Defensive Security Project
by: Alex, Nickson, Liz, Samantha, Iain, and Samuel

Table of Contents

This document contains the following resources:

01 **Monitoring Environment**

02 **Attack Analysis**

03 **Project Summary & Future Mitigations**

Monitoring Environment

Scenario

- Today, you will play the role of an SOC analyst at a small company called Virtual Space Industries (VSI), which designs virtual-reality programs for businesses.
- VSI has heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business.
- As an SOC analyst, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.
- The VSI products that you have been tasked with monitoring include:
  - An administrative webpage: https://vsi-corporation.azurewebsites.net/
  - An Apache web server, which hosts this webpage
  - A Windows operating system, which runs many of VSI's back-end operations

Whoisxml IP Geolocation API

Whoisxml IP Geolocation API

Whoisxml IP Geolocation API for Splunk is a tool designed to provide geolocation data for IP addresses directly within the Splunk platform.

- This add-on allows splunk users to search for geographical information based on the IP addresses present in their logs or datasets. Add-on information:
  - Country
  - City
  - Latitude
  - Longitude
  - Postal Code
  - VPN

This integration allows for the filtering of geographical origins of network traffic, users, or other relevant data points, assisting in security analysis, compliance, and business intelligence. This API retrieves information of IP address data, providing accurate and up-to-date geolocation data to enhance the analysis capabilities of Splunk users.

Whoisxml IP Geolocation API

This tool is helpful for being able to note specific locations of ip addresses better than the cluster map itself.

On the cluster map, it's very easy to miss any small new locations without zooming in and inspecting every country very closely. With this, we were able to find a new clientip location in Kiev, Ukraine.

Whoisxml IP Geolocation API (example)

Spain

El Salvador

Logs Analyzed

1 | **Windows Logs**

These logs contained incidents that occurred on the Windows server. The incident signatures had a correlated ID and severity level, and displayed whether they were a success or failure. Some of these incidents included successful logins, deleted accounts, and user activity on the server.

2 | **Apache Logs**

These logs examine routine activity from the Apache web server for VSI. The activities display the HTTP type, the top 10 domains, and the quantity of each HTTP response code.
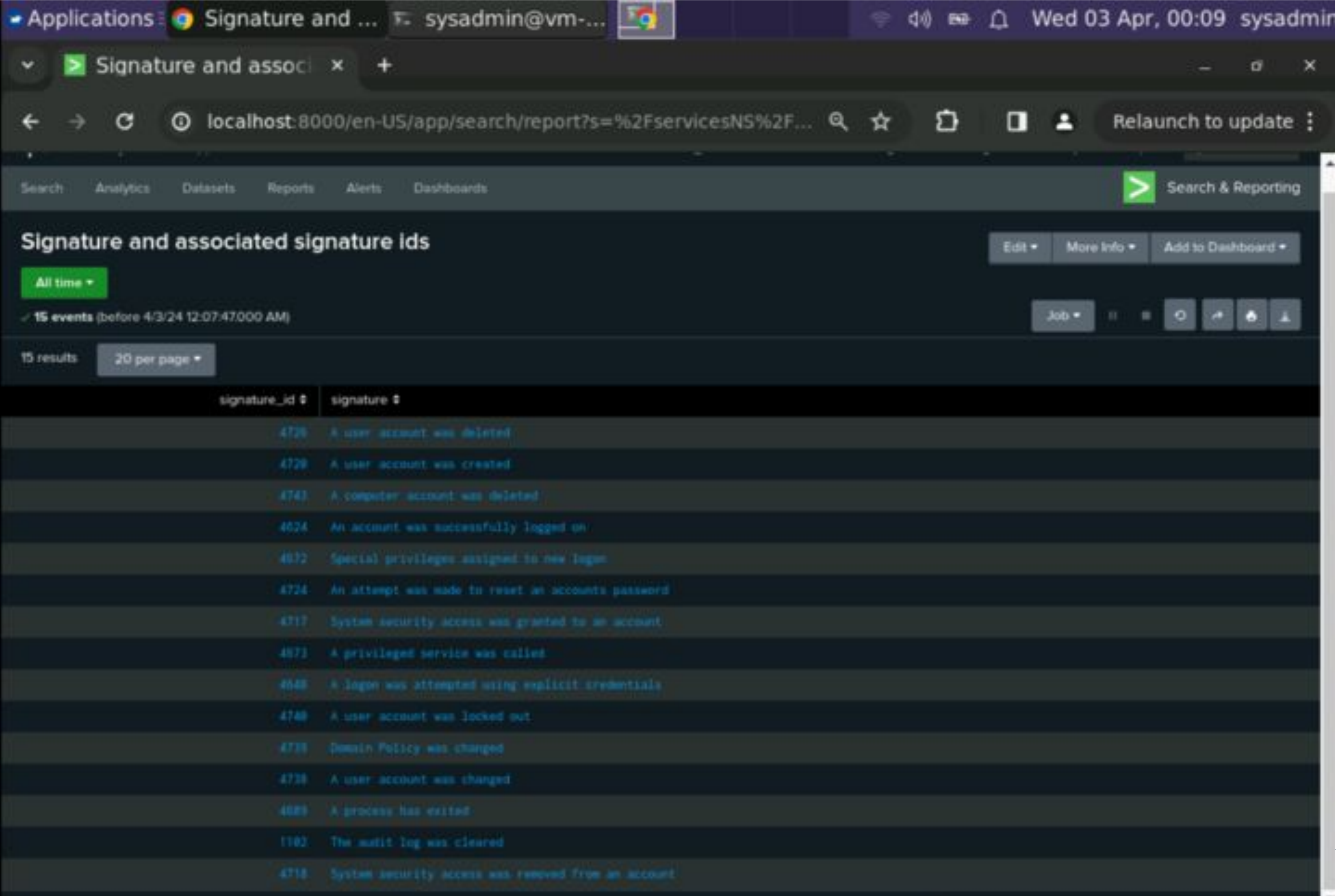
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signature and associated signature IDs	A table of signatures and associated signature IDs
Severity level, count, and percentage	Severity levels with count and percentage of each
Success vs. failure	Comparison of success and failures of windows activities

