

Defensive Security Project

Ankush Verma Daniella Adjei
Malek Slimi Nicholas Babcock
Serge Yapi Tameem Faizi

Scenario

- Virtual Space Industries (VSI) is a top-tier company specializing in designing virtual reality programs for B2B clients.
- Our team was hired as SOC analysts for VSI after there rumours surfaced that a competitor might launch cyberattacks to disrupt VSI's business.
- Upon beginning, our team was tasked with reviewing and analyzing Splunk logs for any suspicious activity. From there, we created reports, alerts and dashboards for VSI.
- Our monitoring focused on VSI's Windows servers and Apache servers, both of which had a plethora of signs indicating numerous attacks.

Monitoring Environment

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

[WhoisXML IP Geolocation API]

WhoisXML Website Categorization API in Splunk

What is it?

- A domain classification API that categorizes websites based on their content.

Why use it in Splunk?

- Helps classify and analyze domains found in logs.
- Enhances threat intelligence by identifying malicious domains.
- Supports incident response and SIEM enrichment.

WHOIS XML IP Geolocation API

Key Use Cases:

- Detecting phishing, malware, and fraudulent websites.
- Enriching firewall and proxy logs with domain categories.
- Strengthening SIEM alerts by classifying suspicious domains.
- Identifying C2 (Command & Control) communications.

Benefits

- Faster investigation of security incidents.
- Improved detection of malicious domains.
- Better policy enforcement for web access control.

Logs Analyzed

1

Windows Logs

The Windows Logs that we monitored were used by VSI for many of their backend operations.

2

Apache Logs

The apache server was primarily used for hosting the VSI webpage. We can analyze the HTTP response codes as well as POST requests.

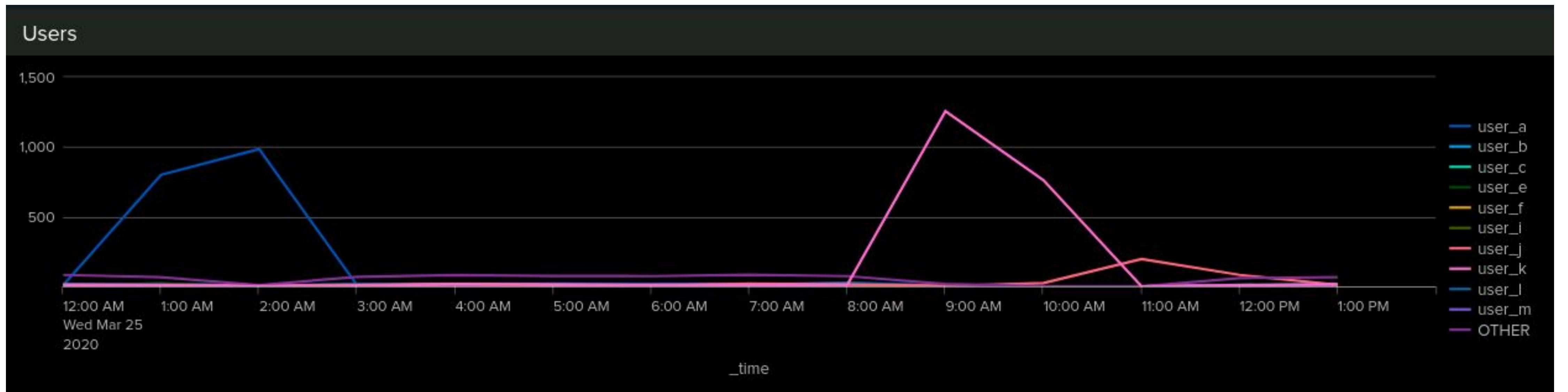
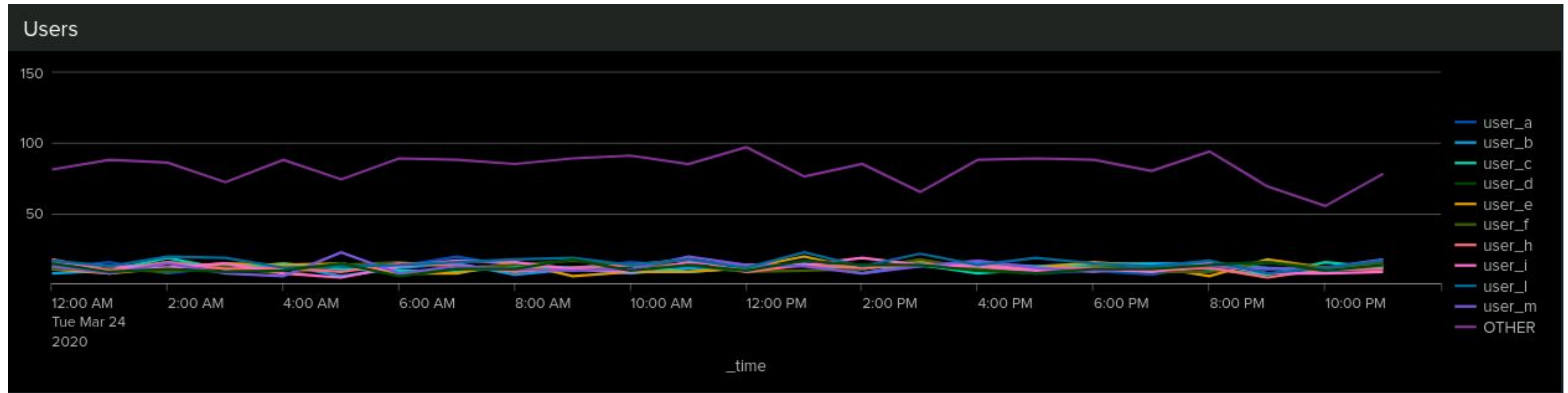
Windows Logs

