Defensive Security Project
by: Juliana

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Our team is made up of SOC analysts at Virtual Space Industries (VSI). Our company designs virtual-reality programs for businesses, and have been alerted that a competitor, JobeCorp, might be planning to launch cyber attacks against our company to disrupt our business.

- Using Splunk, for the first day, we analyzed past logs to develop baselines and create new reports, alerts, and dashboards to monitor activities and warn us of an incoming attack.

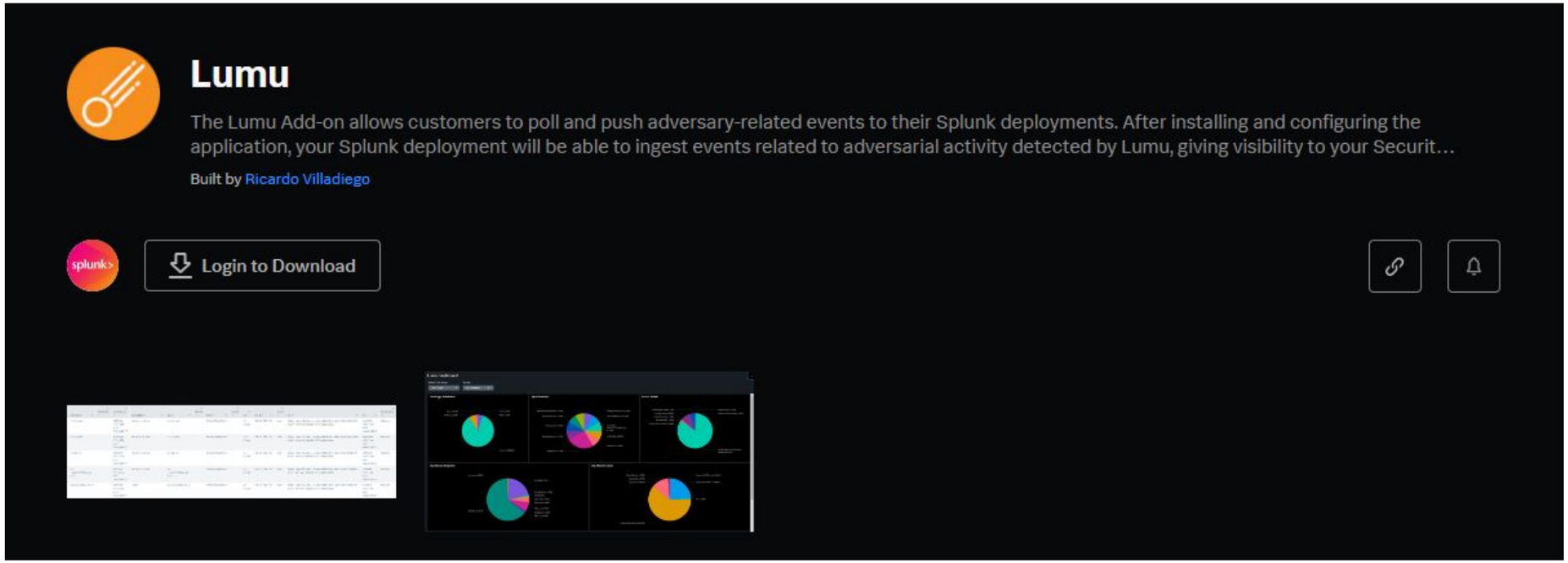
- On the second day, we received logs after attacks had occurred, and analyzed the events that happened, and how effective our measures and alerts from the first day would have been in alerting VSI of the attack.

- Finally, we provide recommendations and mitigations for the future to make stronger preventative measures for any future attack.

Lumu Add-on

Lumu Add-On

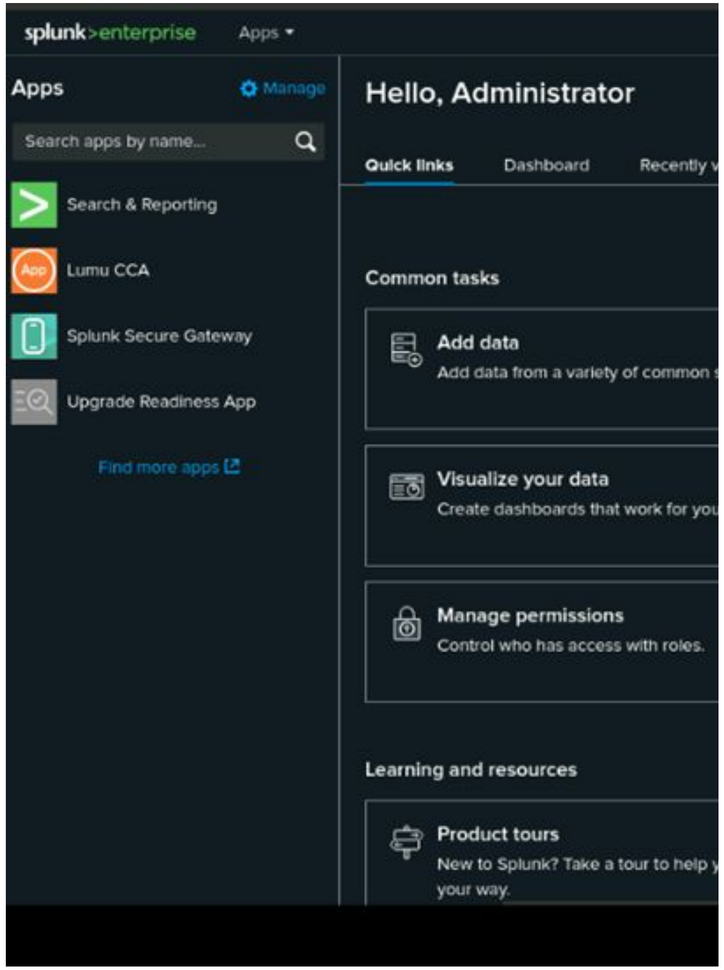
The Lumu Add-on allows users to analyze adversary-related events to their Splunk deployments. After installing and configuring the application, your Splunk deployment should be able to ingest events related to adversarial activity detected by Lumu, giving visibility to your Security Operations team.



