Defensive Security Project by:

Chet Flowers

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations


Monitoring Environment

Scenario

Monitoring and Security for VSI

Objective: Implement a comprehensive monitoring solution for Virtual Space Industries (VSI) using Splunk.

Setup: Deployed Splunk Docker container; analyzed Windows (`windows_server_logs.csv`) and Apache (`apache_logs.txt`) logs.

Focus Areas:

- **Windows Logs:** `signature_id`, `signature`, `user`, `status`, `severity`
- **Apache Logs:** `method`, `referer_domain`, `status`, `clientip`, `useragent`

Reports Created:

- **Windows:** Signature IDs, severity levels, success vs. failure
- **Apache:** HTTP methods, top referrers, response codes

Alerts Configured:

- **Windows:** Failed/successful logins, account deletions
- **Apache:** International traffic, high POST request volume

Dashboards Designed:

- **Windows:** Signature trends, user activity, event counts
- **Apache:** HTTP methods, URI counts, traffic distribution

Enhancement: Installed additional Splunk add-on for improved monitoring.

Outcome: Provides VSI with robust detection and response capabilities for security and operational oversight.


Whois XML Website Categorization API for Splunk

Whois XML Website Categorization API for Splunk

Whois XML Website Categorization API for Splunk provides real-time website categorization and threat intelligence. It enhances security by classifying web traffic based on categories like malicious, suspicious, or benign.

Key Features:

- **Real-Time Monitoring:** Provides immediate categorization of referrer domains and websites, allowing for instant insights into their nature and potential risks.
- **Troubleshooting:** Helps in identifying and categorizing domains associated with malware, phishing, or other security threats.
- **Alerting:** Configurable alerts for detecting and responding to traffic from suspicious or malicious domains.
- **Scalability:** Efficiently handles large volumes of domain data, making it suitable for extensive web environments.
- **Integration:** Seamlessly works with other Splunk apps.

! **Seamlessly integrates with Splunk to provide real-time website categorization, enhancing threat detection and overall security monitoring.**

Whois XML Website Categorization API for Splunk

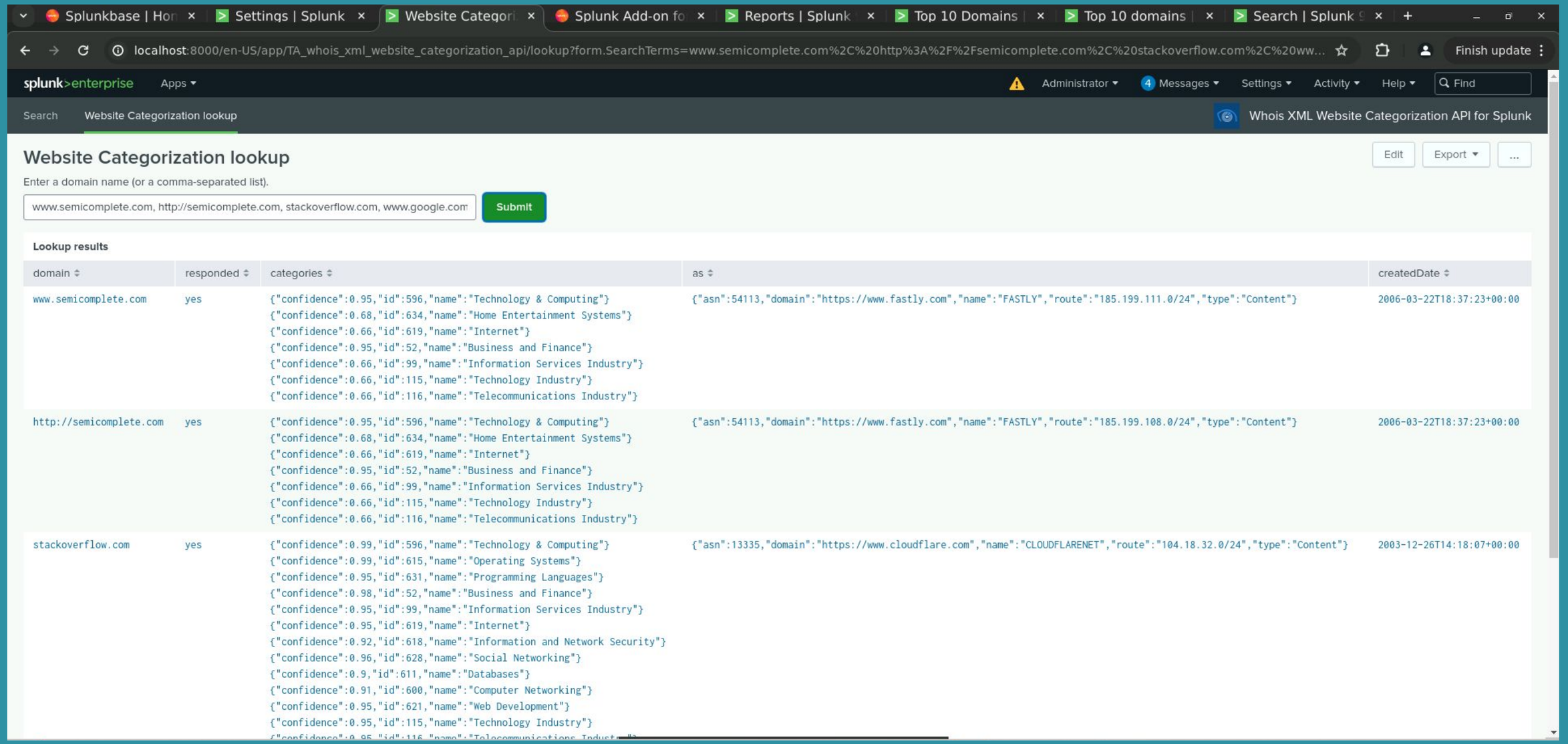
A security team notices a spike in outbound traffic to various domains, potentially indicating data exfiltration or access to malicious websites through:

- **Integration:** The team integrates the Whois XML API with Splunk.
- **Monitoring:** They monitor network traffic and categorize domains in real-time.
- **Categorization:** The API categorizes domains, flagging potential exploits.
- **Analysis:** The team identifies legitimate traffic and suspicious activity.
- **Alerting:** Alerts are set for malicious categories, triggering investigations.
- **Mitigation:** Compromised endpoints are isolated, and malicious domains blocked.

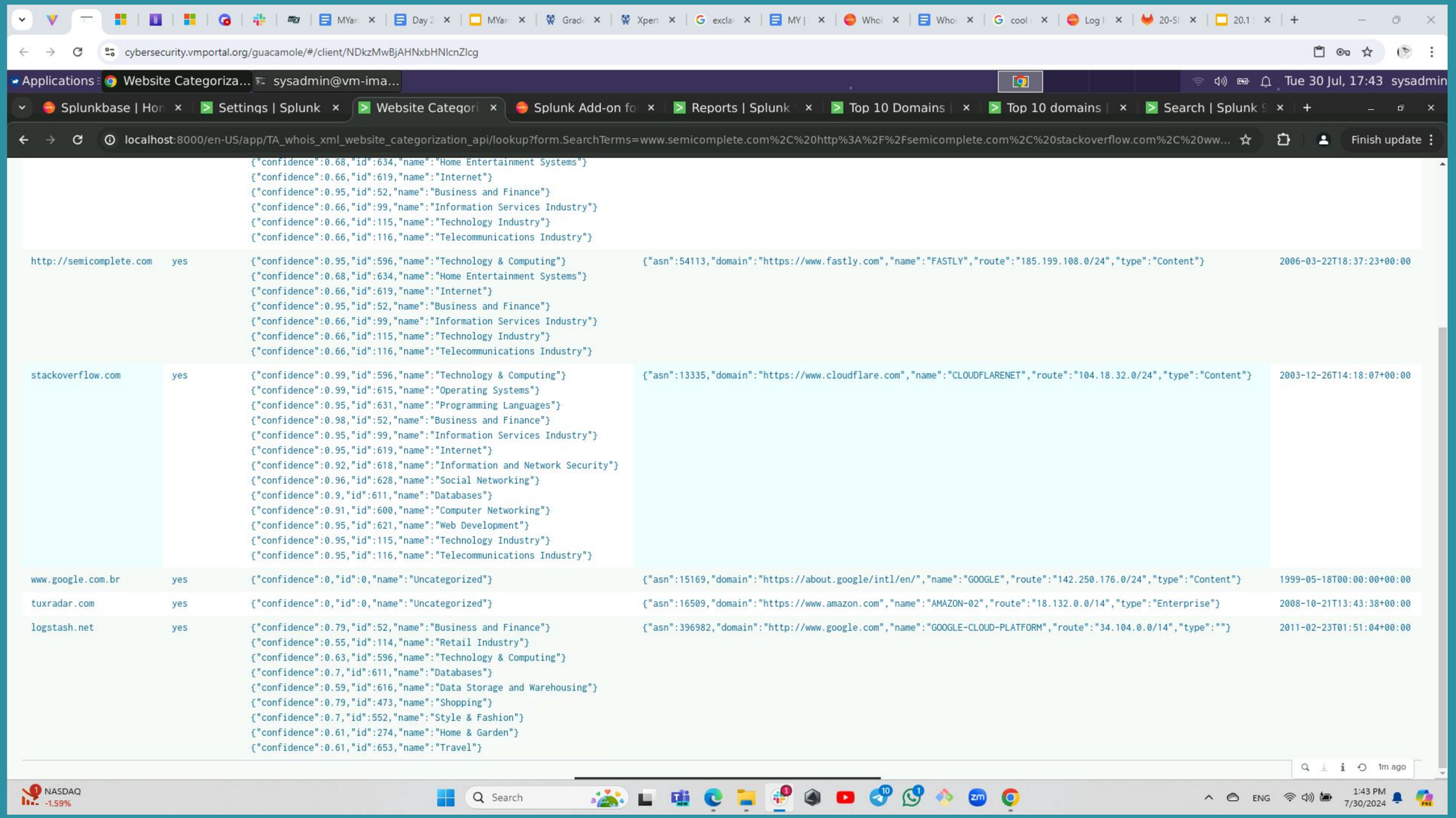
The team quickly identifies and mitigates threats with:

- **Proactive Detection:** Early detection of malicious activity.
- **Efficient Analysis:** Distinguishes between legitimate and suspicious traffic.
- **Enhanced Security:** Quick response to threats, reducing data breach risks.
- **Improved Network Safety:** Blocking malicious domains ensures safer internet usage.

