Defensive Security Project
by: [Group 2]

Group 2 consisted of the following students: Bailey, Max, Sunath, Wayne and Adriel

Table of Contents

This document contains the following resources:

01

Monitoring Environment

- Splunk log analysis
- Configured to accommodate Splunk Add-on applications such as MITRE & ATTK Heatmap

02

Attack Analysis

- Data containing logs from window and apache attacks
- Comprehensive overview of reports, alerts and dashboards which are you used to monitor logs and identify key areas of interest

03

Project Summary & Future Mitigations

- Final conclusions and breakdown of logs and events
- Implementation and strategies that can help mitigate risks and work as an early intervention process

Monitoring Environment

Scenario

- As a cyber security analyst we are working for a large organization (VSI). The organisation has configured Splunk for security purposes to monitor log and identify suspicious activity. Our role as a security analyst is to aid in the implementation of reports, alerts and dashboard to monitor VSI logs in realtime in the event of any possible attacks. We are also responsible for addressing potential security incidents that could affect the organisations IT infrastructure and how these risks can be mitigated for the future. We have found that there has been suspicious activity identified on their windows server logs and their apache logs, both with very different scopes of attacks. Using implemented Splunk alert interventions we will navigate the data and narrow down where the problem is and how we can mitigate it for future attacks.

[“Add-On” App]

MITRE ATT&CK Heatmap for Splunk

The application chosen displays across the board tactics and techniques from the MITRE ATT&CK Framework. Each row represents a form of tactic used by cybercriminals and each column represents a technique that's contained within that tactic. The add on displays a heat map type of visual representation through color coding and shading to indicate increased activity related to a particular technique. An example being that the more activity is identified, the darker the shading for the select node.

MITRE ATT&CK Heatmap for Splunk

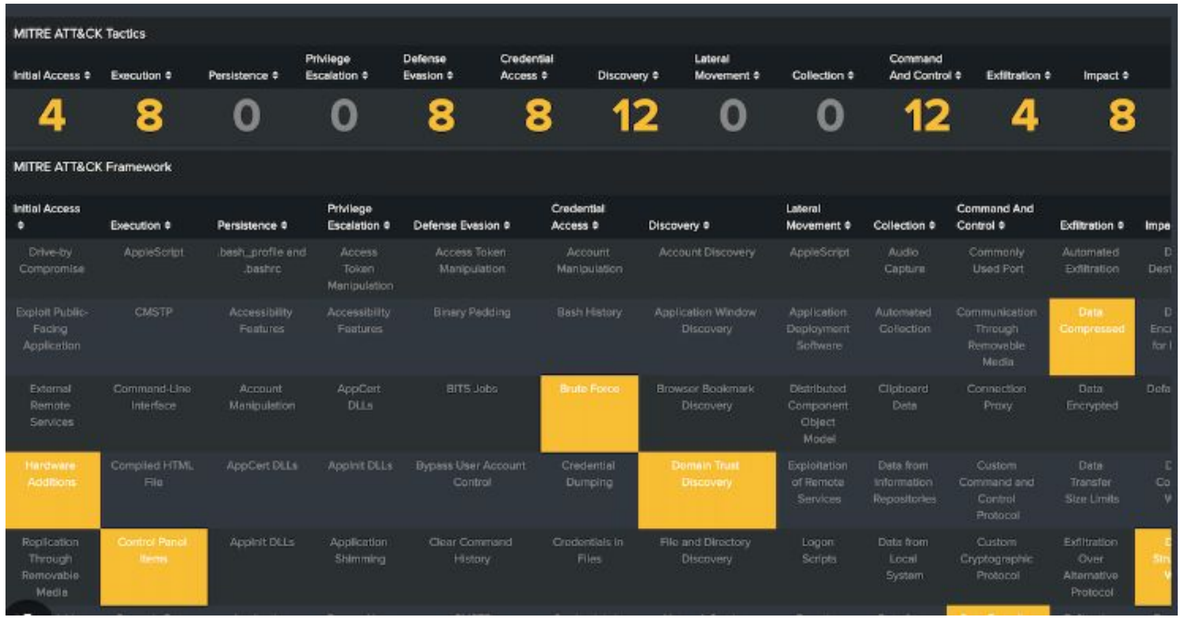
Enhanced Threat Detection and Analysis: The heatmap provides a visual representation of ATT&CK techniques and tactics, allowing security teams to quickly identify which techniques are being used in their environment. This improves the detection of advanced threats and enhances the ability to analyze attack patterns.

Prioritized Defense Measures: By visualizing which ATT&CK techniques are most commonly observed, the heatmap helps prioritize defensive measures and resource allocation. Security teams can focus on strengthening controls and responses for techniques that are most relevant to their environment.

Improved Incident Response: The heatmap integrates with Splunk to map out attack vectors and techniques observed during an incident. This enables more efficient incident response by providing a clear view of the tactics and techniques involved, helping teams to address the root cause and mitigate the threat effectively.

Strategic Security Planning: The heatmap facilitates strategic planning by showing trends and gaps in the company's security posture over time. It helps in understanding the evolution of threats and the effectiveness of existing security measures, guiding future investments in security technology and training.

MITRE ATT&CK Heatmap for Splunk



MITRE ATT&CK Tactics

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
4	8	0	0	8	8	12	0	0	12	4	8

MITRE ATT&CK Framework

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impe
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	D Dest
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	D Enc for
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defa
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	E Co W
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	E Sin

Logs Analyzed

1 Windows Logs

- Comprised of a set of system and event logs from a windows system
- Features logs which recorded successful logons, privileges, account management (creation and deletion)
- Domain policies
- System security access
- Users and activities
- All logs contain severity levels, date and time information

2 Apache Logs

- Includes network device logs
- HTTP requests
  - GET
  - POST
  - HEAD
  - OPTIONS
- Logs included user, uri_paths, date and time
- Information relating to client IPs can also be identified within the logs

Windows Logs [pre attack]

Reports—Windows

Designed the following reports:

Report Name	Report Description
Windows Success and Failure Activities Report	The report is comprised of data in relation to how many successful attempts related to window activities and failed attempts and compares them to the normal activity baseline and how far outside of the threshold it falls.
Severity Levels Report	The report will contain data that gives insights into the severity levels of events or incidents being monitored. It can help identify the distribution of severity levels across logs or events, allowing users to prioritize and address critical issues promptly. This includes statistics such as the count of events per severity level, trends over time, and comparisons between different severity categories.
Signature and Signature ID Reports	This report will contain data about any signature names and IDs to detect known patterns or signatures of malicious activities. These reports typically involve analyzing logs or network traffic for specific patterns that match predefined signatures of known threats.