Reports—Windows

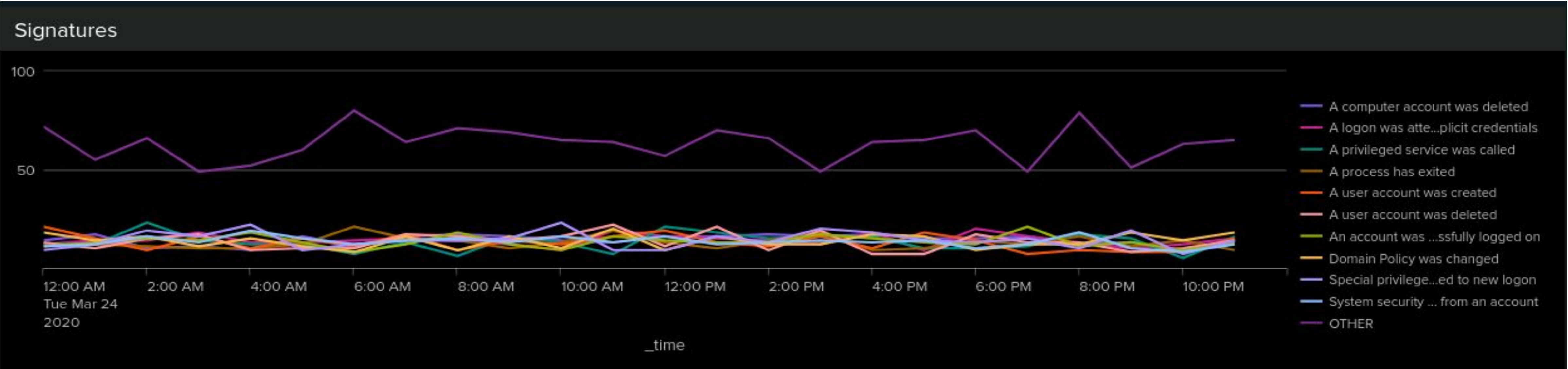
Designed the following reports:

Report Name	Report Description
Windows Log Success vs Failures	Compares the number of successful and failed login attempts, helping VSI to identify any suspicious activity on their server.
Windows Log Severity Report	Analyzes the severity level of all logged events within the Windows environment.
Windows Signature Report	Displays the unique IDs associated with specific signatures within the Windows environment.

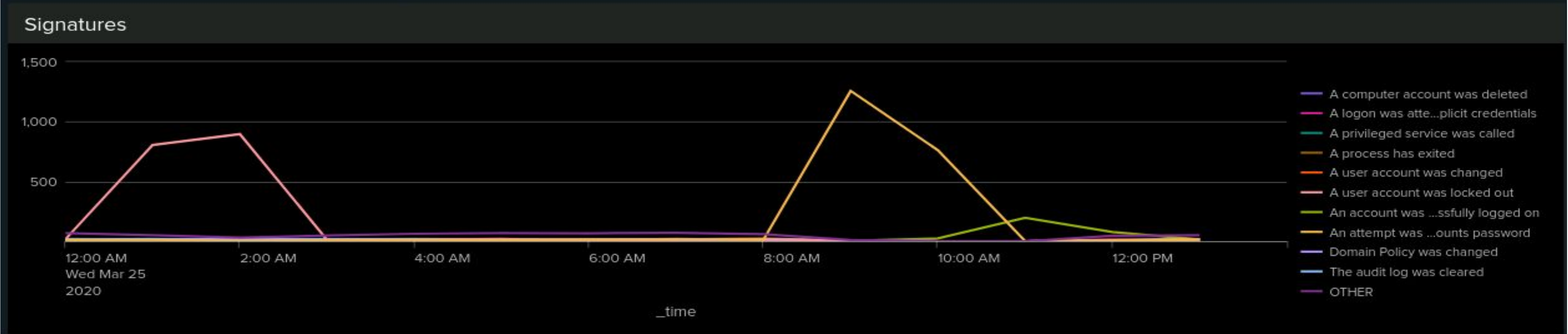
Images of Reports-Windows



Images of Reports—Windows



Windows Server Monitoring



Alerts—Failed Logins-Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Hourly Failed Log-Ons	Threshold for Windows failed activity	5	6

JUSTIFICATION: The baseline for failed Windows activities was determined to be an average of 5, with no instances reaching 6. Any failure count exceeding 6 serve as a strong indicator of suspicious activity.

Alerts—Successful Logins-Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Successful Logins	Threshold for successful login by Account	13	15

JUSTIFICATION: The baseline for successful Windows login activities was determined to be an average of 13, with no instances approaching 15. Any failure count exceeding 15 would be a strong indicator of suspicious activity.


Alerts—Deleted Accounts-Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Account Deletion	This will alert VSI if there is an unusual amount of accounts being deleted	13	14

JUSTIFICATION: The baseline of 13 was determined based on the average number of deletions per hour, which was considered normal. Anything exceeding 14 was flagged suspicious.

Alerts—Windows

 Successful Logins

threshold for the hourly count of the signature “an account was successfully logged on.”


Enabled: Yes. [Disable](#)


Permissions: Private. Owned by admin. [Edit](#)

Modified: Mar 10, 2025 11:40:21 PM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 15. [Edit](#)

Actions:  1 Action [Edit](#)

 Send email

Failed Windows Activity

displays the severity levels, and the count and percentage of each.


