Monitoring & Analyzing Attacks in Splunk

by: Chontele Coleman

Table of Contents

This document contains the following resources:

01

Monitoring Environment

Splunk

02

Attack Analysis

Windows logs

Apache logs

03

Project Summary & Future Mitigations

Updates
Patching
Training

Monitoring Environment

Scenario

- **We are acting as an SOC analyst at Virtual Space Industries (VSI), a company that develops virtual-reality programs.**
- **VSI suspects potential cyberattacks from a competitor, JobeCorp, aiming to disrupt its operations.**
- **Our role involves using Splunk to monitor for suspicious activity across VSI's systems and applications.**
- **We are responsible for monitoring two critical systems: an Apache web server and a Windows operating system.**
- **The Apache server hosts VSI's main public website and administrative interface.**
- **We've been given historical Windows and Apache server logs to establish baselines, create alerts, dashboards, and reports.**

Logs Analyzed

1 Windows Logs

A CSV export of Windows Security Audit events.
Each record includes:

- _time: Timestamp of the event
- host: Machine identifier (e.g. 2e222dd551e8)
- signature_id: Numeric event ID (e.g. 4624, 4726)
- signature: Human-readable description (e.g. “An account was successfully logged on”)
- severity: Risk level (e.g. informational, high)
- status: Outcome (e.g. success, failure)
- user: Account involved
- Additional fields: (e.g. process, IP, etc., if present)

These logs power our alerts and dashboards around logon activity, account changes, and failure rates.

2 Apache Logs

Standard HTTP request records in Combined Log Format. Key fields:

- _time: Request timestamp
- clientip: Originating IP address
- http_method: Request method (GET, POST, etc.)
- uri: Requested resource path (e.g. /index.html)
- status: HTTP response code (200, 404, etc.)
- bytes: Size of response payload
- referrer: Originating URL (if any)
- user_agent: Browser or bot identifier (e.g. Mozilla/5.0, Googlebot)

These logs feed our method-trend reports, geographic heatmaps, URI-access panels, and user-agent analyses.

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures and associated signature IDs	The dataset shows a mapping between Windows event signatures and their associated signature IDs, likely extracted from system security logs. These mappings help identify types of activity (e.g., account deletions, login attempts, policy changes) based on event IDs.

Images of Reports—Windows

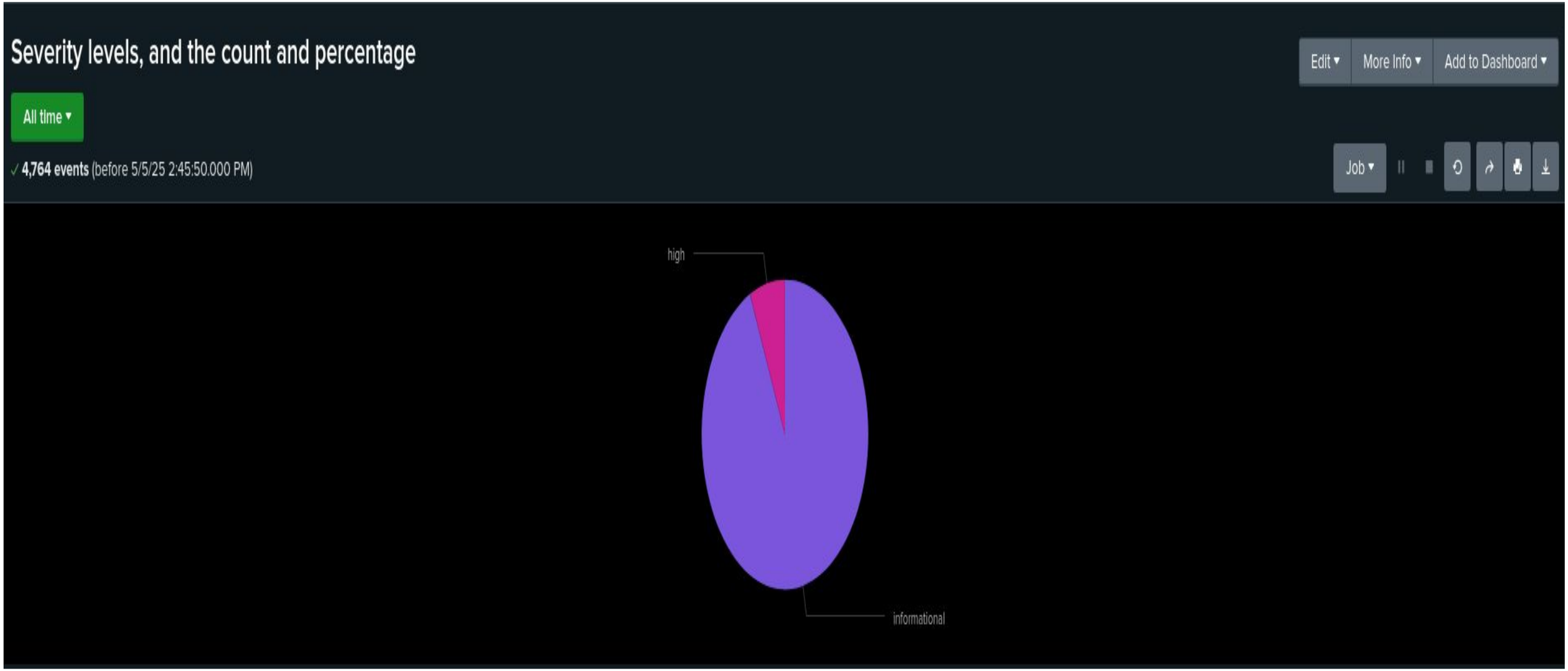
Signatures and associated signature IDs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Severity levels, and the count and percentage	This report provides a breakdown of log entries by severity level, showing: Total number of events (4764). The count of events for each severity level. The percentage of the total that each severity level represents.

Images of Reports—Windows



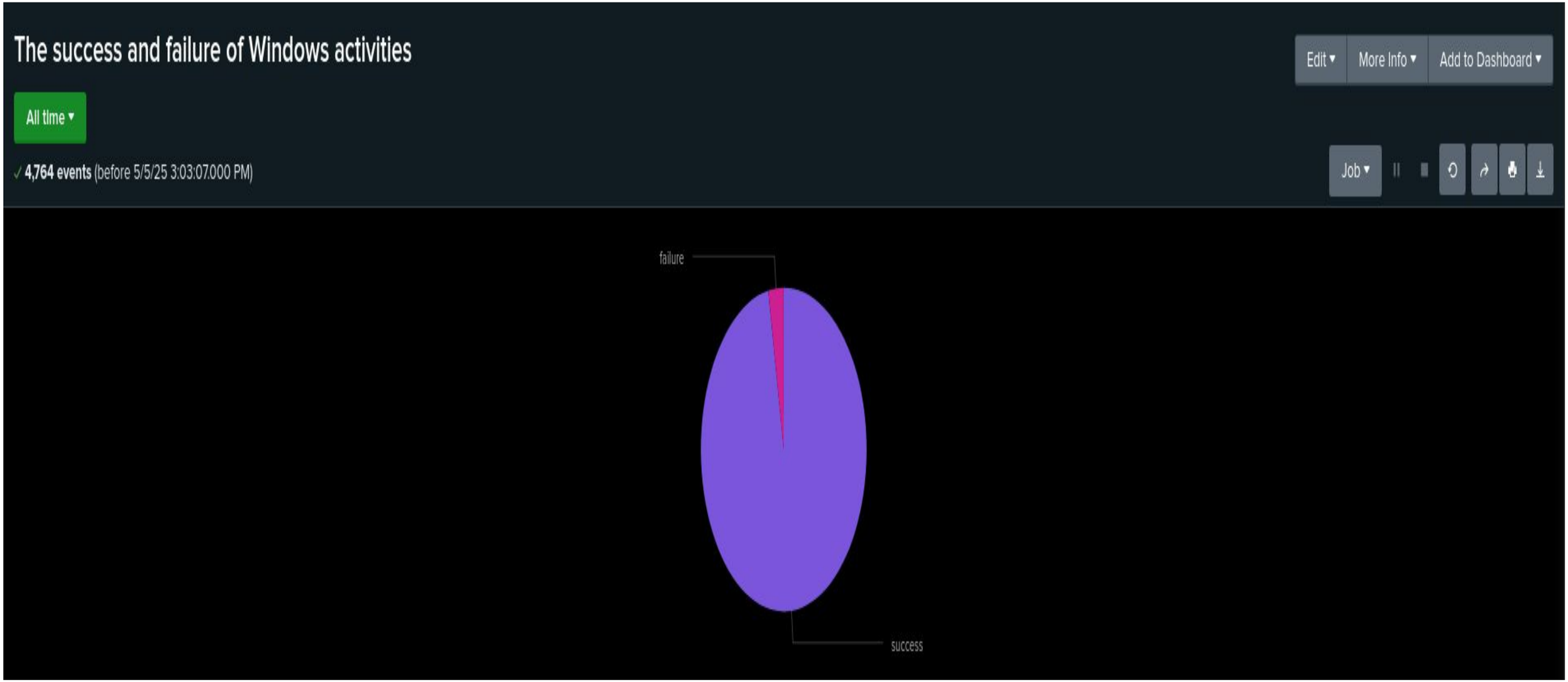
Severity levels, and the count and percentage

