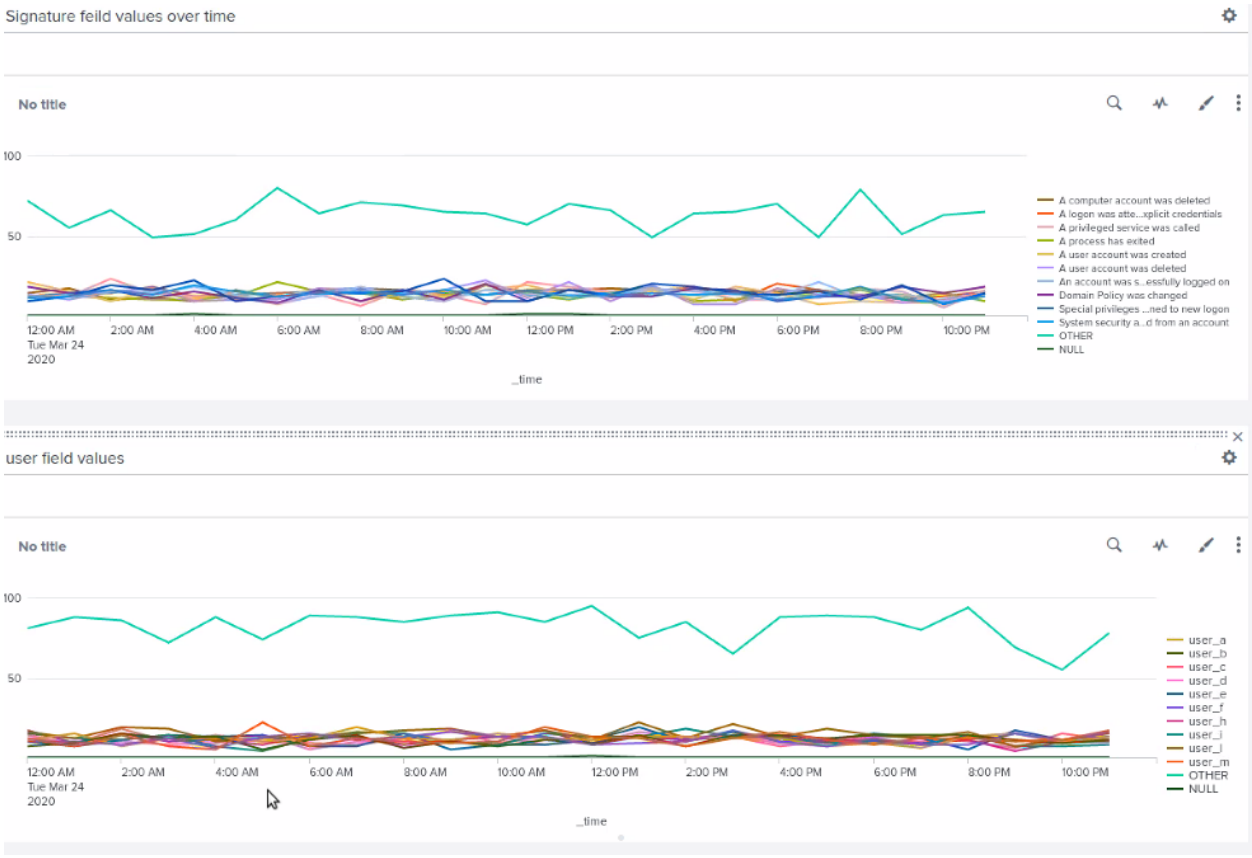
After



Just like the successful login alert, there is a significant dip in activity between the times of 9-11 AM.

- Did you detect a suspicious volume of deleted accounts? From 0900 to 1100 there are suspiciously low amounts of deleted accounts. DoS attack possible?

Before



After

User A was locked out around 2, User K had over 1k attempts for a password change at 9 am.

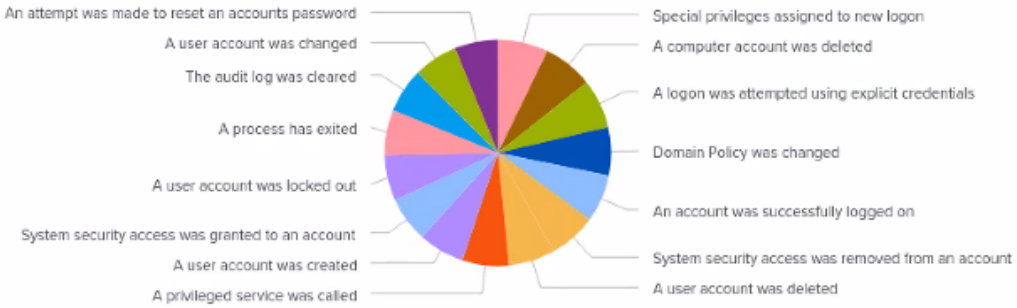
Signature field

- Does anything stand out as suspicious?
  User A was locked out around 0200 & user K had over 1000 attempts for a password change at 9AM.
- What signatures stand out? A user account was locked out, an attempt was made to rest a password
- What time did each signature's suspicious activity begin and stop? 0000-0300, 0800-1100
- What is the peak count of the different signatures? 1258