Signature and Signature ID Report

Signatures and Associated IDs Daily report of signatures and associated IDs	Edit ▾	Run	View Recent	Report	2024-08-04 00:00:00 UTC	none	admin

Title Signatures and Associated IDs

Description Daily report of signatures and associated IDs

Search

```
source="windows_server_logs.csv" signature="*" signature_id="*" | top limit=50
    signature signature_id | dedup signature signature_id
```

Earliest time -24h@h

Time specifiers: y, mon, d, h, m, s Learn More

Latest time now

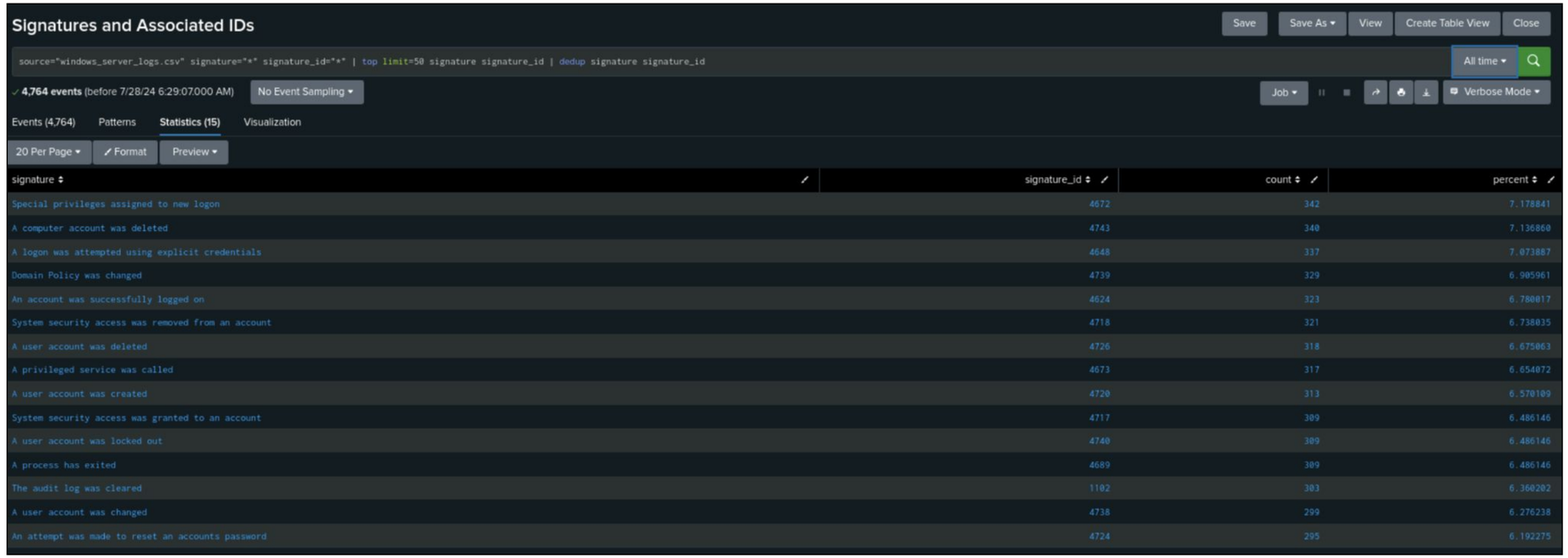
Time specifiers: y, mon, d, h, m, s Learn More

Breakdown

Upon reviewing the results we identified the following signatures, their corresponding IDs and their total counts:

Below are the top 3 signatures, each with signature name, ID and total count:

- “Special privileges assigned to new logon” (4672) = total count of 342
- “A computer account was deleted” (4743) = total count of 340
- “A logon was attempted using explicit credentials” (4648) = total count of 337



signature	signature_id	count	percent
Special privileges assigned to new logon	4672	342	7.178841
A computer account was deleted	4743	340	7.136860
A logon was attempted using explicit credentials	4648	337	7.073887
Domain Policy was changed	4739	329	6.905961
An account was successfully logged on	4624	323	6.780017
System security access was removed from an account	4718	321	6.738035
A user account was deleted	4726	318	6.675063
A privileged service was called	4673	317	6.654072
A user account was created	4720	313	6.570109
System security access was granted to an account	4717	309	6.486146
A user account was locked out	4740	309	6.486146
A process has exited	4689	309	6.486146
The audit log was cleared	1102	303	6.360202
A user account was changed	4738	299	6.276238
An attempt was made to reset an accounts password	4724	295	6.192275

Severity Report

Severity Levels	Edit ▾	Run	View Recent	Report	2024-08-04 00:00:00 UTC	none	admin

Title Severity Levels

Description optional

Search

```
source="windows_server_logs.csv" severity="*" | top severity
```

Earliest time -24h@h

Time specifiers: y, mon, d, h, m, s Learn More

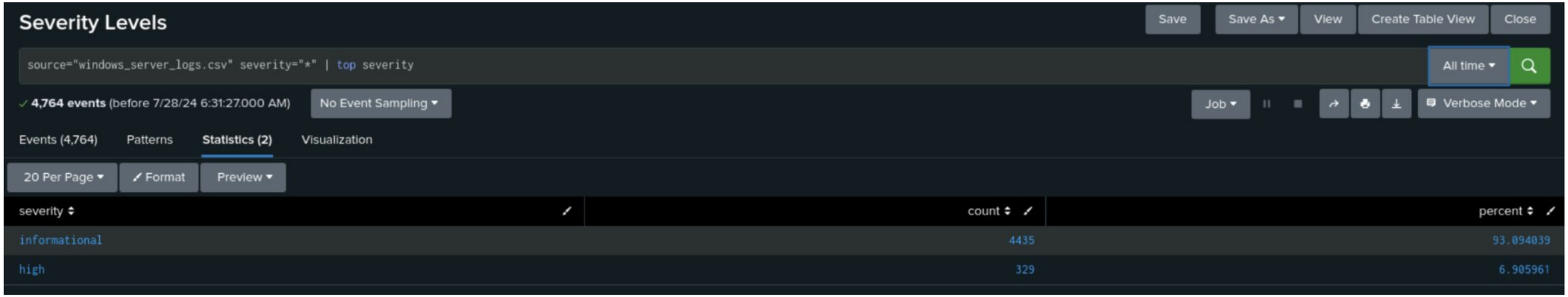
Latest time now

Time specifiers: y, mon, d, h, m, s Learn More

Breakdown

Upon reviewing the data available, we identified the results of informational and high severity events:

- Informational Severity events had a count of 4435 within the logs, totalling at 93.09% of all combined events
- High Severity events had a count 329 within the logs, totalling at 6.90% of all combined events



Windows Success/Failures Activities Report

Windows Success/Failures Activities	Edit ▾	Run	View Recent	Report	2024-08-04 00:00:00 UTC	none	admin