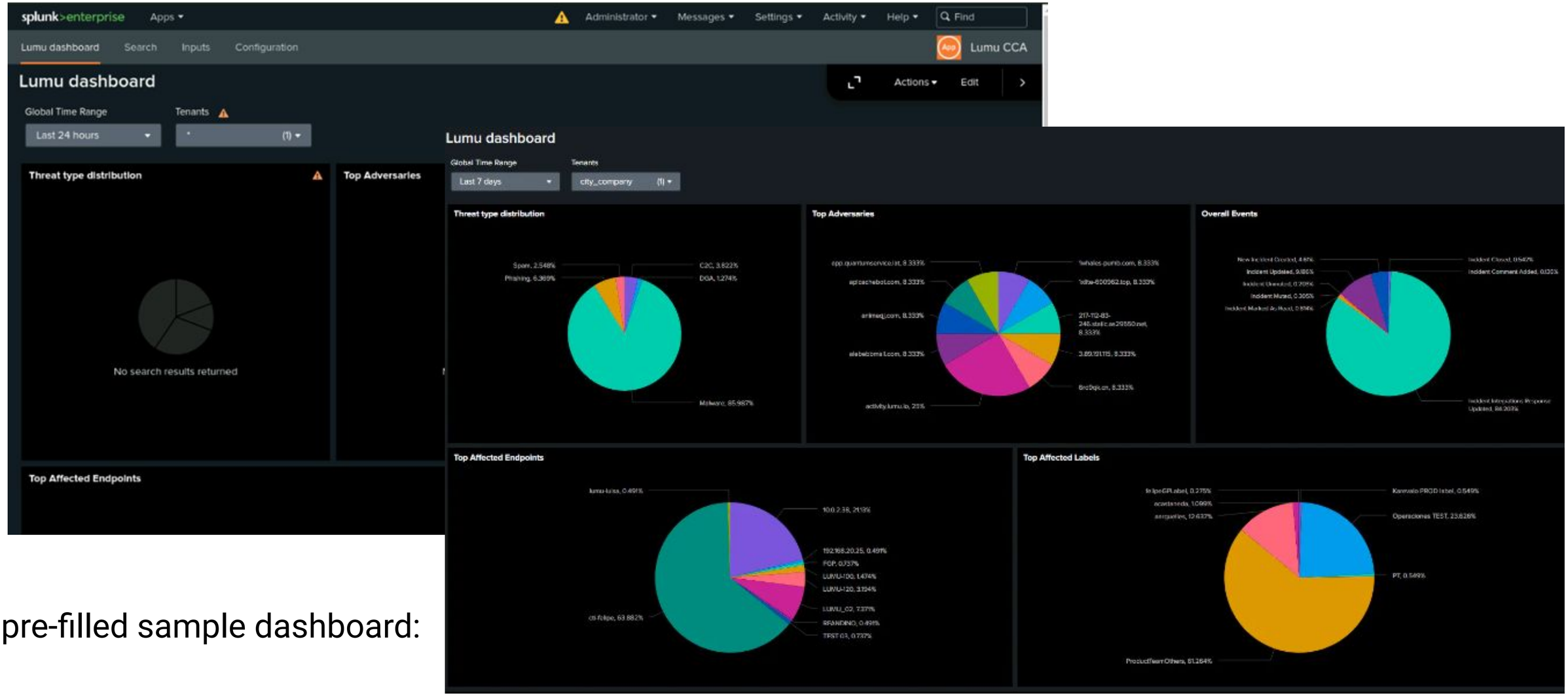
Lumu Add-On

The Lumu Add-On is designed to alert the team of security threats. In the event that a threat occurs outside of the pre-established alerts and reports you've set up, this add-on should bring it to your attention – giving addition support and reporting on potential threats you may not have considered.

The customizable dashboard examines logs for incoming threats, and provides quick visibility of those activities, which might include information on top adversaries, most affected endpoints, and the attack's distribution.



Lumu Add-On



pre-filled sample dashboard:

Logs Analyzed

1 Windows Logs

Windows server logs before and after the attack. Contains user account activity including login failures.

2 Apache Logs

Apache server logs before and after the attack. Contains HTTP methods data and web activity, such as URL information.

Windows Logs

Reports—Windows

Report Name	Report Description
Signatures table	A table of signatures and associated signature IDs
Severity levels	Severity levels (informational and high) and counts for each
Success and failure	Comparison of success and login failure rates

Images of Reports—Windows

Status

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Before 4/24/24 ▾

✓ **4,764 events** (1/28/20 1:00:48.000 PM to 4/24/24 12:00:00.000 AM)

Job ▾

2 results 20 per page ▾

status	count	percent
success	4622	97.019312
failure	142	2.980688

Severity Levels

Edit ▾ | More Info ▾ | Add to Dashboard ▾

Before 4/24/24 ▾

✓ **4,764 events** (1/28/20 1:00:48.000 PM to 4/24/24 12:00:00.000 AM)

Job ▾

2 results 20 per page ▾

severity	count	percent
informational	4435	93.094039
high	329	6.905961

✓ **4,764 events** (before 4/30/24 12:08:34.000 AM)

Job ▾

15 results 20 per page ▾

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

Alerts—Windows

Designed the following alerts:

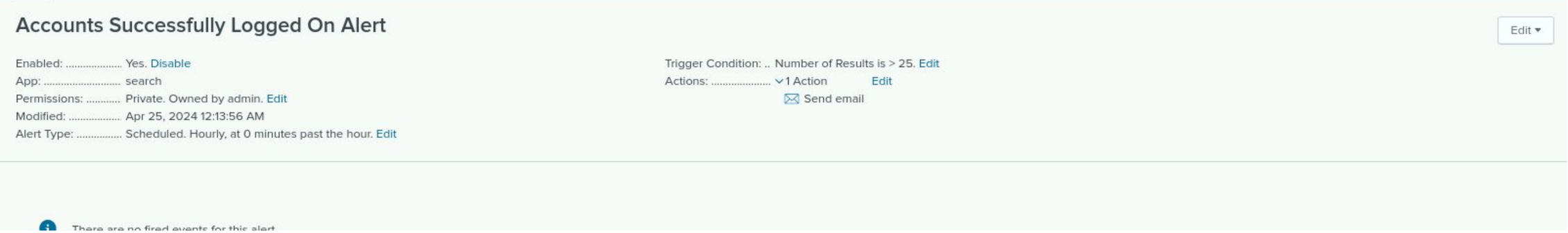
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Alert	Failure rate for logins hourly - Windows	9	13

JUSTIFICATION: The average login failure rate was less than 10 per hour for a routine day. We increased the threshold count to indicate an attack and abnormal activity for levels above what is normal.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Accounts Successfully Logged On	Successful login attempts	15	25

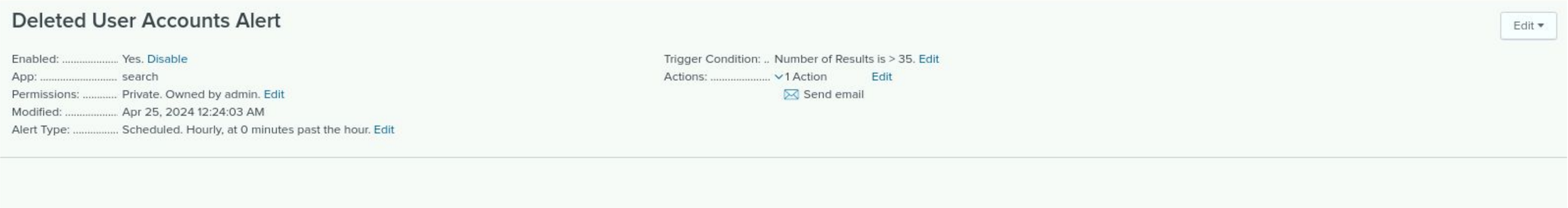


JUSTIFICATION: The average success failure level was roughly 8-20 per hour for a routine day. We increased the threshold count to indicate an attack and abnormal activity above what is normal.