Images of Reports—Signature and associated signature IDs

Images of Reports—Severity level, count, and percentage

Images of Reports—Success vs. failure

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Status failure	An email is sent to SOC@VSI-company.com when the threshold of failed windows activity is crossed.	6	greater than 7

JUSTIFICATION: The average amount of failed Windows activity averaged around 6 to establish our baseline yet never got close to 7. Failures exceeding 7 would certainly indicate suspicious activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful logins	An email is sent to SOC@VSI-company.com when the threshold of successful logins is crossed.	14	greater than 15

JUSTIFICATION: The average amount of logins, designated by signature id "4624," averaged around 14 to establish our baseline yet never got close to 15. Failures exceeding 15 would certainly indicate suspicious activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User account deleted	An email is sent to SOC@VSI-company.com when the threshold of deleted accounts is crossed.	13	greater than 14

JUSTIFICATION: With the amount of user accounts deleted, designated by signature id "4743" in this log, we were able to determine a baseline of 13 seemed on par with a "normal" hour. Exceeding 14 would raise suspicion levels and indicate a problem.

Dashboards—Windows

Trends for signatures over time
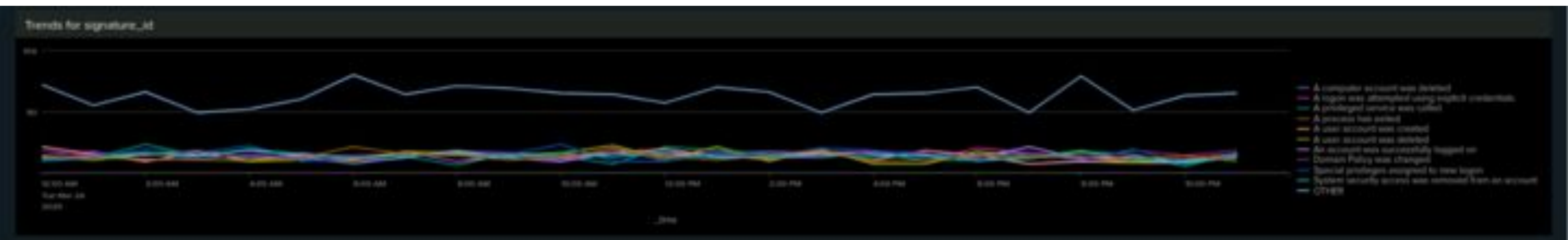
Different User field values over time