Whois XML Website Categorization API for Splunk



Whois XML Website Categorization API for Splunk



Logs - Analyzed

1 Windows Logs

File: `windows_server_logs.csv`
Content: Logs from a Windows server
Purpose:

- Track and monitor user activity
- Detect and identify potential security incidents
- Record and store data for forensic analysis

Use Case: Helps monitor server activities and understand the security posture

2 Apache Logs

File: `apache_logs.txt`
Content: Logs from an Apache server
Purpose:

- Track HTTP requests & responses
- Detect and identify potential security incidents
- Analyze user behavior and web traffic patterns

Use Case: Provides insights into web traffic, server health, and security monitoring

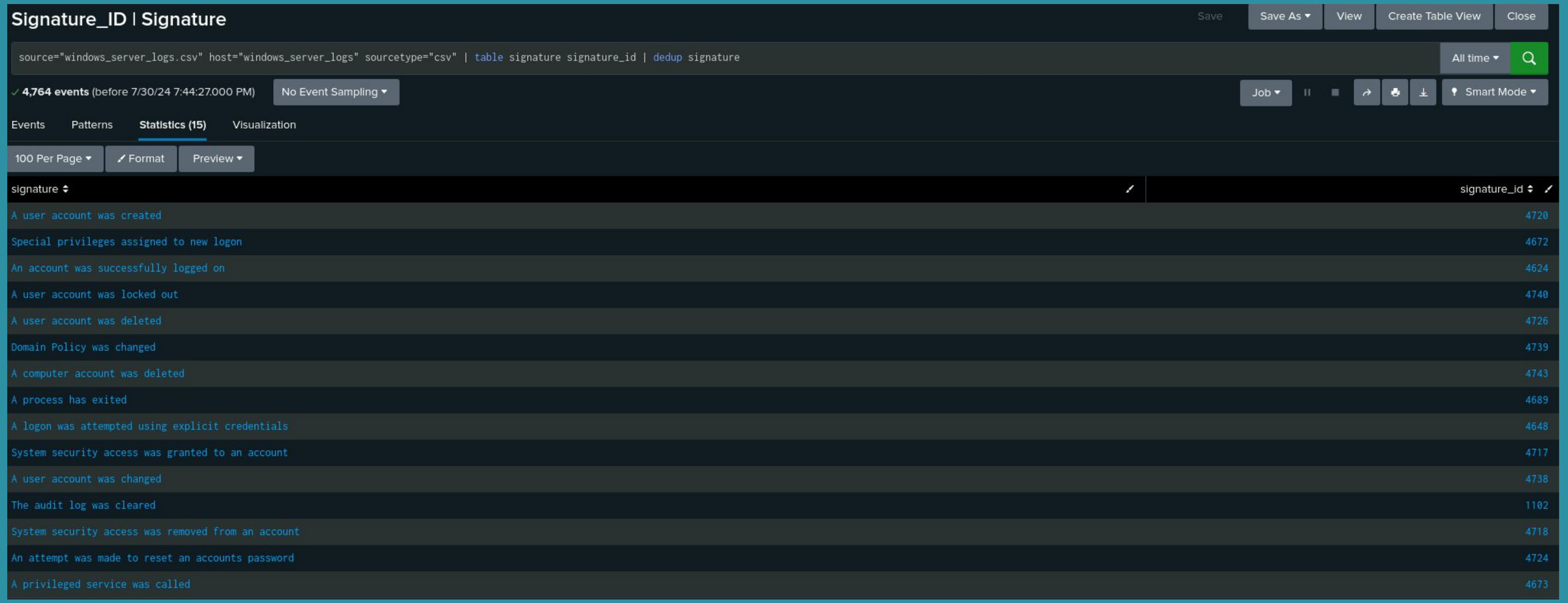

Windows Logs

Reports – Windows

Designed the following reports:

Report Name	Report Description
Table of Signature and Signature ID's	The 'signature' field describes the event, providing context about what occurred and the 'signature_id" helps pinpoint specific types of events as a unique identifier.
Severity Levels by Count and Percentage	The 'severity' field reflects the seriousness of the event, allowing us to prioritize incidents based on their potential impact.
Status by Success and Failure	The 'status' field indicates whether the event was successful or not, helping us identify failed login attempts or other unsuccessful actions.

Images of Reports – Windows



Images of Reports – Windows (cont.)

Severity Levels by Count and Percentage

Save | Save As | View | Create Table View | Close

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv"
| stats count by severity
| eventstats sum(count) as total
| eval percentage=round((count * 100)/total, 2)
| table severity, count, percentage
```

All time

✓ **4,764 events** (before 7/30/24 7:46:02.000 PM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (2)** | Visualization

100 Per Page | Format | Preview

severity	count	percentage
high	329	6.91
informational	4435	93.09

Status by Success and Failure

Save | Save As | View | Create Table View | Close

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv"
| stats count by status
| eventstats sum(count) as total
| eval percentage=round((count * 100)/total, 2)
| table status, count, percentage
```

All time

✓ **4,764 events** (before 7/30/24 7:48:15.000 PM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (2)** | Visualization

100 Per Page | Format | Preview

status	count	percentage
failure	142	2.98
success	4622	97.02

Alerts – Windows

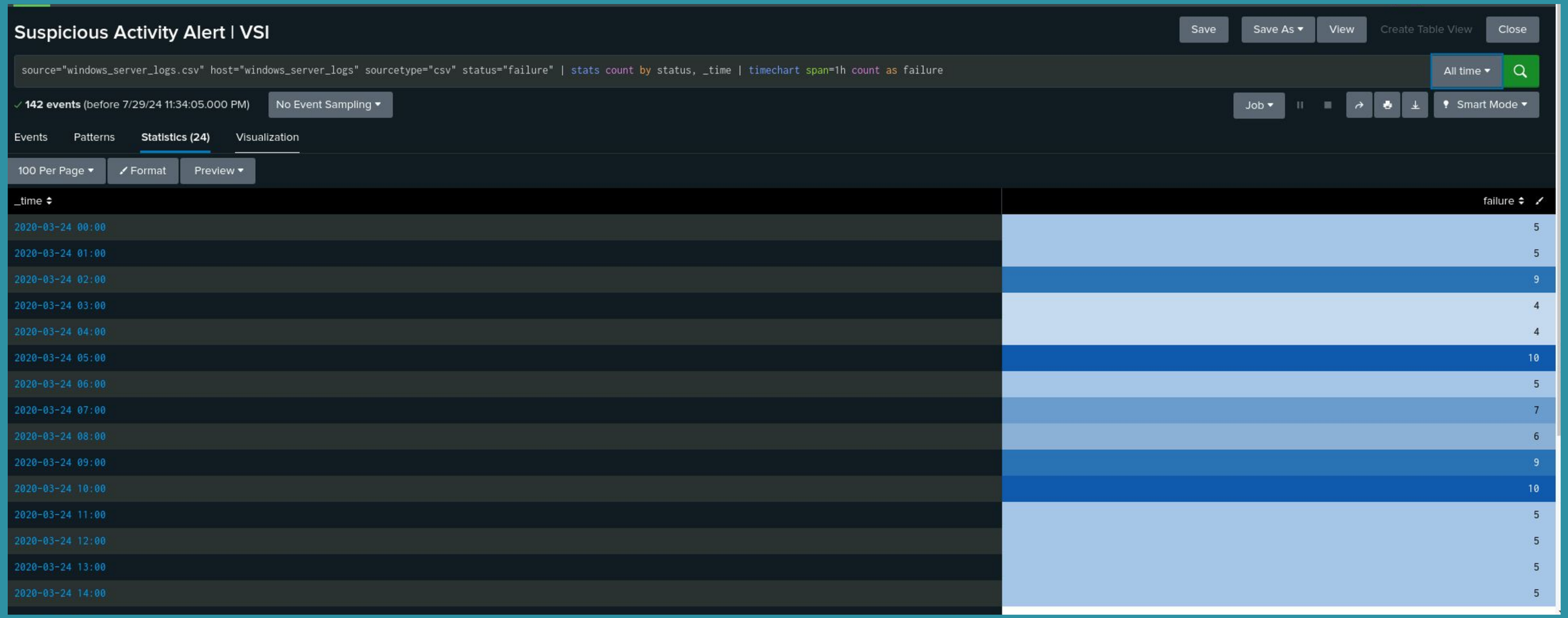
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Failed Attempts	**Alert Purpose:** Monitor Windows security logs **Trigger Condition:** High number of failed login attempts within a specified time frame **Potential Threats:** • Brute force attacks • Unauthorized access attempts	**Average Failed Attempts per Hour = 5**	**Threshold = 8 Failed Attempts Per Hour**

JUSTIFICATION:

- **Total Events:** 4,764
- **Failed Attempts:** 142 (Approx. 2.98%)
- **Average Failed Attempts per Hour:** 5
- **Peak Failed Attempts:** 10
- **Threshold Recommendation:** Set at 8 attempts per hour
- **Reasoning:** Balances sensitivity to detect unusual spikes while minimizing false alarms

Images of Alerts – Windows



_time	failure
2020-03-24 00:00	5
2020-03-24 01:00	5
2020-03-24 02:00	9
2020-03-24 03:00	4
2020-03-24 04:00	4
2020-03-24 05:00	10
2020-03-24 06:00	5
2020-03-24 07:00	7
2020-03-24 08:00	6
2020-03-24 09:00	9
2020-03-24 10:00	10
2020-03-24 11:00	5
2020-03-24 12:00	5
2020-03-24 13:00	5
2020-03-24 14:00	5

Alerts – Windows (cont.)