User field values

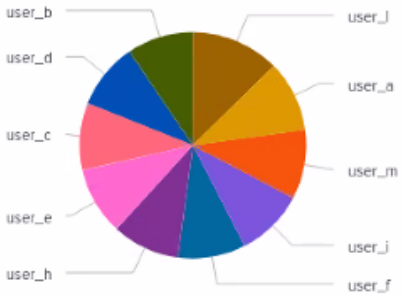
- Does anything stand out as suspicious? YES
- Which users stand out? A and K
- What time did each user's suspicious activity begin and stop? 0000-0300, 0800-1100 What is the peak count of the different users? 1256

Before



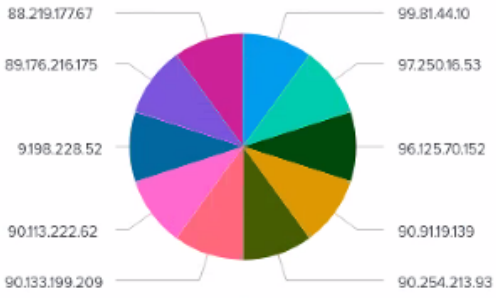
count of different users

No title

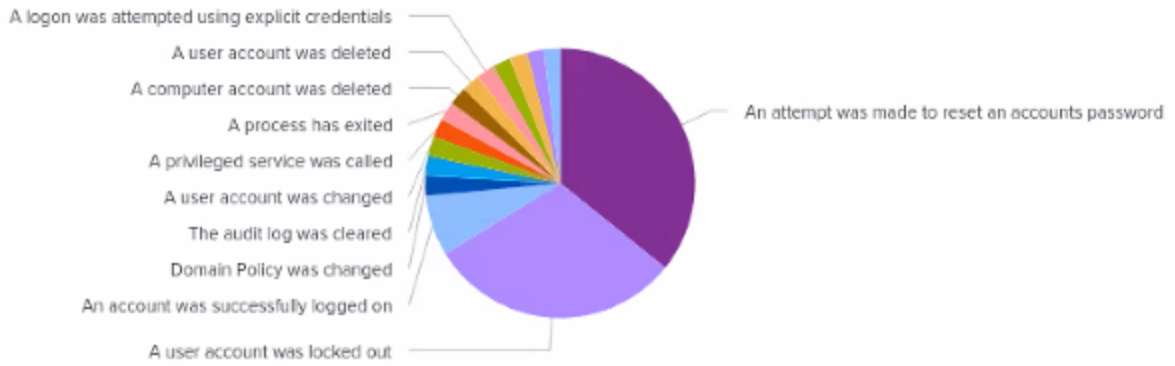


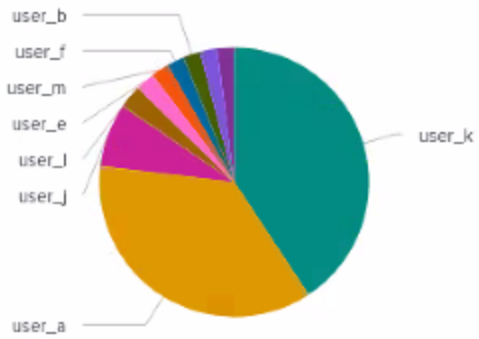
src_ip top 10

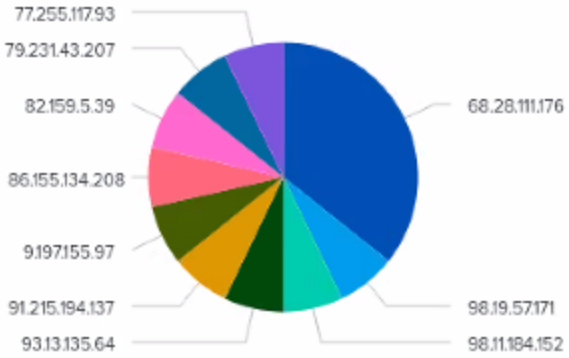
No title



After


A logon was attempted using explicit credentials
A user account was deleted
A computer account was deleted
A process has exited
A privileged service was called
A user account was changed
The audit log was cleared
Domain Policy was changed
An account was successfully logged on
A user account was locked out
An attempt was made to reset an accounts password