Title Windows Success/Failures Activities

Description optional

Search

```
source="windows_server_logs.csv" | stats count(eval(status="success")) as
    success_count, count(eval(status="failure")) as failure_count
| eval success_percentage=100 * (success_count / (success_count + failure_count
    )), failure_percentage=100 * (failure_count / (success_count + failure_count
    ))
| table success_count, failure_count, success_percentage, failure_percentage
```

Earliest time -24h@h

Time specifiers: y, mon, d, h, m, s Learn More

Latest time now

Time specifiers: y, mon, d, h, m, s Learn More

Breakdown

Upon reviewing the logs, we identified the following event information:

- Events had a success count totalled at 4622, totalling 97.01% of all events
- Total events had a failure count of 142, totalling 2.98% of all events

```
source="windows_server_logs.csv" | stats count(eval(status="success")) as success_count, count(eval(status="failure")) as failure_count
| eval success_percentage=100 * (success_count / (success_count + failure_count)), failure_percentage=100 * (failure_count / (success_count + failure_count))
| table success_count, failure_count, success_percentage, failure_percentage
```

All time

✓ **4,764 events** (before 7/28/24 6:33:22.000 AM) | No Event Sampling | Job | Verbose Mode

Events (4,764) | Patterns | **Statistics (1)** | Visualization

20 Per Page | Format | Preview

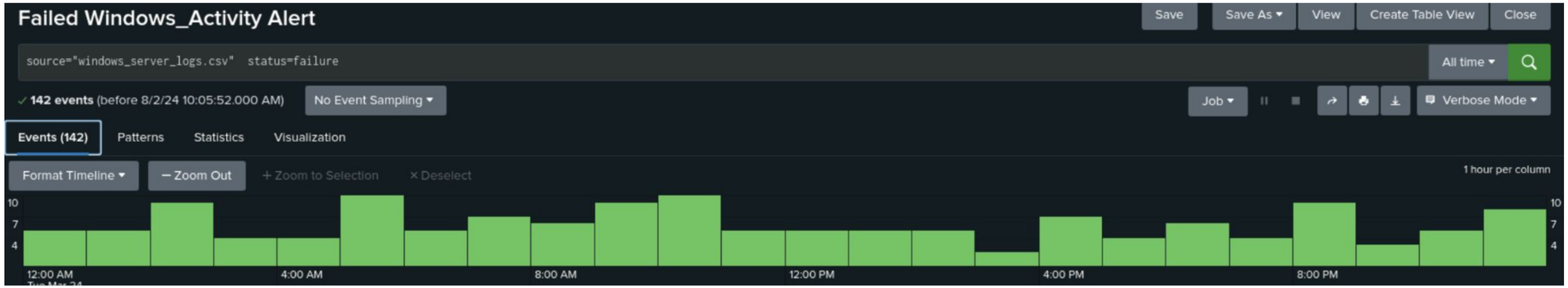
success_count	failure_count	success_percentage	failure_percentage
4622	142	97.0193115029387	2.980688497061293

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity Alert	The alert works to monitor failed Windows related activities, and failed attempts. Its designed purpose is to be able to detect any suspicious patterns once they exceed a given threshold and escalating the situation to a member of VSI for investigation.	Baseline of 6	Threshold of 12

JUSTIFICATION:
Upon reviewing the data, we identified event counts ranging between 2 and 10 and concluded that an appropriate baseline would be 6 events. Using this information, we estimated that a threshold of 12 would be suitable to trigger positive results, instead of false positives.



Screenshots

Failed Windows_Activity Alert	Edit ▾	Run	View Recent	Alert	2024-07-28 07:00:00 UTC	none	admin	search	0	Private	✓ Enabled