Dashboards—Windows
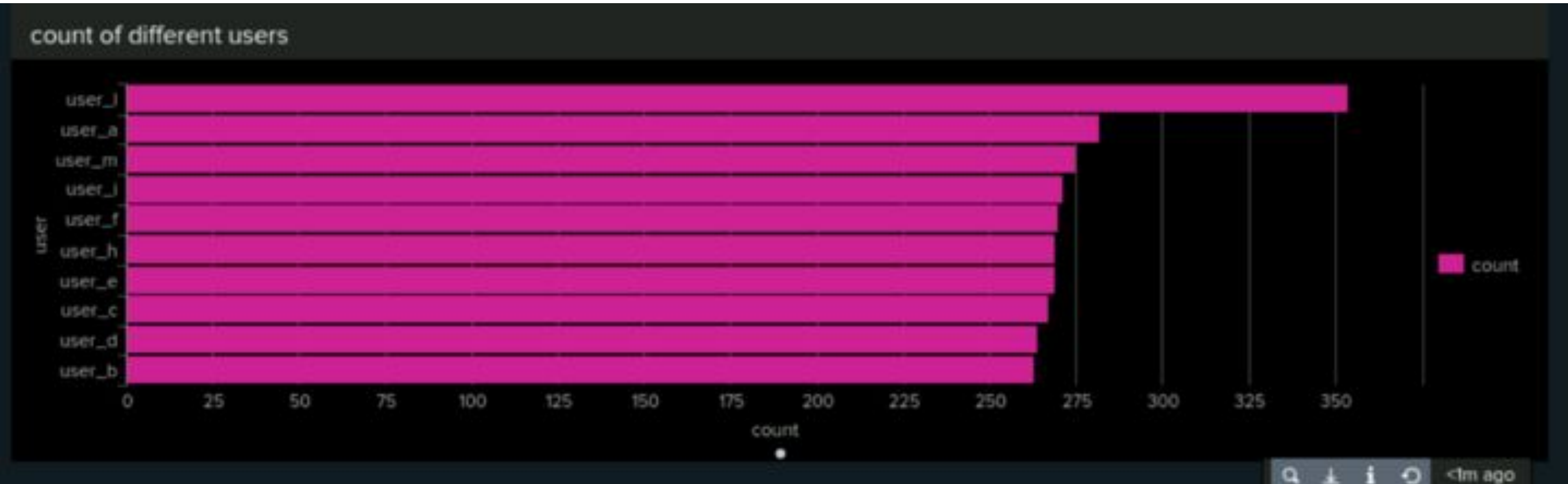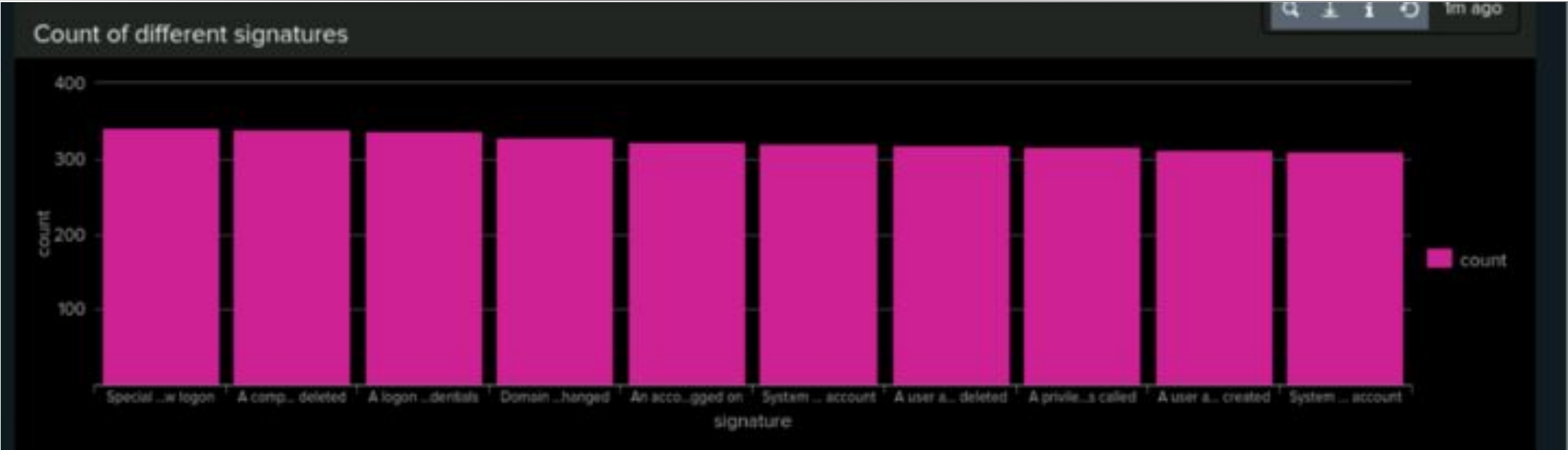
Dashboards—Windows