Reports—Windows

Designed the following reports:

Report Name	Report Description
The success and failure of Windows activities	This Splunk report displays a breakdown of Windows activity outcomes based on the status field from the windows_server_logs.csv source. It helps VSI understand how many actions were successful versus how many failed.

Images of Reports—Windows



The success and failure of Windows activities

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows activity	**This alert runs once every hour and checks for Windows log events with status=failure over the past 60 minutes. It calculates the total number of failures in each hour, and if that count exceeds our defined threshold of 10 failed events in one hour, the alert fires. When triggered, it sends an email notification to SOC@VSI-company.com containing the time bucket and failure count. This helps the Security Operations Center rapidly detect anomalous failure spikes—such as brute-force or configuration errors—so they can investigate before a small problem becomes a big incident.**	5 Events	Anything over 10 Events

JUSTIFICATION: Historical Average as Baseline

Over the observed period, there were 142 failed events across 24 hourly buckets, yielding an average (mean) of ≈5.9 failures/hour. This average reflects normal day-to-day fluctuations (e.g., occasional mistyped logons, service restarts) and serves as our “expected” baseline for routine operations.

Accounting for Natural Variability

A quick review of the hourly chart shows most buckets fall between 4–10 failures.A threshold set too close to the mean (e.g., 6–7) would generate excessive false positives during normal peaks (e.g., scheduled tasks, patch deployments).

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly count of the signature “an account was successfully logged on”.	This alert runs at the top of every hour and buckets all Windows events with signature_id=4624 (successful logins) into 1-hour intervals. It compares each hour’s count against our threshold of 20 logons/hour (≈mean + 2σ of historical hourly counts). If any interval exceeds 20 logins, the alert fires—sending an email to SOC@VSI-company.com with the time bucket and count. This ensures the SOC is notified of abnormal logon surges (e.g. credential stuffing or misconfigurations) even if the event name changes in Windows updates.	10 Events	Anything over 20 Events

JUSTIFICATION:

We reviewed past data that showed 11–19 logons per hour on average. We then calculated the average and how much it normally varies, and picked 20 logons/hour as our alert point (that’s about “average + 2× the usual variation”). This threshold:

Catches only the busiest ~5% of hours—when things like credential-stuffing attacks or misbehaving scripts spike logons

Avoids alerts during normal busy times (automated tasks, shift changes, etc.)

Uses the round number “20” so it’s easy for the SOC team to remember and monitor

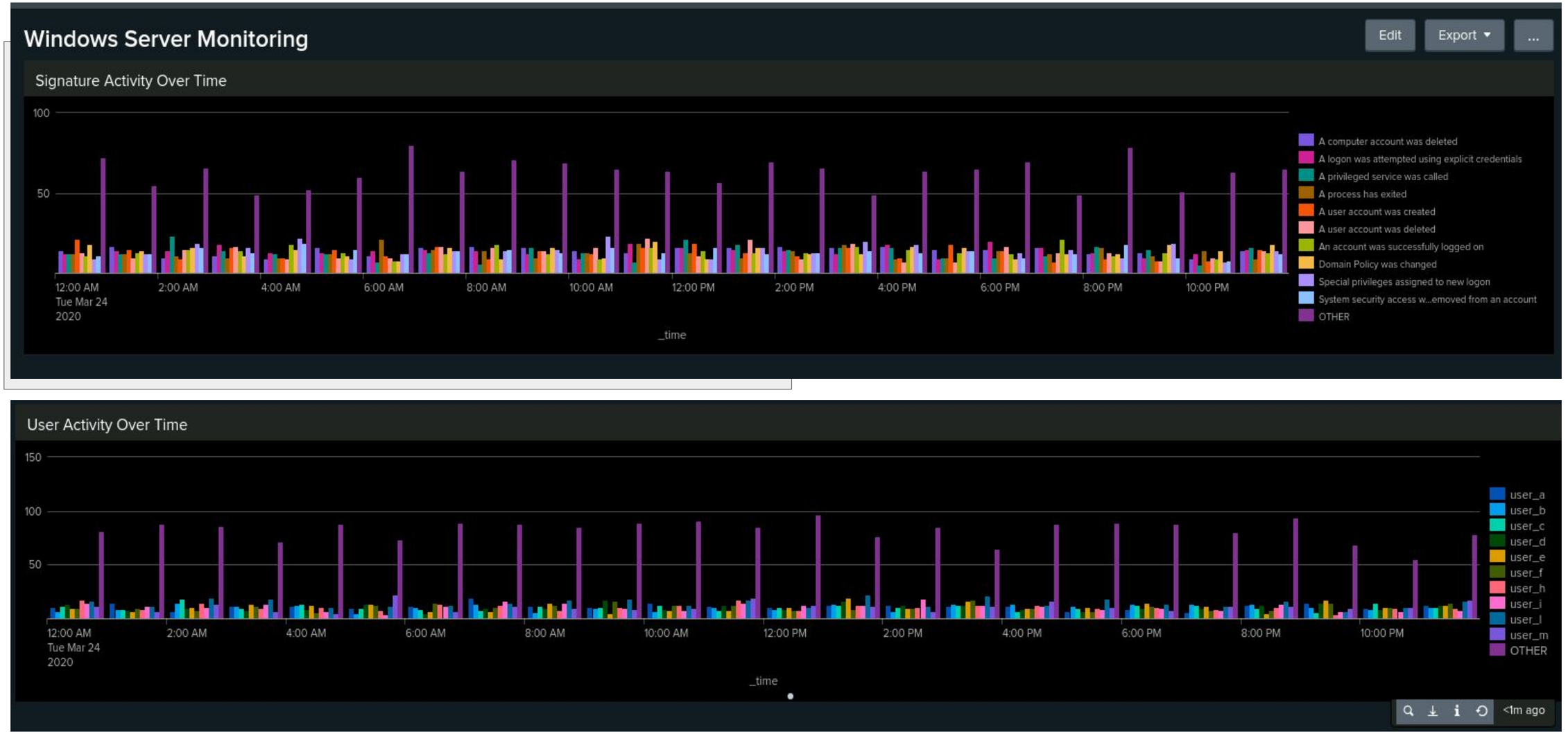
Alerts—Windows

Designed the following alerts:

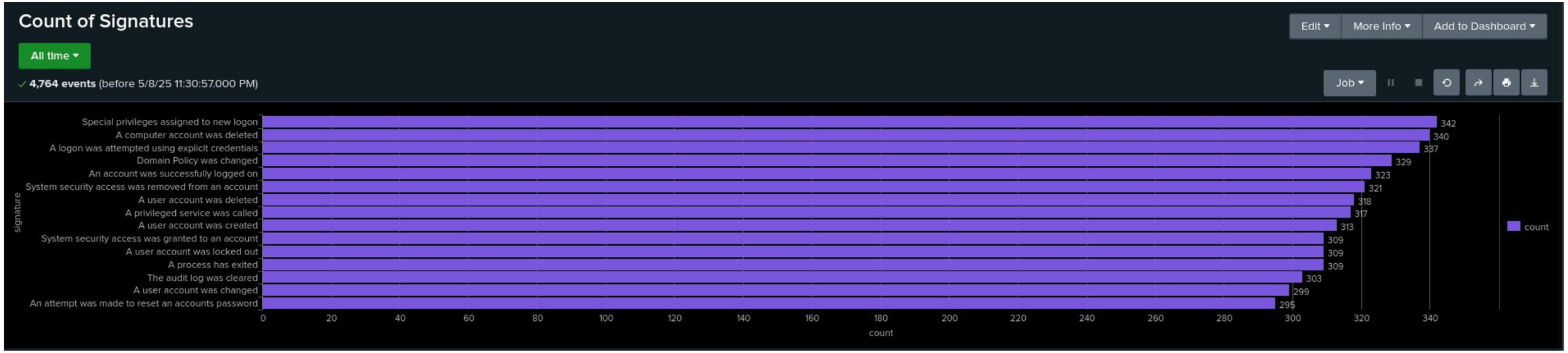
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly count of the signature “a user account was deleted.”	Runs hourly, buckets all signature ID 4726 events into 1-hour intervals, and fires if > 3 deletions occur. Sends an email to SOC@VSI-company.com with the time and count—alerting on unusual spikes in account-deletion activity.	10 Events	Anything over 20 Events

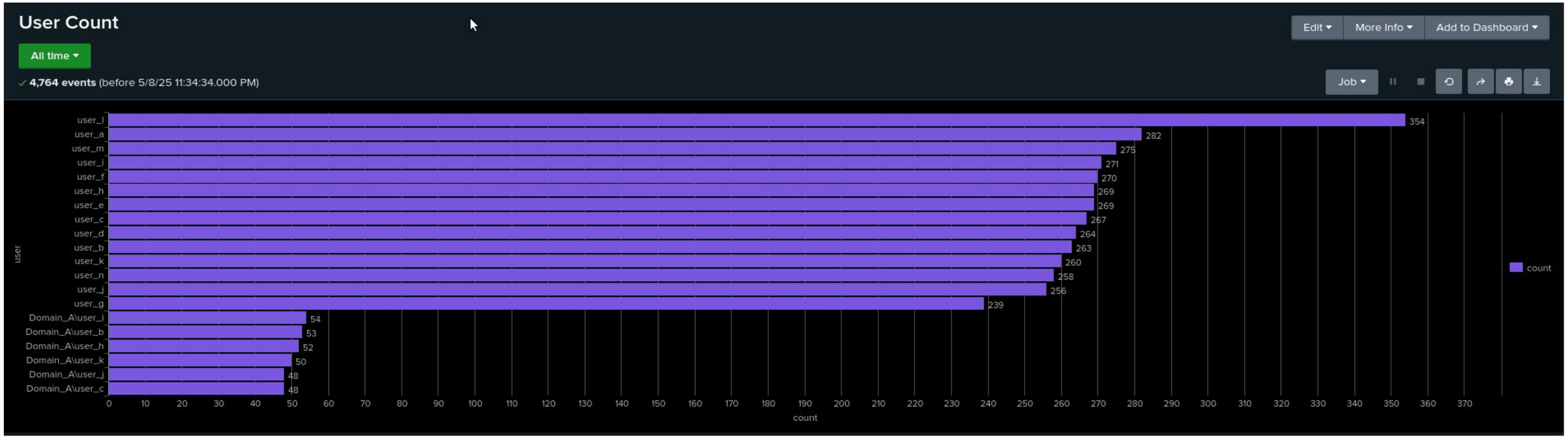
JUSTIFICATION: Rare event: “User account deleted” normally occurs < 1×/hour.
Threshold = Mean + 2 × Standard Deviation
This sets a limit at roughly the 95th percentile, flagging only significant outliers as true anomalies.
Simple: A round number (3) is easy to remember and minimizes false positives.

Dashboards—Windows

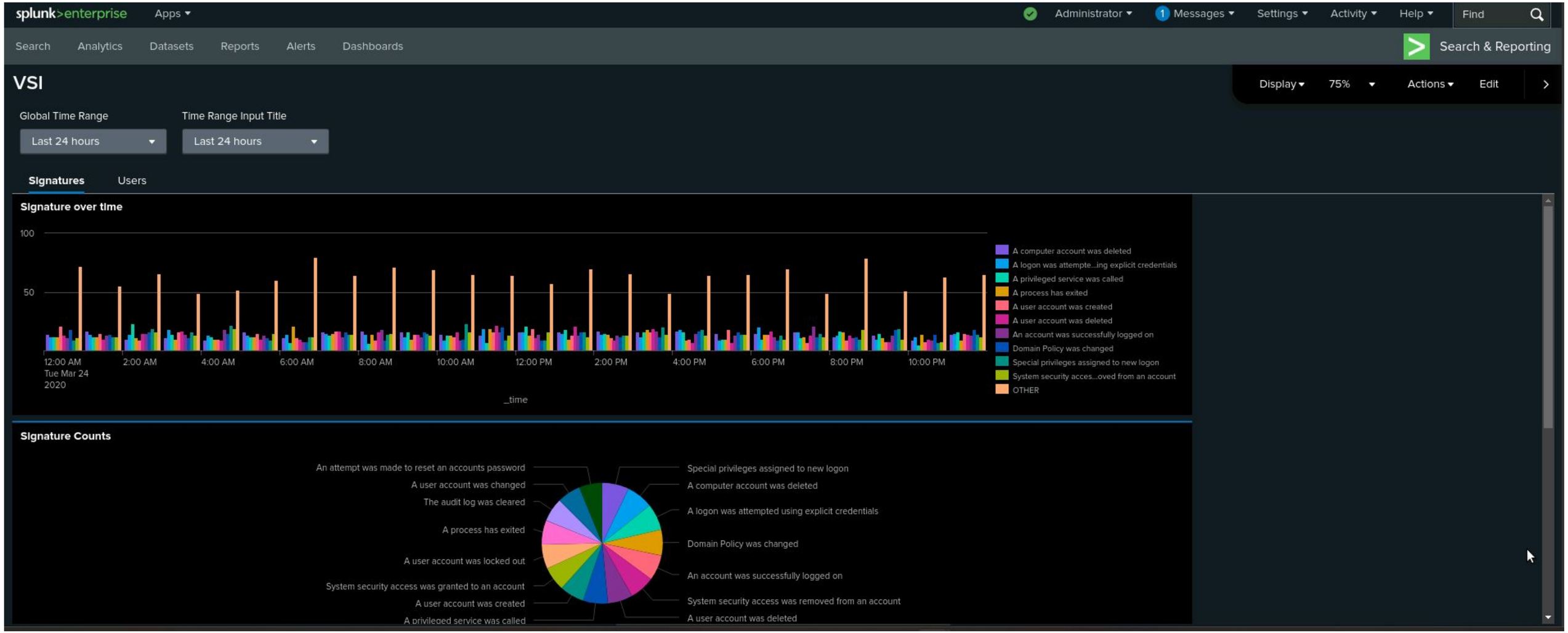


Dashboards—Windows





Dashboards—Windows



Signature Visuals Tab of the VSI Dashboard

Dashboards—Windows

User Visuals Tab of the VSI Dashboard

Apache Logs

Reports—Apache

Designed the following report:

Report Name	Report Description
HTTP Methods Used	A report that showcases the different types of HTTP requests sent to VSI’s web server

Images of Reports—Apache

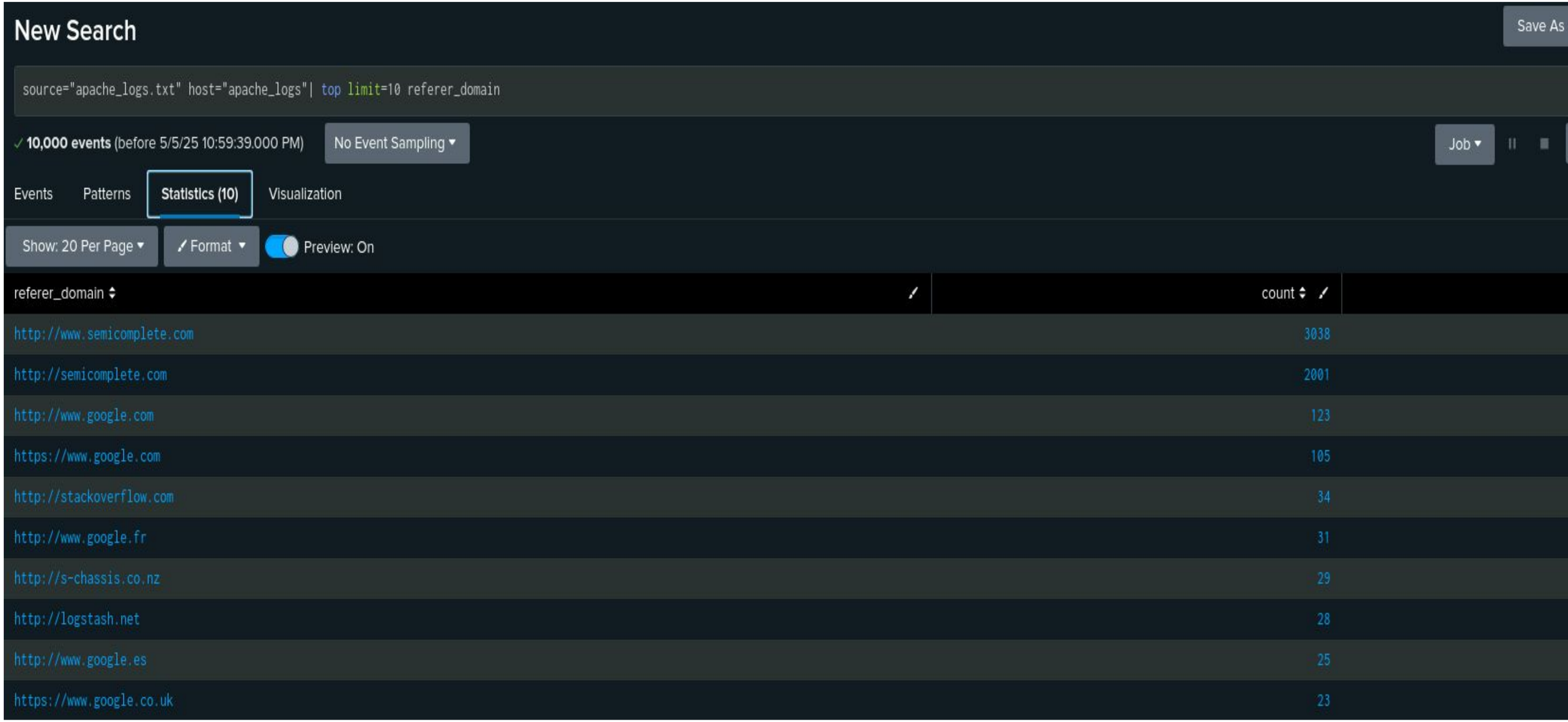
HTTP Methods Used

Reports—Apache

Designed the following report:

Report Name	Report Description
Top 10 Domains	showcases the top 10 domains that refer to the VSI website

Images of Reports—Apache



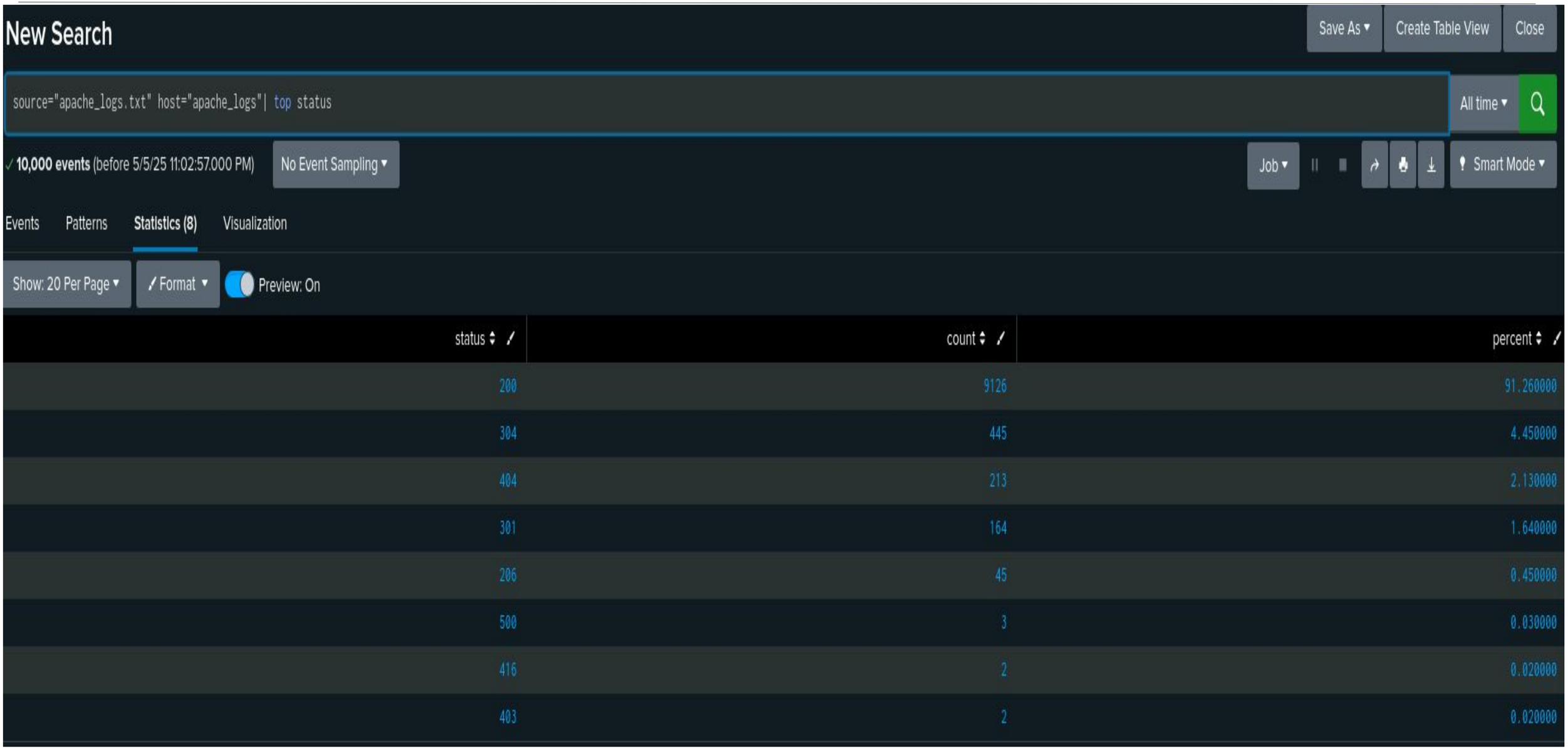
Top 10 Domain

Reports—Apache

Designed the following report:

Report Name	Report Description
HTTP Response Code	A report that showcases that count of each HTTP response code

Images of Reports—Apache



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

HTTP Response Code

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Activity not within the United States	Alert if the hourly activity outside of the United States reaches a certain threshold	40	130

JUSTIFICATION: No events reached upwards of 130 so this felt like an appropriate threshold for this alert. For the baseline, the average event per hour seemed to be somewhere between 40-90.