Search: `source="windows_server_logs.csv"  status=failure`

Alert type: Scheduled | Real-time

Run every hour ▾

At 0 ▾ minutes past the hour

Expires: 24 hour(s) ▾

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ 12

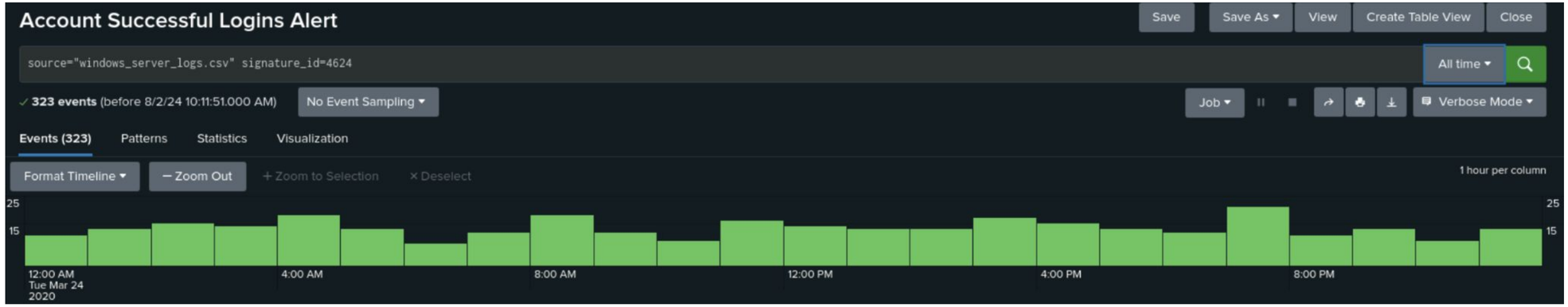
Trigger: Once | For each result

Alerts—Windows

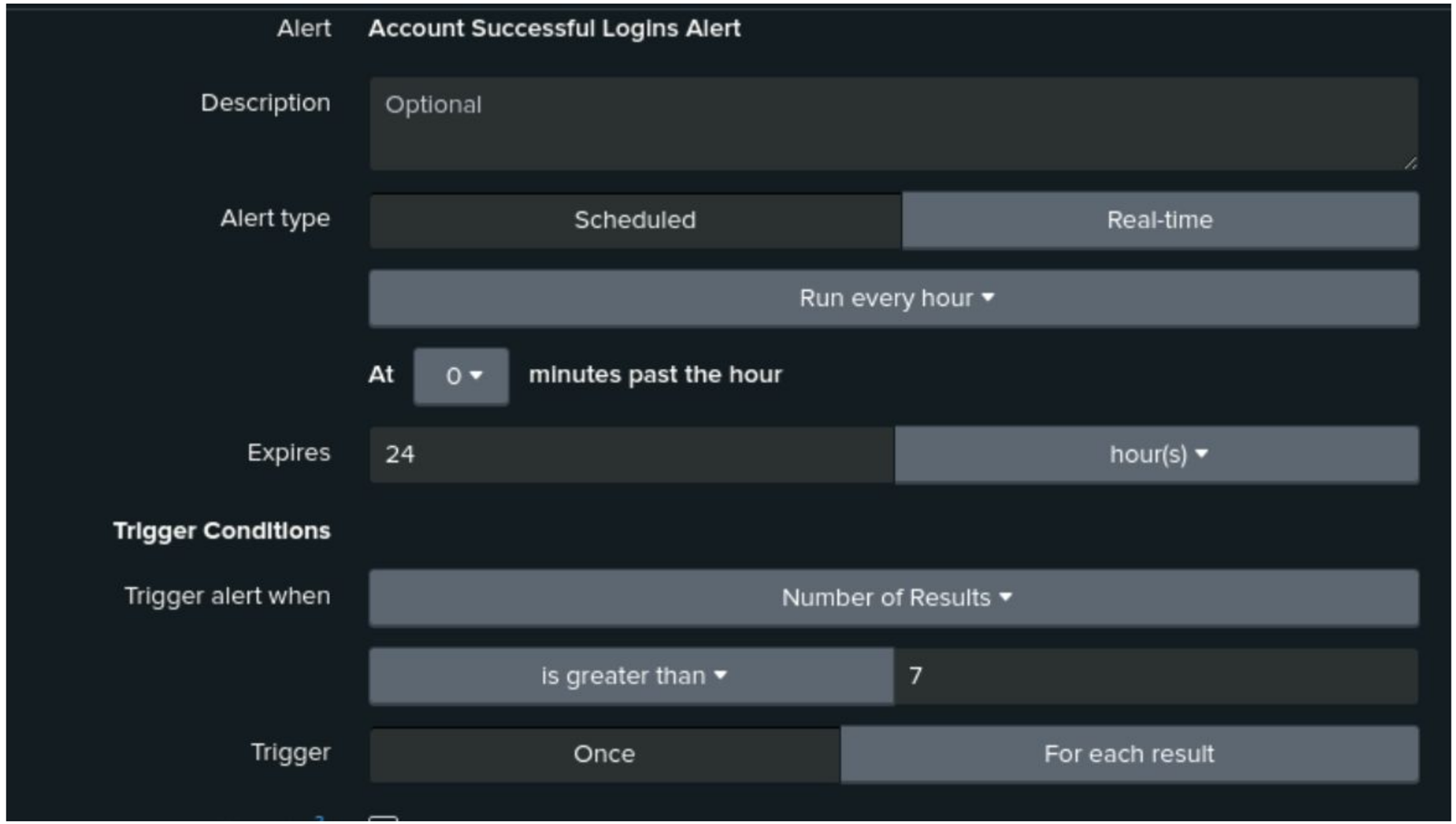
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Successful logins Alert	Alert is triggered by success logins outside the normal range	15	7

JUSTIFICATION:
We identified a range of 9-21 successful logins based on previous data, giving us an appropriate baseline of 15. Since we wanted to be alerted when successful logins dropped below the baseline, a threshold of 7 events was decided upon.



Screenshots



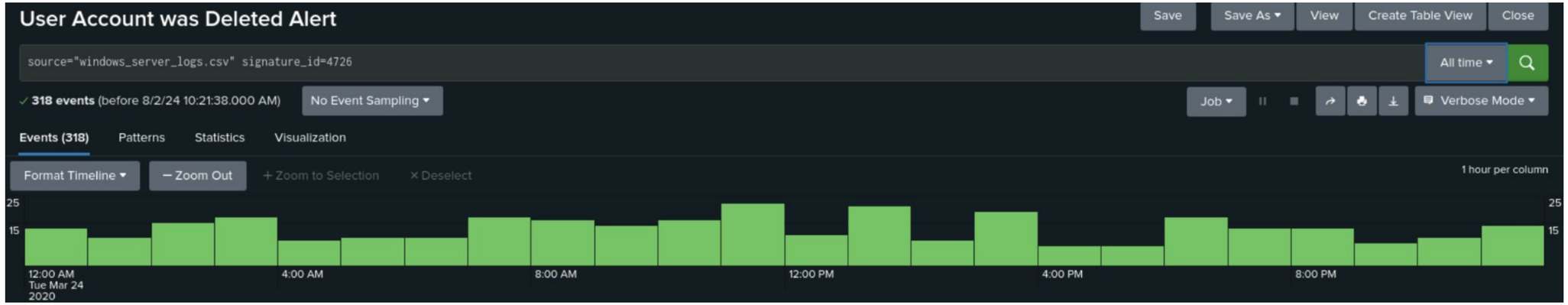
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User account was deleted alert	The alert monitors windows activity in relation to signature 4726, which states ‘a user account was deleted”.	15 events each hour	29 events per hour

JUSTIFICATION:

We identified that during normal operations event counts ranged between 7 and 22, giving us an average of 14/15 events which we used for our baseline. Using this data we concluded that an appropriate threshold to trigger such an alert would be 29 events per hour.