Alerts—Windows

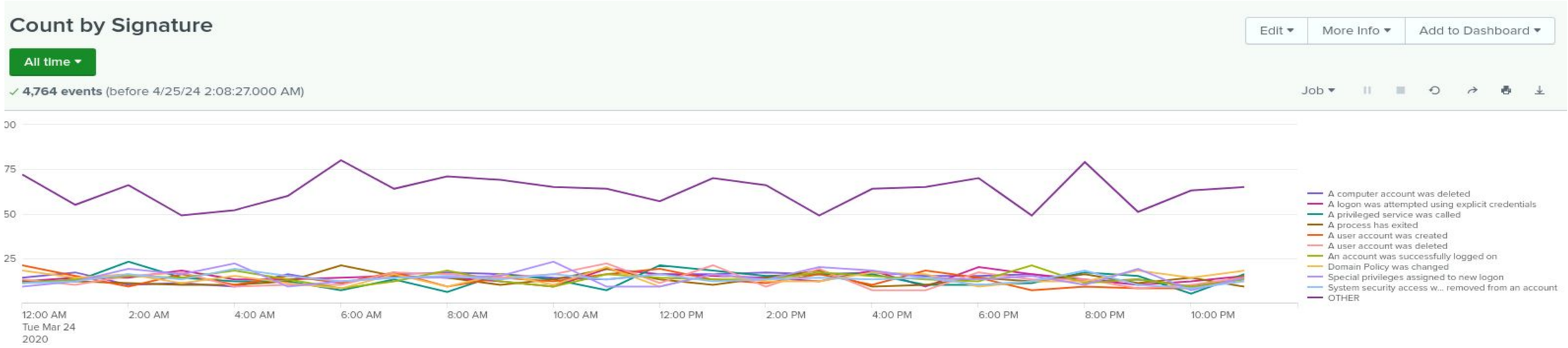
Designed the following alerts:

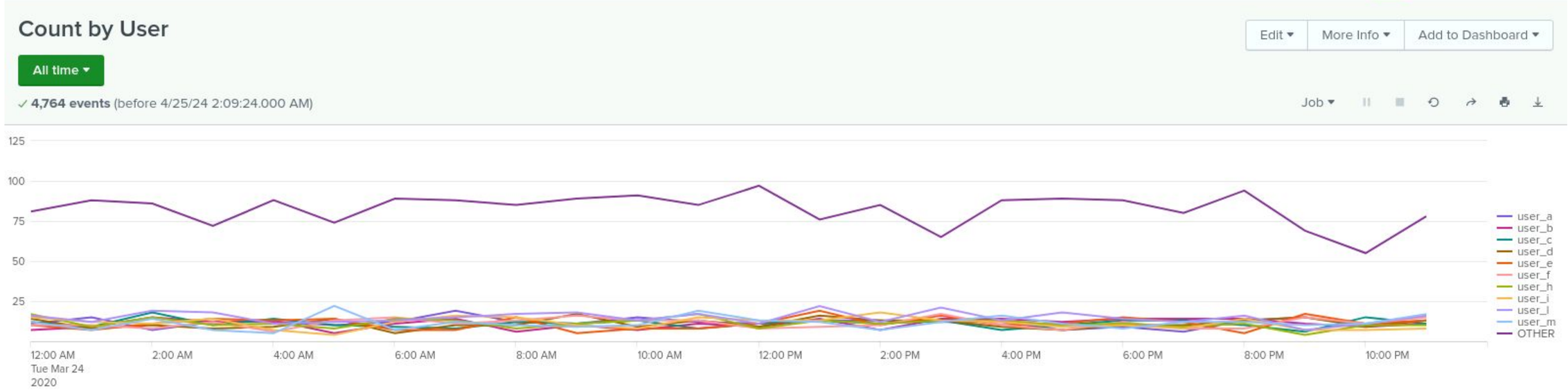
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account deletion	Excessive user account deleted	20	35



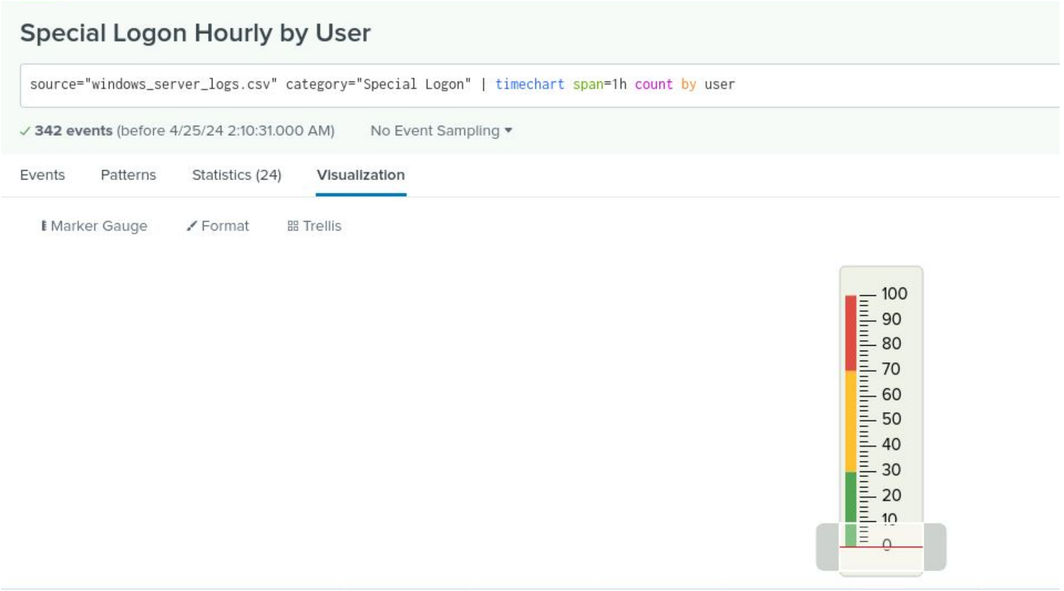
JUSTIFICATION: The average account deletion rate ranged from 8-22 per hour for a routine day. We increased the threshold count to indicate an attack and abnormal activity.