Enabled: Yes. [Disable](#)


Permissions: Private. Owned by admin. [Edit](#)

Modified: Mar 9, 2025 6:05:22 PM

Alert Type: Real-time. [Edit](#)

Trigger Condition: .. Custom. "search failed_events > 6" in 5 minutes. [Edit](#)

Actions:  1 Action [Edit](#)

 Send email

Account Deletion on Windows

Threshold for the hourly count of the signature “a user account was deleted


Enabled: Yes. [Disable](#)


Permissions: Private. Owned by admin. [Edit](#)

Modified: Mar 7, 2025 1:00:52 AM

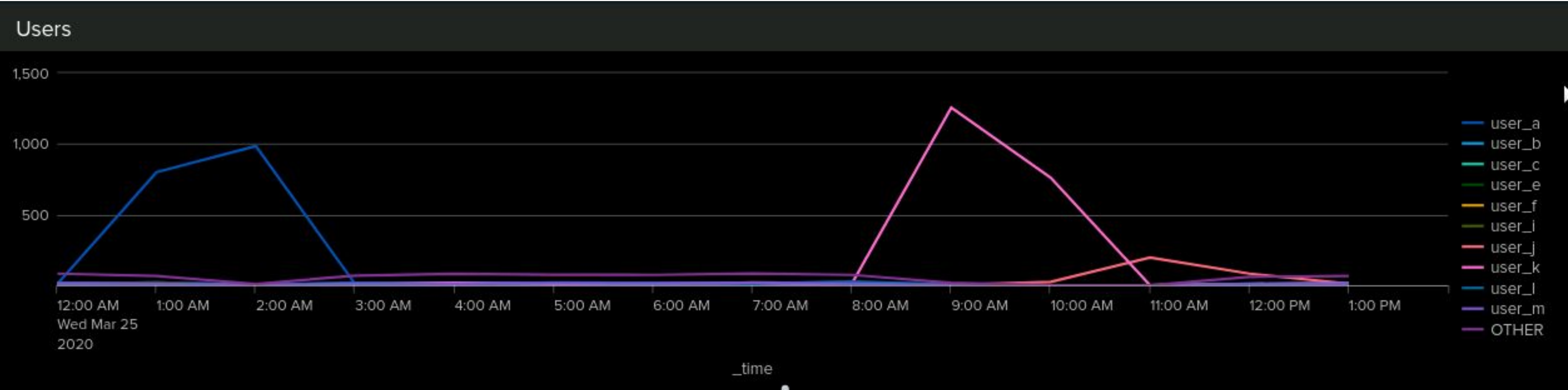
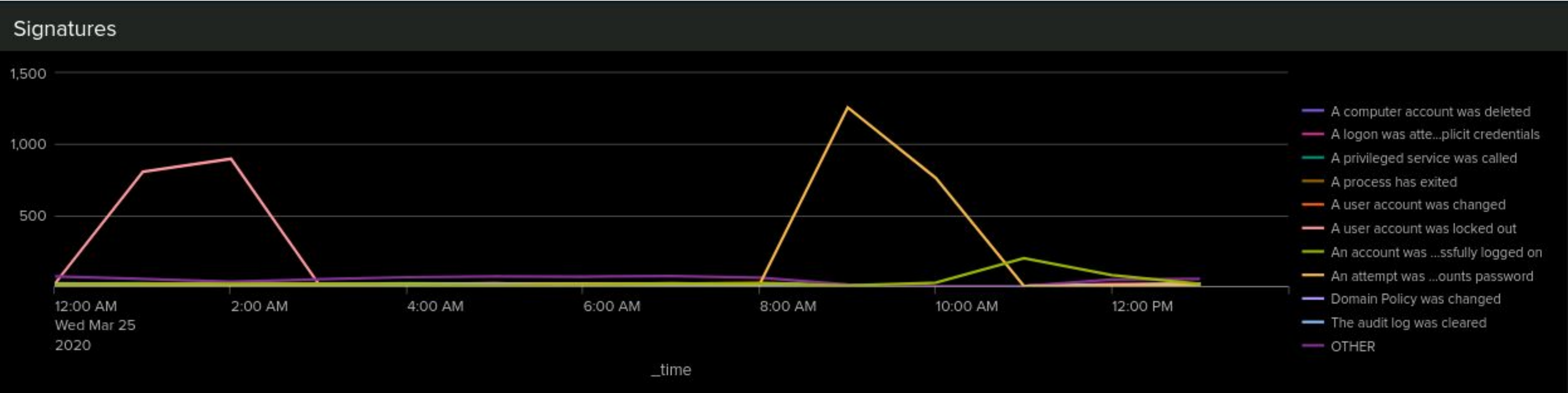
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 14. [Edit](#)

Actions:  1 Action [Edit](#)