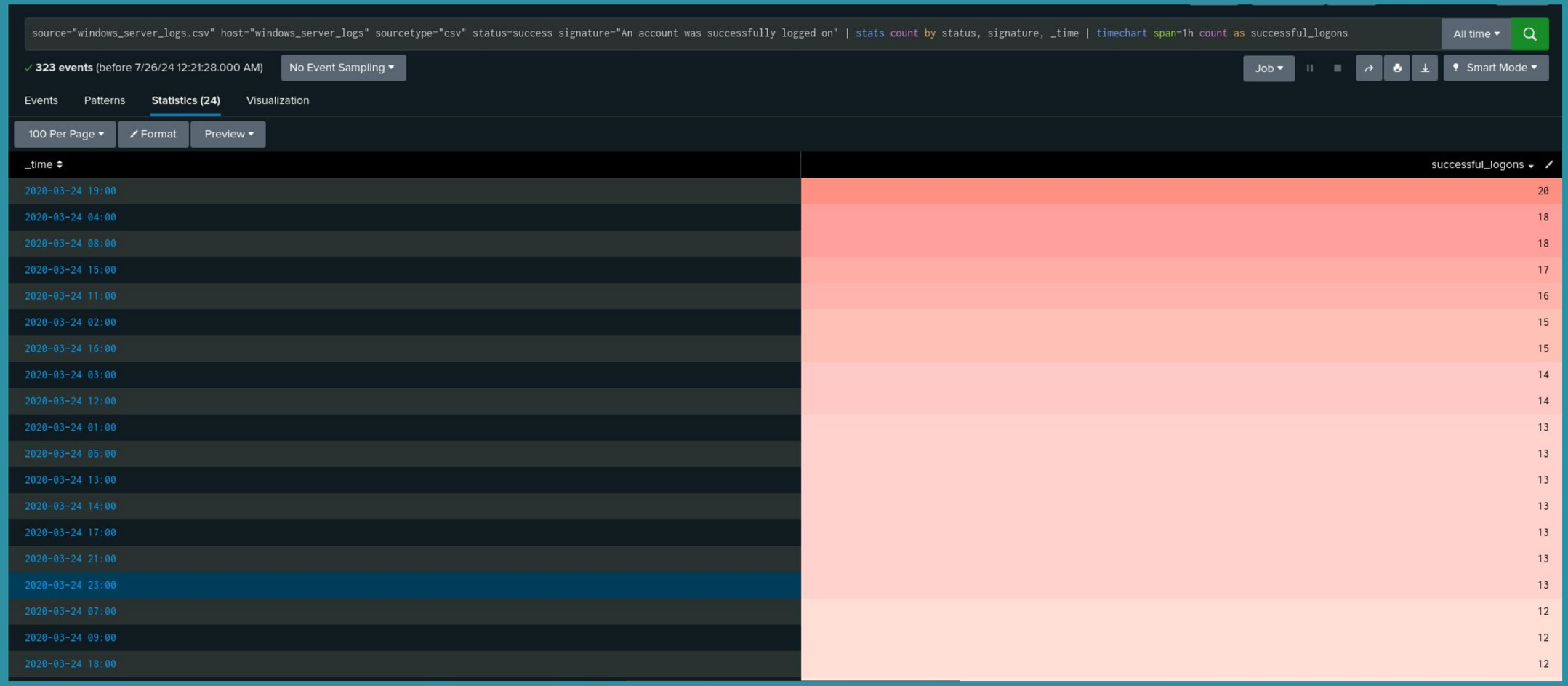
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Number of Successful Windows Logon Attempts	**Alert Purpose:** Monitor Windows security logs **Trigger Condition:** High number of successful logon attempts within a specified time frame **Potential Threats:** • Unauthorized access • Compromised accounts **Indicator:** Sudden increase in successful logins	**Average Successful Logins per Hour =** 13	**Allowed Successful Login Attempts Per Hour =** 17

Justification:

- **Average Successful Logins per Hour:** 13.46 (baseline for normal activity)
- **Peak Successful Logins:** 20 per hour
- **Threshold Recommendation:** Set at 17 logins per hour
- **Reasoning:** Balances between preventing false alarms and detecting unusual spikes in activity

Images of Alerts – Windows (cont.)



Alerts – Windows (cont.)

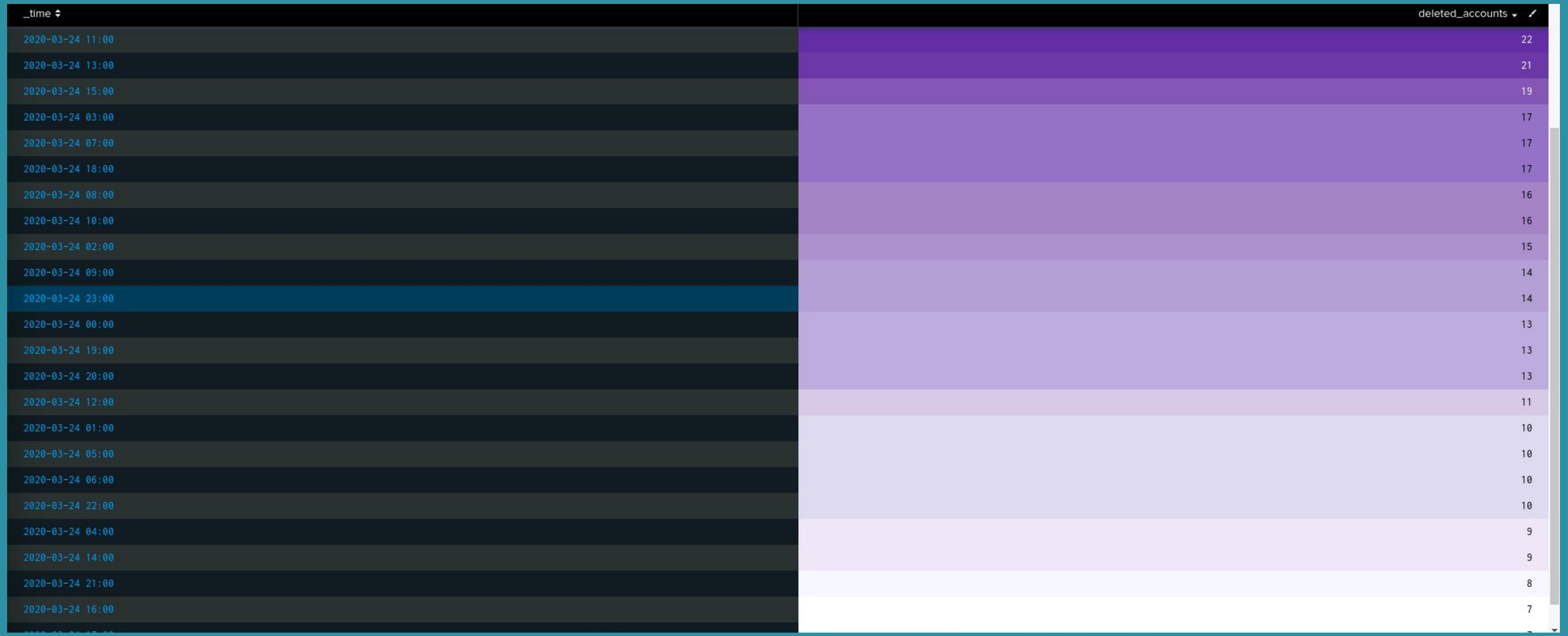
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
High Number of User Account Deletions	**Alert Purpose:** Monitor Windows security logs **Trigger Condition:** Unusually high number of user account deletions in time frame **Potential Threats:** • Unauthorized activity • Security breaches **Indicator:**Sudden spike in account deletions	**Average Deleted Accounts Per Hour =** 13	**Allowed Deleted Account Attempts per Hour =** 17

JUSTIFICATION:

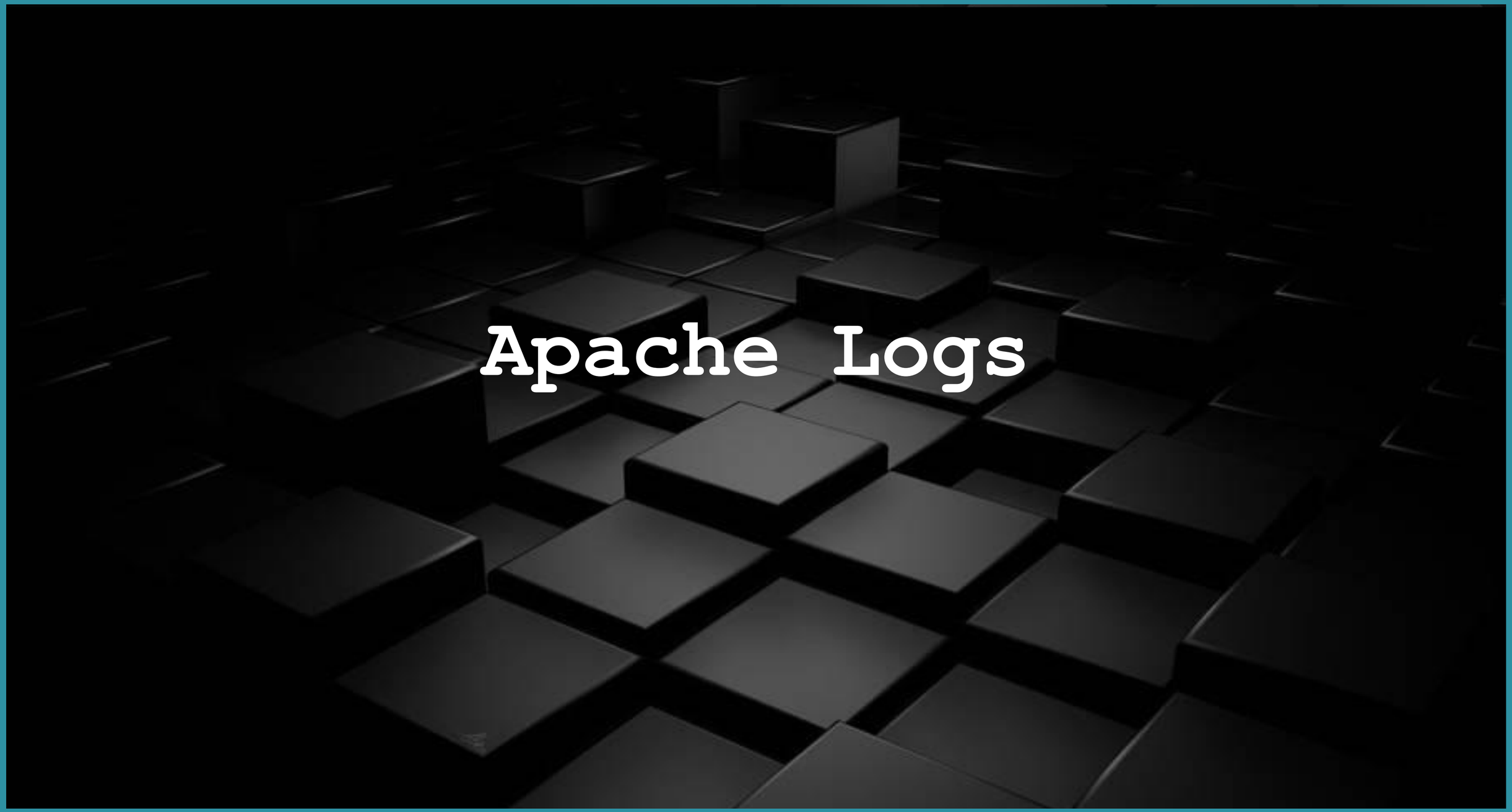
- **Baseline for Normal Deletions:**13.25 (reference point for typical behavior)
- **Threshold Recommendation:** Set at 17 deletions
- **Reasoning:**Captures significant deviations above the average while considering the peak of 22 deletions
- **Goal:**Detect unusual spikes in account deletions while minimizing false alarms

Images of Alerts – Windows (cont.)