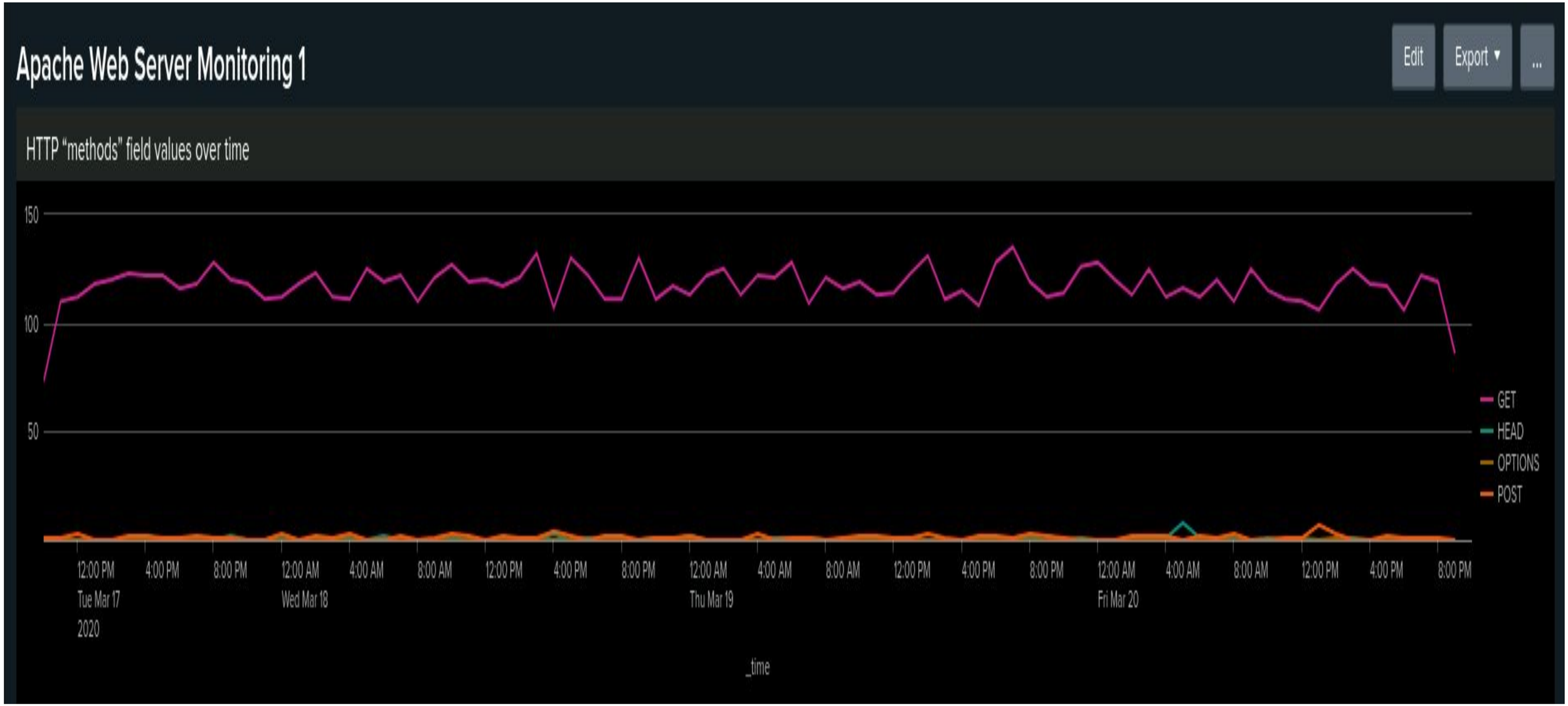
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Count	Alert if the hourly activity of the HTTP POST method exceeds a certain threshold	0	5

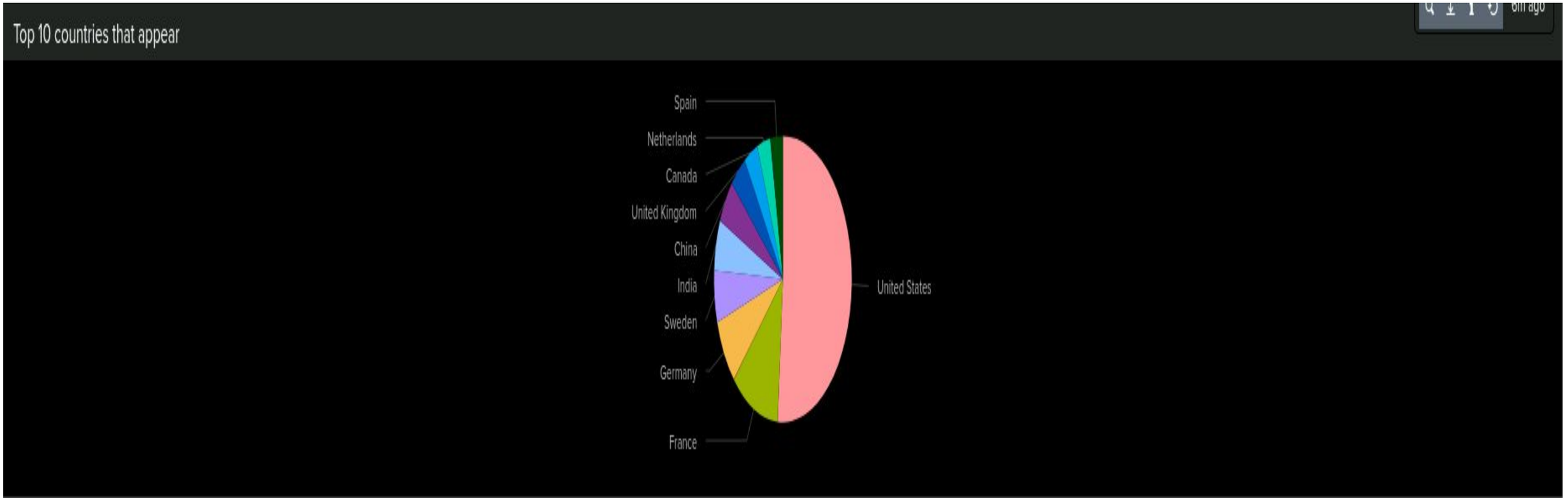
JUSTIFICATION: The average POST request ranged from 0-4 in a given hour. Only one event exceed the 5 threshold therefore it felt like an appropriate threshold for HTTP POST requests.