Different user counts
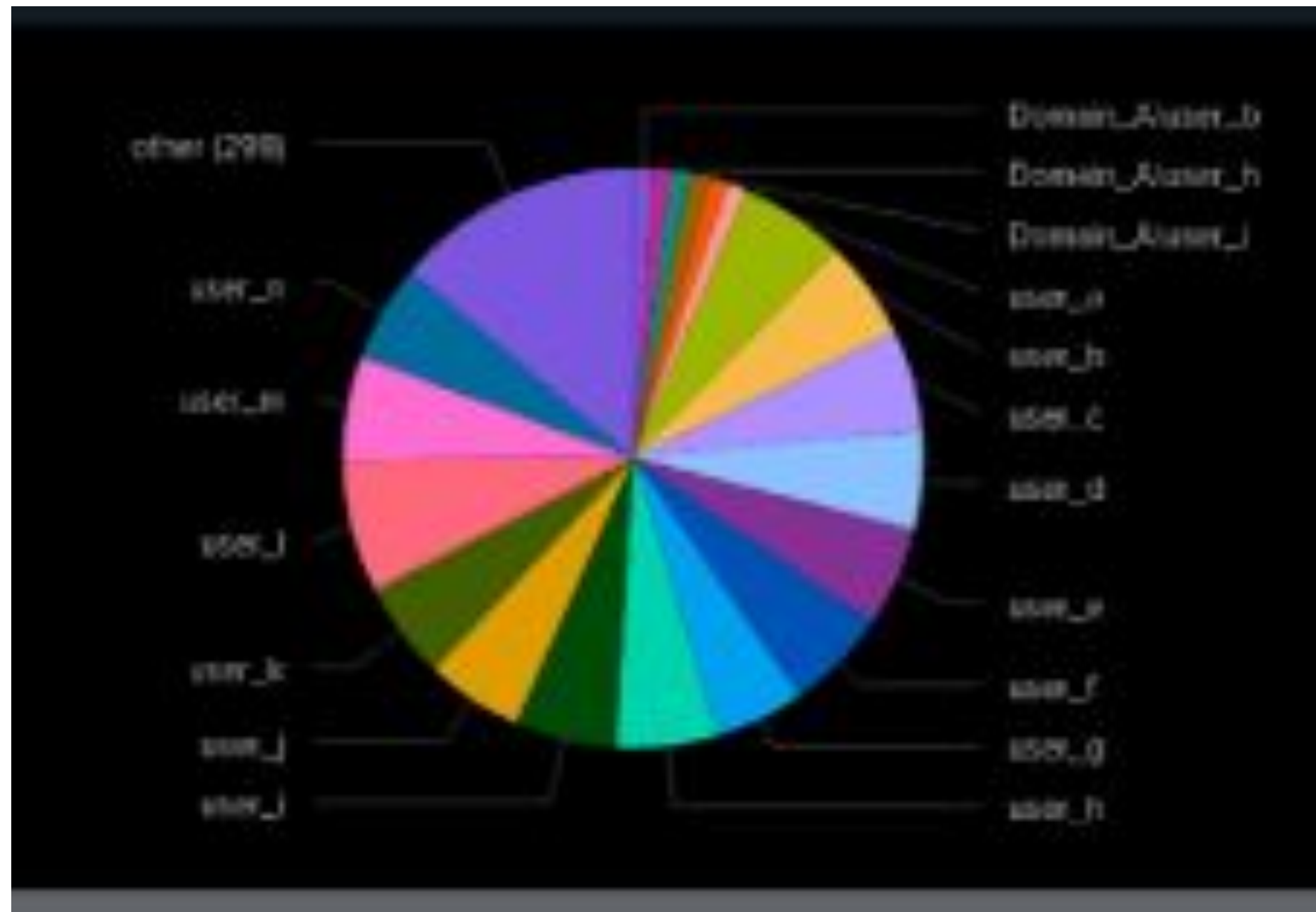
Timechart signature ID
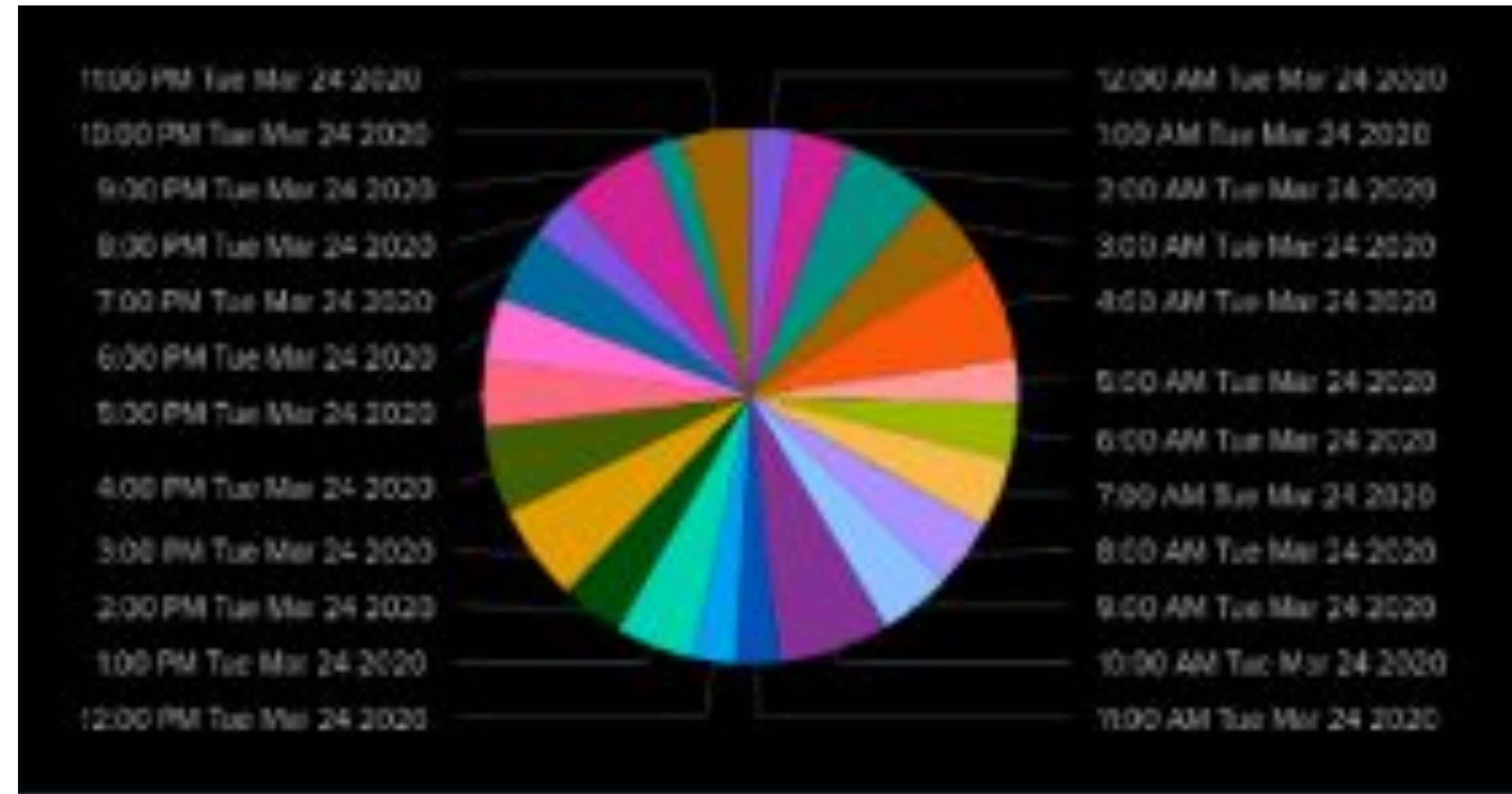
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Provides insight into the type of HTTP activity being requested against VSI's web server.
Top 10 Domains	Shows the top 10 domains that refer to VSI's website.
Count of HTTP Response Code	Shows the count of each HTTP response code.