user_b
user_f
user_m
user_e
user_l
user_j
user_a
user_k

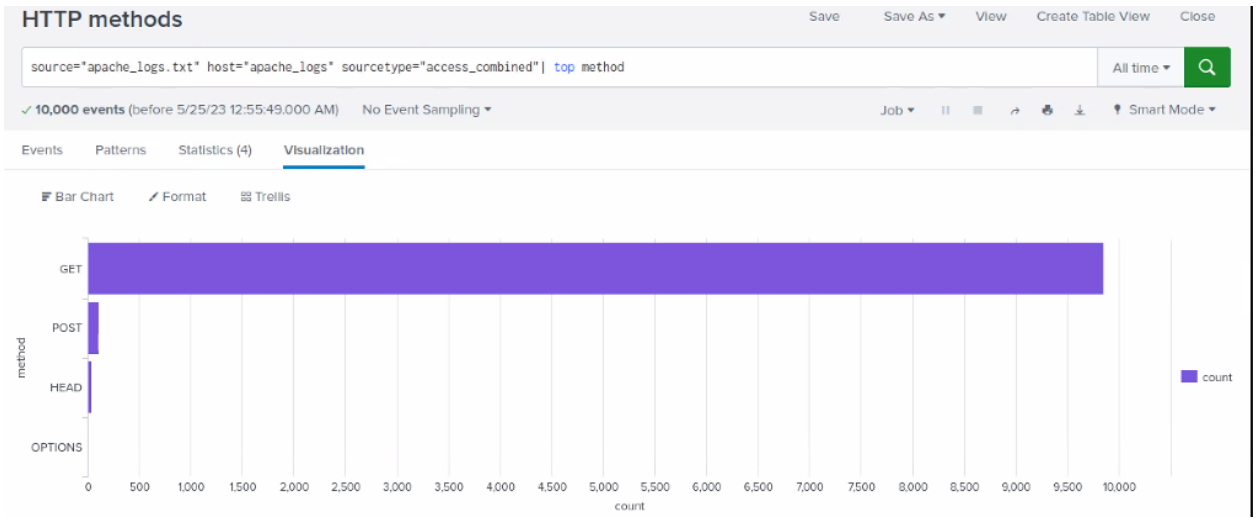

77.255.117.93
79.231.43.207
82.159.5.39
86.155.134.208
9.197.155.97
91.215.194.137
93.13.135.64
68.28.111.176
98.19.57.171
98.11.184.152

Does anything stand out as suspicious?

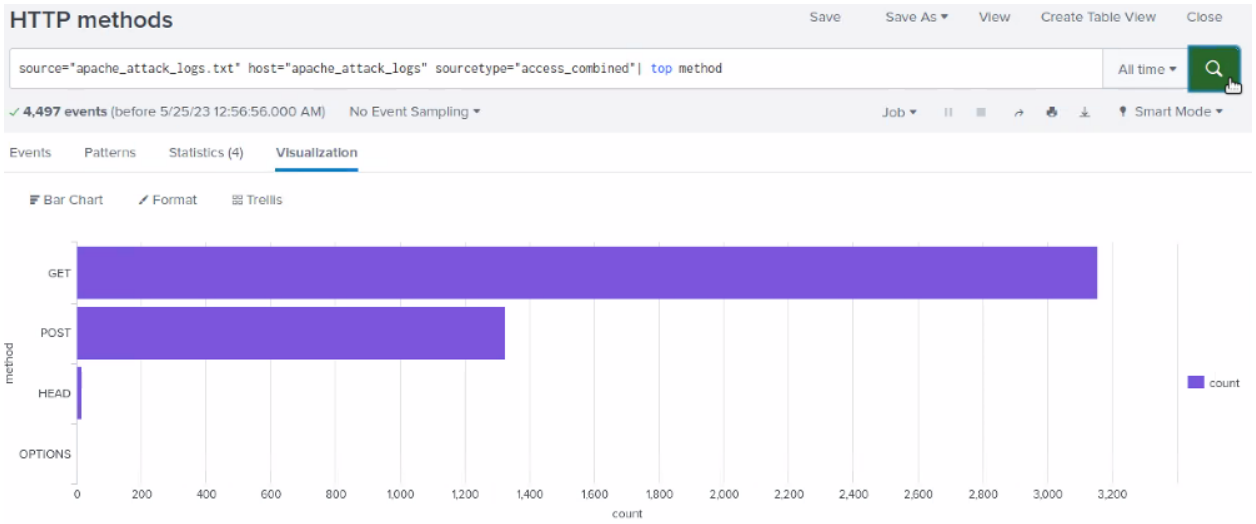
- What signatures stand out?
    - An attempt was made to reset an accounts password
    - A user account was logged out
- What time did each signature's suspicious activity begin and stop?
    - Attempt for password started at 8 Am and ended at 11 Am
    - Account log out started at midnight and ended at 3 Am on march 25th
- What is the peak count of the different signatures?
    - Signatures peak =1,258
    - Lock out =896
    - Peak users = 1,256