_time	deleted_accounts
2020-03-24 11:00	22
2020-03-24 13:00	21
2020-03-24 15:00	19
2020-03-24 03:00	17
2020-03-24 07:00	17
2020-03-24 18:00	17
2020-03-24 08:00	16
2020-03-24 10:00	16
2020-03-24 02:00	15
2020-03-24 09:00	14
2020-03-24 23:00	14
2020-03-24 00:00	13
2020-03-24 19:00	13
2020-03-24 20:00	13
2020-03-24 12:00	11
2020-03-24 01:00	10
2020-03-24 05:00	10
2020-03-24 06:00	10
2020-03-24 22:00	10
2020-03-24 04:00	9
2020-03-24 14:00	9
2020-03-24 21:00	8
2020-03-24 16:00	7

Dashboards – Windows


Apache Logs

Reports – Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods Analysis	**Report Focus:** Analysis of HTTP methods used in requests to VSI's web server **Monitored Methods:** GET, HEAD, OPTIONS, POST **Purpose:** • Highlight frequency of each method • Provide insights into request patterns • Identify unusual traffic behavior
Top 10 Referring Domains	**Report Focus:** Top 10 external domains referring traffic to VSI's website **Purpose:** • Identify sources generating the most traffic • Understand referral patterns • Spot unusual or potentially suspicious referrers
HTTP Response Codes Report	**Report Focus:** Summary of HTTP response codes generated by VSI's web server **Purpose:** • Analyze server response patterns • Track successful requests • Identify various error types (e.g., 4xx, 5xx codes)

Images of Reports – Apache

HTTP Methods Analysis

Save | Save As | View | Create Table View | Close

```
source="apache_logs.txt" host="apache_logs.txt" sourcetype="access_combined"
| stats count by method
| where method IN ("GET", "POST", "HEAD", "OPTIONS")
| eventstats sum(count) as total_count
| eval percentage=round((count * 100) / total_count, 2)
| table method, count, percentage
| rename method as "Method", count as "Count", percentage as "Percentage"
```

All time

✓ **10,000 events** (before 7/30/24 8:14:28.000 PM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (4)** | Visualization

100 Per Page | Format | Preview

Method	Count	Percentage
GET	9851	98.51
HEAD	42	0.42
OPTIONS	1	0.01
POST	106	1.06

HTTP Response Code

Save | Save As | View | Create Table View | Close

```
source="apache_logs.txt" host="apache_logs.txt" sourcetype="access_combined" | stats count as response_count by status | sort - response_count | rename status to response_code
```

All time

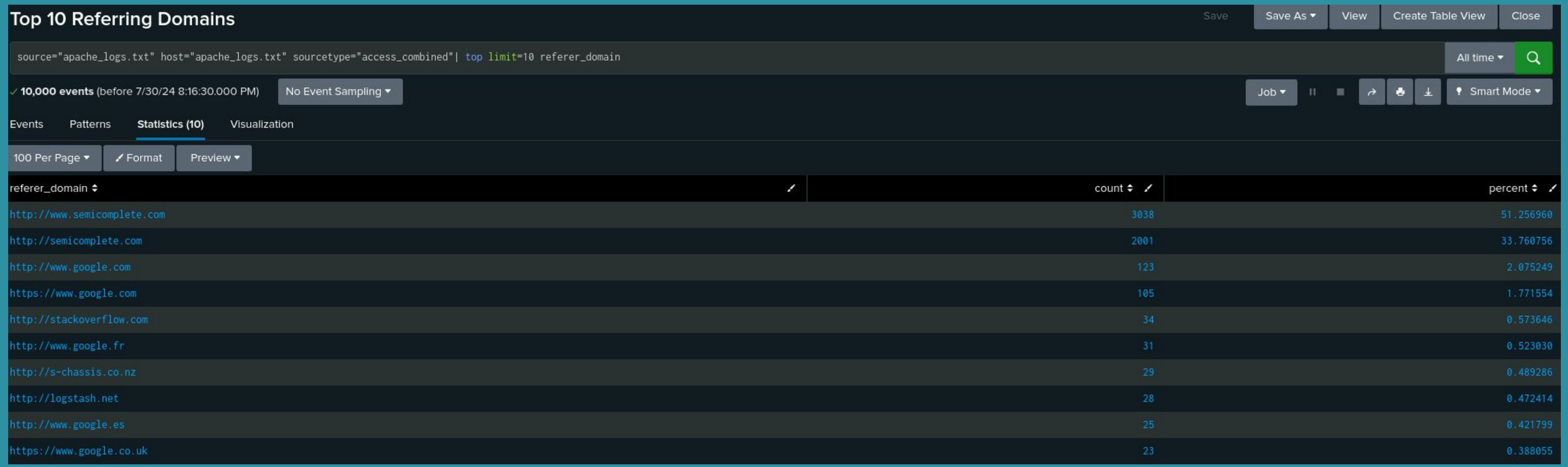
✓ **10,000 events** (before 7/26/24 3:00:35.000 AM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (8)** | Visualization

100 Per Page | Format | Preview

response_code	response_count
200	9126
304	445
404	213
301	164
206	45
500	3
403	2
416	2

Images of Reports – Apache (cont.)



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
International Traffic Alert	**Alert Purpose:** Monitor web traffic volume originating from outside the US **Trigger Condition:** Unusual spikes in international traffic **Potential Threats:** • Security threats from foreign sources • Unauthorized access attempts **Insight:** Helps detect suspicious international activity	**Average number of international web traffic instances per hour =** 76	**Allowed number of international web traffic instances per hour =** 91

Images of Alerts – Apache

Hourly Activity from any country

Edit | More Info | Add to Dashboard

All time

✓ 6,140 events (before 7/28/24 4:20:42.000 PM)

Job

84 results | 100 per page

_time	count
2020-03-20 00:00	120
2020-03-19 19:00	113
2020-03-19 23:00	111
2020-03-19 08:00	108
2020-03-19 18:00	108
2020-03-20 01:00	108
2020-03-20 09:00	107
2020-03-19 11:00	106
2020-03-19 06:00	102
2020-03-19 16:00	100
2020-03-19 21:00	99
2020-03-20 10:00	98
2020-03-19 15:00	97
2020-03-19 13:00	96
2020-03-20 03:00	95
2020-03-19 20:00	94
2020-03-19 04:00	91
2020-03-20 10:00	98
2020-03-19 15:00	97
2020-03-19 13:00	96
2020-03-20 03:00	95
2020-03-19 20:00	94
2020-03-19 04:00	91
2020-03-19 10:00	91
2020-03-19 22:00	91
2020-03-19 14:00	90
2020-03-20 07:00	90
2020-03-18 21:00	89
2020-03-19 09:00	88
2020-03-20 02:00	88
2020-03-18 23:00	86
2020-03-18 20:00	85
2020-03-20 05:00	85
2020-03-17 13:00	84
2020-03-19 17:00	84
2020-03-17 17:00	83
2020-03-19 12:00	83
2020-03-19 05:00	82
2020-03-19 02:00	81
2020-03-20 04:00	81
2020-03-20 19:00	81

Alerts – Apache (cont.)

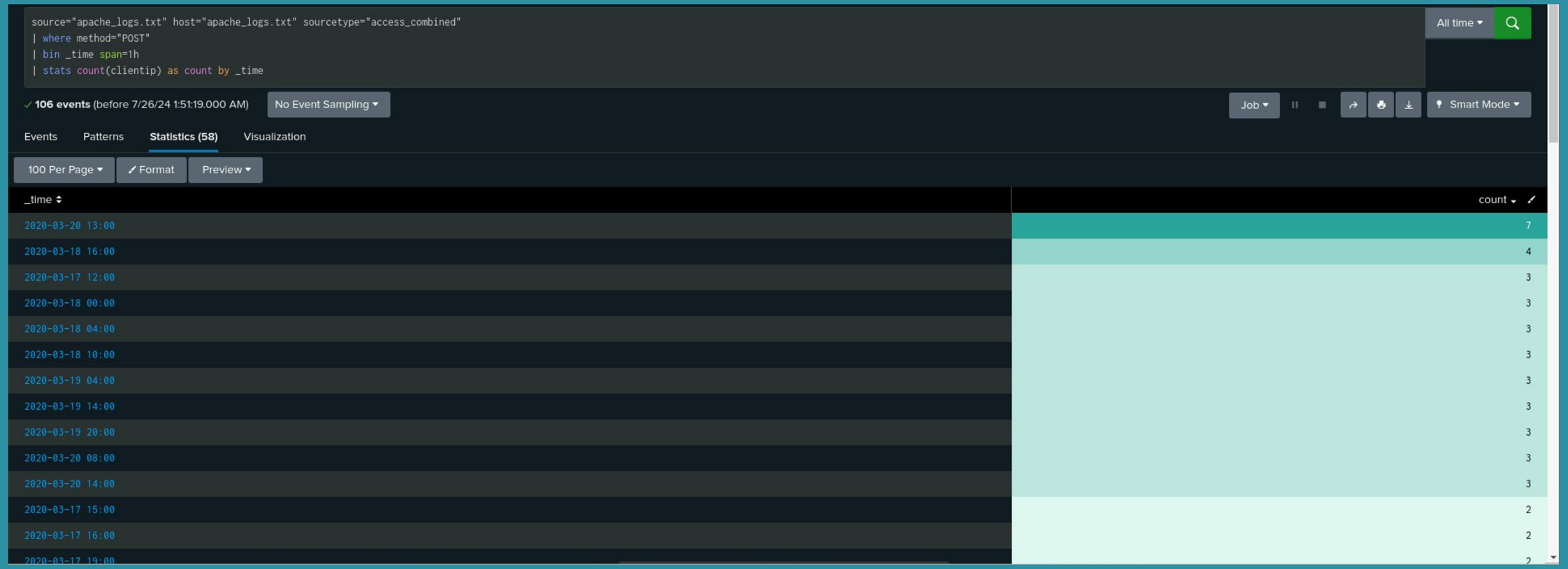
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Requests	**Alert Purpose:** Monitor HTTP POST requests per hour **Trigger Condition:** Abnormal spikes in POST requests **Potential Threats:** • Suspicious form submissions • Unauthorized file uploads • Potential attacks (e.g., data exfiltration)	**Average number of HTTP Post Requests per hour =** 3	**Allowed number of HTTP Post Requests per hour =** 6