Images of Reports—Top 10 Domains

Images of Reports—HTTP Methods

Images of Reports—Count of HTTP Response Code

Count of each HTTP response code

All time ▾

✓ **10,000 events** (before 4/3/24 1:59:41.000 AM)

Edit ▾   More Info ▾   Add to Dashboard ▾

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	0.030000
416	2	0.020000
403	2	0.020000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-USA Activity	Alert if the hourly activity from any country besides the United States exceeds the threshold.	94	95 or above

JUSTIFICATION: 94 events in a hour seemed standard in the logs, yet exceeding 95 seemed unlikely on a normal day. Seeing any number of events greater than the threshold would indicate issues.

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Count	Alert if the hourly count of the HTTP POST method exceeds the threshold	3	4 or above

JUSTIFICATION: Most events per hour hovered between 1 and 3 and never surpassed 3. A threshold of 4 seemed like a number that would be out of reach of "normal" hourly events but small enough to catch malicious activity.

Dashboards—Apache

Different HTTP methods
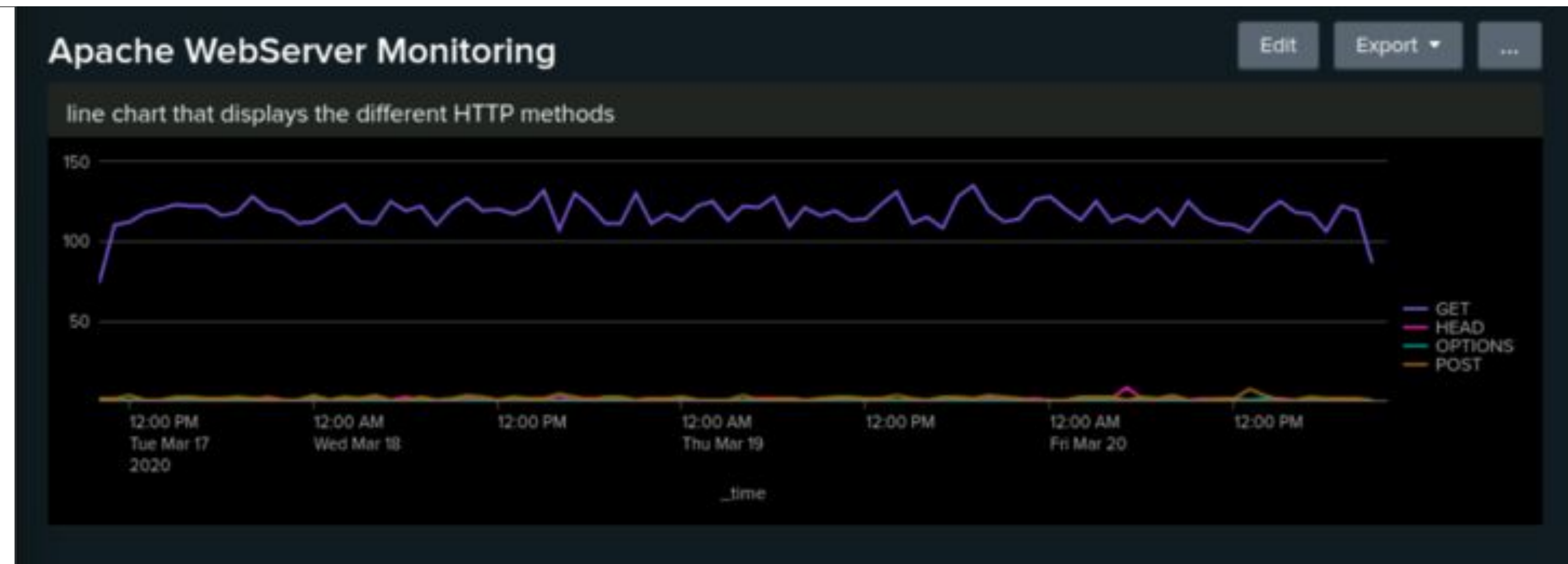
Geographical map
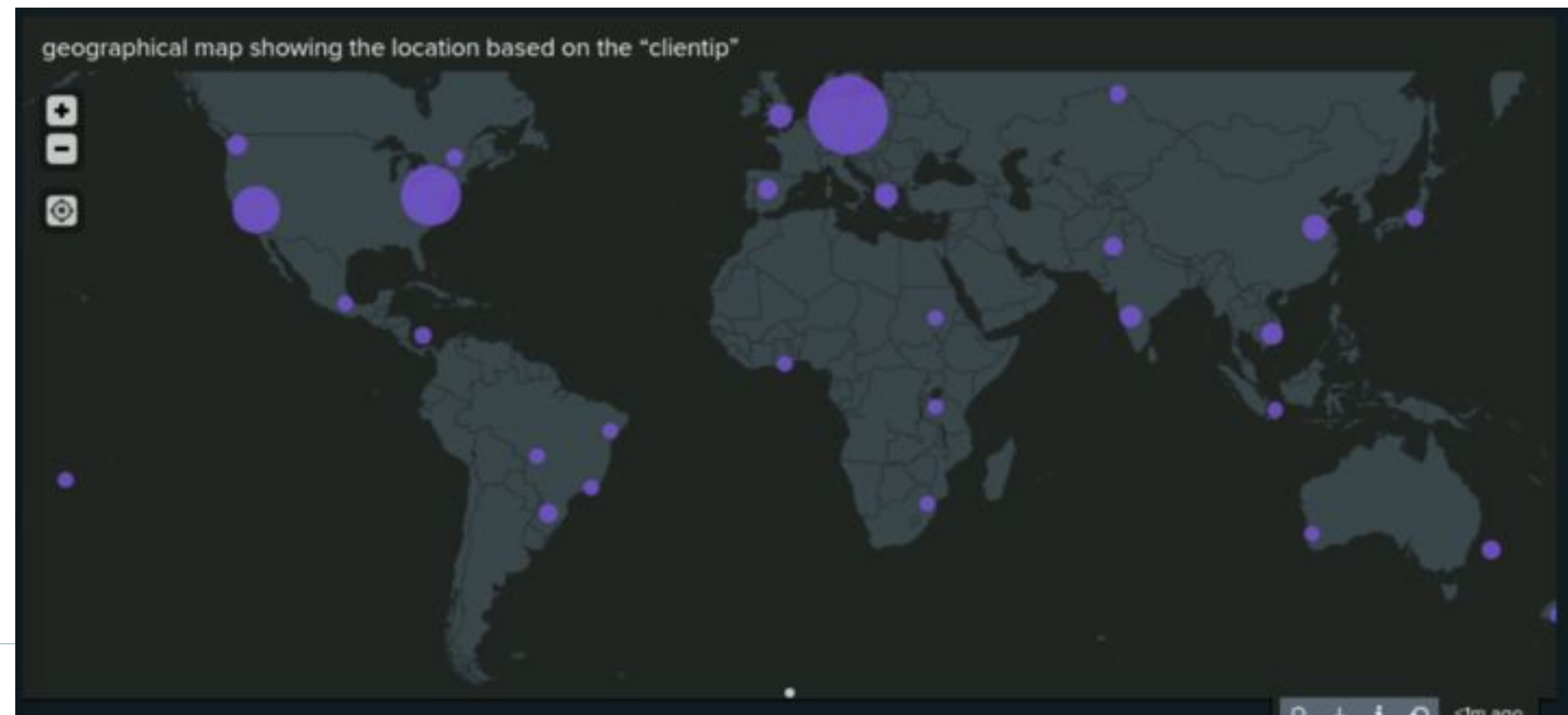
Dashboards—Apache