User Account was Deleted Alert

User Account was Deleted Alert Edit ▾ Run View Recent Alert

Alert: User Account was Deleted Alert

Description: Optional

Search:
```
source="windows_server_logs.csv" signature_id=4726
```

Alert type: Scheduled | Real-time

Run every hour ▾

At 0 ▾ minutes past the hour

Expires: 24 hour(s) ▾

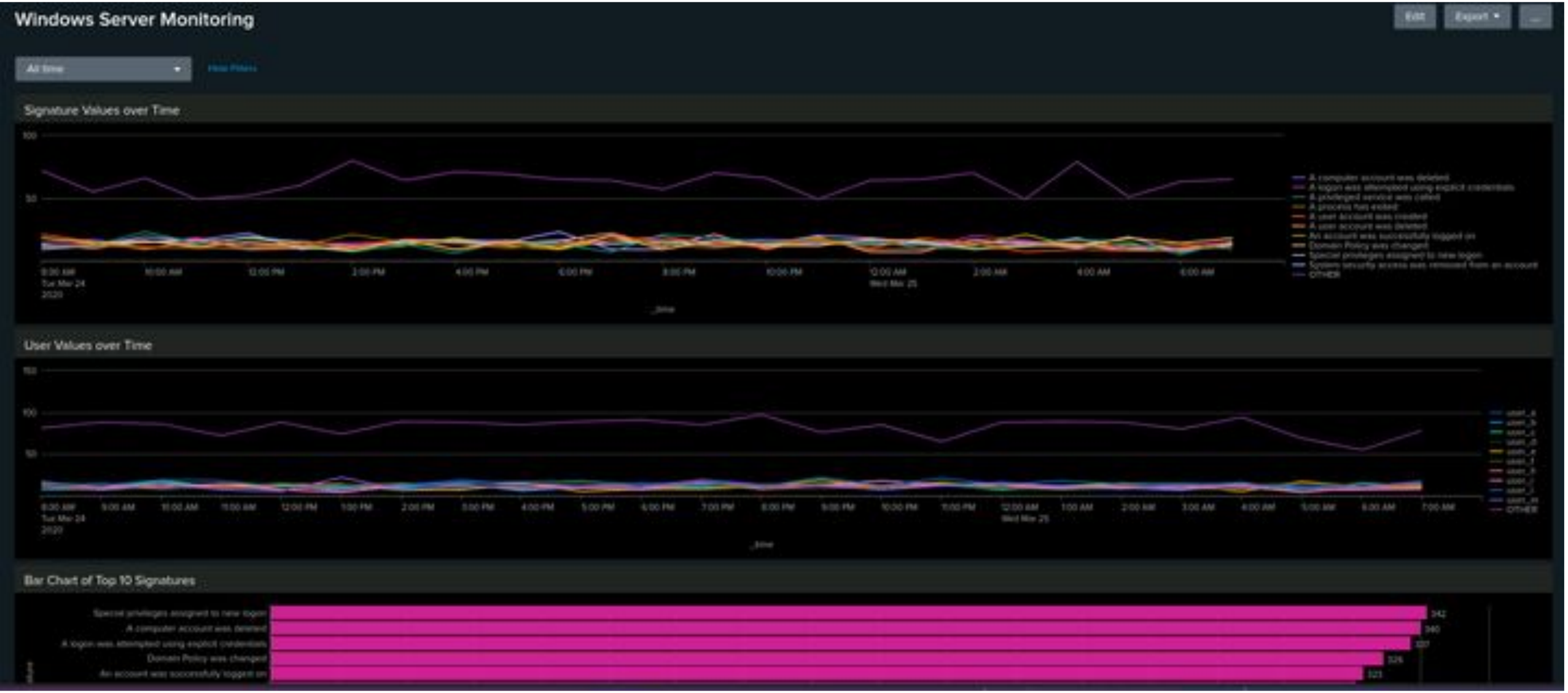
Trigger Conditions

Trigger alert when: Number of Results ▾

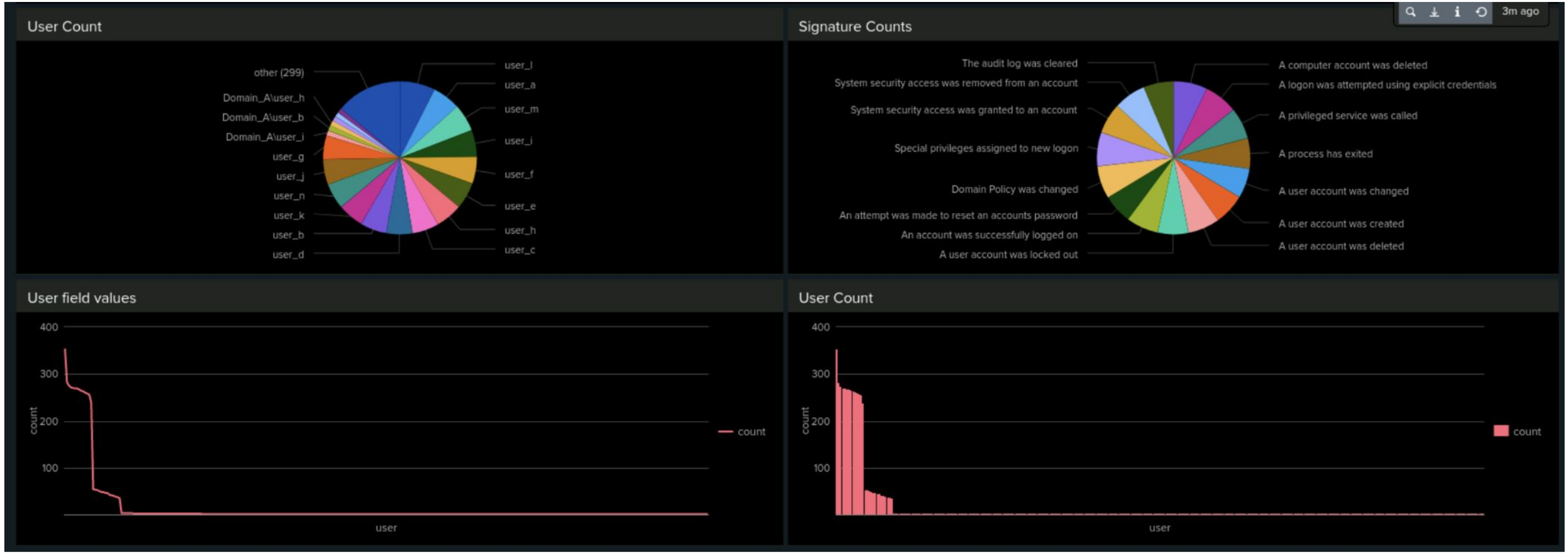
is greater than ▾ 29

Dashboards

Windows Server Monitoring Dashboard



Dashboard - continued



Apache Logs [pre attack]

Reports—Apache

Designed the following reports:

Report Name	Report Description
VSI HTTP Methods	The report refers identifies the various HTTP methods (POST, GET, OPTIONS, HEAD) and displays their count and relative percentage based on the total data available.
Apache International Activity Report	The report expands on the deviation that occurs when activity is outside of the US, specifically if concentrated within a particular country and the potential rise in suspicious activities.
VSI Top Domain Referred	This will assist VSI with identifying suspicious referrers.
VSI HTTP Responses Codes	This will provide insight into any suspicious levels of HTTP responses, such as 404 responses. The report also shows data of successful HTTP response codes, allowing the data to be compared and analyzed against other data points/events.

VSI HTTP Methods Report

VSI HTTP Methods	Edit ▾	Run	View Recent	Report	2024-07-29 00:00:00 UTC	none	admin	search	0	Private	✓ Enabled