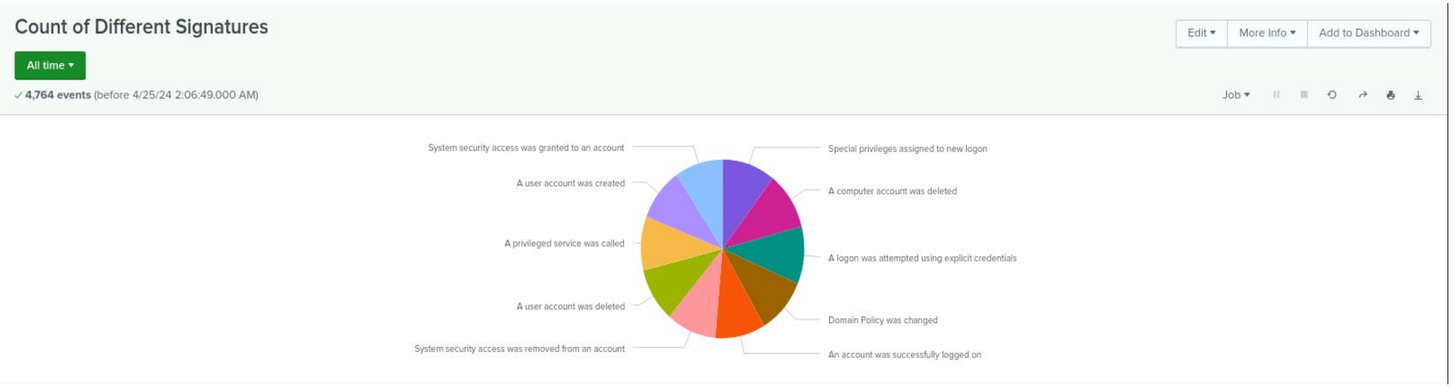
Dashboards—Windows

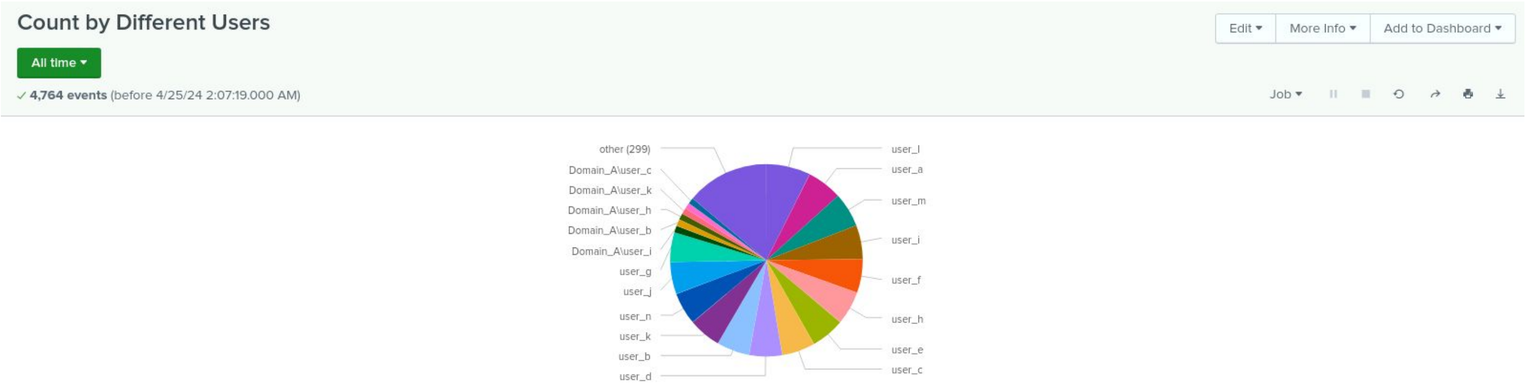




Dashboards—Windows







Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
Apache HTTP Methods	Table showing different HTTP methods (GET, POST, HEAD) and the counts for each
Top Domain Referers	Top 10 domains that sent traffic to VSI's website
HTTP Response Codes	Counts for each HTTP response code (200 for success, 404 for error, etc)

Images of Reports—Apache

Different HTTP methods

Edit | More Info | Add to Dashboard

All time

✓ **10,000 events** (before 4/25/24 2:14:46.000 AM)

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

Count of HTTP Responses

Edit | More Info | Add to Dashboard

All time

✓ **10,000 events** (before 4/25/24 2:16:04.000 AM)

Job

8 results 20 per page

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	
416	2	
403	2	

Domain Referer

Edit | More Info | Add to Dashboard

All time

✓ **10,000 events** (before 4/25/24 2:15:30.000 AM)

Job

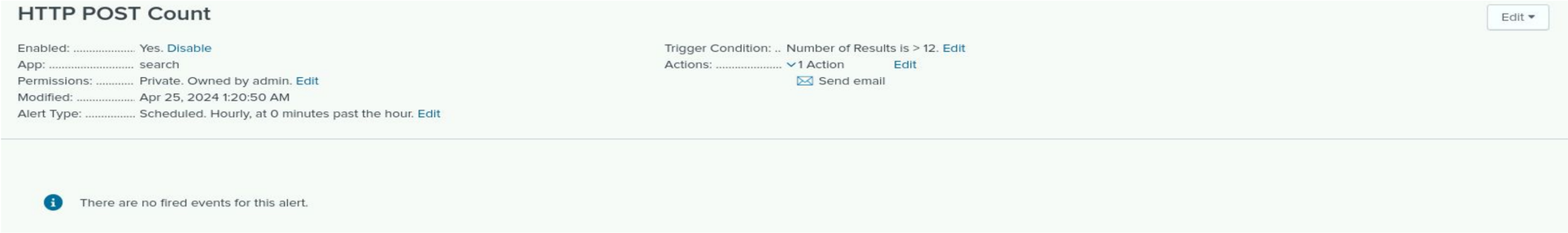
10 results 20 per page

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

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST hourly count	Increased activity	7	12

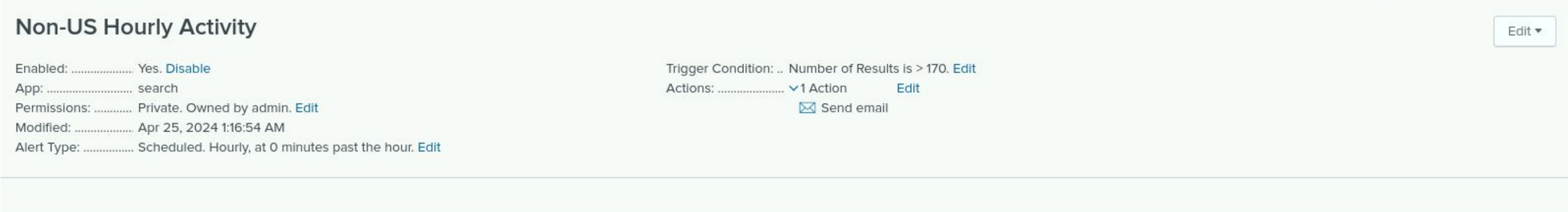


JUSTIFICATION: The highest peak per hour of normal POST activity was 7/hour, so we increased the alert to almost double that (12).

