Defensive Security Project

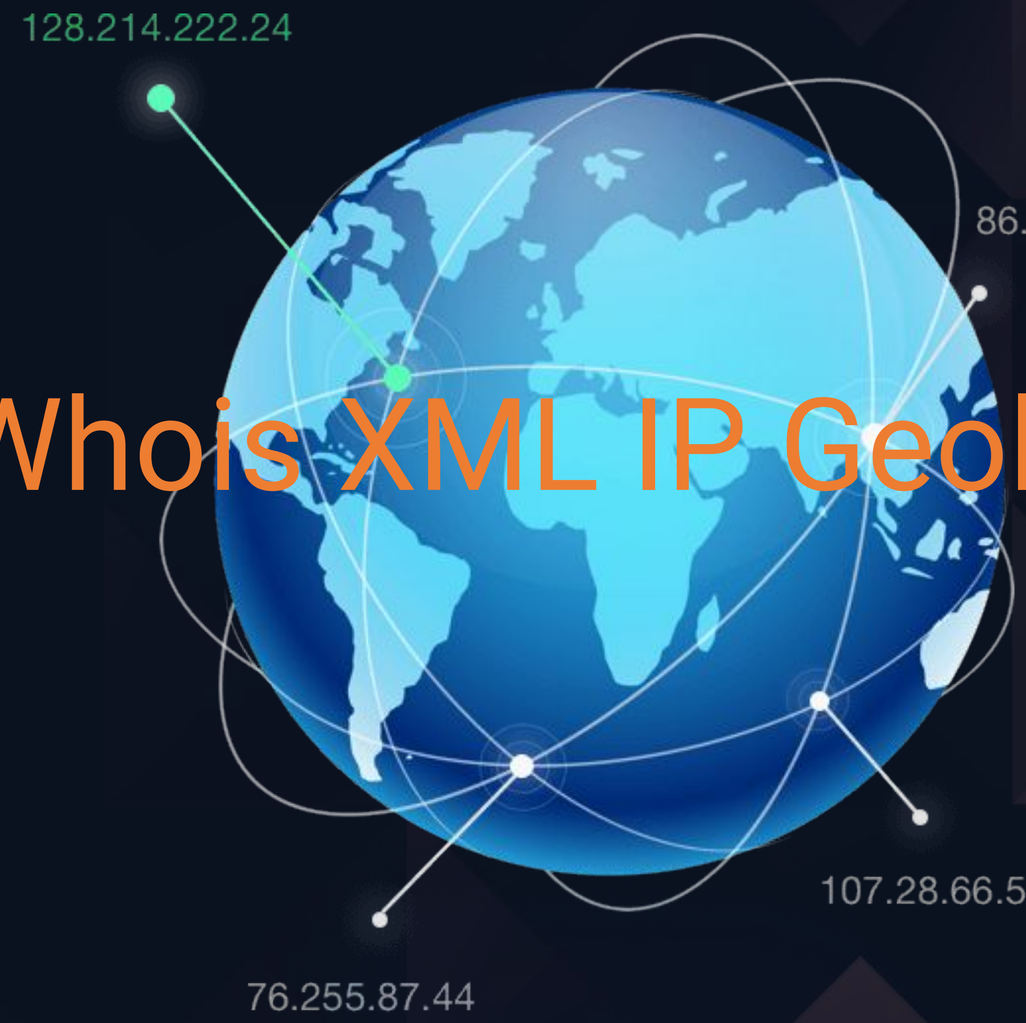
Matthew Borg
Owen Jones
Scott Stapleton
Alec Ward
Harrison Wright