Methods report

Before



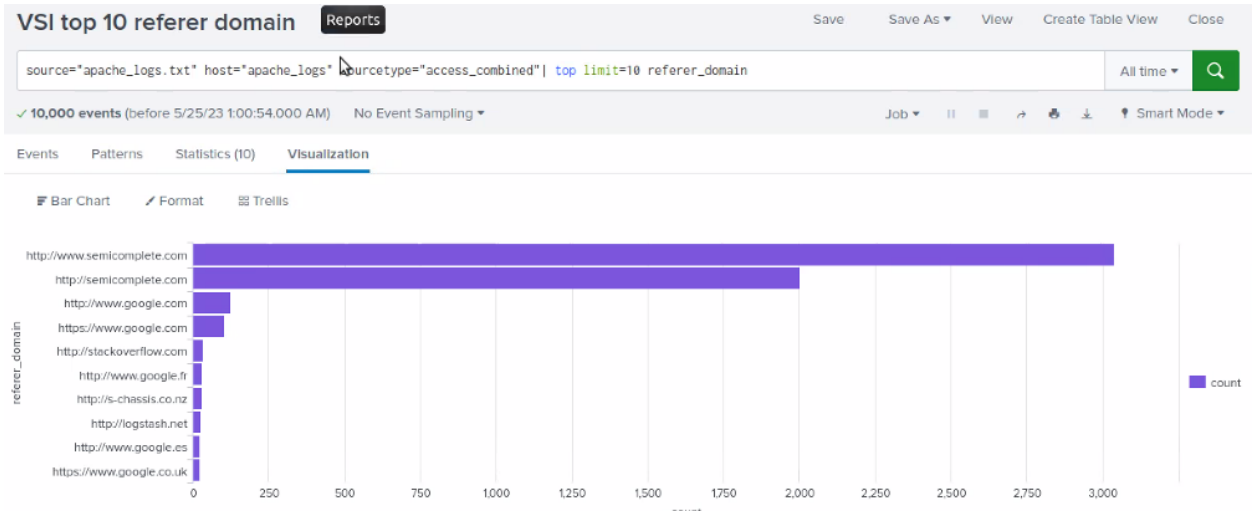
After



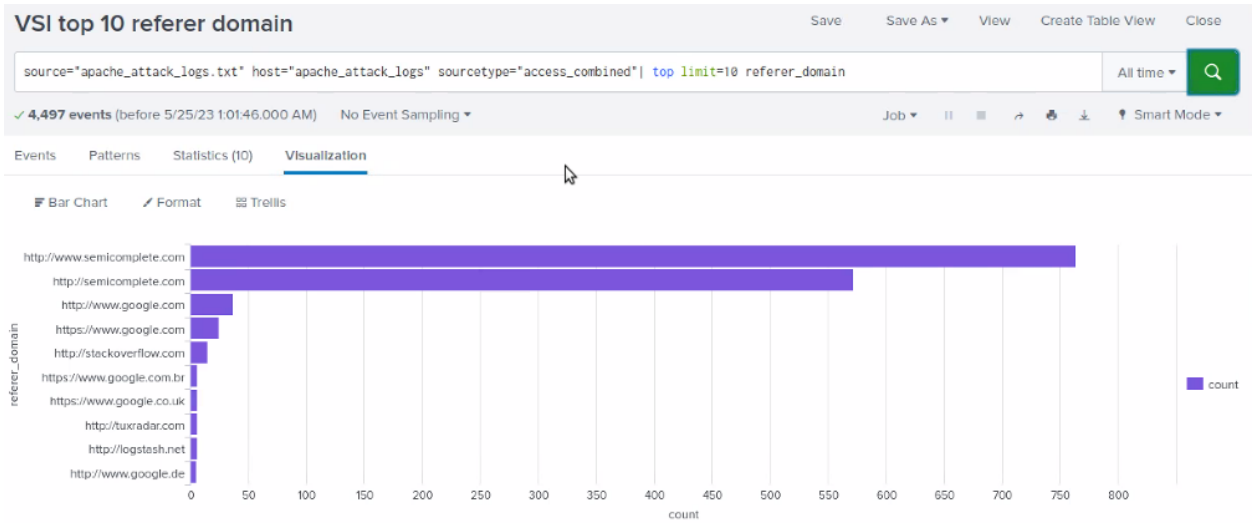
1. Review the updated results, and answer the following questions in the review document:
    - Did you detect any suspicious changes in HTTP methods? If so, which one?
        i. There was a marked increase in POST methods from 106 to 1324
    - What is that method used for?
        i. POST is used to make changes