Different URIs
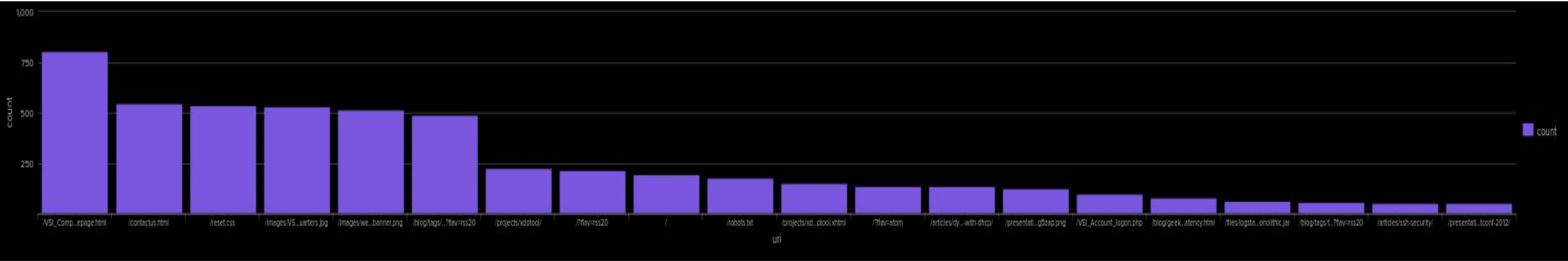
Top 10 Countries
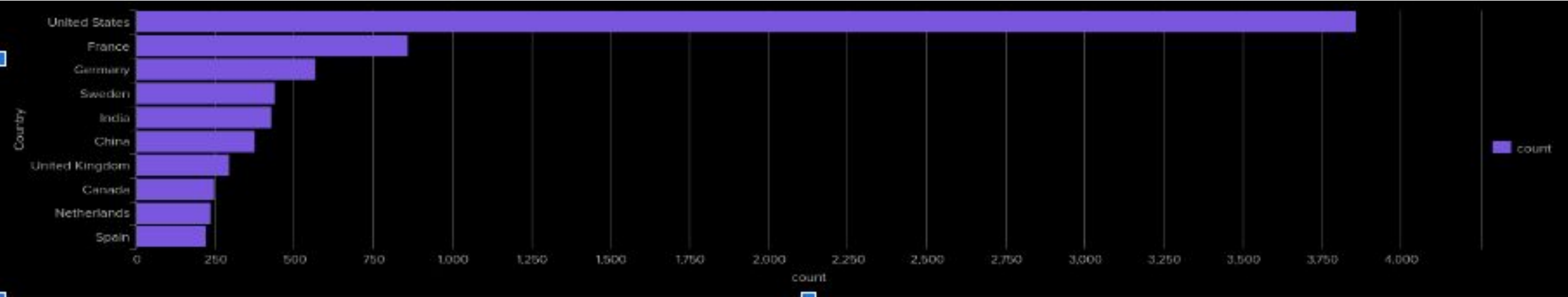
Dashboards—Apache