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

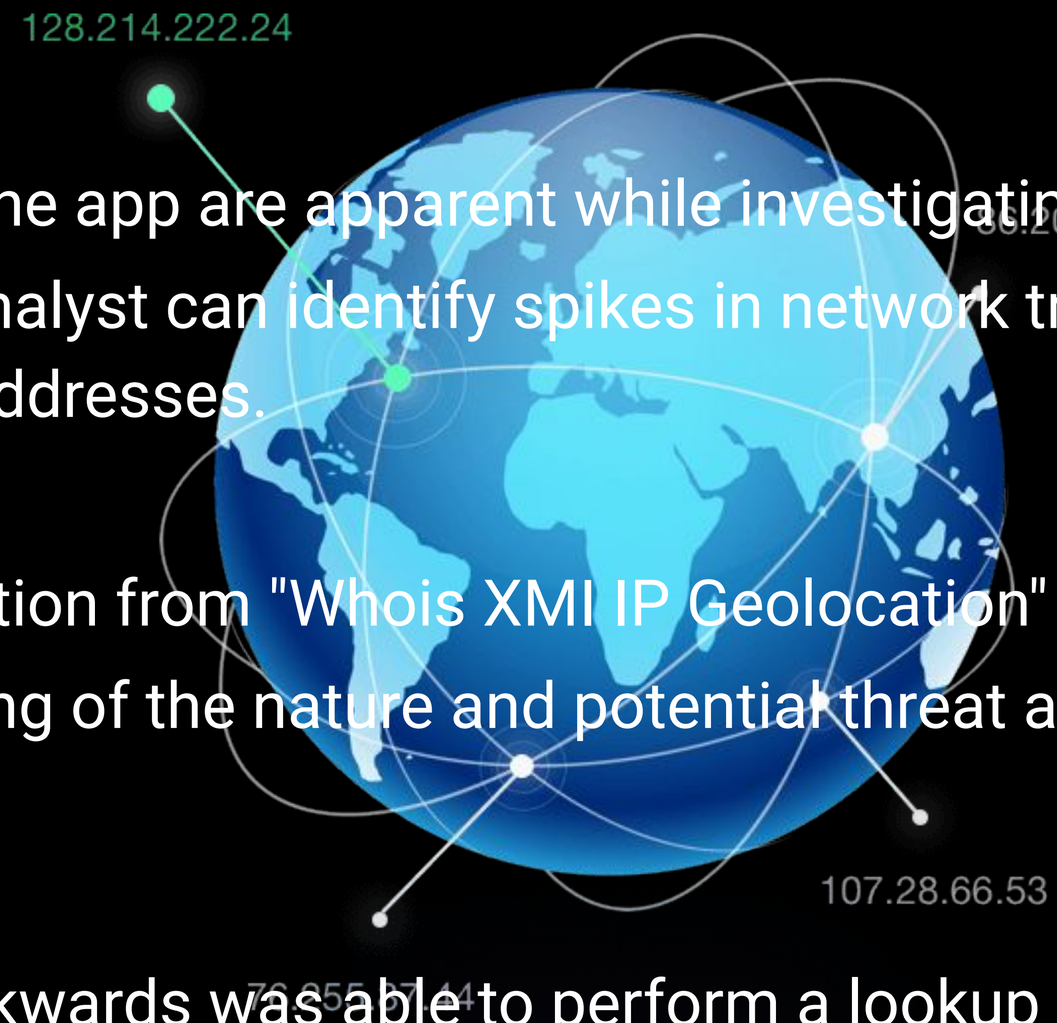


Whois XML IP Geolocation

Whois XMl IP Geolocation

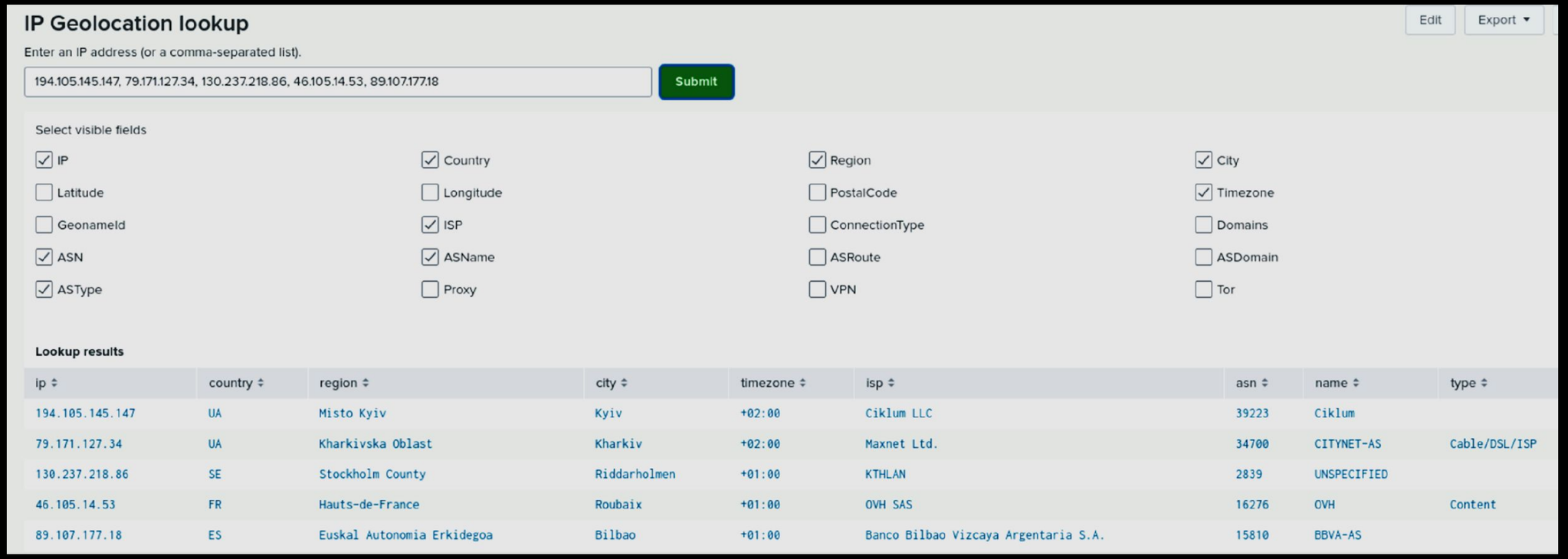
- The Whois XML IP Geolocation API app for Splunk is an app that allows you to identify the geographical location of your web visitors and users based on their IP addresses.
- This app can customise web experiences, prevent fraud, ensure regulatory compliance, and more.
- You can perform instant lookups on the IP Geolocation lookup page, or you can integrate the app into your script using the wxageoip command.