Refer Domains Report

Before



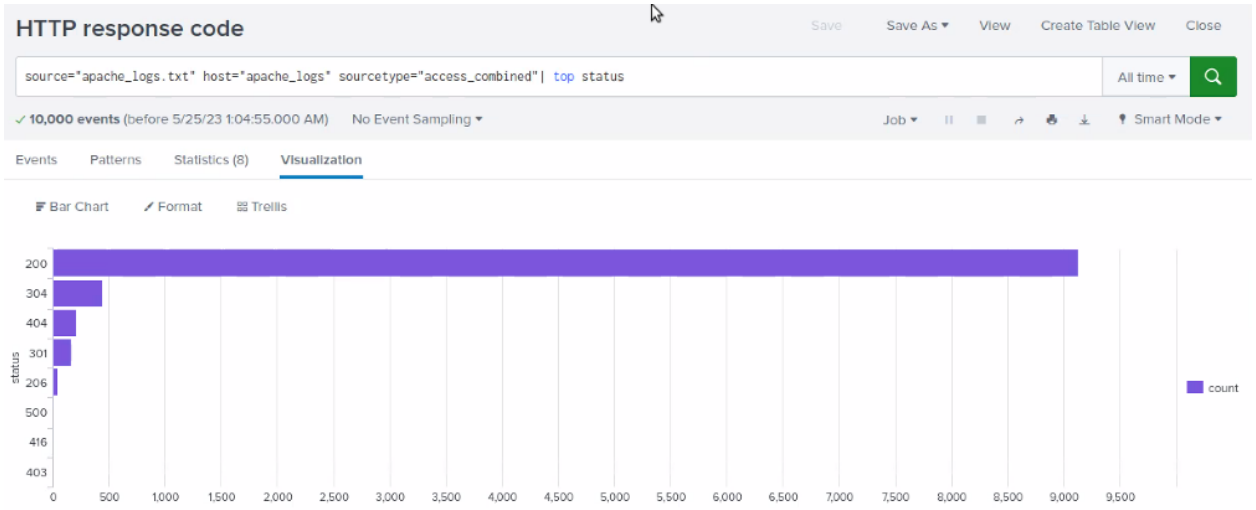
After



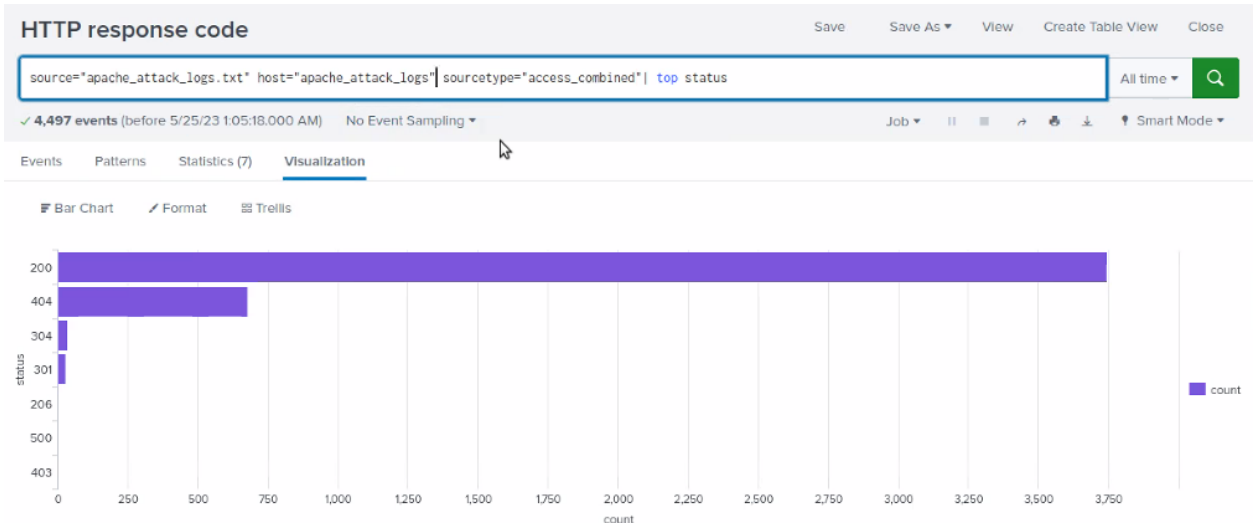
- Did you detect any suspicious changes in referrer domain?
    - Yes there was a significant drop in requests.

HTTP Response Codes Report

Before



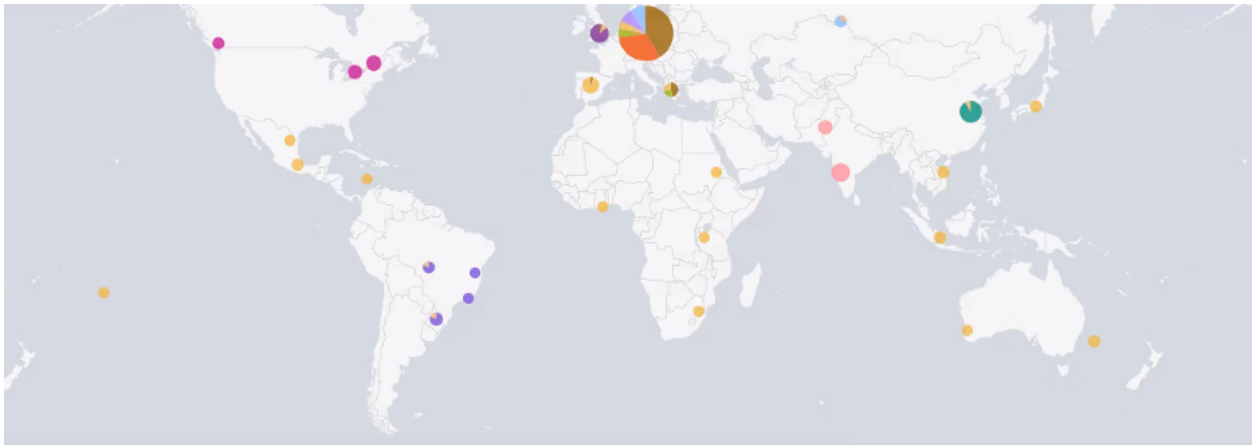
After



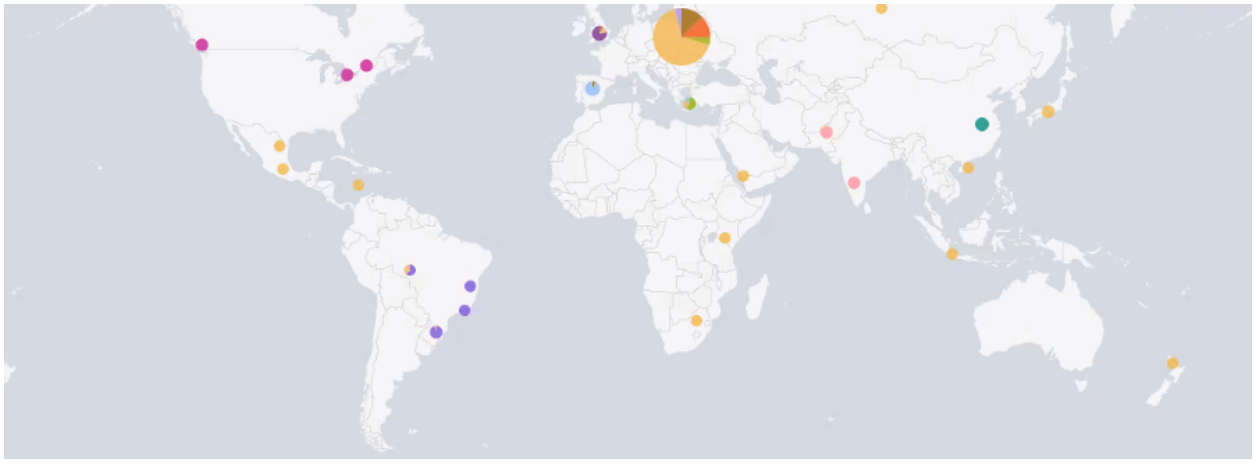
1. Did you detect any suspicious changes in HTTP response codes?
    a. A marked increase in 404 response codes. And 200 responses dropped by the thousands.