User Agents

Root Processes
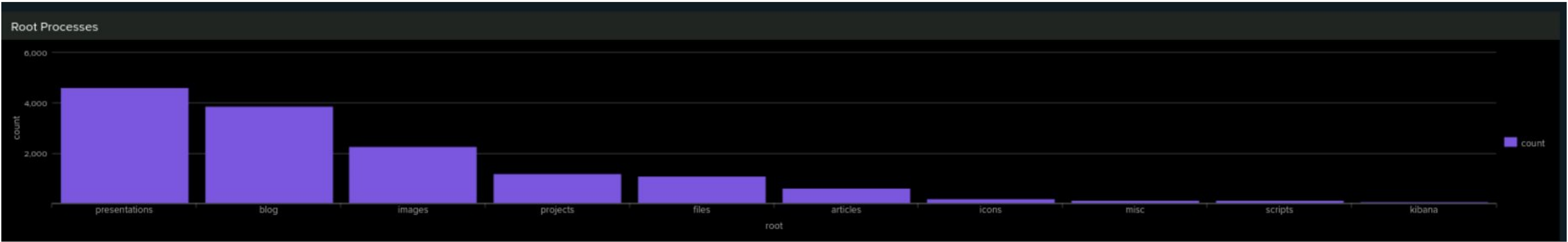
Attack Analysis

Attack Summary—Windows

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

- Upon analyzing Windows attack logs, it was found that the Windows attack system exhibited more severity levels in the "high" category(20%) compared to almost 7% in the "high" category observed before the attack. Furthermore, there were more successes(97% to 98%) than failures(2.9% to 1.5%) noted after the attack. Alert analysis indicated a suspicious volume of failed windows activity. Specifically, 35 failed logins occurred at 8 am on 3/25/2020, exceeding the threshold, with no recommended changes. Additionally, suspicious volumes of successful logins were detected, with 1256 events recorded in one hour, primarily attributed to the user "user_k" logging in at 10 am to 1 pm on 3/25/2020. The alert threshold of >15 was exceeded, suggesting a sufficient threshold.

Attack Summary—Windows

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

- An alert analysis indicated a suspicious volume of failed activity. There was a suspicious volume of deleted accounts, with the threshold set to >14. Notable signatures included "A user account was locked out" and "An attempt was made to reset an account's password," with specific start and stop times for each signature. "A user account was locked out" occurred from 12:00 am to 3:00 am, while "An attempt was made to reset an account's password" happened from 8:00 am to 11 am, peaking at 896 and 1258, respectively. Successful logons happened from 10:00 am to 1:00pm and peaked 196.

Attack Summary—Windows

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

Findings from dashboards analyzing attack logs revealed suspicious activity associated with 3 users:

- User_a (locked out) 12am - 3am

- User_k (password reset) 8am-11am

- User_j (an account successfully logged on) 10am-1PM

Attack Summary—Windows

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

Findings from our alerts when analyzing the attack logs indicated the following:
We detected a suspicious volume activity in 3 hour increments:

- User locked out 12am - 3am

- Password reset 8am-11am

- An account successfully logged on 10am-1PM

Our thresholds were set a little bit lower than they were supposed to be, but our alert would have been triggered for all 3 alerts not long after suspicious activity started.

Attack Summary—Windows

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

- Suspicious activity was observed in two users, User_A and User_K. User_A's activity occurred from 12 am to 3 am, while User_K's activity spanned from 8 am to 11 am. The peak count of different users was 984 for User_A and 1256 for User_K.

- There was suspicious activity associated with signatures, particularly "A user account was locked out" and "An attempt was made to reset an account's password," both exhibiting very high volumes of activity. The first signature lasted from 12 am to 3 am, while the second occurred from 8 am to 11 am. "A user account..." peaked at a count of 896, and "An attempt..." peaked at 1258.

Screenshots of Windows Attack Logs

Successful Logins
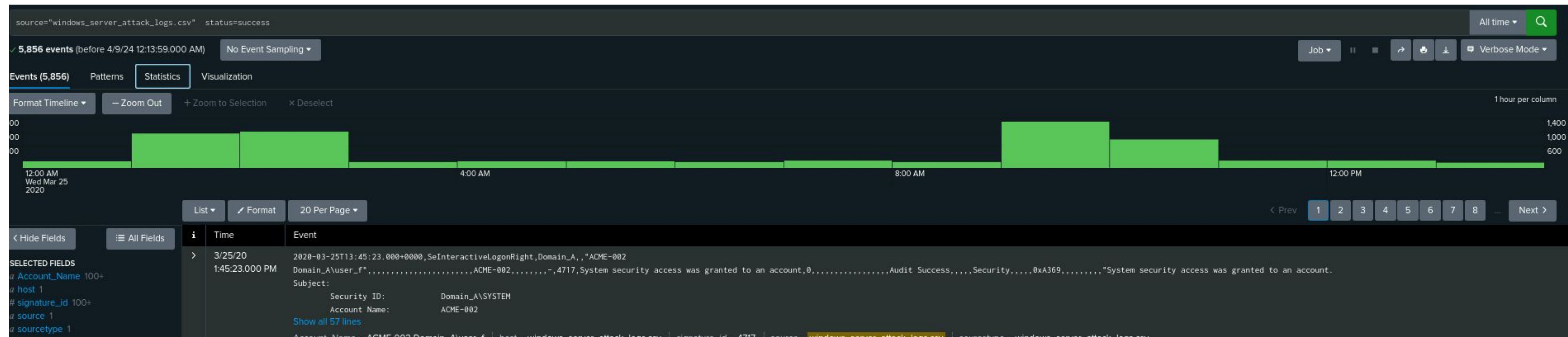
Failed Logins

Attack Summary—Apache

Summarize your findings from your reports when analyzing the attack logs

Findings from our reports when analyzing the attack logs indicated the following:

- We saw an increase in POST requests by around 1,200.