Whois XMl IP Geolocation



- Benefits of the app are apparent while investigating potential security incidents. Analyst can identify spikes in network traffic originating from a specific IP addresses.
- The information from "Whois XMl IP Geolocation" can be leveraged to gain understanding of the nature and potential threat associated with this IP address.
- LookingHackwards was able to perform a lookup on several IPs

Whois XMl IP Geolocation



Logs Analyzed

1 Windows Logs

- Event IDs
- Severity Levels
- User/Account Information
- Event activity Data

2 Apache Logs

- IP Address
- HTTP Request Method
- HTTP Status Code
- User-Agent
- Referrer

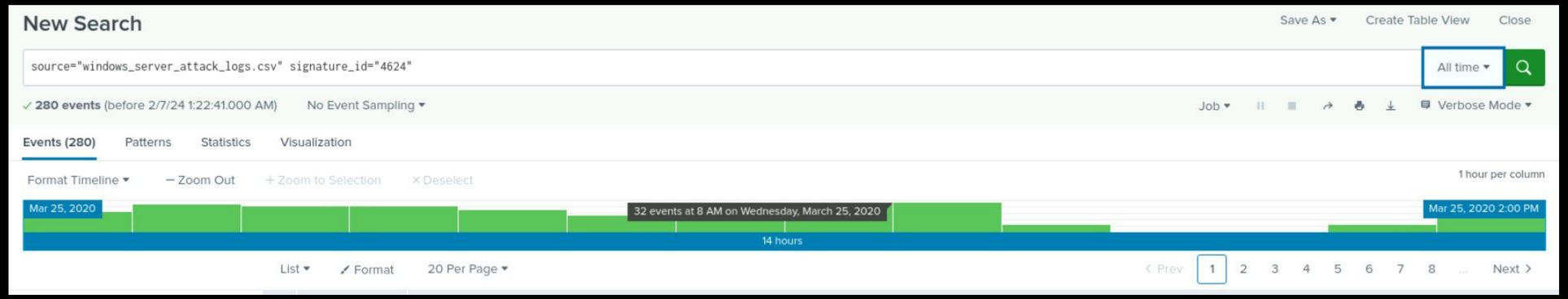
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures & ID’s	The Signature describes an event and the ID is the number that correlates to that event
Severity Count	The number of events grouped by the severity of the incident
Status Comparison	The comparison between successful and failed log attempts

Images of Reports—Windows



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Status Failure	Alerts the SOC when there are an inordinate amount of Status Failures	8	12

JUSTIFICATION: The average failure status was approximately 8 per hour. We set the baseline at 12 to allow for some deviation

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins Exceeded	The number of Logins rises above a reasonable level	10	24

JUSTIFICATION: Baseline chosen because the low was 8 and the high was 18. The chosen threshold is to allow for anomalous days when there are more staff logging in.

Alerts—Windows

Designed the following alerts:

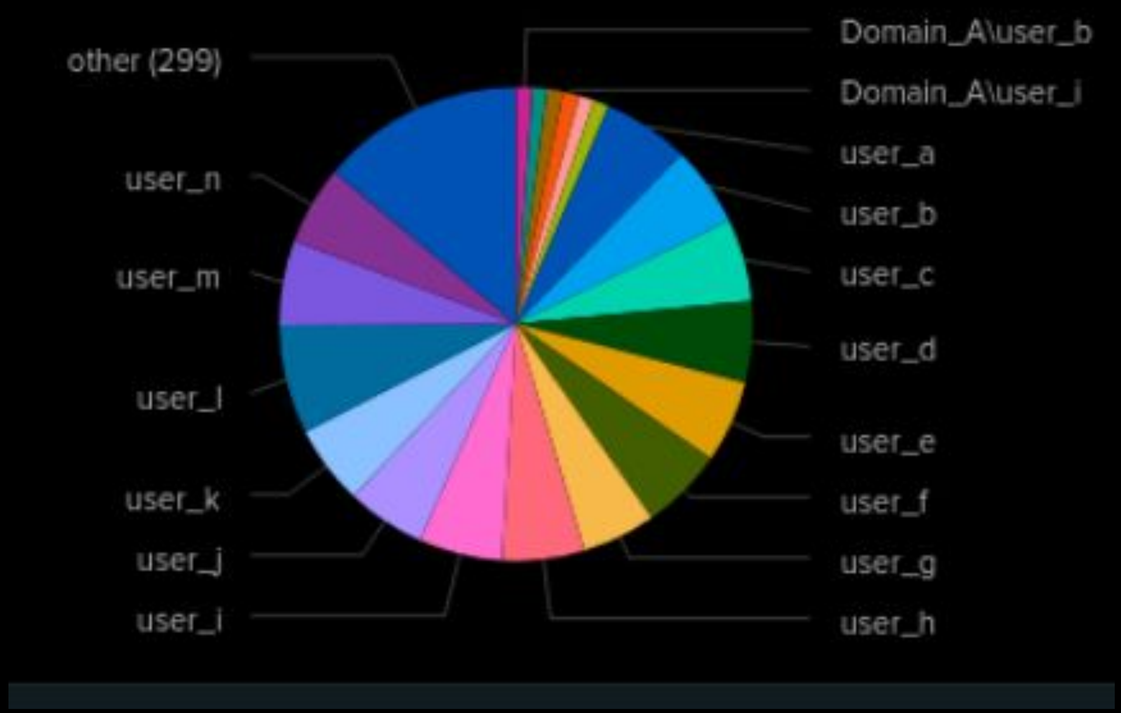
Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted	Alert triggered when the number of User Accounts deleted reaches 25	15	25

JUSTIFICATION: Baseline chosen as the normal activity had a high of 22 and the average looked to be around 15. The Threshold was chosen as during what looked like the attacks the deleted accounts rose above 25.