Title **VSI HTTP Methods**

Description optional

Search
```
source="apache_logs.txt" | top method
```

Earliest time -24h@h

Time specifiers: y, mon, d, h, m, s Learn More

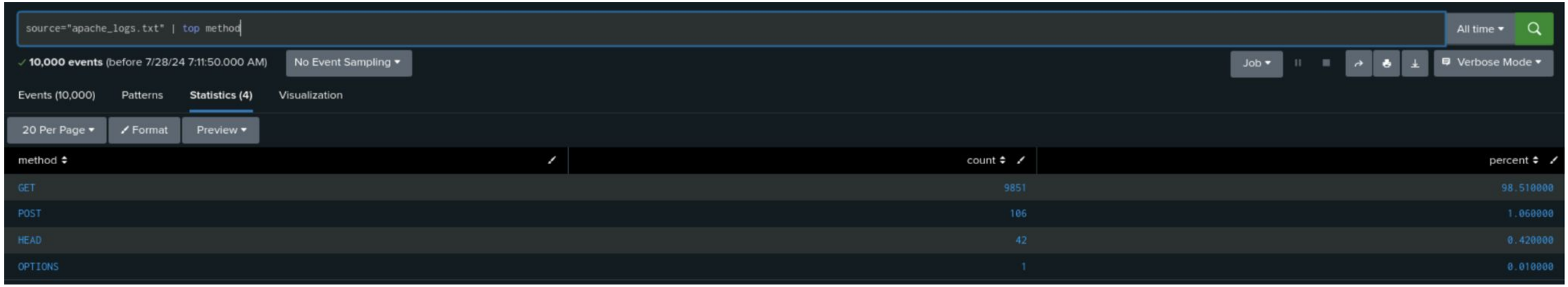
Latest time now

Time specifiers: y, mon, d, h, m, s Learn More

Breakdown

From the data, we identified:

- Total GET method count of 9851 (98.51%)
- Total POST method count of 106 (1.06%)
- Total HEAD method count of 42 (0.42%)
- Total OPTIONS method count of 1 (0.01%)



method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

VSI Top Domain Referred Report

VSI Top Domain Referred	Edit ▾	Run	View Recent	Report	2024-07-29 00:00:00 UTC	none	admin	search	0	Private	✓ Enabled

Title **VSI Top Domain Referred**

Description optional

Search

```
source="apache_logs.txt" | top limit=10 referer_domain
```

Earliest time -24h@h

Time specifiers: y, mon, d, h, m, s Learn More

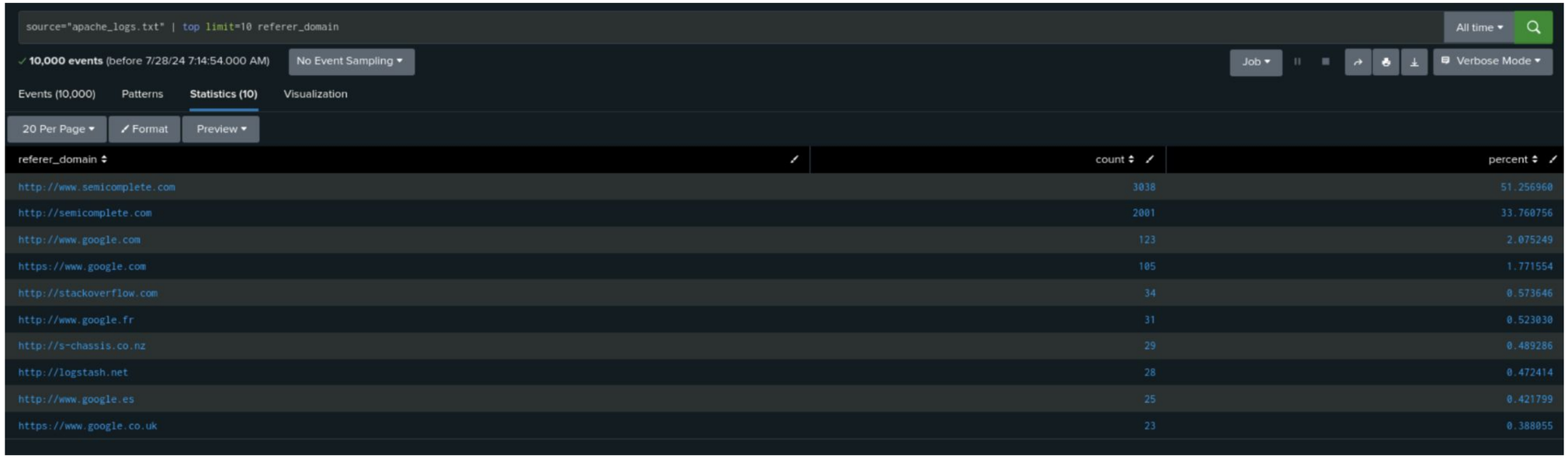
Latest time now

Time specifiers: y, mon, d, h, m, s Learn More

Breakdown

Upon reviewing the data, the top 3 domains identified in the logs are:

- http://www.semicomplete.com totalling at 3038 counts (51.23%)
- http://semicomplete.com totalling at 2001 counts (33.76%)
- http://www.google.com totalling at 123 counts (2.07%)



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

VSI HTTP Response Codes Report

VSI HTTP Response Codes	Edit ▾	Run	View Recent	Report	2024-07-29 00:00:00 UTC	none	admin	search	0	Private	✓ Enabled

Title **VSI HTTP Response Codes**

Description optional

Search

```
source="apache_logs.txt" | top status
```

Earliest time -24h@h

Time specifiers: y, mon, d, h, m, s Learn More

Latest time now

Time specifiers: y, mon, d, h, m, s Learn More

Breakdown

From the data below, the top 3 results for HTTP responses are as follows:

- 200 status codes had a count of 9126, totalling at 91.26%
- 304 status codes had a count of 445, totalling at 4.45%
- 404 status codes had a count of 213, totalling at 2.13%

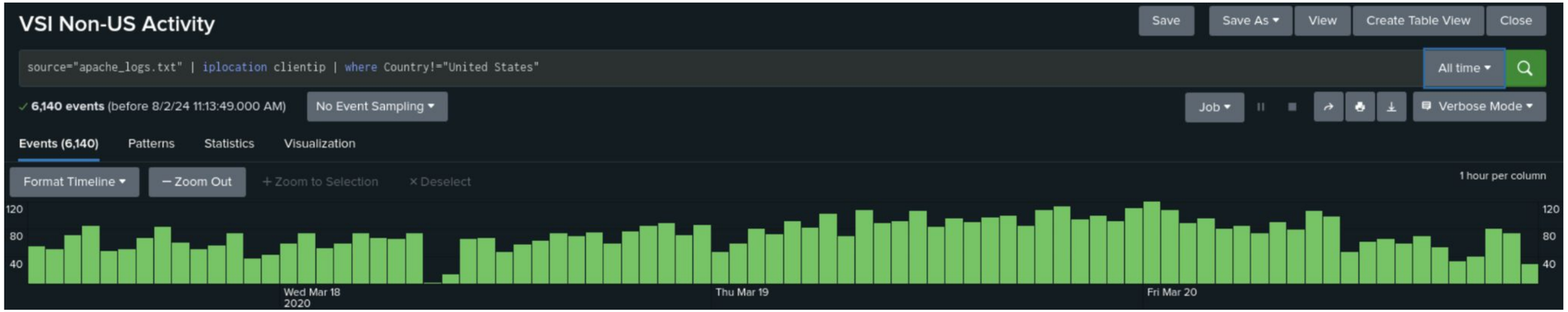
status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