Alerts—Apache

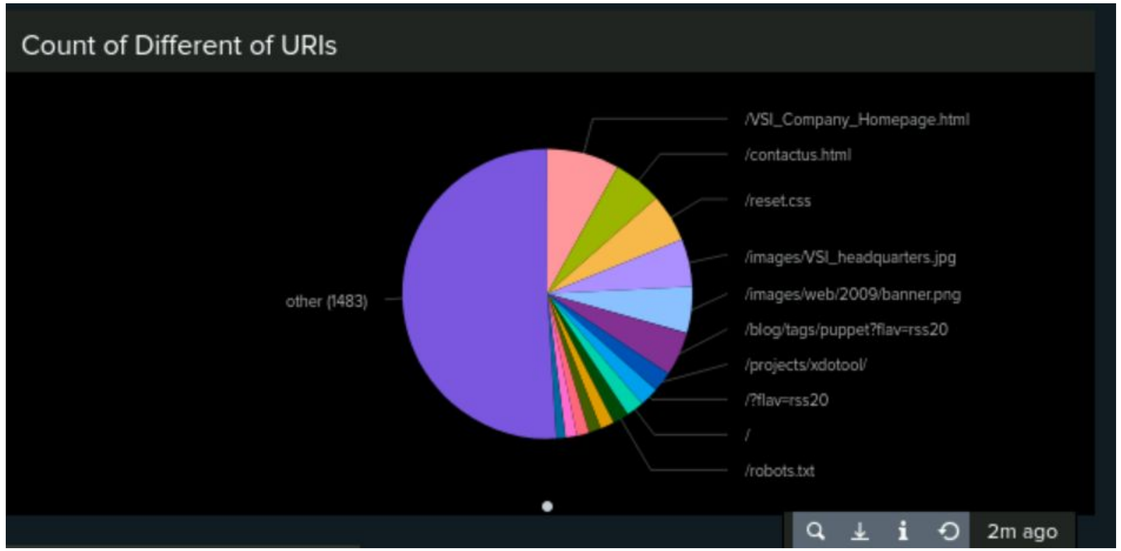
Designed the following alerts:

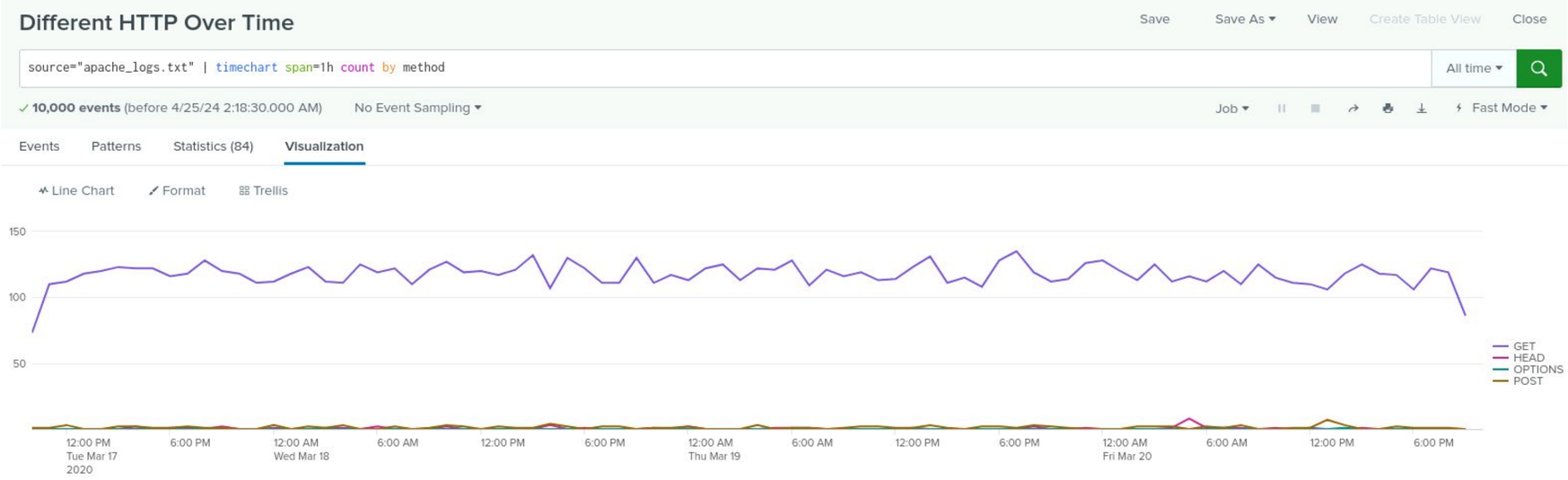
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Hourly Activity	Increased activity from outside the US	100	170



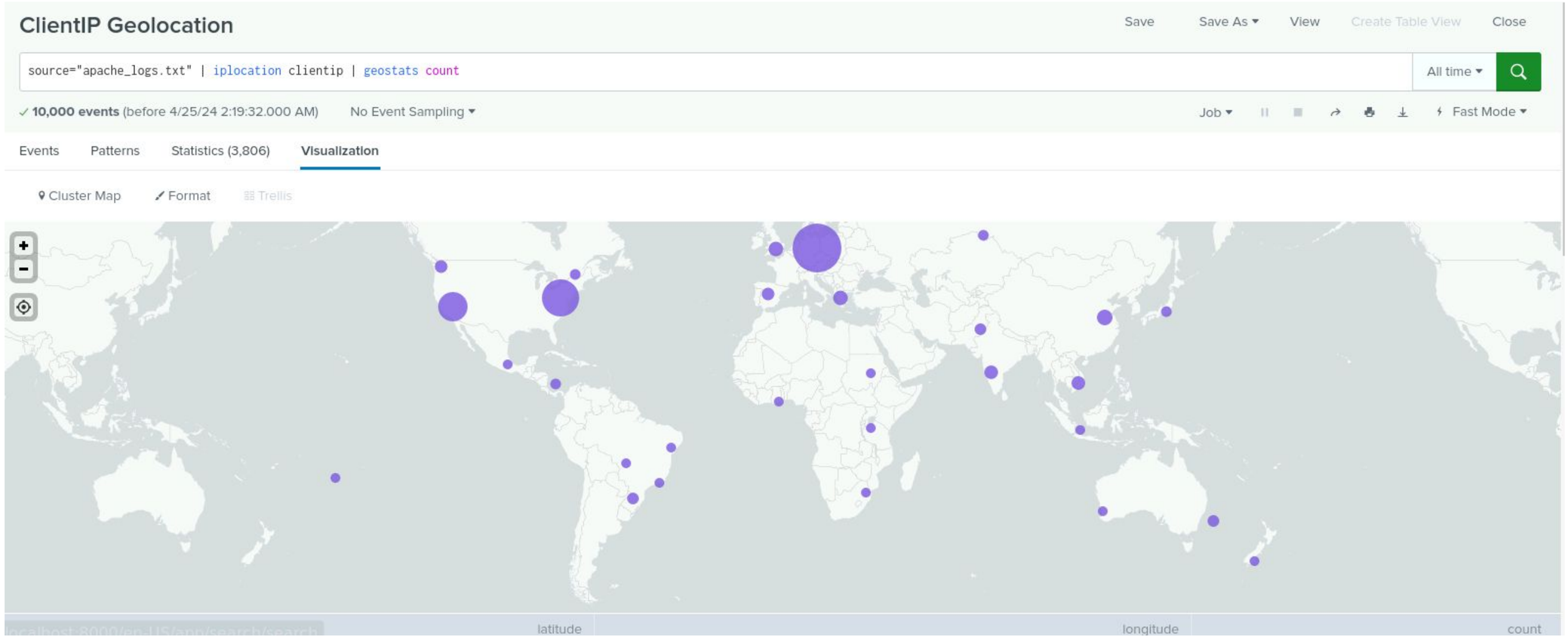
JUSTIFICATION: The average during normal activity was around 80-90 per hour. We doubled that to look for abnormal activity.