Dashboards—Windows

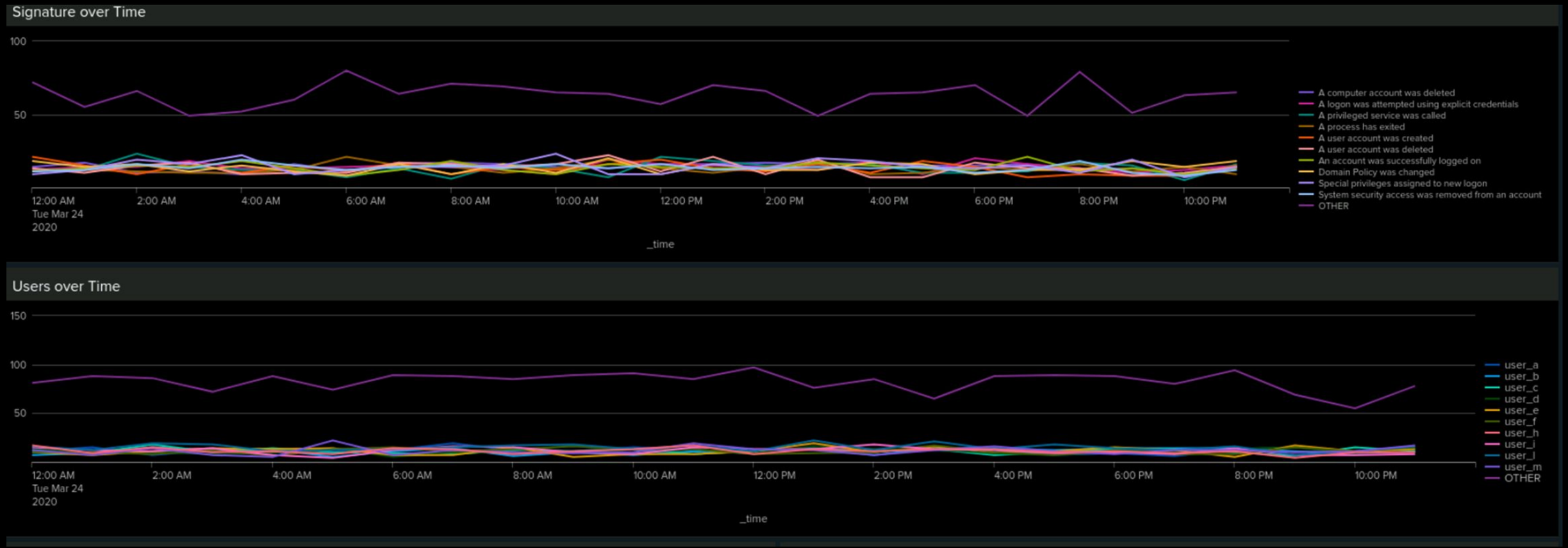
Count by Signature

Count by User



Dashboards—Windows

Line charts of Signatures and Users over Time



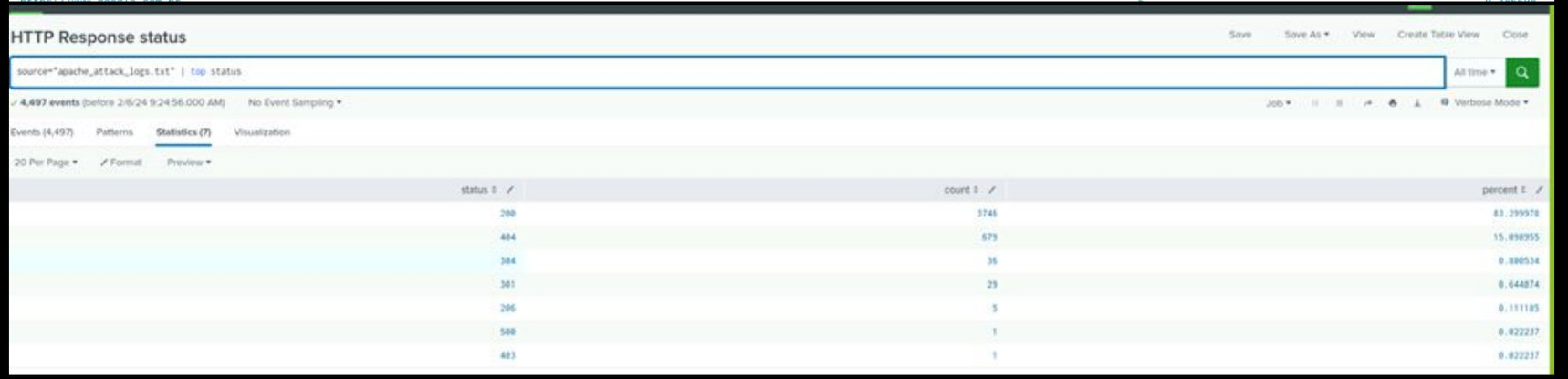
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Reports the various HTTP requests and counts
Referrer Domains	Reports the Domains from which a resource has been requested
HTTP Response Status	Reports the Response codes and totals and percentage

Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Foreign IP activity Exceeded	Email sent when foreign IP activity goes beyond the threshold	125	160

JUSTIFICATION: Baseline was chosen because it was a normal amount of activity per hour. We chose the threshold as the maximum per hour was near 130 to leave some room for error.