- There were no suspicious changes in referrer domains.

- The number of 404 response codes increased by almost 500.

Attack Summary—Apache

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

Findings from our alerts when analyzing the attack logs indicated the following:
- We detected a suspicious volume of international activity between 8pm and 9pm on March 25, reaching a peak of 957 events during that hour.
- We detected a suspicious volume of HTTP POST activity between 8pm and 9pm on March 25, reaching a peak of 1,296 events during that hour

Our threshold for international activity was set appropriately, whereas our threshold for HTTP POST activity was set a bit lower than needed, however our alert would have triggered for both alerts shortly after any suspicious activity started.
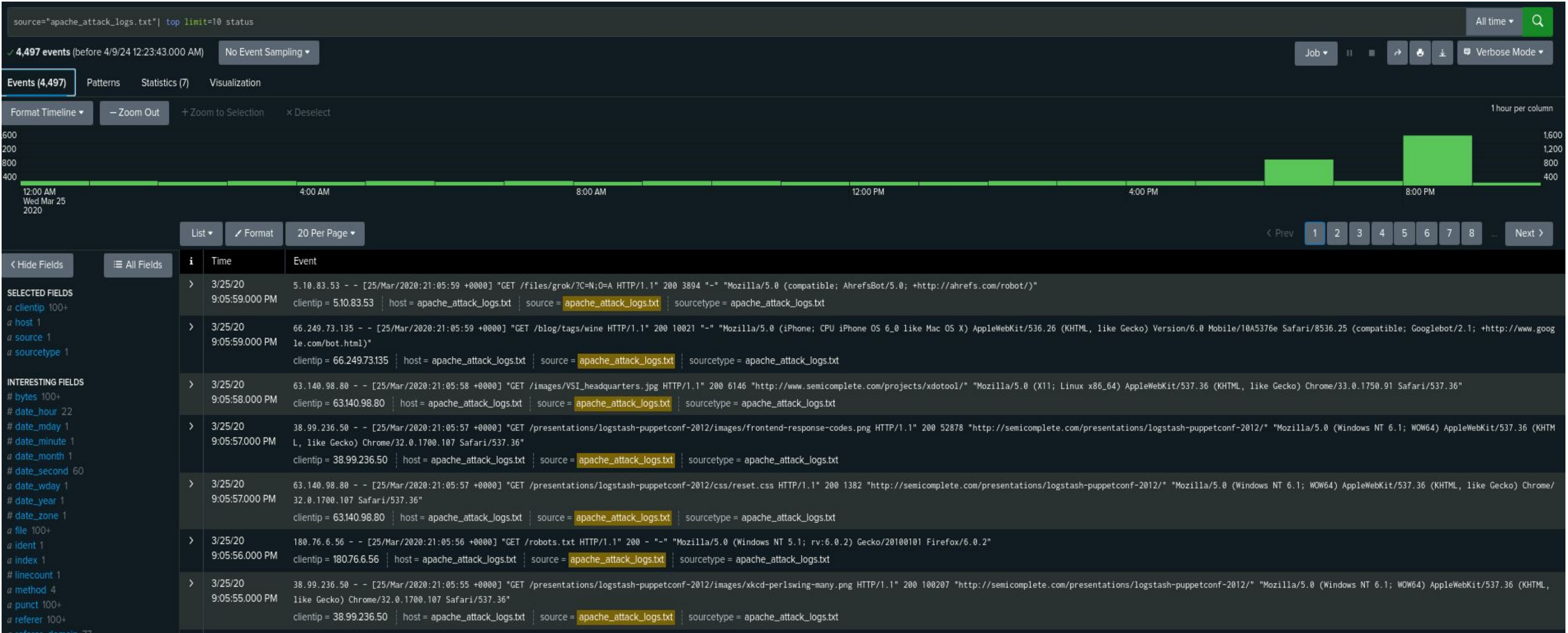
Attack Summary—Apache

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

Findings from our dashboards when analyzing the attack logs are as follows:

- Our Time Chart of HTTP methods revealed suspicious volumes of GET and POST methods. Specifically, the GET attack occurred from 5 pm to 7 pm and peaked with a count of 729, while the POST attack spanned from 7 pm to 9 pm and peaked with a count of 1,296.

- Our Cluster Map revealed suspicious activity from several cities, including Kiev (439) and Kharkiv (433), all exhibiting high volumes of activity.

- Our URI Data flagged "/VSI_Account_logon.php" as having suspiciously high volume.

Screenshots of Apache Attack Logs

Summary and Future Mitigations

Project 3 Summary

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

  Our investigation revealed that on March 25th, VSI experienced multiple attacks on both its Windows and Apache servers. These attacks primarily involved brute-force attacks originating from various regions and countries worldwide.

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

  To safeguard VSI from future attacks, we recommend implementing the following mitigations:

  Adoption of two-factor authentication, serving as the primary defense mechanism against brute-force attacks.

  Implementation of user lockout mechanisms after a specified number of unsuccessful login attempts to deter and mitigate potential future attacks