Dashboards—Apache

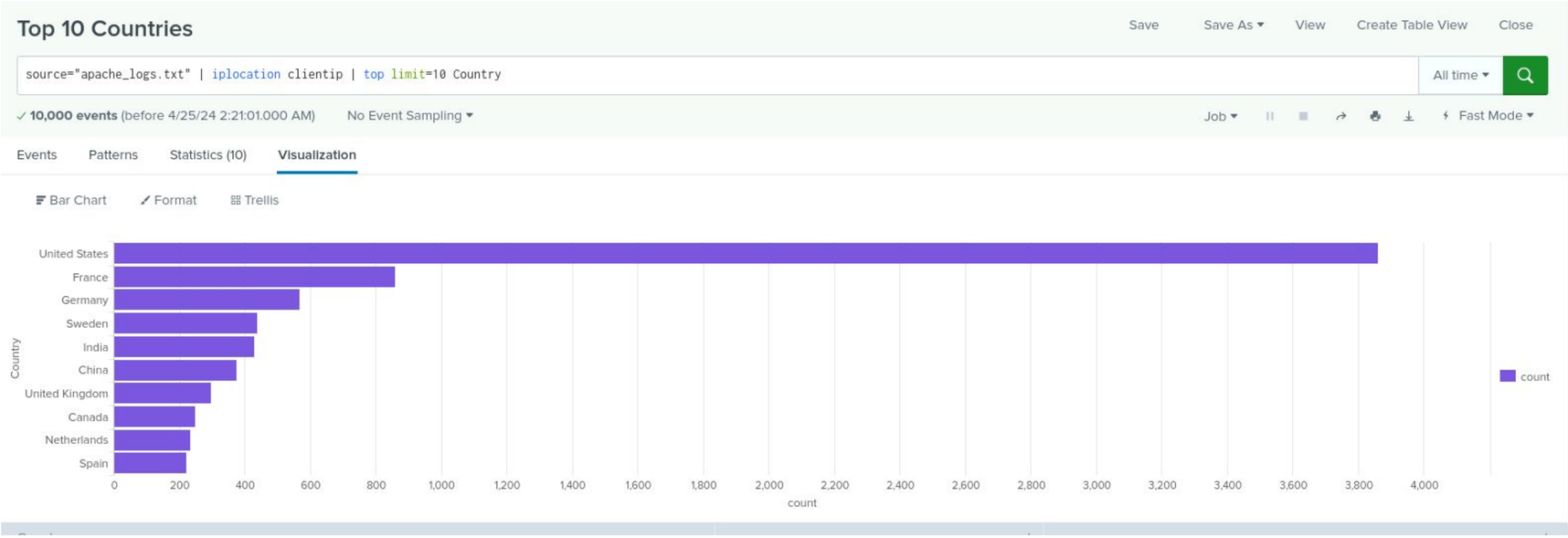


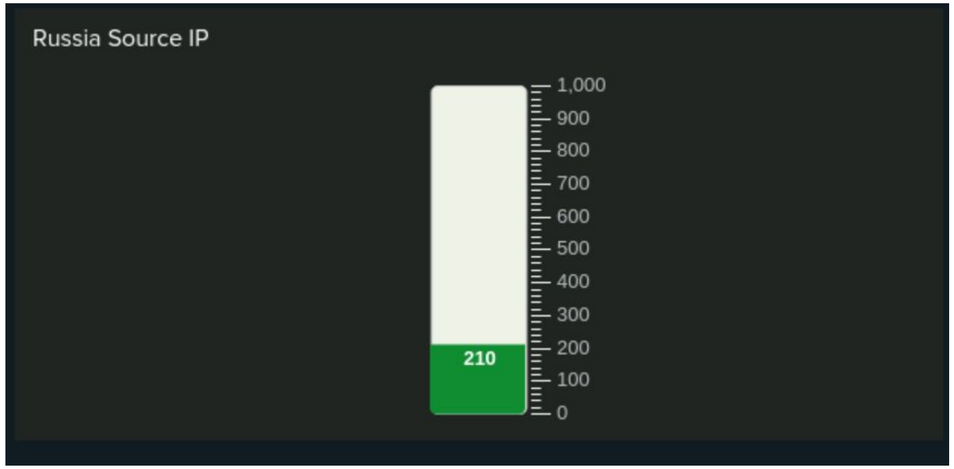


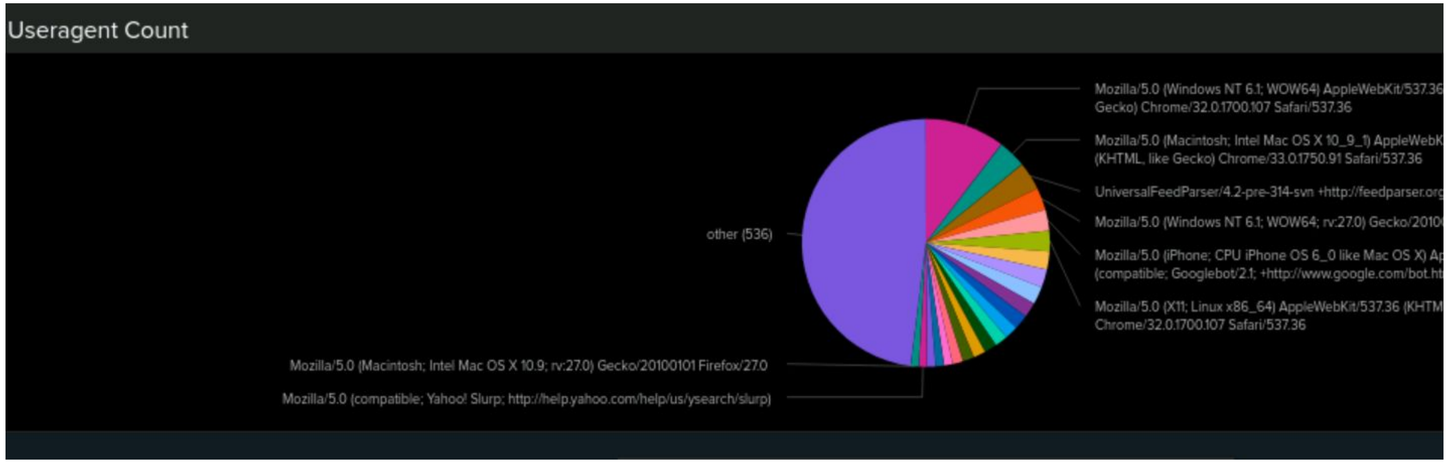
Dashboards—Apache



Dashboards—Apache (2)







Attack Analysis

Attack Summary—Windows

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

- We noticed an increase in high severity level activities indicating a potential attack. We also noticed a spike in failed windows activities at 8am on the 25th.