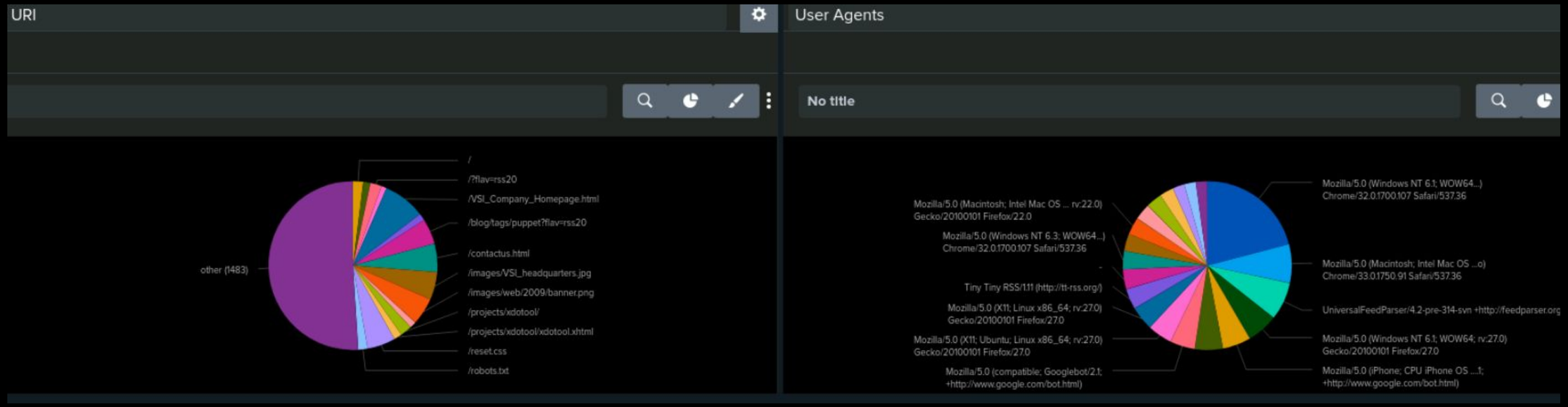
Alerts—Apache

Designed the following alerts:

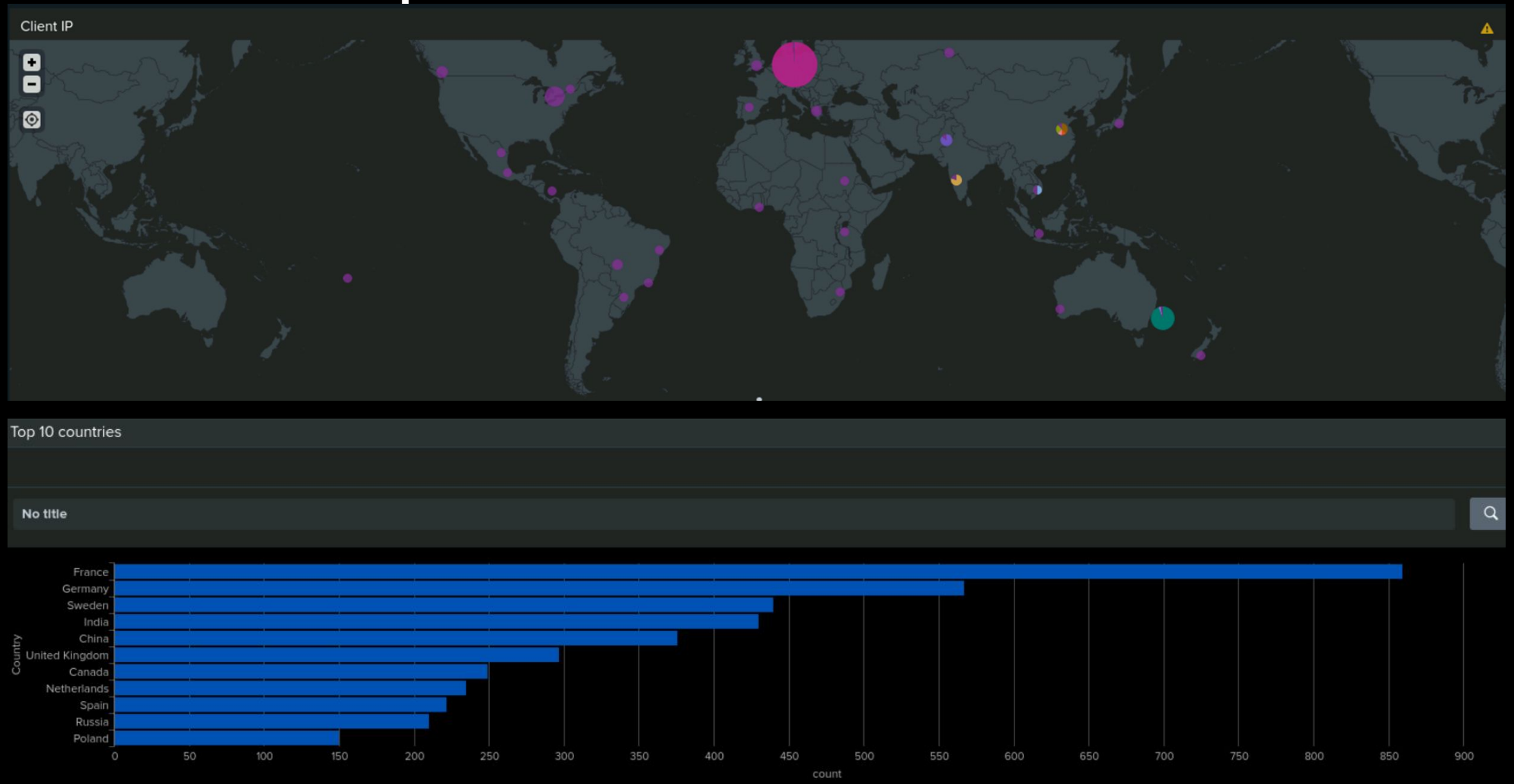
Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST request	SOC is sent an email when POST request exceed 4 indicating a possible DDoS attack	4	15