Activity outside of the US Alert

Before



After



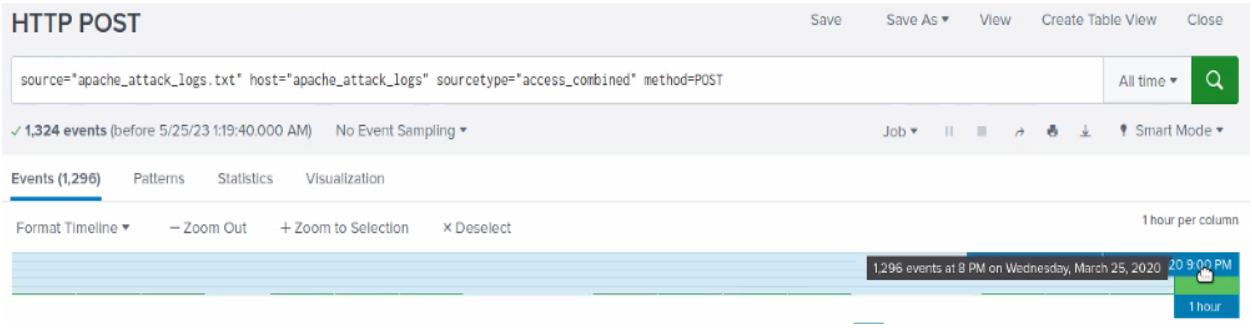
- Did you detect a suspicious volume of international activity?
    i. Yes, an increased amount of activity from Ukraine.
- If so, what was the count of events in the hour(s) it occurred?

    i. Attacks occurred approximately at 20:00
- Would your alert be triggered for this activity?
    i. NO
- After reviewing, would you change the threshold you previously selected?
    i. We would change it to 800 from 900