JUSTIFICATION:

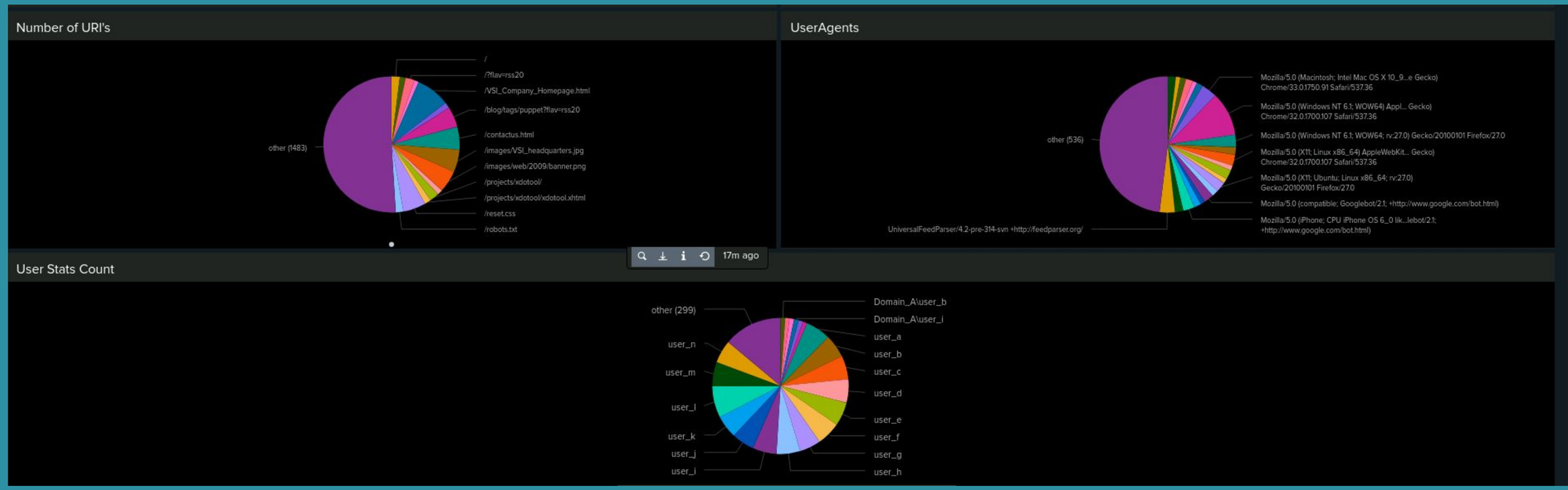
Threshold Strategy: Detect significant deviations from average POST request rate
Threshold Level: Set 25% above the average
Reasoning: Captures sudden spikes in POST requests and minimizes false positives
Goal: Enable timely responses to potential threats through early detection

Images of Alerts – Apache (cont.)



Dashboards – Apache

Dashboards – Apache (cont.)




Attack Analysis

Attack Summary — Windows

Severity Changes

- The severity level of incidents increased significantly from 6.91% to 20.22%.
- This rise suggests a shift towards more serious or critical attacks, indicating potentially severe security issues or sophisticated attacks.

Failed Activities

- There was a notable increase in failed activities.
- This spike in failed activities may point to potential unauthorized access attempts or other security concerns requiring investigation.

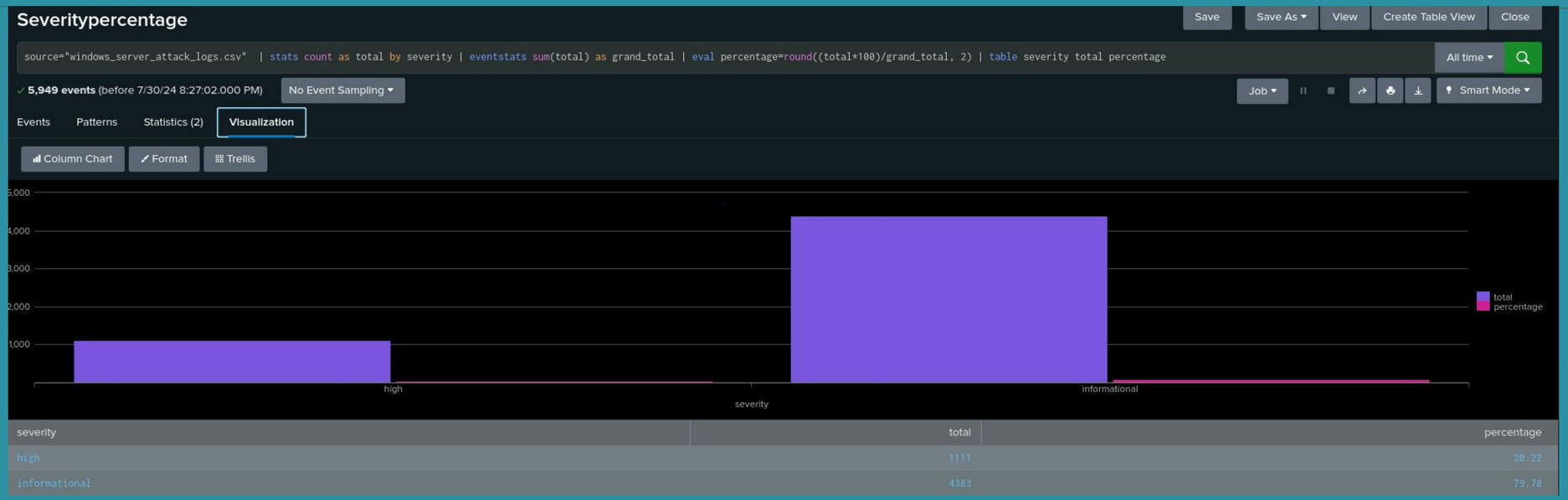
Failed Windows Activity

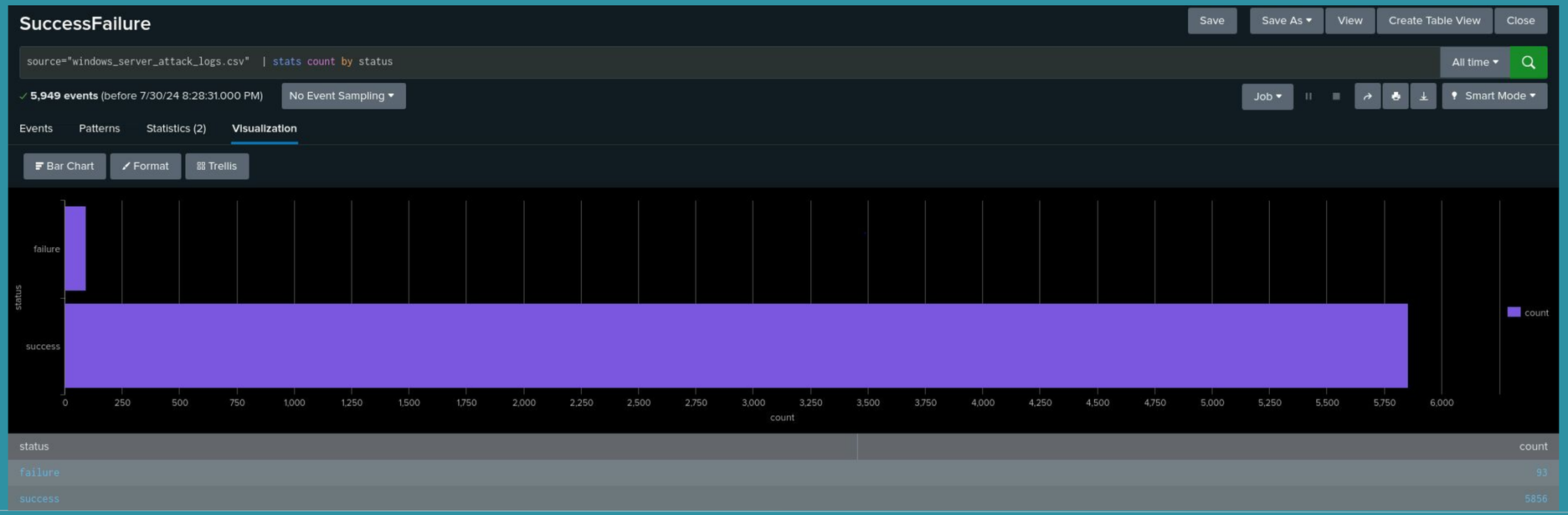
- There was a significant spike in failed login attempts.
- On March 25, 2020, at 8:00 a.m., there were 34 failed login events.
- This pattern may indicate a brute-force attack or other login-related issues, warranting further analysis and potential response measures.

Successful Logins

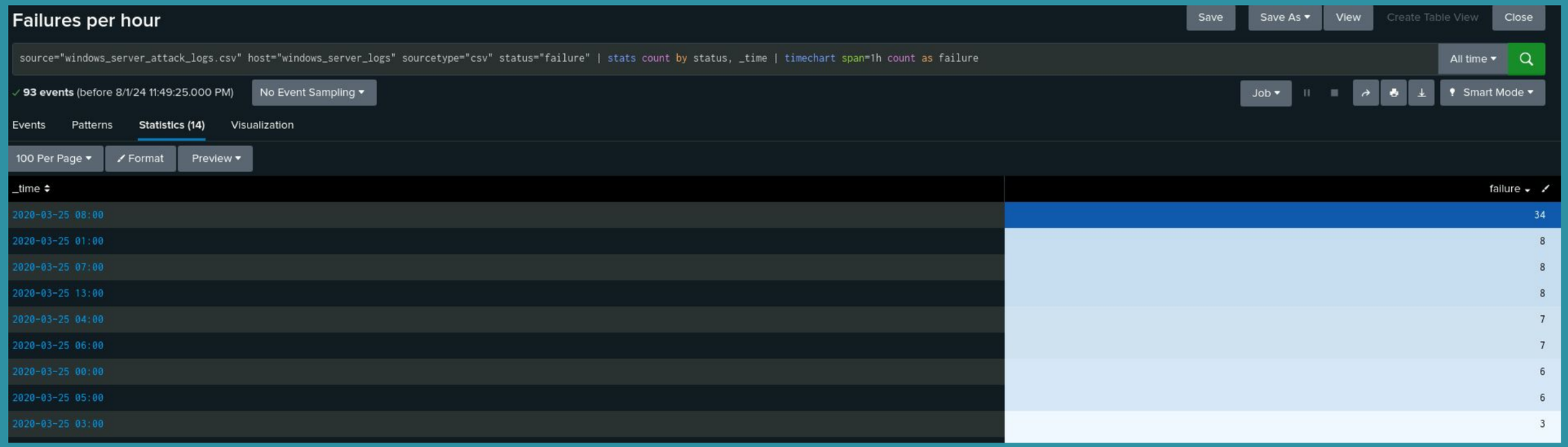
- Our alerts were triggered, there were peaks in successful logins.
- On March 5, 2020, the logs showed high login volumes at 11 a.m. (194 logins) and 12 p.m. (75 logins), primarily by User (J).
- These peaks could be either legitimate high activity or signs of account compromise, necessitating further scrutiny of User (J) and associated login patterns.