JUSTIFICATION: Baseline was chosen as the maximum normal POST requests were 7. The threshold was changed to 15 to allow for deviation at times. During the attack the amount of requests rose to over 1,296.

Dashboards—Apache



Dashboards—Apache



Attack Analysis

Attack Summary—Windows

Suspicious activity

- The alert indicated suspicious amount of failed activity. We detected a 15% rise in high severity logs.
- At 8 am on the 25th of March, there were 35 failed logins attempts. The first spike: 1AM - 2AM. Second Spike: 9AM - 10AM. Threshold was exceeded. No changes are recommended.
- The threshold we have set is at a safe level, which should mitigate false positives and provide leeway for capturing attacks.

Attack Summary—Windows

Suspicious activity

- There was suspicious activity at 11:00 a.m. and 12:00 p.m. on Wednesday, March 25th with a large amount of successful logins detected.
- 196 events at 11:00 a.m. and 77 events at 12:00 p.m were detected
- Alert triggered as the threshold was exceeded.

Deleted accounts

- There were no signs of unusual volumes of deleted accounts.

Attack Summary—Windows

Time chart of signatures

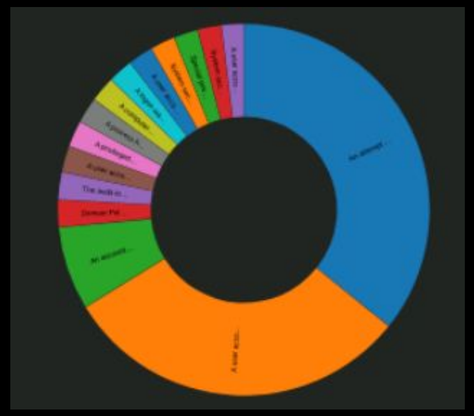
- There were 2,128 events attempting to reset account passwords, with 1,258 of those attempts occurring around 9am.
- The signature that stood out was “An attempt was made to reset an account’s password” between 8-11am on the 25th March
- Between 12-3am on the same day the other signature which stood out was “A user account was locked out”.

Suspicious users

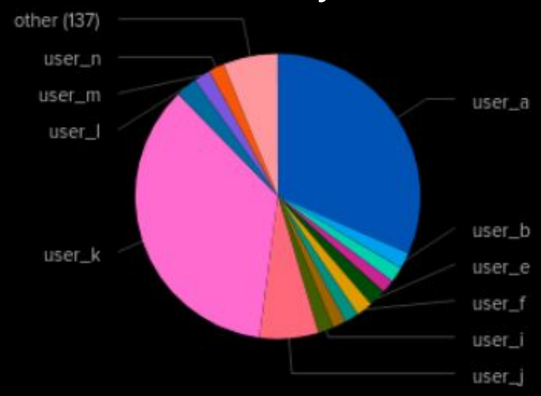
- user_a; between the hours of 12 – 3am with a peak of 1,968
- user_k; between the hours of 8 – 11pm with a peak of 2,512