HTTP Post activity alert

Before

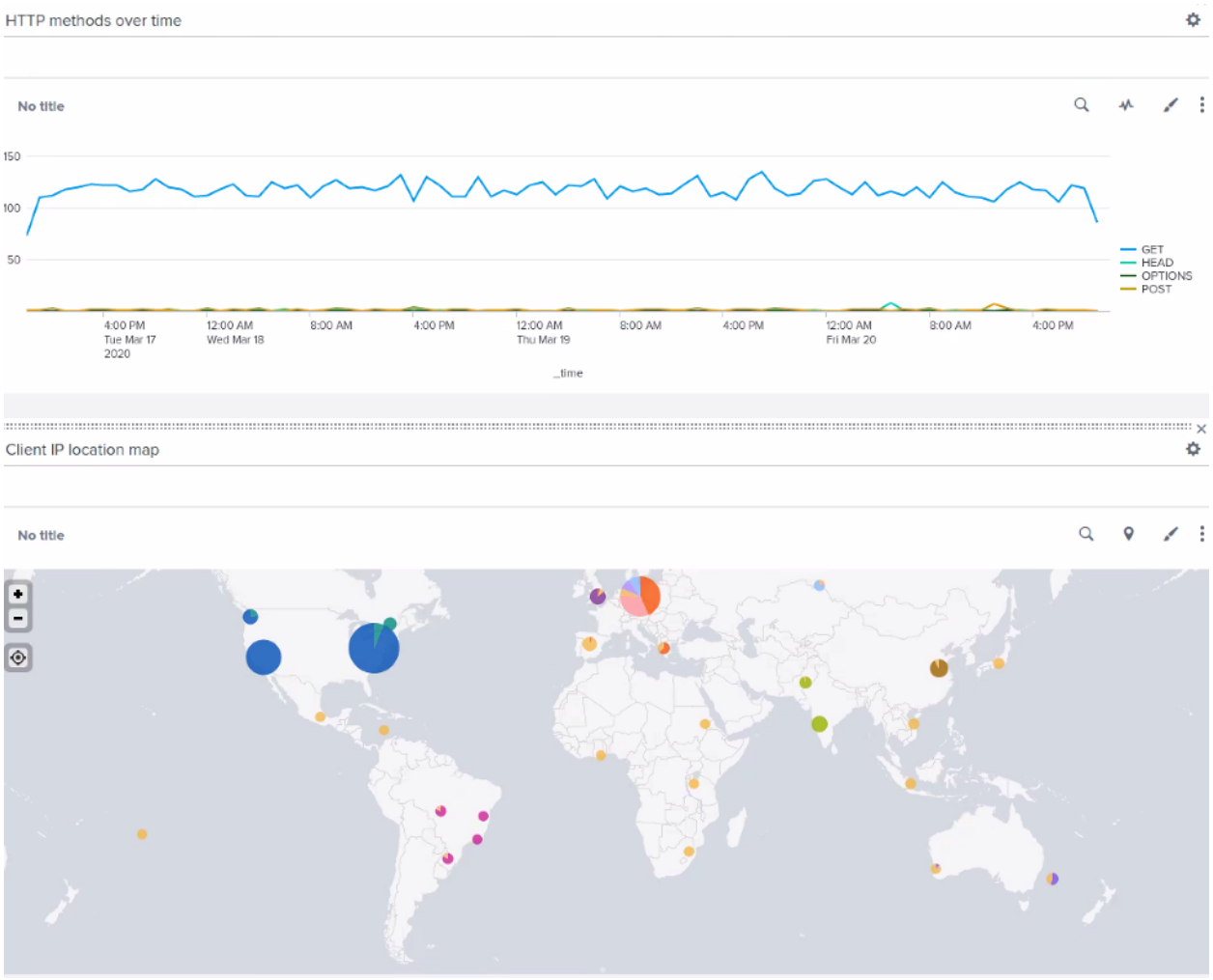
After



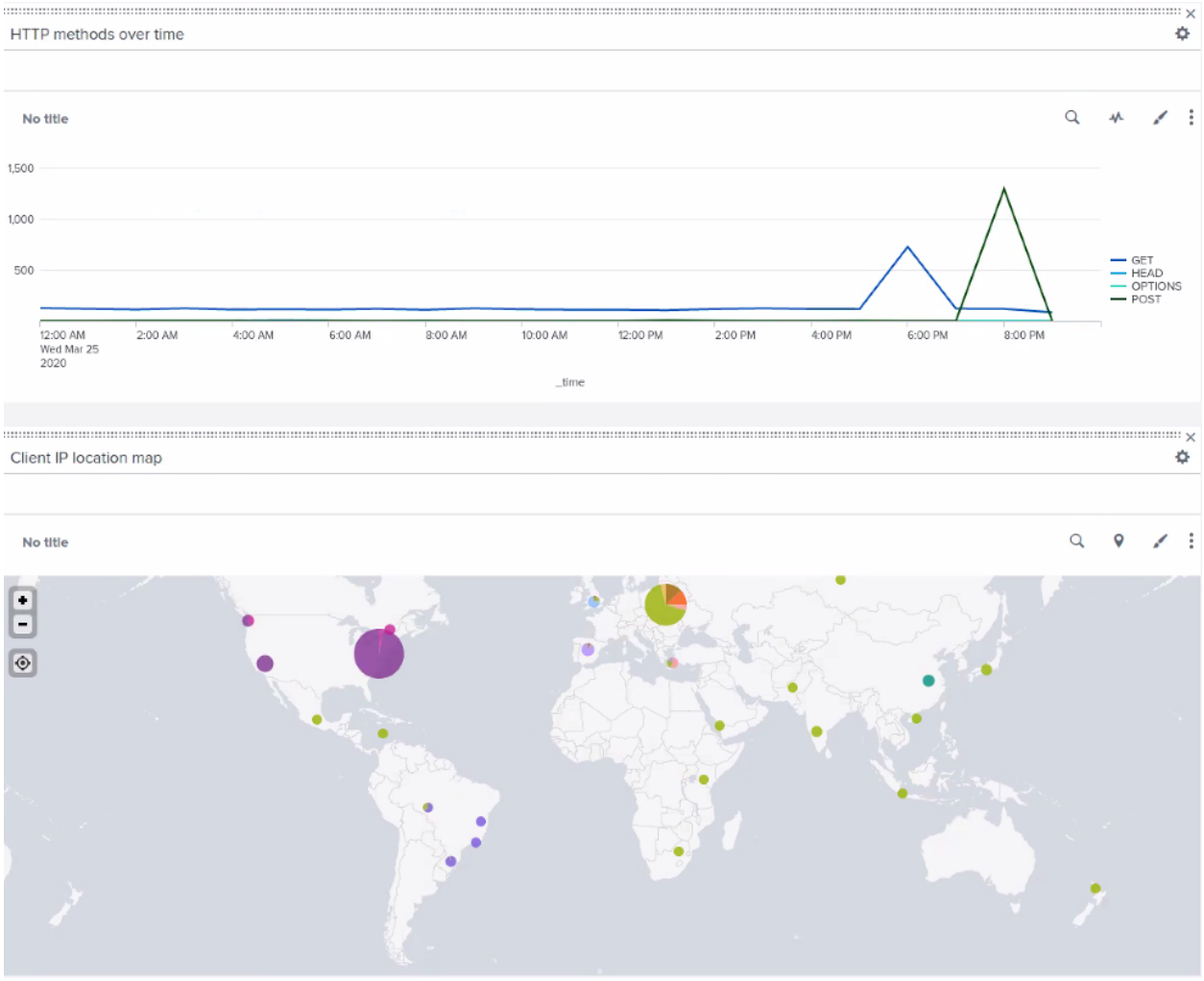
- Did you detect any suspicious volume of HTTP POST activity? Yes, at 9pm on March 25th
- If so, what was the count of events in the hour(s) it occurred? 1296
- When did it occur? Between 8pm and 9pm on March 25th
- After reviewing, would you change the threshold that you previously selected? Our threshold was 15, and would have triggered.