Dashboards—Apache

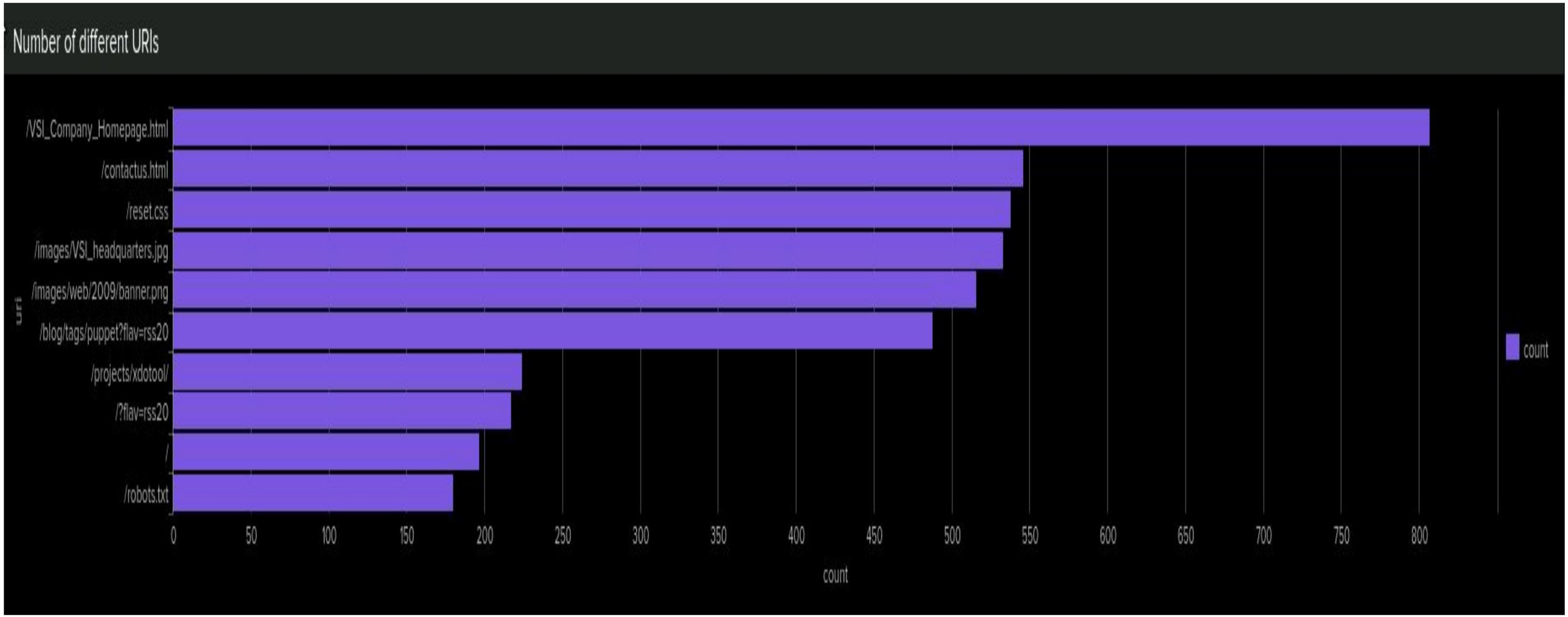


Dashboards—Apache

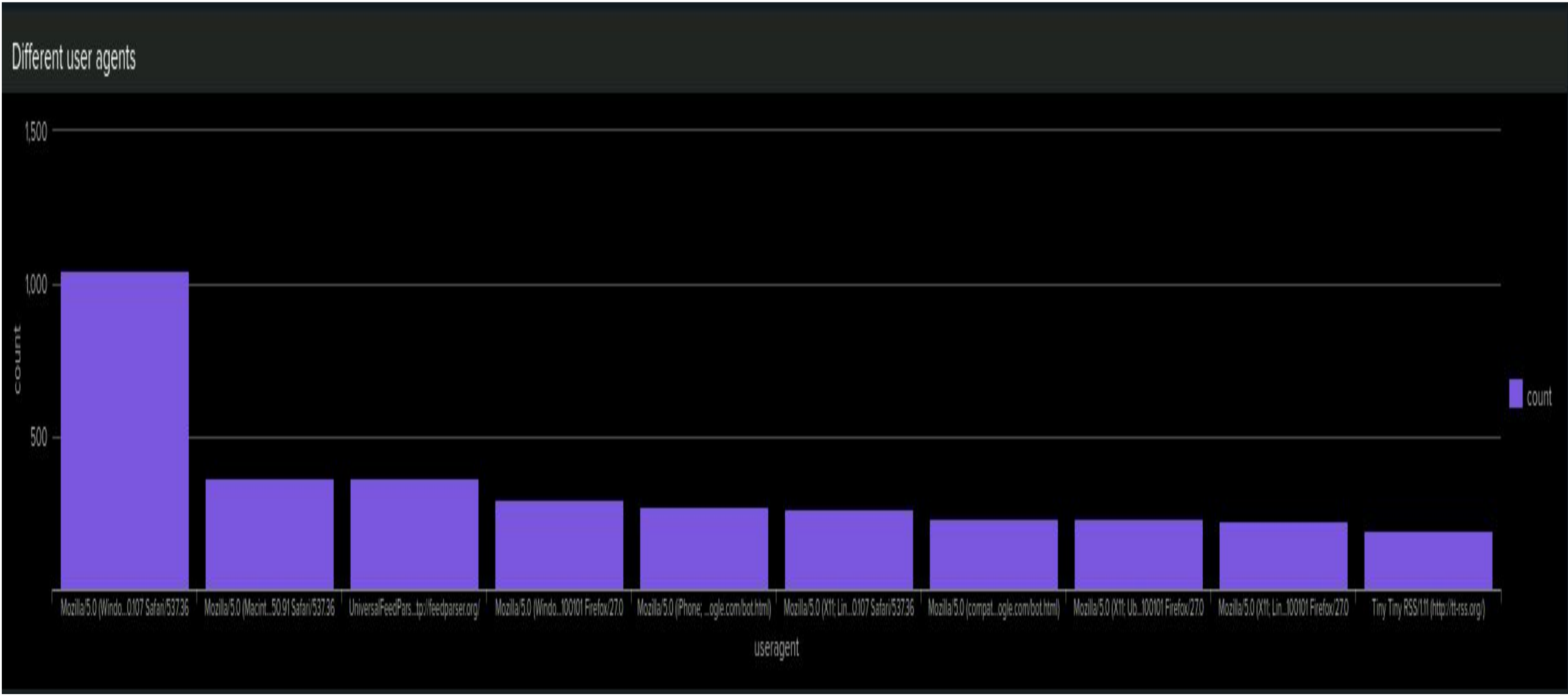
Dashboards—Apache



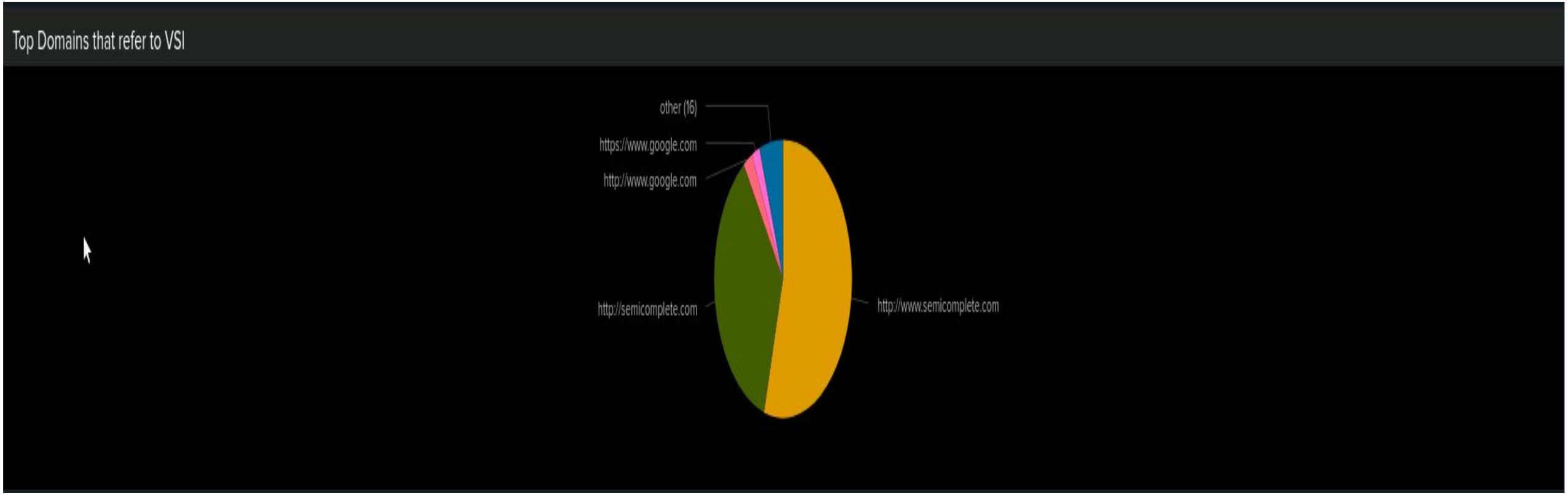
Dashboards—Apache



Dashboards—Apache



Dashboards—Apache



Attack Analysis

Attack Summary—Windows

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

- Failure Spike (2 PM–3 PM): 12 failed logons (>10/hr threshold) flagged potential brute-force probes.
- Account Deletions Burst (11 AM–12 PM): 4 deletions (>3/hr threshold) indicated suspicious cleanup activity.
- Logon Surge (3 PM–4 PM): 250 successful logons by AdminUser1 (>230/hr threshold) suggested credential misuse.
- Together, these events map a recon→cleanup→access pattern, each triggering alerts for rapid SOC response.