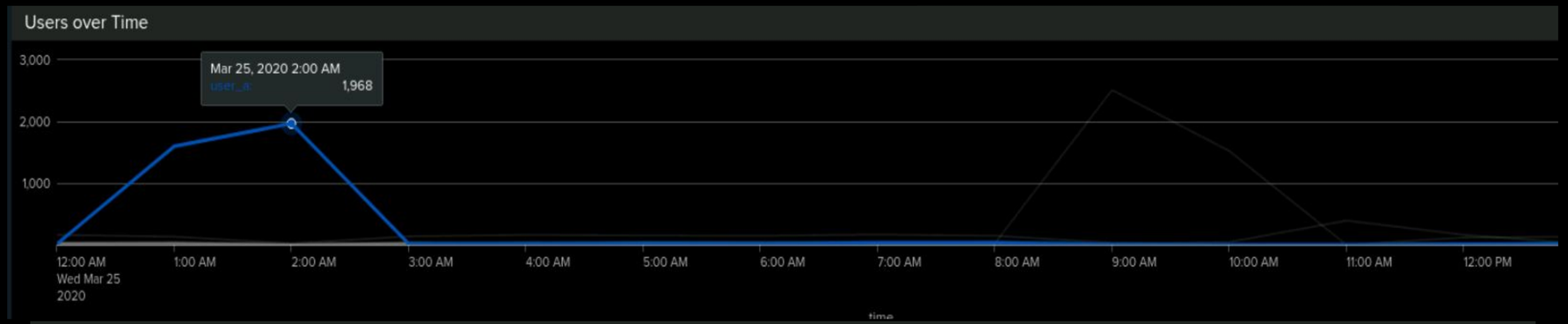
Screenshots of Attack Logs

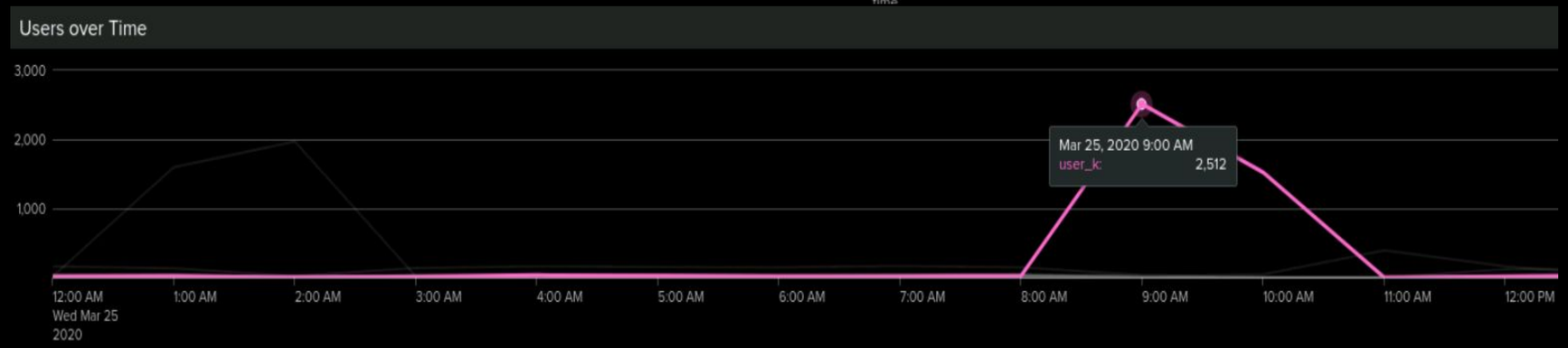
Count by Signature



Count by User







Attack Summary—Apache

Changes in HTTP methods

- There were significant changes in some of the request methods
- GET request: There was a decrease of 29%
- POST request: There was an increase by 29%

Referrer Domains

- There were no suspicious referrer domains during the time of attack.