Images of Attack Logs - Windows





Images of Attack Logs - Windows (cont.)



Images of Attack Logs - Windows (cont.)

Successful Logins | Day 2

Save | Save As | View | Create Table View | Close

```
source="windows_server_attack_logs.csv" host="windows_server_logs" sourcetype="csv" status=success signature="An account was successfully logged on"
| stats count by status, signature, _time
| timechart span=1h count as successful_logons
```

All time

✓ **429 events** (before 8/1/24 11:37:53.000 PM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (14)** | Visualization

100 Per Page | Format | Preview

_time	successful_logons
2020-03-25 11:00	194
2020-03-25 12:00	76
2020-03-25 10:00	23
2020-03-25 01:00	15
2020-03-25 07:00	15
2020-03-25 03:00	14
2020-03-25 13:00	14
2020-03-25 08:00	13
2020-03-25 04:00	12
2020-03-25 00:00	11

High Login Volumes | User

Save | Save As | View | Create Table View | Close

```
source="windows_server_attack_logs.csv" host="windows_server_logs" sourcetype="csv" status=success signature="An account was successfully logged on" | stats count by status, signature, user
```

All time

✓ **429 events** (before 8/1/24 11:45:51.000 PM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (14)** | Visualization

100 Per Page | Format | Preview

status	signature	user	count
success	An account was successfully logged on	user_j	302
success	An account was successfully logged on	user_a	20
success	An account was successfully logged on	user_e	13
success	An account was successfully logged on	user_n	13

Attack Summary – Windows (cont.)

Deleted Accounts

No suspicious volume of deleted accounts was detected.

The alert settings for account deletions appear appropriate, as no unusual activity was observed.

Signature Analysis

Significant spikes were noted in account lockouts and password resets.

Details:

Account lockouts peaked from 12:00 a.m. to 3:00 a.m., reaching 896 events at 2:00 a.m..

Password resets peaked from 8:00 a.m. to 11:00 a.m., reaching 1258 events at 9:00 a.m..

These spikes suggest unusual activity patterns that could indicate security incidents or administrative issues requiring further investigation.

User Activity

Peaks in account lockouts and password resets were noted.

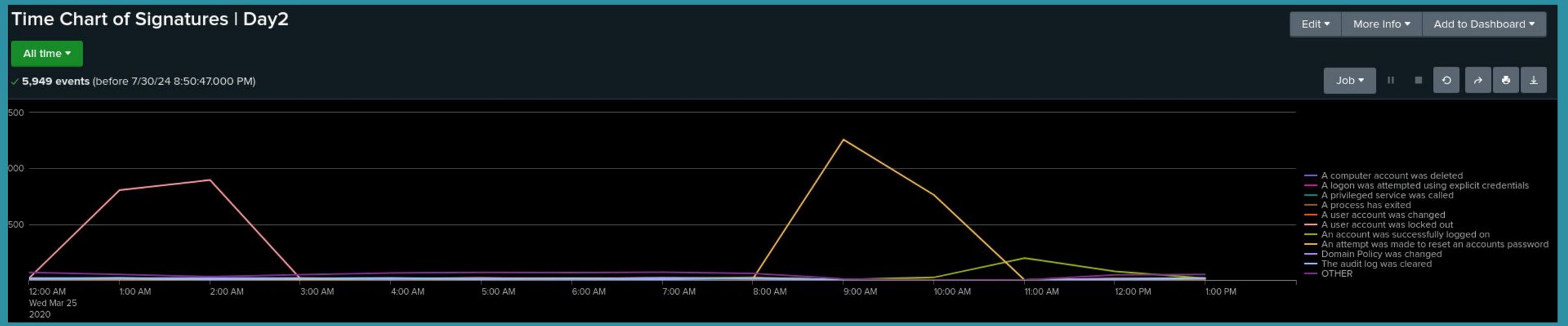
Details:

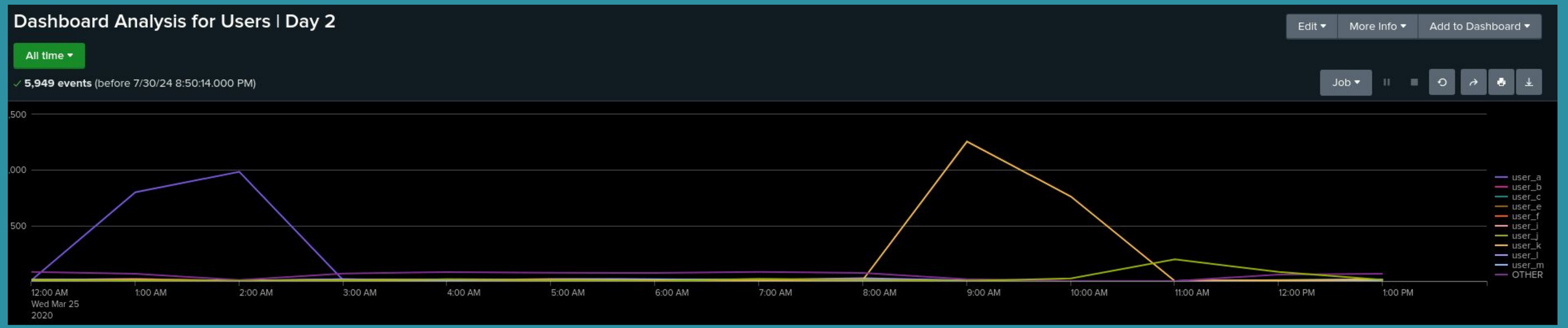
User A recorded 984 events, with the highest activity occurring at 2:00 a.m.

User K recorded 1256 events, with the highest activity occurring at 9:00 a.m.

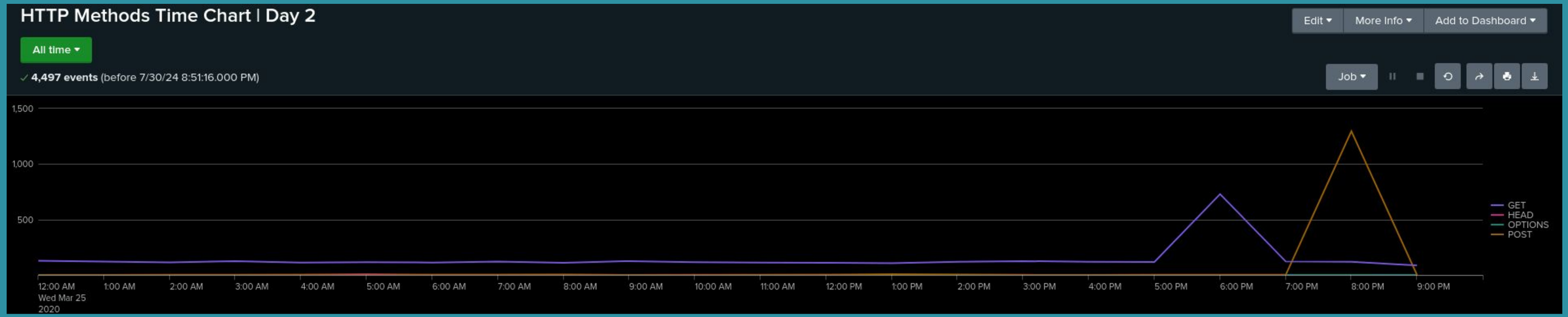
The high activity levels for these users might reflect abnormal behavior or potential security concerns, requiring closer examination of User A and User K's activities.

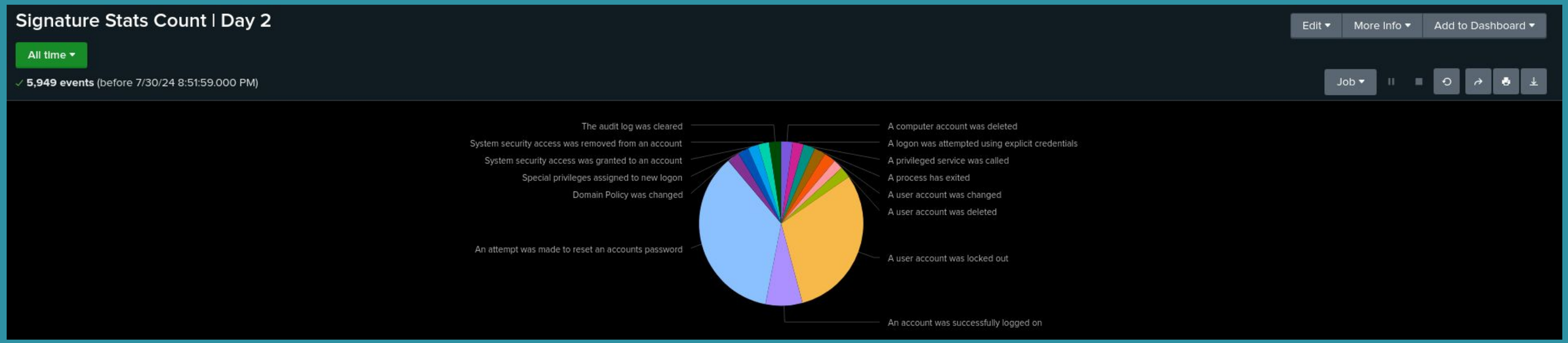
Images of Attack Logs - Windows (cont.)





Images of Attack Logs - Windows (cont.)