Alerts—Apache

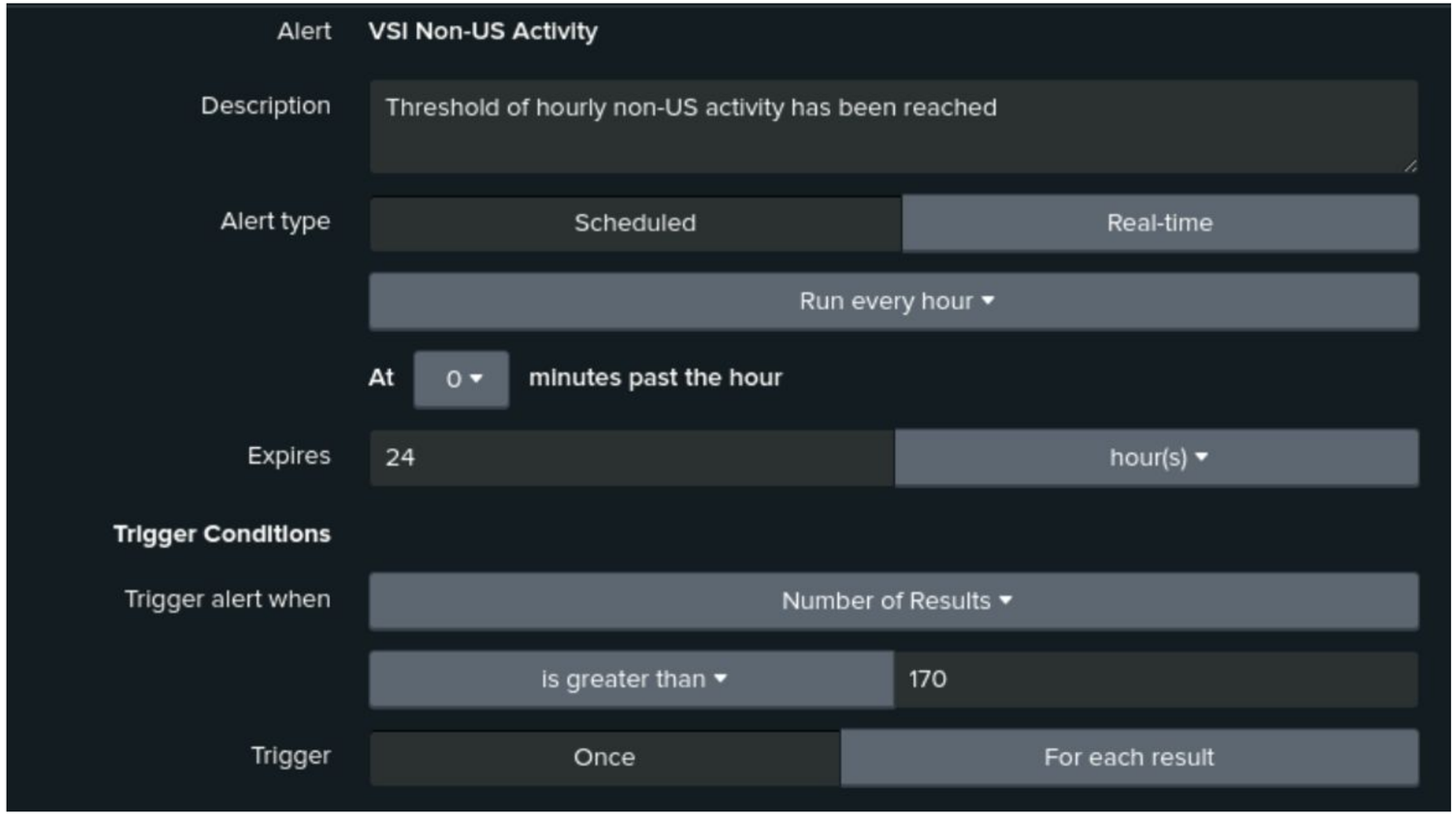
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI Non-US activity	Alert targets activity outside of the US	Baseline was set for 70	Threshold set at 170

JUSTIFICATION:
We identified that the event count on a normal day of operations ranged between 1 and 120, averaging at slightly over 60 counts per events. Due to this information, we identified the data to have a baseline of 70, and decided to set a threshold of 170 for when the alert would be triggered.



Screenshots



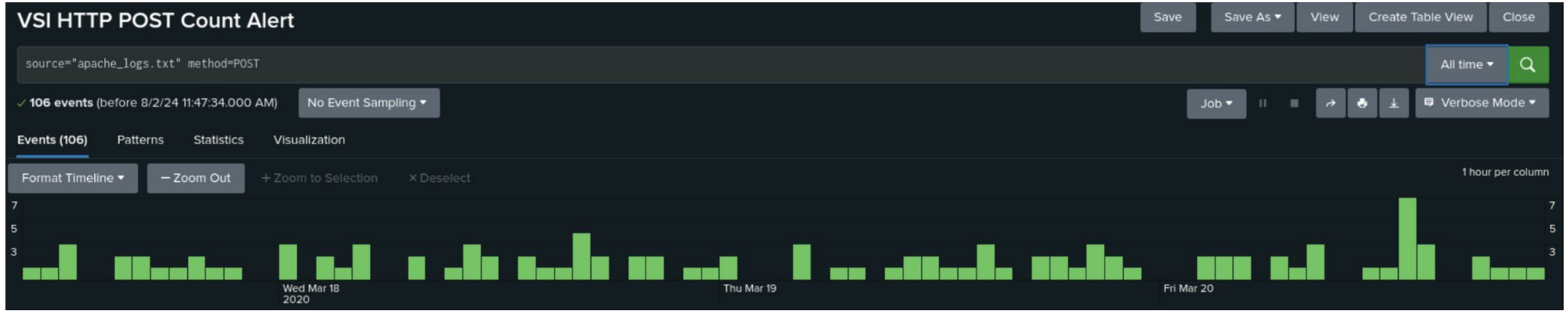
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI HTTP POST Count Alert	This alert monitors and follows activity related to the usage of HTTP methods in apache logs, focusing on POST. The alert is aimed at detecting suspicious changes in activity that could indicate a security related incident.	Baseline was set at 3	Threshold is set at 11

JUSTIFICATION:

Upon reviewing the results, we identified that event counts ranged between 0 and 7 per hour. As a result of this, we concluded that a value of 4 would represent a suitable baseline for the given data. As a result of this, we set the alert threshold to be 11.