 Send email

Dashboards—Windows



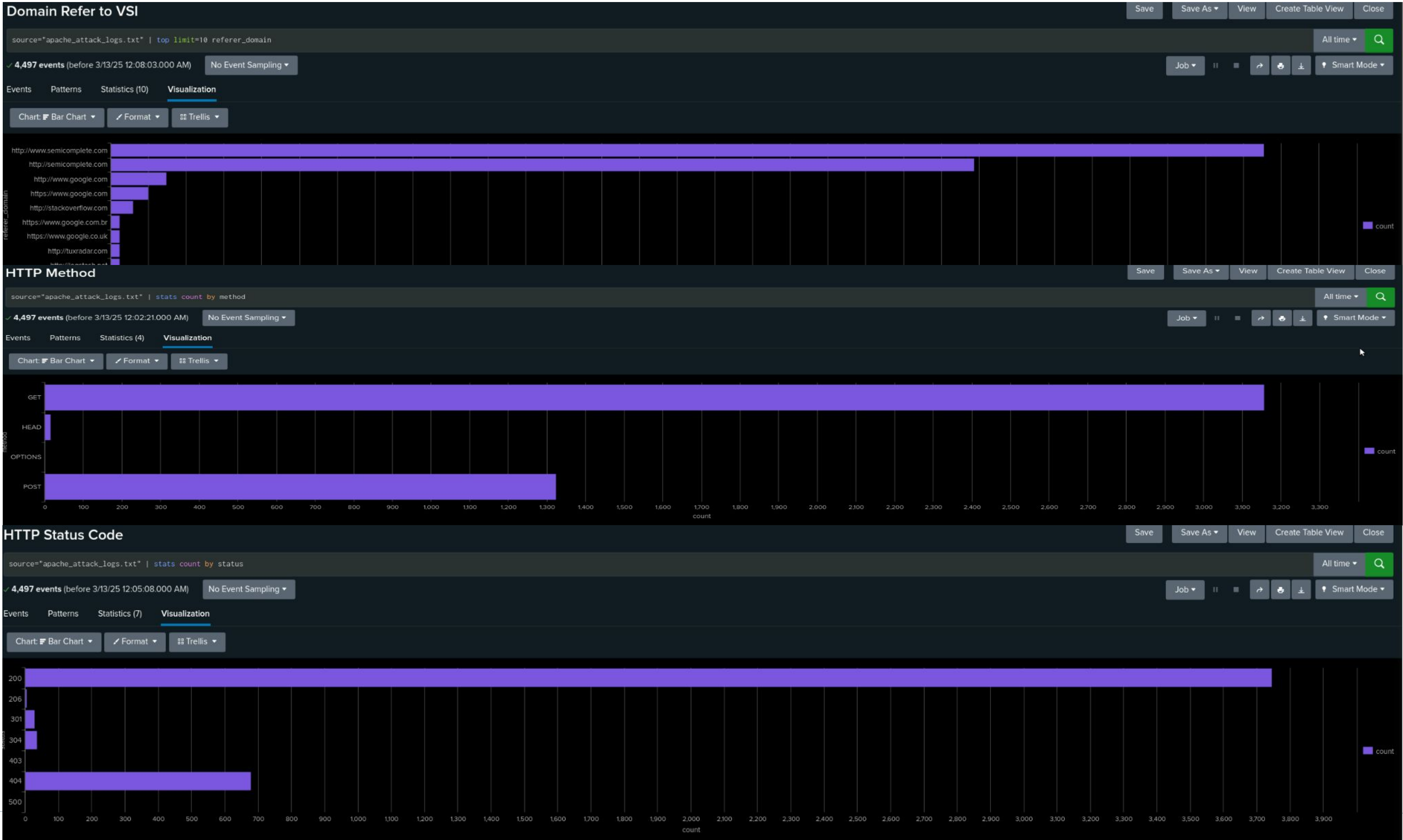
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Displays the most frequently used HTTP methods in VSI’s web traffic.
Top 10 Domains	Highlights the top 10 domains generating the most traffic to VSI’s web servers.
Count of each HTTP Response Code	Provides insight towards the count and distribution of HTTP response codes.

Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Threshold activity	This alert is triggered when the number of attempted via apache exceeds our threshold	118	120

JUSTIFICATION: The baseline of 118 events per hour was determined to be standard. However, any count exceeding the threshold of 120 would indicate suspicious activity.

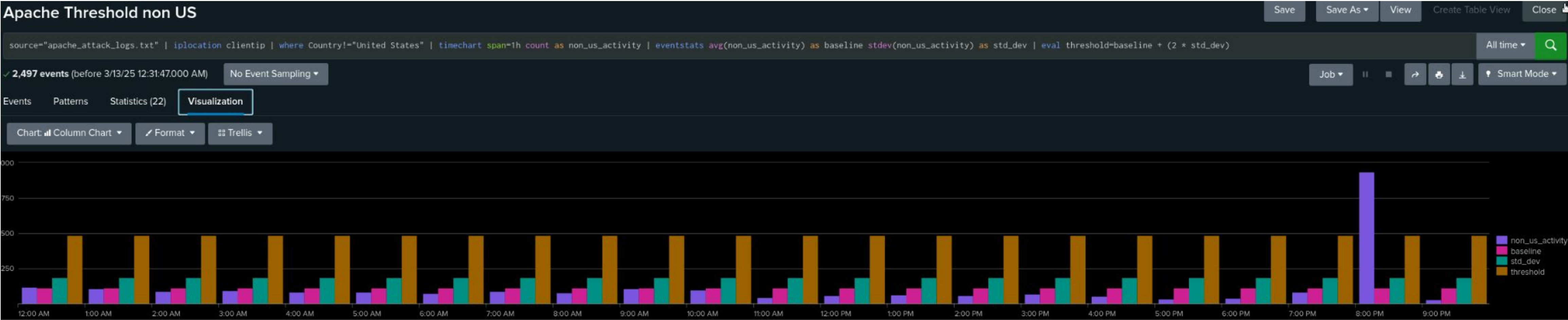
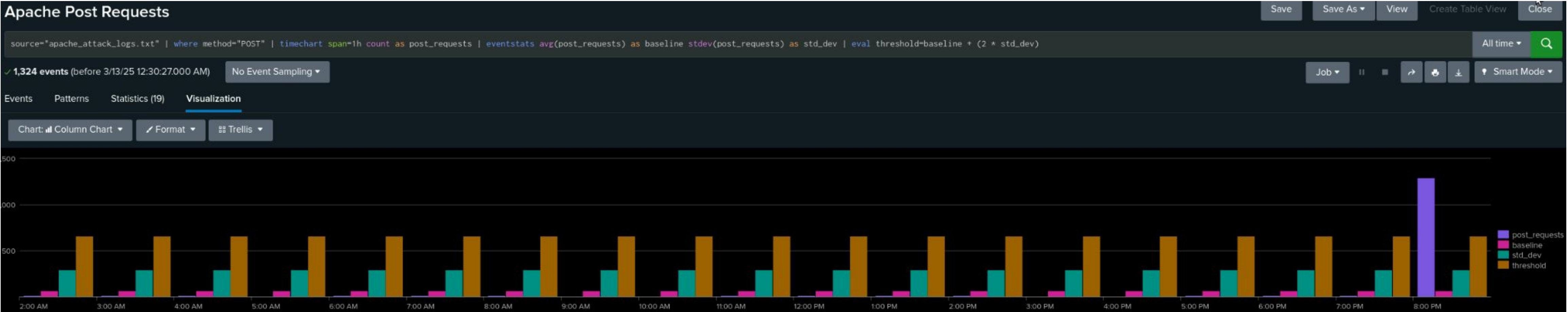
Alerts—Apache