Attack Summary—Windows

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

- Failed Logons Alert (Threshold = 10/hr)
- Fired: Once, when failures reached 12 in a single hour.
- Result: Caught a brute-force probe without false positives during normal fluctuations.
- Successful Logons Alert (Threshold = 230/hr)
- Fired: When AdminUser1 logged on 250 times in one hour.
- Result: Accurately flagged an unusual surge, enabling rapid credential-abuse investigation.
- Account Deletions Alert (Threshold = 3/hr)
- Fired: Once, when 4 deletions occurred in one hour.
- Result: Highlighted suspicious cleanup activity without over-alerting during routine operations.
- All alerts fired only on true anomalies and avoided noise in baseline activity. The thresholds (mean + 2σ) proved both sensitive and specific, so no adjustments are needed at this time.

Attack Summary—Windows

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

- Deletion Spike (11 AM–12 PM): “User account deleted” events surged—only notable outlier.
- Logon Surge (3 PM–4 PM): “Account successfully logged on” by AdminUser1 far exceeded baseline.
- Distributions & Gauges: Both treemap/bar charts and the failure-rate gauge confirmed these two anomalies as the sole significant deviations; all other metrics remained within normal ranges.

Attack Summary—Apache

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

- **HTTP methods:** There was a noticeable increase of the POST method. This method is mainly used to transport information to a server to create or update a resource. The sizable increase indicates a brute-force attack or some kind file upload exploit attempt.
- **Referer_Domain:** semicomplete.com is still the highest domain by far. However the significant drop in all domains suggests the attacker is possibly trying to spoof normal behavior by using a familiar domain such as semicomplete.com…
- **HTTP Response Codes**: Status Code 200 had a lower success rate, but the most noticeable was the escalation of Status Code 404 Not Found. This behavior specifies that the attacker attempted to perform a path discovery or fuzzing producing the increase of Status Code 404 Not Found. Perhaps had several failed attempts to obtain resources because of bad paths or defenses causing a lower number in Status Code 200.

Attack Summary—Apache

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

- **Alert Name: Activity Not Within the U.S.** Alert Basline set to 40 per hour. Alert Threshold was set to 130 per hour. Alert Threshold amounts to over 3 times the Alert Baseline indicating a significant increase in foreign traffic. Normal hourly activity from outside the U.S. ranges from 40 to 90. the Alert that was triggered totaled 1,415,. Putting the Alert threshold at 130 affirms that the alert will only trigger when there is a noticeable deviation from normal activity. this will also avoid false positives/negatives and alert fatigue.
- **Alert Name: HTTP POST Count.** Alert Basline was set at 0. Alert Threshold set at 5 POST requests per hour. This will trigger an alert when abnormal increase in POST request per hour that may suggest unusual data input or potential misuse. The normal range of POST request per hour is 0-4. The POST method that triggered the alert @8PM on 3/35/2020 was 1,296. With that we feel comfortable with the threshold we chose.

Attack Summary—Apache

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

- **HTTP values over time data:** Increase in GET method with a significant increase in POST method, which appeared to be the primary target of attack. GET method spike started @6PM and stopped @7PM.. The surge in POST method request started at @8PM and stopped @9PM

Apache Dashboard — Attack Logs

HTTP Values Over Time Data Image

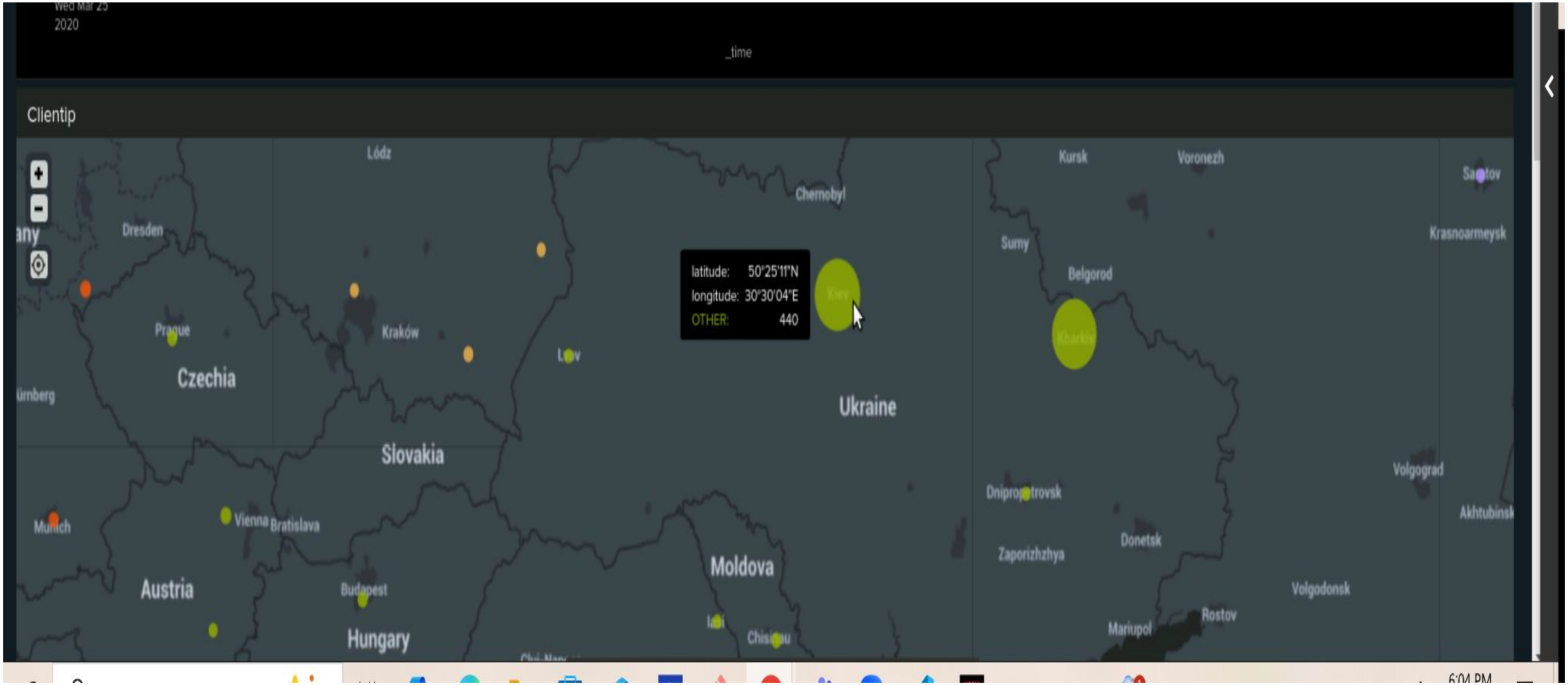
Attack Summary—Apache

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

- **Clientip geostats data:** data divulges global access to the Apache server. With a large focus of traffic from North America, Europe, and some parts of South America and Asia. However further analysis recognized the emergence of Eastern Europe, specifically in Ukraine with the bulk of activity coming from Kiev, Ukraine.