Attack Summary—Apache

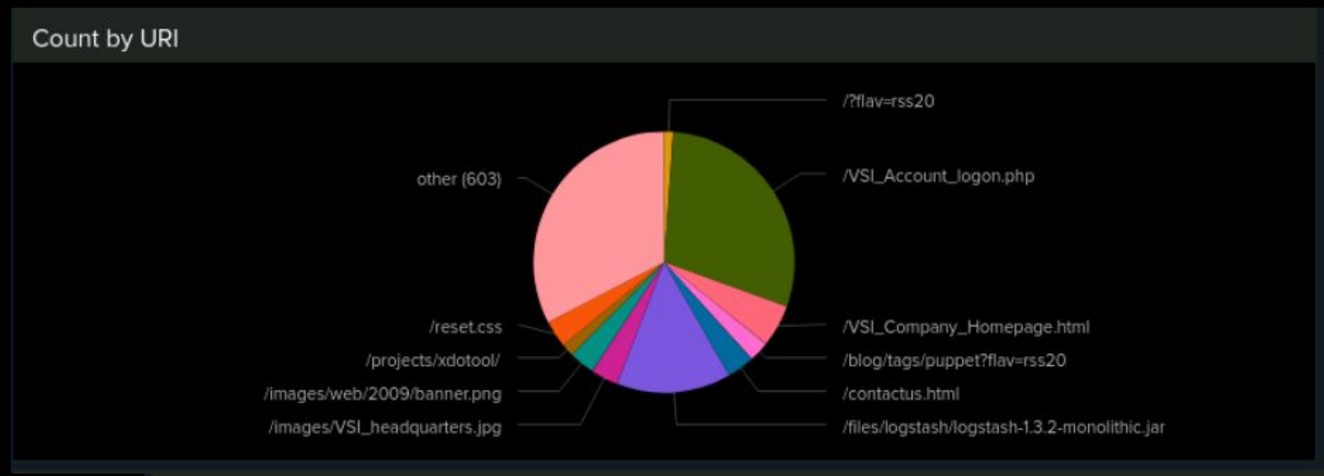
Alerts HTTP Requests

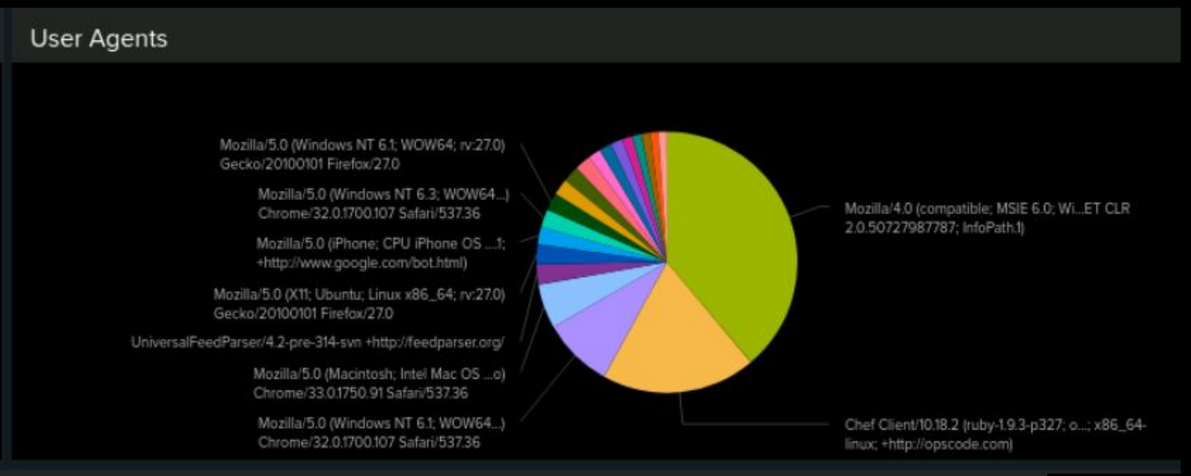
- There was a significant increase in POST requests that occurred at 8pm on Wednesday the 25th of March.
- The threshold set would need to be increased.

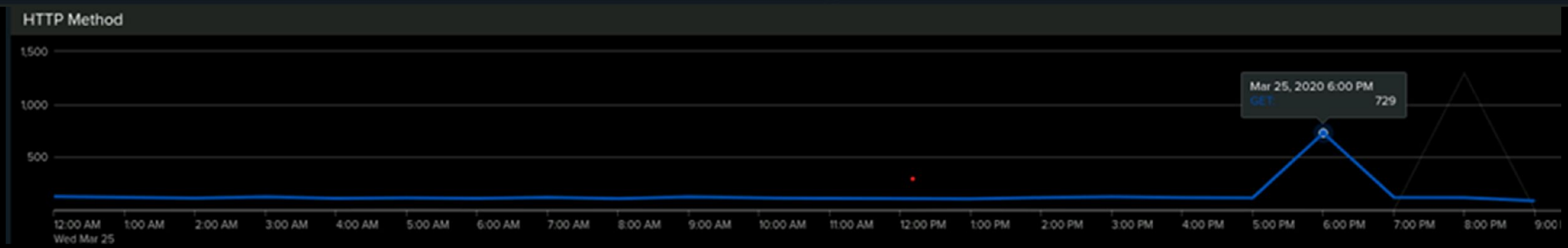
Time chart of HTTP Methods

- A large volume of “GET” requests from 5 PM to 7 PM March 25th
- A second large volume of “POST” requests from 7 PM to 8 PM March 25th
  - “GET”: 1,296
  - “POST”: 729

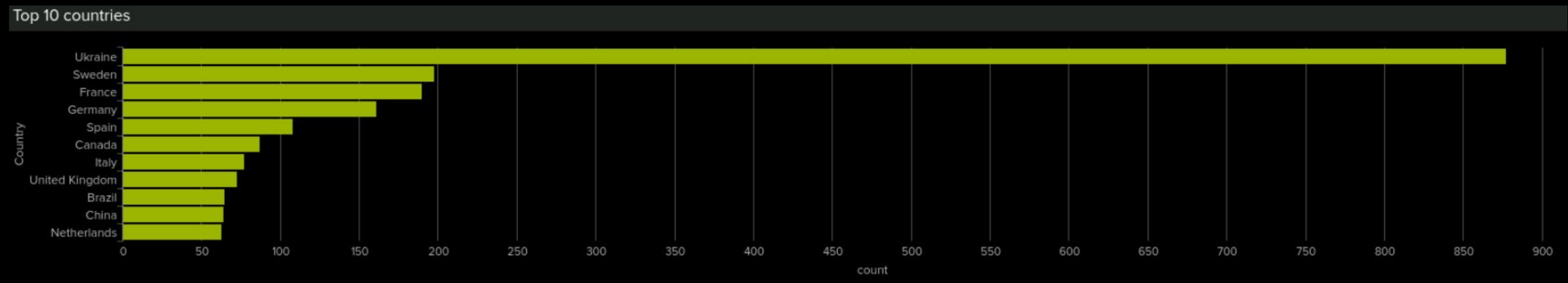
Screenshots of Attack Logs







Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

Overall findings

- Looking Hackwards found that on March 25th VSI had multiple attacks on both the Windows and Apache servers.
- Brute Force logins attack.
- There was an indication that there’d been a DDoS attack.

Future mitigations

- Two-factor authentication is recommended to mitigate Brute Force attacks.
- To prevent future attacks it’s also recommended that users are locked out after a certain number of login attempts .
- Web Application Firewall (WAF) is recommended for DDoS attacks.
- Use of firewalls and ACLs