- After analyzing the failed windows activites, it was evident that this sudden increase in attempts could indicate malicious activity, such as brute force or user enumeration.

Attack Summary—Windows

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

- At 8am on the 25th the number of failed windows activity rose to 35, above normal levels indicating a potential attack.
- We noticed suspicious activities starting 11am with a spike in successful logins particularly from **user_K**. There was no particular spike in the number of deleted accounts was noticed.

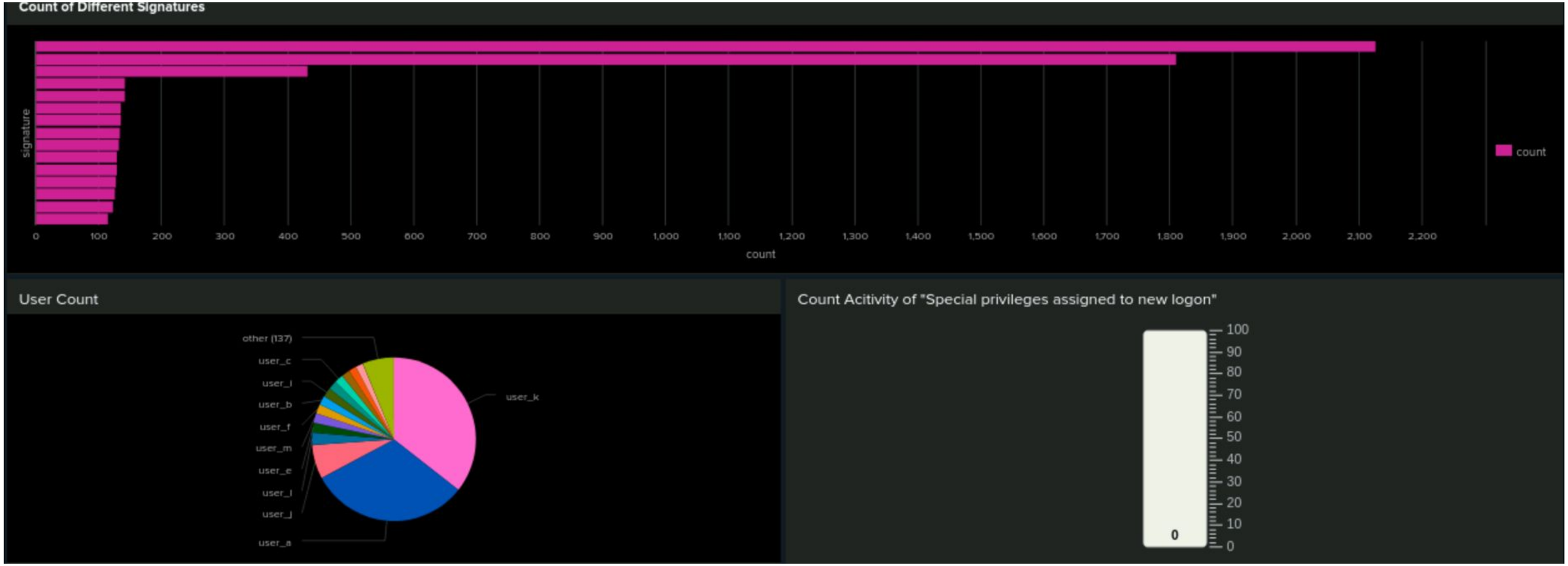
Attack Summary—Windows

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

- **We detected a high volume of event from 2 signatures:**
  - **A user account was locked out:** Starting 12am with a count of 896
  - **An attempt was made to reset an account password:** Starting 8am with a count of 1258
- **We detected spikes is login activities for 2 users:**
  - **user_a**, count of 984 at 12am
  - **user_k**, count of 1256 at 8am

Screenshots of Attack Logs

Screenshots of Attack Logs



Attack Summary—Apache

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

- There was a large increase in POST activity.
- There was in increase in failed (404) responses, indicating we had multiple attempts on accessing a specific site without any redirection.
- Two users in particular, **user_a** and **user_k**, show an increase in activity in two different 3-hour window section, indicating that one of them was responsible for the attack.

Attack Summary—Apache

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

- The alerts would have successfully indicated an increase in non-US domains and an increase in POST activity on the server, further helping with our investigation.

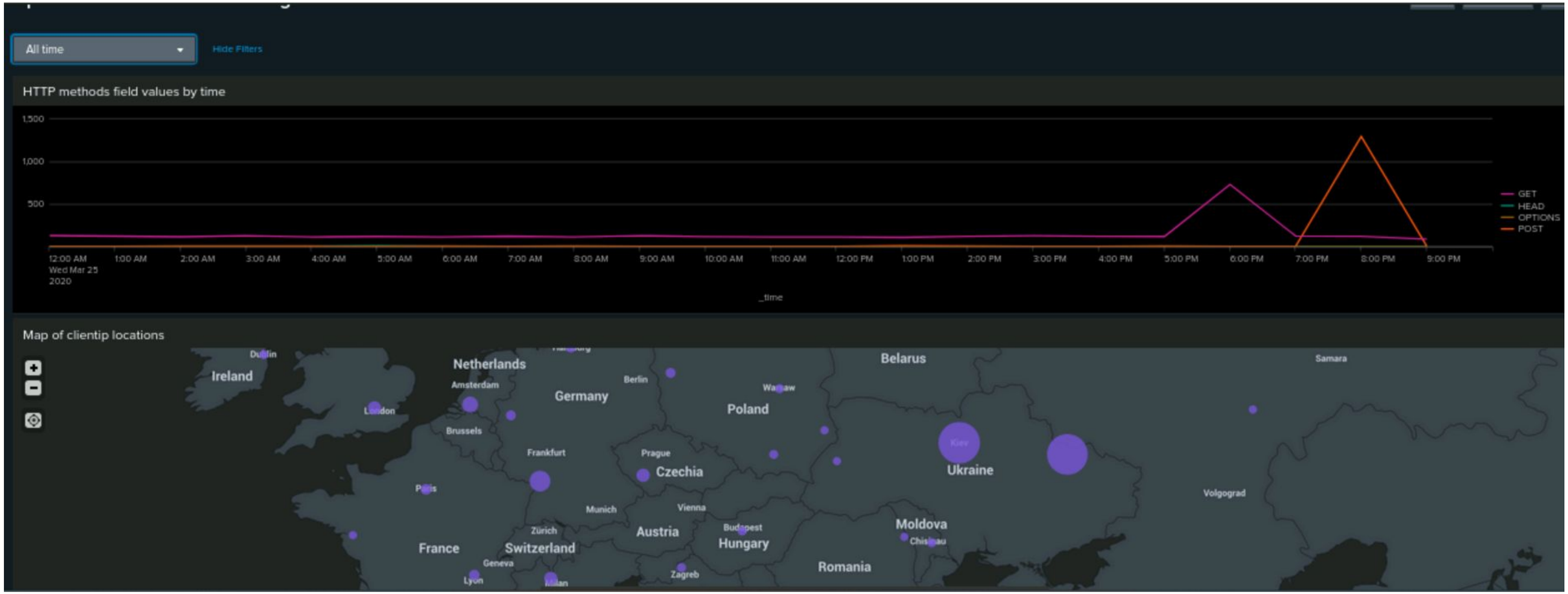
- The thresholds were correct but could've been adjusted and would achieve the same results.