Apache Web server Monitoring Dashboard

Before

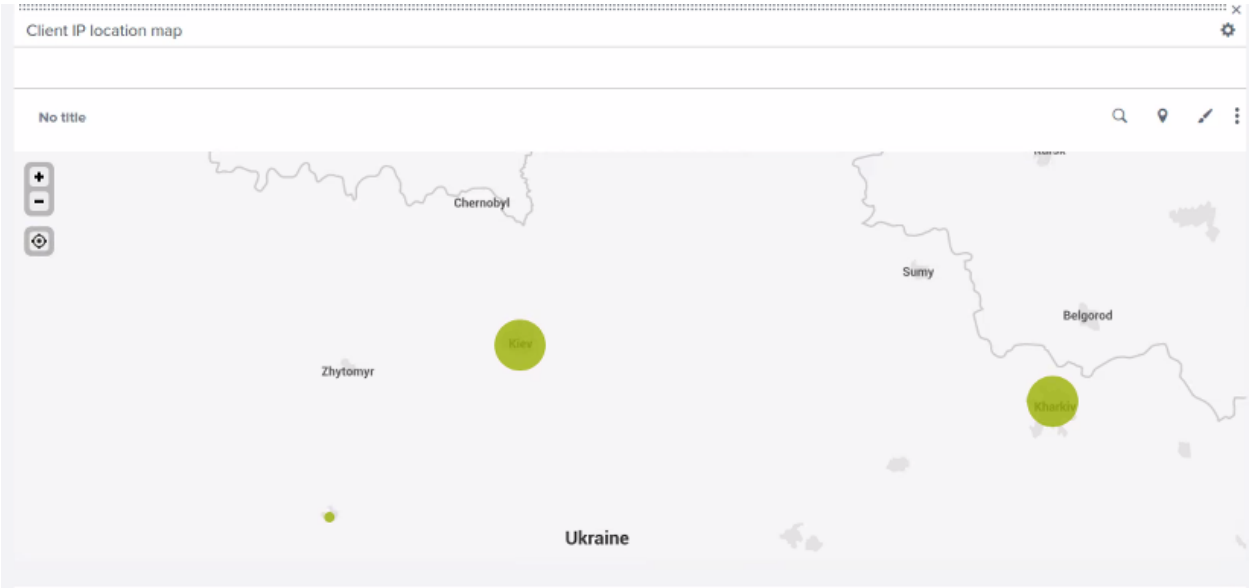


After



- Does anything stand out as suspicious?
    - yes
- Which method seems to be used in the attack?
    - Increase in get & post
- At what times did the attack start and stop?
    - 6pm to 8:30pm
- What is the peak count of the top method during the attack?
    - 1296

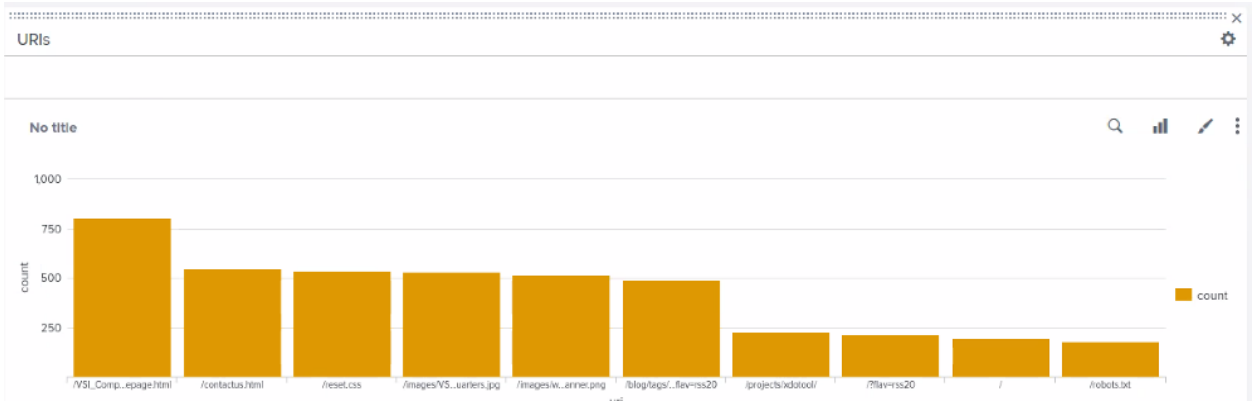
Apache Dashboards analysis for cluster map



- Does anything stand out as suspicious?
    - Increased activity coming from Ukraine
- Which new location (city, country) on the map has a high volume of activity?
    - 438 from Kiev, 433 from Kharkiv in Ukraine
- What is the count of that city?
    - Kiev: 438
    - Kharkiv: 433

URI’s

Before:



After:

Dashboard Analysis for URI Data

Does anything stand out as suspicious?

What URI is hit the most?

VSI_Account_logon.php with a count of 1,323

Based on the URI being accessed, what could the attacker potentially be doing?

Our assumption is a DDOS attack was being induced. This also explains the no activity in the reports before this from the times of 9-11 AM.