Designed the following alerts:

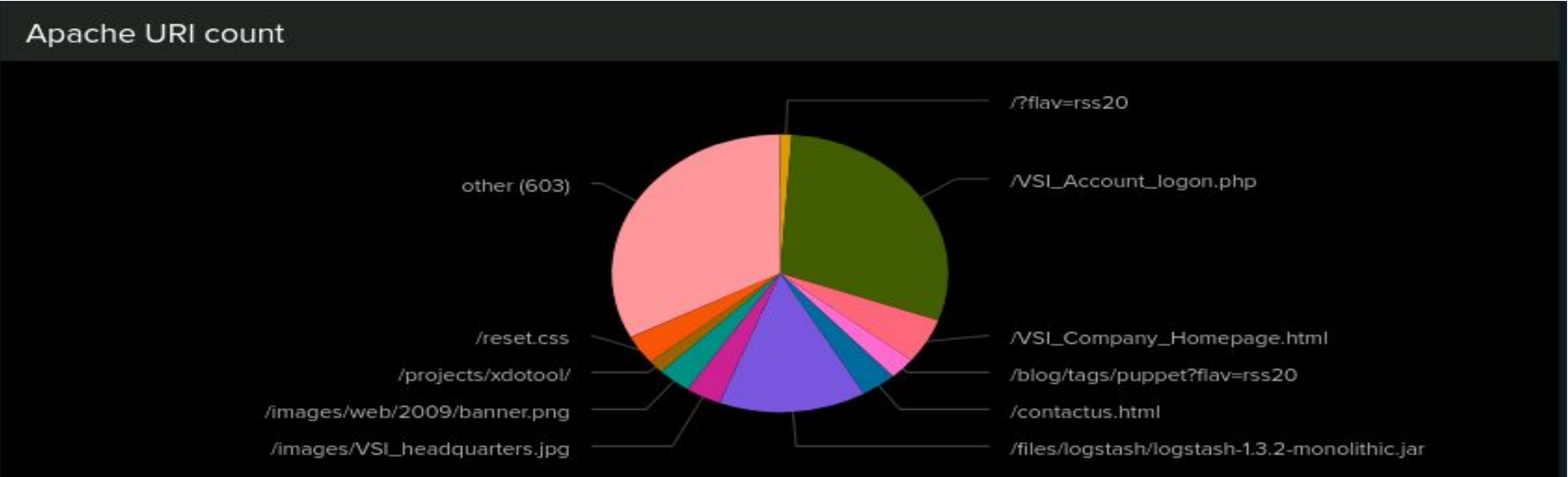
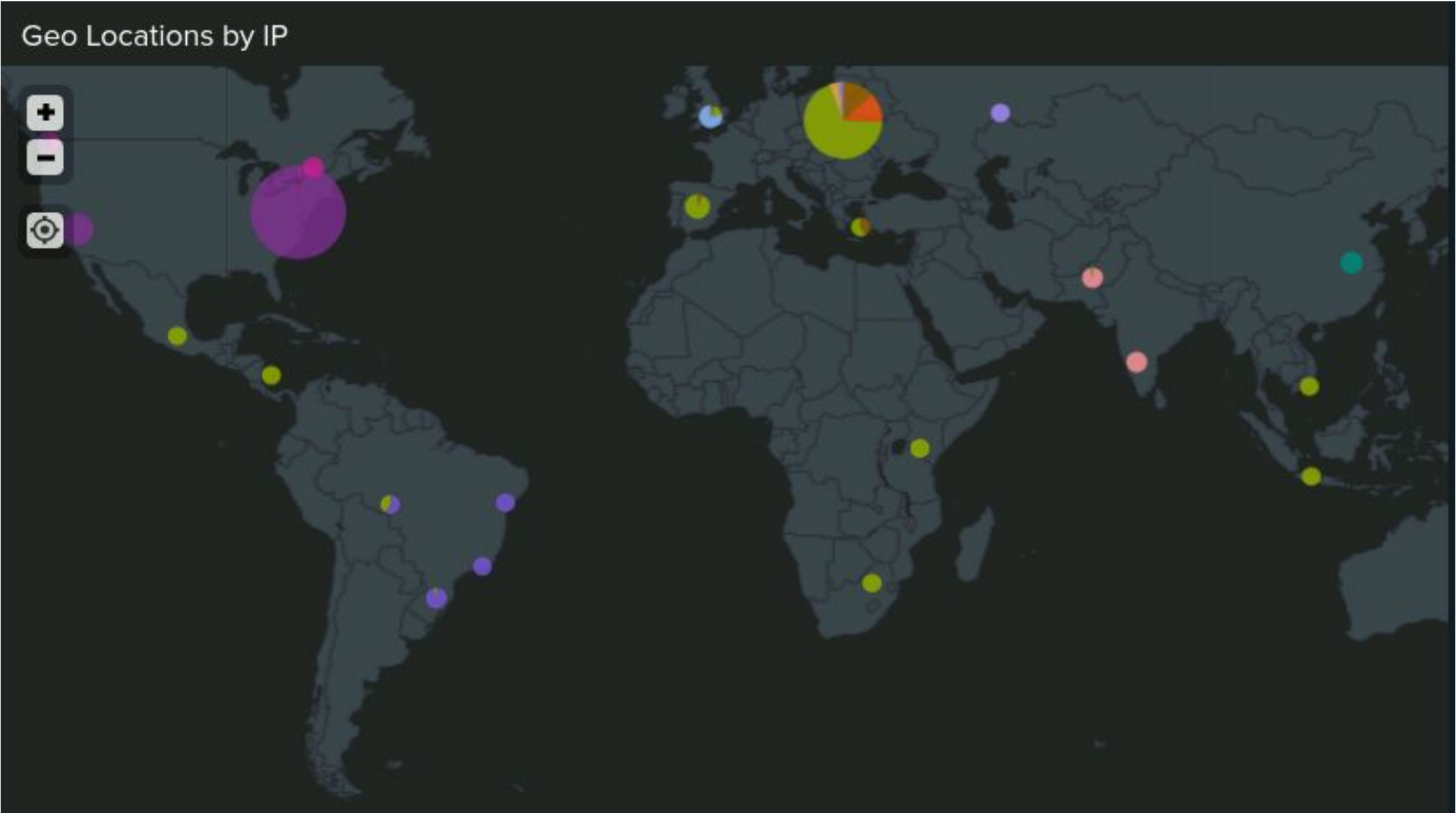
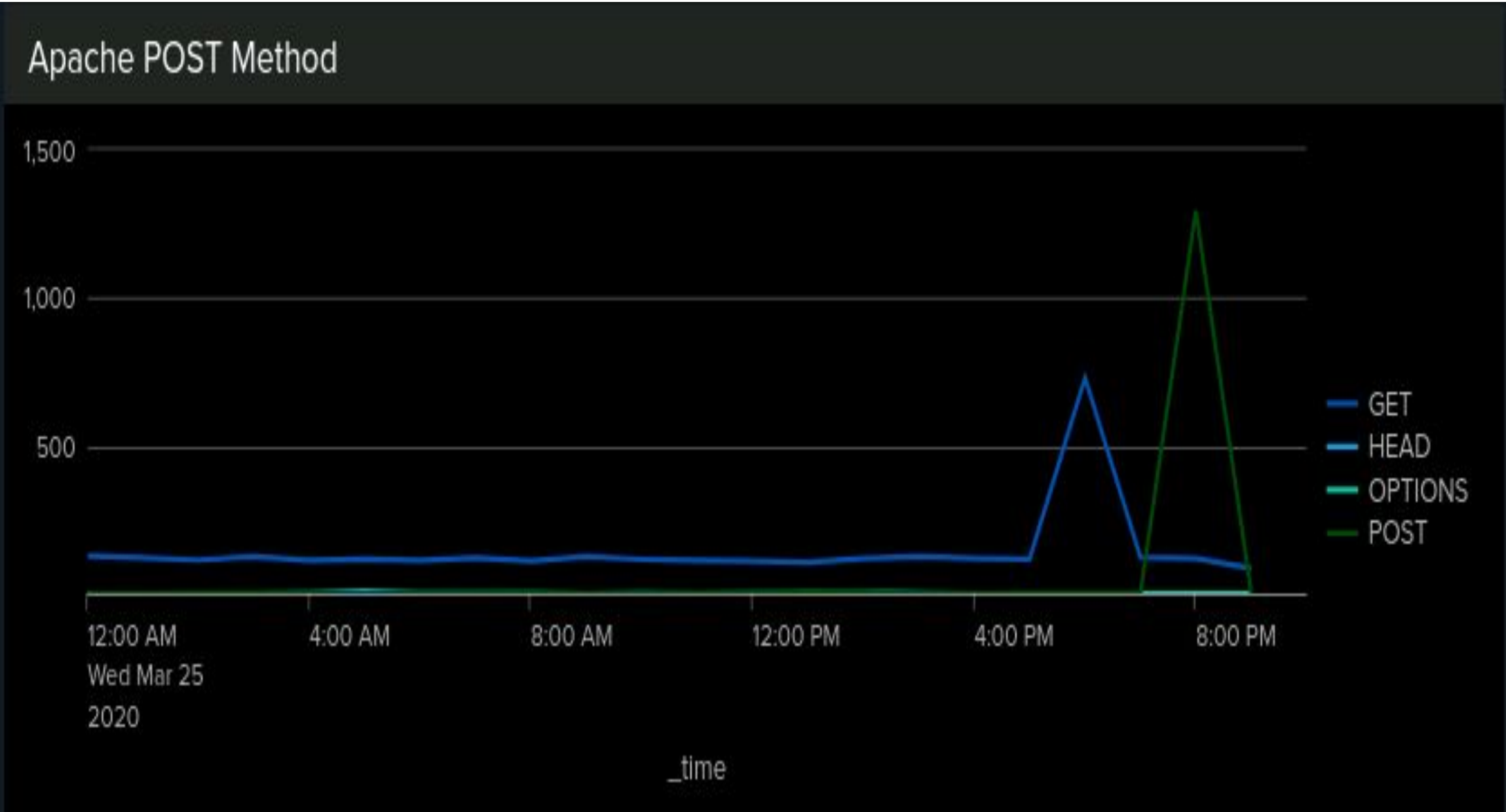
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Request	When the Apache server has more Post requests than we have designated with our threshold an alert will be sent out	2	15