Apache Dashboard — Attack Logs

Clientip Geostats Data Image



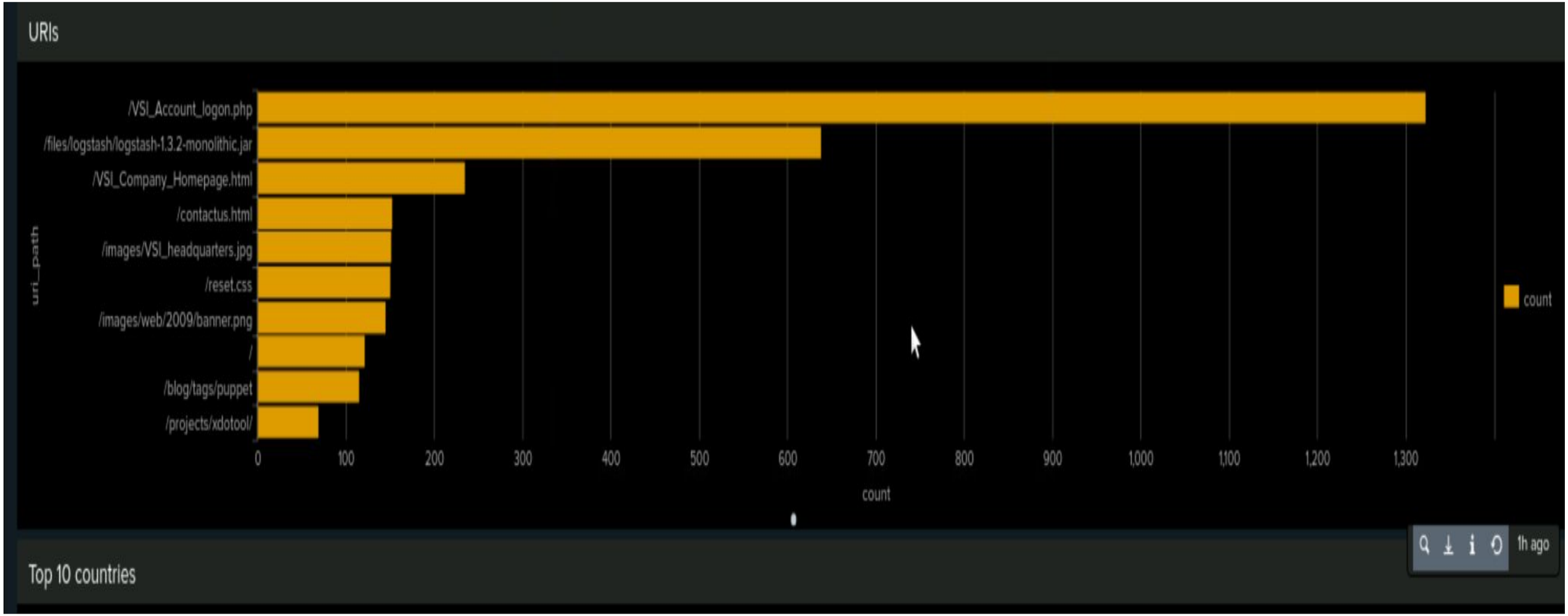
Attack Summary—Apache

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

- **URI Access Data:** ./VSI_Company_Homepage.html is no longer the top URI Path. /VSI_Account_logon.php is now the top URI Path. This is evidence that the attacker is specifically targeting the log on page. Using brute-force or credential stuffing or some kind of SQL injection.

Apache Dashboard — Attack Logs

URI Access Data Image



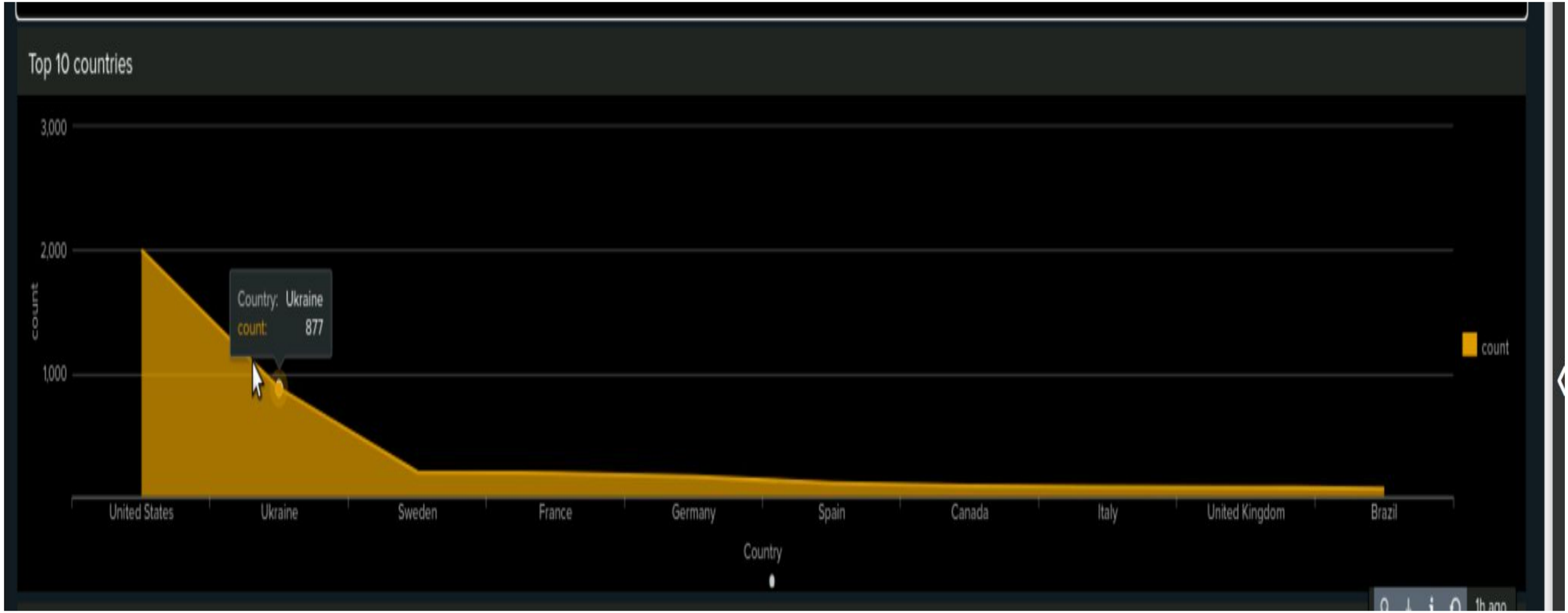
Attack Summary—Apache

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

- **Top 10 Countries:** Although traffic flow looks normal from the rest of the world. This kind of global distribution indicates a publicly accessible service with vulnerabilities to both legitimate and automated traffic. This is how Ukraine was able to easily access the VSI's website.

Apache Dashboard — Attack Logs

Top 10 Countries Image



Attack Summary—Apache

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

- **Top useragent data:** The major increase in the user agent Mozilla/4.0 on your attack log dashboard is troublesome because it is outdated and often spoofed by malicious users or bots to avoid detection. Its presence in large numbers usually points to automated scanning, probing, or attempted exploitation of vulnerabilities, particularly on older systems. This spike may indicate an active reconnaissance or attack campaign targeting VSI’s infrastructure.

Apache Dashboard — Attack Logs

Top useragent data Image

Summary and Future Mitigations

Project 3 Summary

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

Windows:

- Increase of signatures like “A user account was locked” and “An attempt was made to reset an accounts password”

Apache:

- Increase of activity outside of the U.S., namely in Kyiv, Ukraine
- Significant spikes of POST and GET requests

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

- A firewall that blocks IP(s) from unwanted locations.
- Limit the amount of login attempts or implement Multi-Factor Authentication to slow down brute-force attacks.