Attack Summary – Apache

HTTP Methods Analysis

The analysis of HTTP methods revealed frequent use of GET, HEAD, OPTIONS, and POST methods.

Understanding the distribution of these methods helps identify typical traffic patterns and detect unusual behaviors that might indicate an attack or misconfigured server.

Top 10 Referring Domains

The report identified the top 10 external domains referring traffic to VSI's website.

Details:

Peaks were noted, particularly with domains like semicomplete.com on March 25, 2024 with a high of 1336 at 8:00 p.m., suggesting potential scraping attacks or suspicious referral patterns.

Identifying and analyzing referring domains helps in spotting unusual or potentially malicious traffic sources that may indicate security threats.

Attack Summary – Apache (cont.)

HTTP Response Codes Report

Significant changes in HTTP response codes were observed.

Details:

404 Response Code: rose from 213 to an unusually high peak of 679.

Anomalies in response codes may point to issues such as misconfigured server responses, potential attacks, or broken links.

International Activity

An alert was triggered due to a significant increase in international traffic, which reached 937 counts at 20:00.

Details:

At 20:05:59 on March 25, 2020, traffic from Ukraine peaked at 877 hits.

Sudden spikes in international traffic could indicate potential security threats or targeted attacks, necessitating closer monitoring and investigation.

HTTP POST Activity

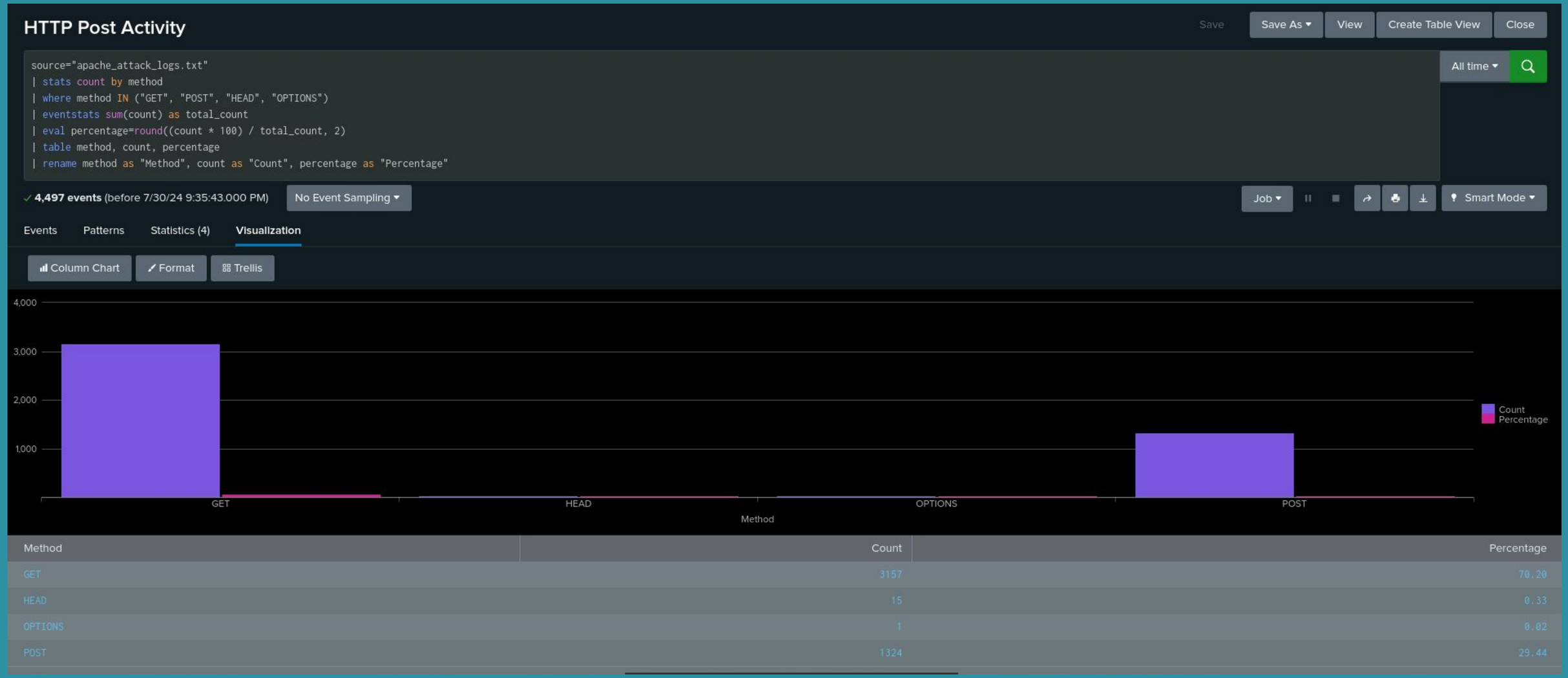
An alert was triggered, there was a high volume of POST requests.

Details:

At 8:00 p.m. on March 25, 2020, there were 1296 POST requests.

An unusually high volume of POST requests might suggest suspicious activity or attempts to exploit vulnerabilities, requiring further analysis.

Images of Attack Logs - Apache



Attack Summary – Apache (cont.)

HTTP Methods:

- **Suspicious:** High volume of POST requests (1296).

Referrer Domains:

- **Suspicious:** Peaks in null referrers and 1337 at 8:00 p.m. on March 25, 2020, indicating potential scraping.

HTTP Response Codes:

- **Suspicious:** Increase in 404 codes (624).

International Activity:

- **Suspicious:** High traffic from Ukraine (877 hits) at 8 p.m. on March 25, 2020.
- **Threshold:** Appropriate.

HTTP POST Activity:

- **Suspicious:** 1296 POST requests at 8:00 p.m. on March 25, 2020.
- **Threshold:** Appropriate.

Dashboard Insights:

- **HTTP Methods:** Peaks in GET (5-7 p.m.) and POST (7-9 p.m.), with POST reaching 1296.
- **Cluster Map:** High activity from Kiev (440 hits).
- **URI Data:** Frequent hits on /VSI_Account_logon.php, suggesting possible brute-force attacks.

Attack Summary – Apache (cont.)

HTTP Methods Analysis:

- **Suspicious Activity:** High volume of POST requests (1,296 recorded)
- **Potential Threats:** Exploitation attempts or web form stress testing

Referrer Domains:

- **Suspicious Peaks:** Traffic spikes from 'null' domain and 1,337 hits at 8:00 p.m. on 3/25/2020
- Indicators: Potential scraping or unusual referral sources

HTTP Response Codes Report:

- **404 Response Code Anomalies:** Peak of 624, indicating broken links or non-existent pages

Attack Summary – Apache (cont.)

International Activity:

- **Suspicious Traffic:** Influx from Ukraine with 877 hits at 8:00 p.m. on 3/25/2020
- **Indicators:** Potential security threats or targeted attacks

HTTP POST Activity:

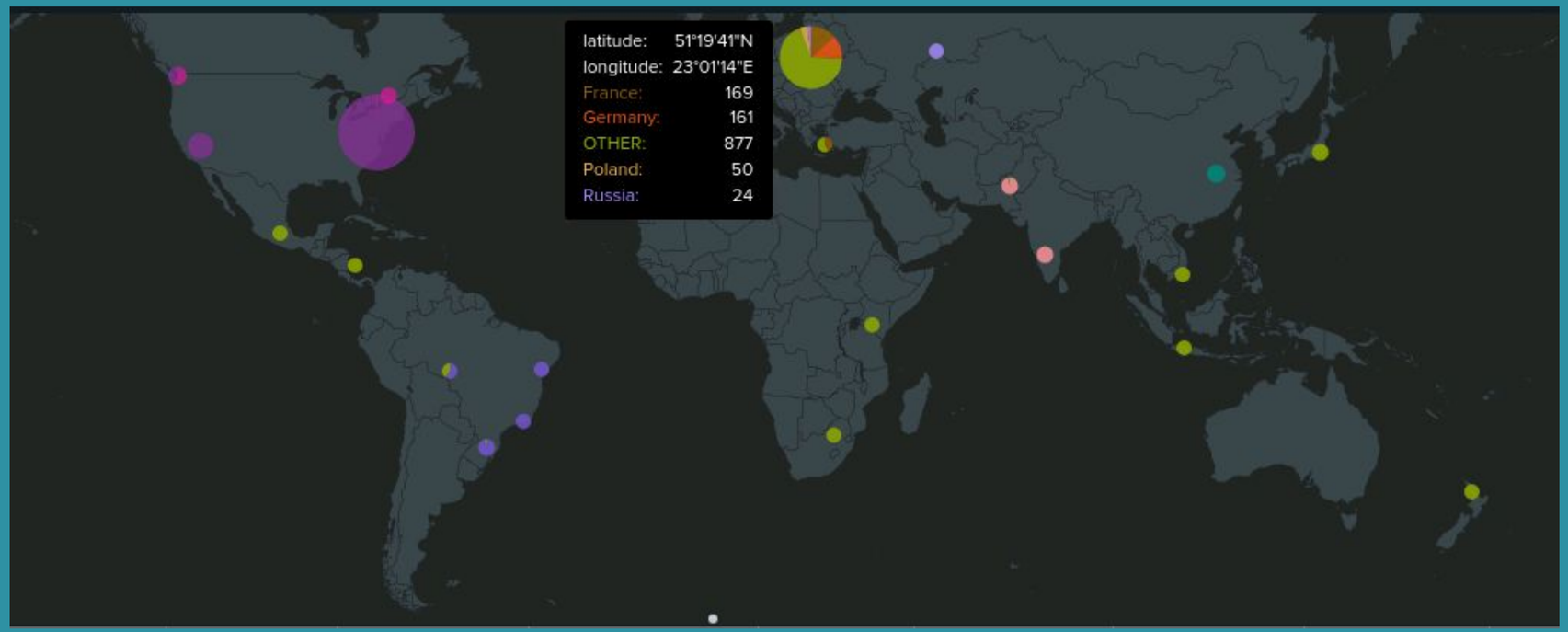
- **High Volume:** Peak of 1,296 POST requests at 8:00 p.m.
- **Potential Threats:** Possible attempts to exploit web form vulnerabilities