JUSTIFICATION: Most events per hour ranged between 1 to 5, never surpassed 7. Therefore, a threshold of 12 considered normal, making 15 a sufficient enough to trigger alert and detect potential malicious activity.

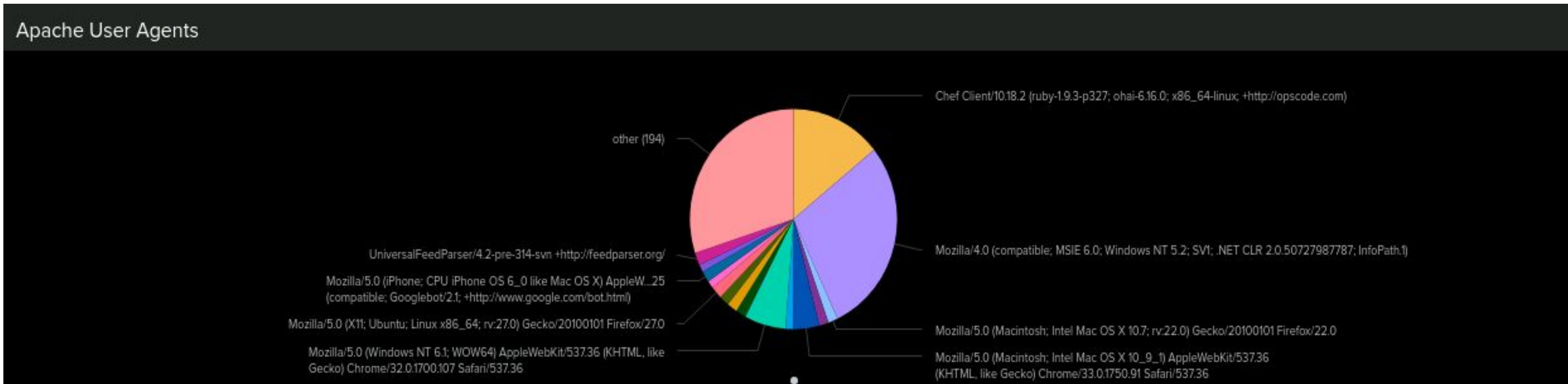
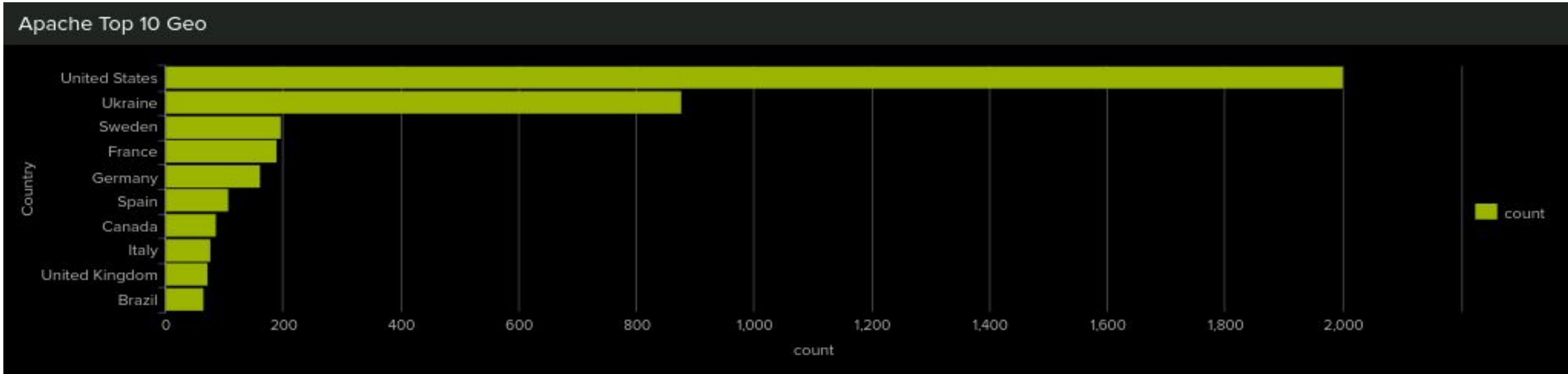
Alerts—Apache



Dashboards—Apache



Dashboards—Apache



Attack Analysis

Attack Summary—Windows

The analysis of attack logs revealed a significant shift in severity levels compared to events recorded before the previous attack.

Key findings include:

- **Failed Logins:** A total of 35 failed logins attempts were recorded at 8:00 am on March 25, 2020., exceeding the established threshold of 5, indicating potential unauthorized access attempts. .
- **Successful Logins:** A suspicious number of login attempts were detected, warranting further investigation.
 - At approximately 11:00 AM on March 25, 2020, 196 events were recorded within one hour, surpassing the threshold of 15, triggering an alert.
- **Account Deletion:** No suspicious activity was detected

Attack Summary—Windows

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

- An examination of the Windows attack logs reveals an increasing intensity in attack severity, with successful breaches outpacing failed attempts. Notably, there is an alarming volume of failed login activity and an unusually high number of successful logins linked to a specific user. To strengthen security monitoring and improve threat response, changing the threshold for successful logins is advised.

Attack Summary—Windows

Suspicious activity was observed for two users, **User A** and **User K**

- **User A:** Activity spanned from 1:00 AM to 2:00 AM.
- **User K:** Activity spanned from 9:00 AM to 10:00 AM.

The key signs of suspicious behaviour included high volumes of two specific event signatures:

1. “A user account was locked out”

Peak count: 896

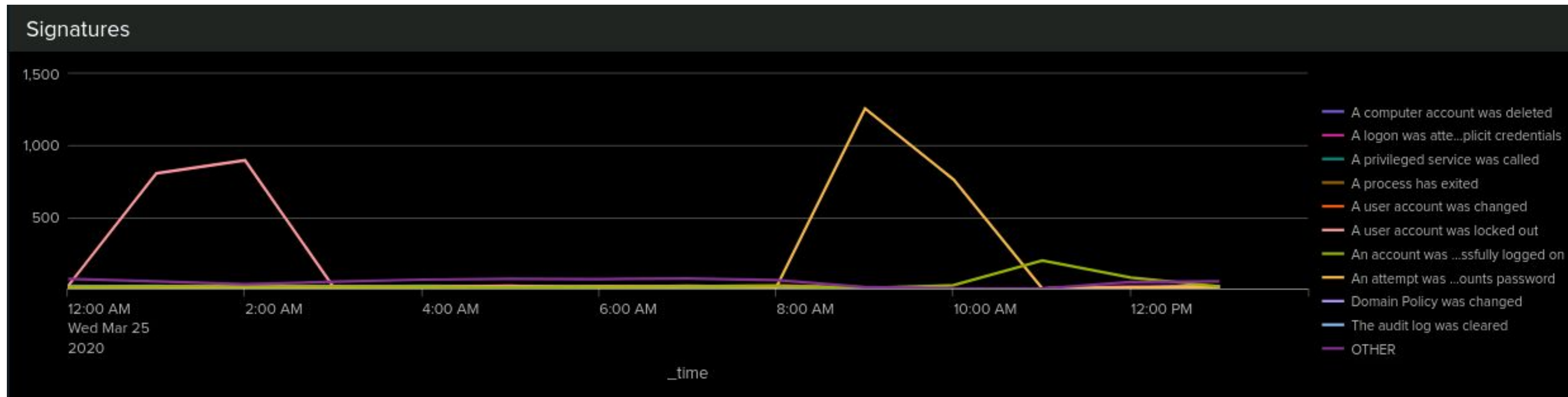
Duration: 1:00 AM to 2:00 AM (User A)