Attack Summary—Apache

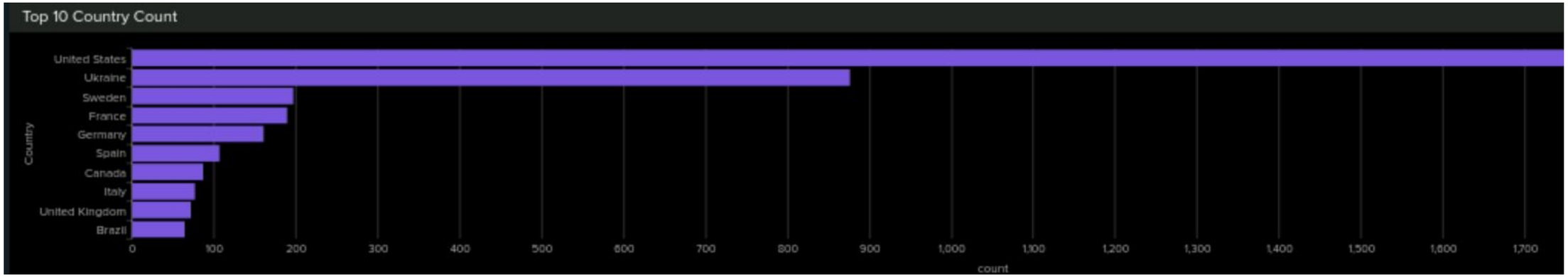
Summarize your findings from your dashboards when analyzing the attack logs.

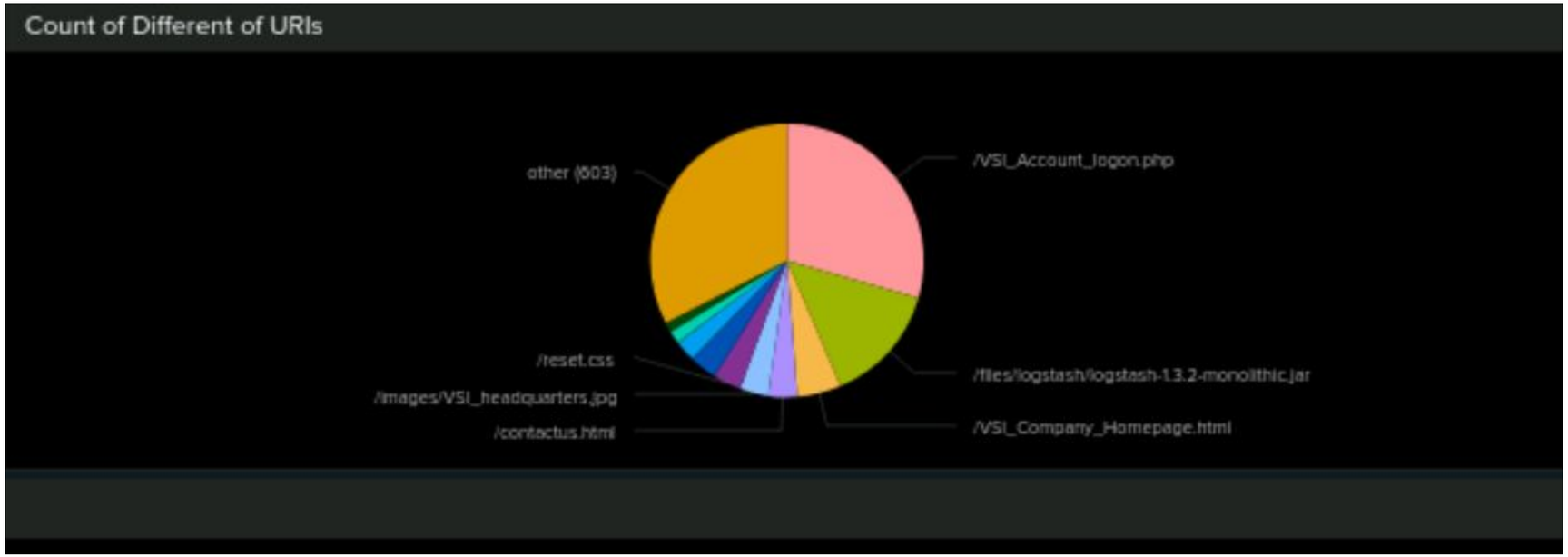
- We detected a spike in activities for GET at 6PM and in POST activity at 8PM; count of 1296.
- Geolocation data showed a spike in activity from Ukraine, Kiev (Kyiv).
- We also detected a spike in activities for 2 URIs 6-8pm with the most hit being: /VSI_Account_logon.php (1,296 events at 8PM), indicating a potential brute force attack.

Screenshots of Attack Logs



Screenshots of Attack Logs (2)





Summary and Future Mitigations

Project 3 Summary

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

There was a brute force attack that originated in Ukraine. After further analysis, we concluded that **user_a** was responsible for the attack although there was other suspicious user activities.

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

- Two-Factor Authentication (2FA)
- Account lockout after 5 failed attempts
- IP Access Restrictions

TRUE STORY

International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war

More than 20 investigators from Norway, France, Germany and the United States were deployed to **Kyiv** to assist the Ukrainian authorities in November 2023.

These attacks are believed to have affected over 1,800 victims in 71 countries. The perpetrators targeted large corporations, bringing their business to a standstill and causing losses of at least hundred millions of euros.

Those responsible for breaking into networks did so through techniques including brute force attacks, SQL injections and sending phishing emails with malicious attachments in order to steal usernames and passwords.

The forensic analysis carried out in the framework of this investigation also allowed the Swiss authorities to develop, together with the No More Ransom partners and Bitdefender, decryption tools for the LockerGoga and MegaCortex ransomware variants. These decryptions tools have been made available for free on: www.nomoreransom.org.