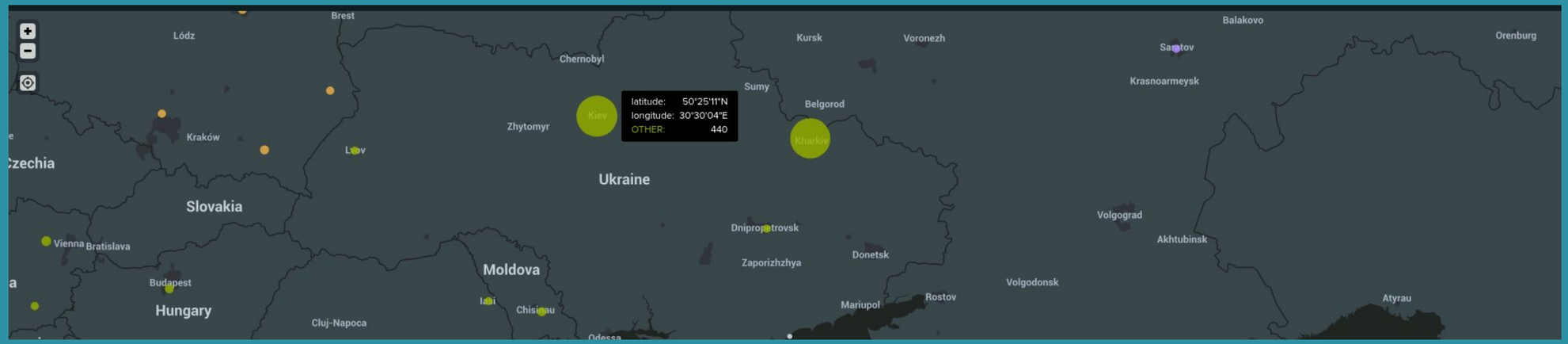
Dashboard Insights:

- **HTTP Methods:** GET requests peaked between 5-7 p.m., POST requests peaked between 7-9 p.m.
- **Cluster Map:** High activity from Kyiv, totaling 440 hits
- **URI Data:** Frequent hits on `/VSI_Account_logon.php`, suggesting possible brute-force attacks

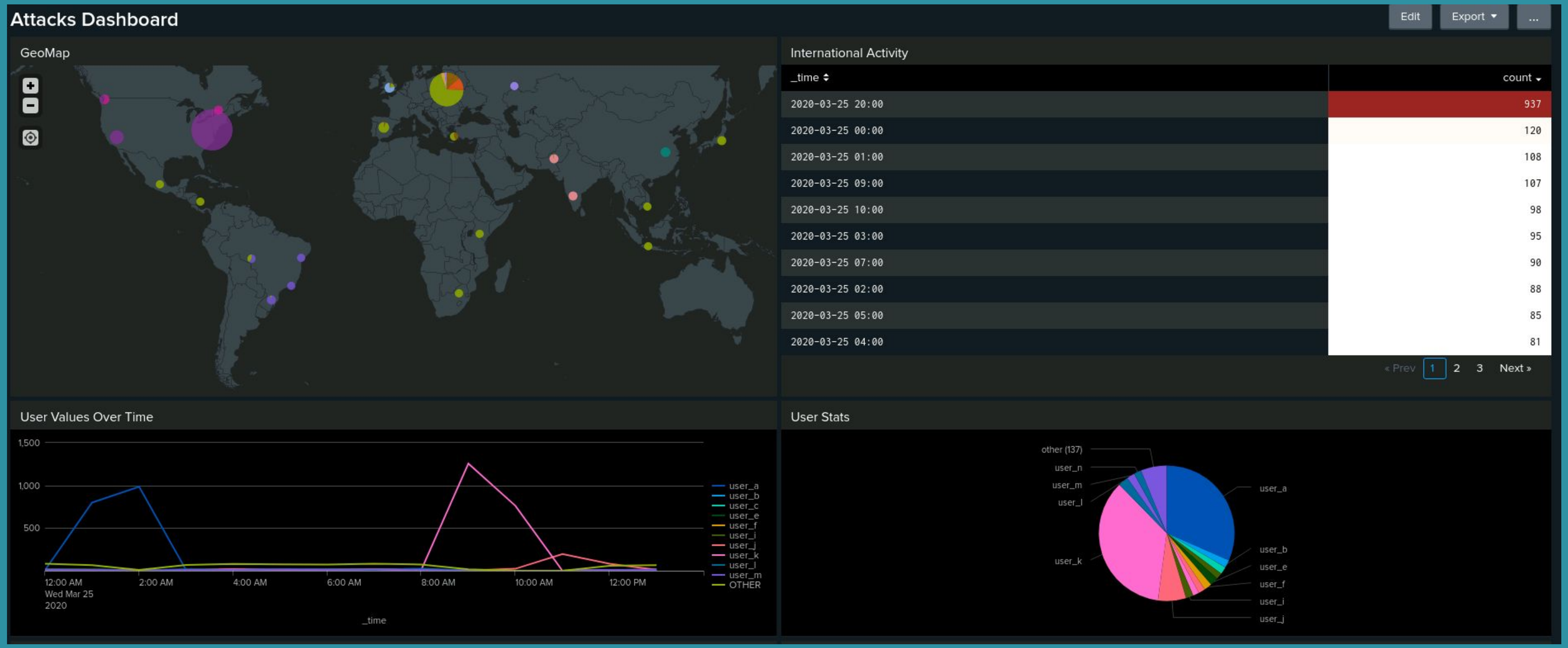
Images of Attack Logs - Apache (cont.)

| International Activity |



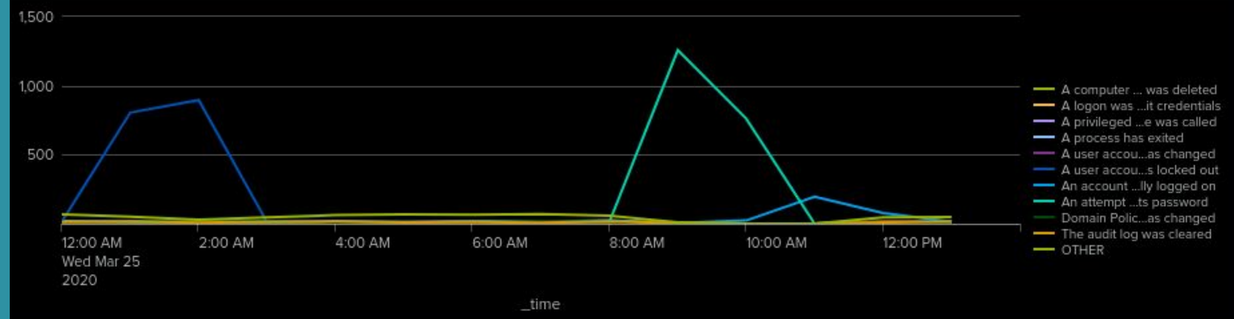


Images of Attack Logs - Apache (cont.)

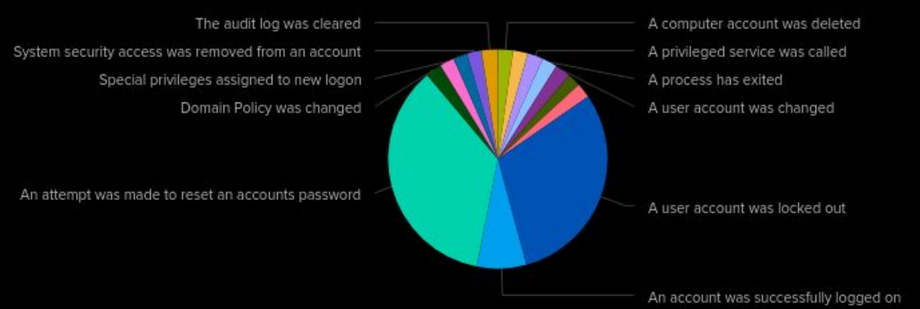


Images of Attack Logs - Apache (cont.)

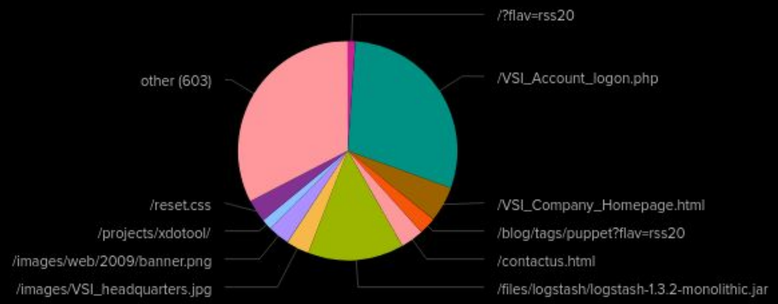
Signature Values Over time



Signature Stats



URIs



Top 10 Referer Domains

referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165


Summary and Future Mitigations

Project 3 - Summary

Project Overview:
Successfully utilized Splunk to analyze and monitor Windows Server and Apache Web Server logs.

Windows Server Logs:

- **Key Findings:** Trends in failed/successful logins, account deletions, and spikes in account lockouts/password resets.
- **Alert Effectiveness:** Thresholds were set to capture significant anomalies and peak activities.

Apache Web Server Logs:

- **Key Findings:** Detected suspicious HTTP POST activity, spikes in international traffic, and unusual HTTP response codes.
- **Indicators:** Potential scraping and brute-force attacks identified.

Conclusion:
The monitoring setup proved robust in detecting and responding to security threats, with well-calibrated alerts and thresholds ensuring timely identification of suspicious activities.

Project 3 - Summary (cont.)

Strengthening Authentication:

- Implement MFA and enforce strong password policies.

Improving Log Management:

- Centralize and enhance log analysis for better anomaly detection.

Deploying Advanced Threat Detection:

- Use Intrusion Detection and Prevention Systems (IDPS) and Endpoint Detection and Response (EDR) tools.

Enhancing Network Security:

- Implement network segmentation and update firewall rules.

Regular Updates:

- Maintain a patch management process and conduct regular vulnerability scans.

Project 3 - Summary (final)

Conducting Security Training:

- Provide ongoing training and simulate attacks to improve awareness.

Strengthening Incident Response:

- Develop and update an incident response plan and establish a response team.

Performing Security Audits:

- Conduct regular penetration tests and security audits.

Securing Web Applications:

- Use a Web Application Firewall (WAF) and perform regular application security testing.

Enhancing Data Protection:

- Encrypt sensitive data and use Data Loss Prevention (DLP) tools.

Thank you for your attention!

Key Takeaways:

Robust Monitoring:

- The project showcased the importance of continuous monitoring and timely alerts.

Proactive Defense:

- Implementing recommended mitigations can significantly enhance VSI’s security posture.

Next Steps:

- Begin implementing the proposed mitigations.
- Schedule follow-up meetings for progress reviews.

Stay Secure!

Questions? We’re here to help!