2. “An attempt was made to reset an account’s password”

Peak count: 1258

Duration: 9:00 AM to 10:00 AM. (User K)

Screenshots of Attack Logs



Attack Summary—Apache

- **Suspicious HTTP Methods:** There was a big spike in **POST** requests, hitting **1,296** between **7 PM – 9 PM**, which could indicate a brute-force attack or data extraction attempt.
- **HTTP Response Codes:** A noticeable rise in **404 errors** and a drop in **200 responses** suggest attackers were scanning for vulnerabilities or hidden pages.
- **Unusual Traffic:** A sharp increase in requests from **Ukraine** around **8 PM** stood out as potentially suspicious.
- **Thresholds:** The alerts did their job, but some tweaks might help reduce false positives, especially for **POST** activity.

Attack Summary—Apache

- The international activity threshold was effective, accurately triggering an alert for **937** requests, which was well above the set value of **118**.
- The **HTTP POST** activity threshold was set too low at **3 requests per hour**, as the attack had **1,296 POST** requests. To improve accuracy and reduce the alert fatigue, the threshold was adjusted to **15 requests per hour**.
- Overall, the thresholds were effective but may require fine-tuning especially for **POST** activity.

Attack Summary—Apache

- **HTTP POST** spiked significantly between **7 PM and 9 PM**, with **POST** peaking at **1,296** requests.
- This surge in **POST** traffic suggests a targeted attack, possibly brute force or injection attempts.

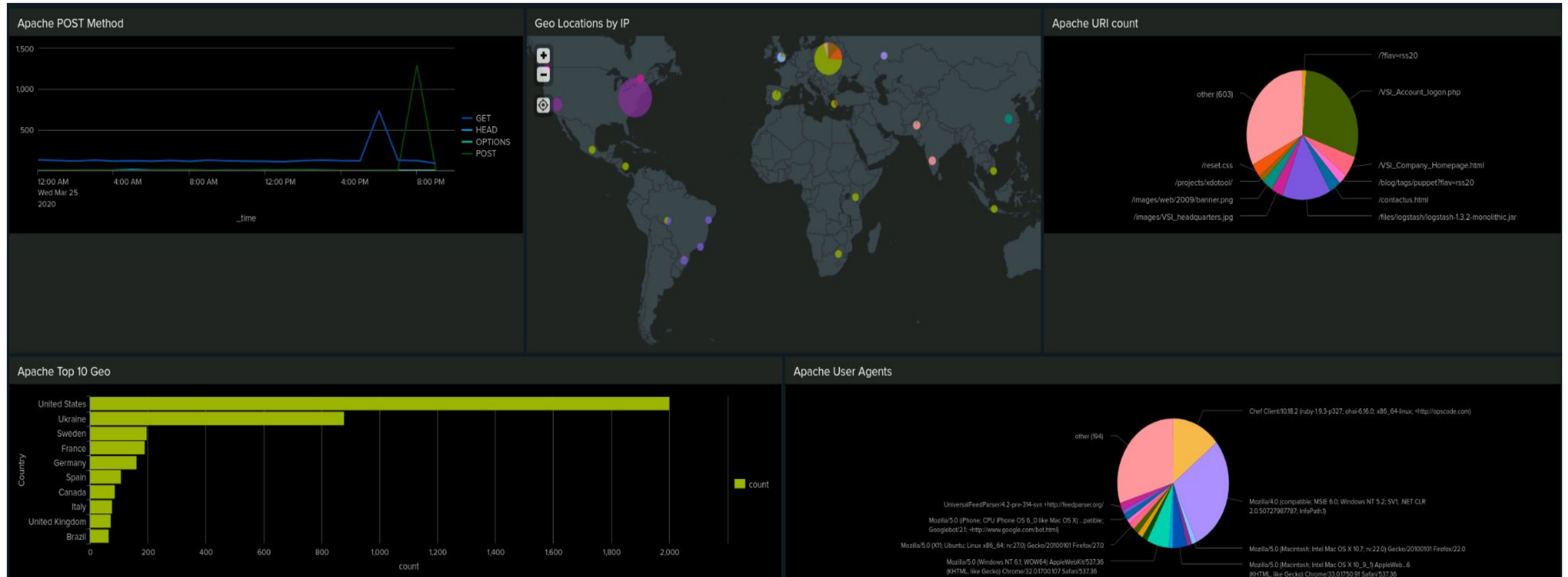
Cluster Map Findings

- Unusual traffic from **Kiev (439 hits)** and **Kharkiv (433 hits)** in Ukraine indicates potential external threats originating from these locations.

URI Analysis

- **/VSI_Account_logon.php** was accessed **1,323** times, pointing to brute force or SQL injection attempts.
- A high number of **404 errors** suggests attackers were also scanning for hidden or vulnerable pages.

Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

Our analysis revealed that VSI experienced multiple attacks on both Windows and Apache servers. The primary attack vectors involved brute force password attempts, originating from various locations across the globe.

To enhance VSI's security and mitigate future attacks, we recommend the following measures:

1. **Implement Multi-Factor Authentication (MFA)** - Adds an extra layer of security.
- 2.
3. **Enforce Strong Password Policies** - Require complex passwords with , sufficient length and regular updates to strengthen account security.



Thank You