Screenshots

VSI HTTP POST Count Alert	Edit ▾	Run	View Recent	Alert	2024-08-02 12:00:00 UTC	none	admin	search

Alert: **VSI HTTP POST Count Alert**

Description: Optional

Search: `source="apache_logs.txt" method=POST`

Alert type: Scheduled | Real-time

Run every hour ▾

At 0 ▾ **minutes past the hour**

Expires: 24 hour(s) ▾

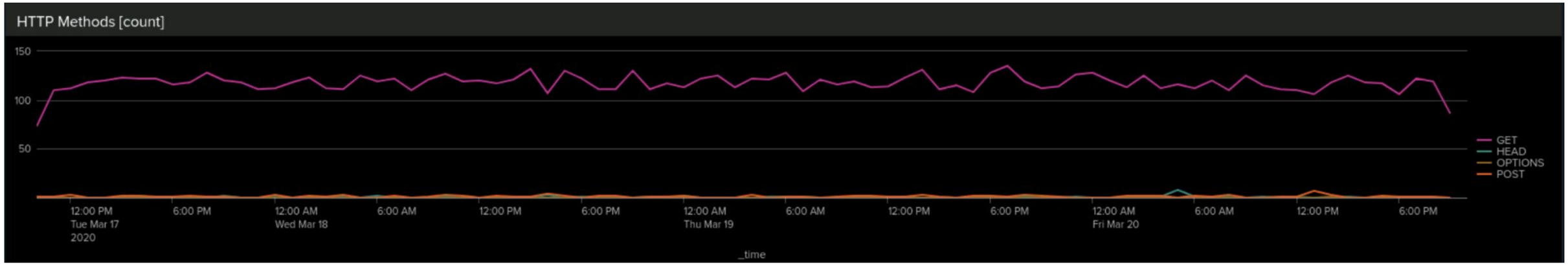
Trigger Conditions

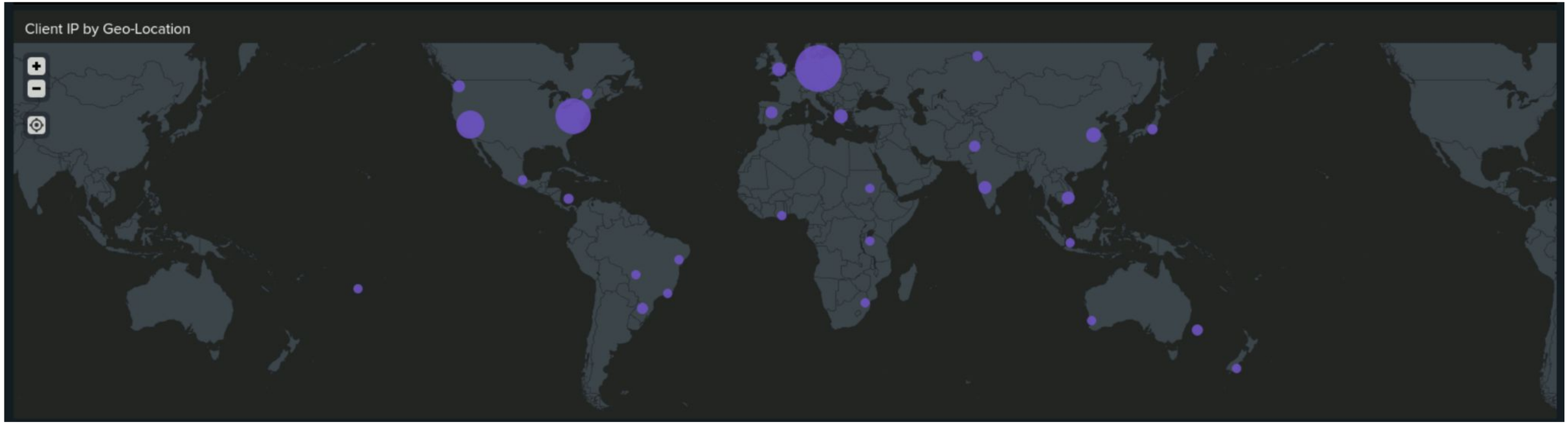
Trigger alert when: Number of Results ▾

is greater than ▾ 11

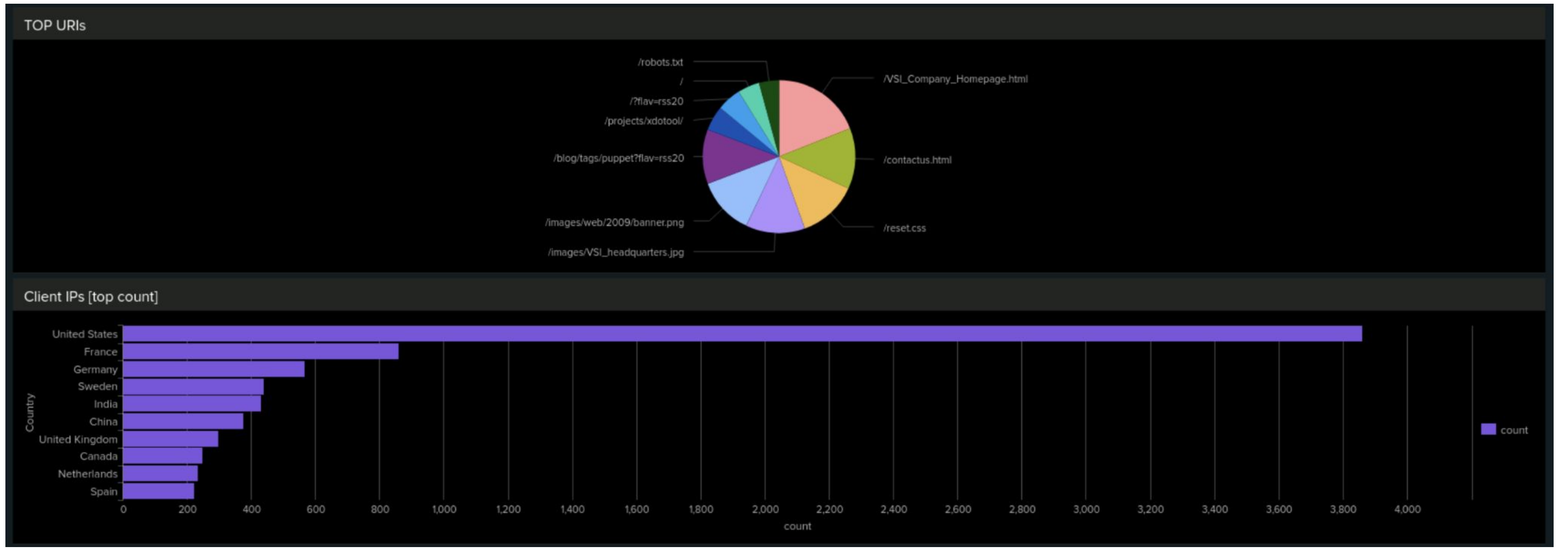
Dashboards

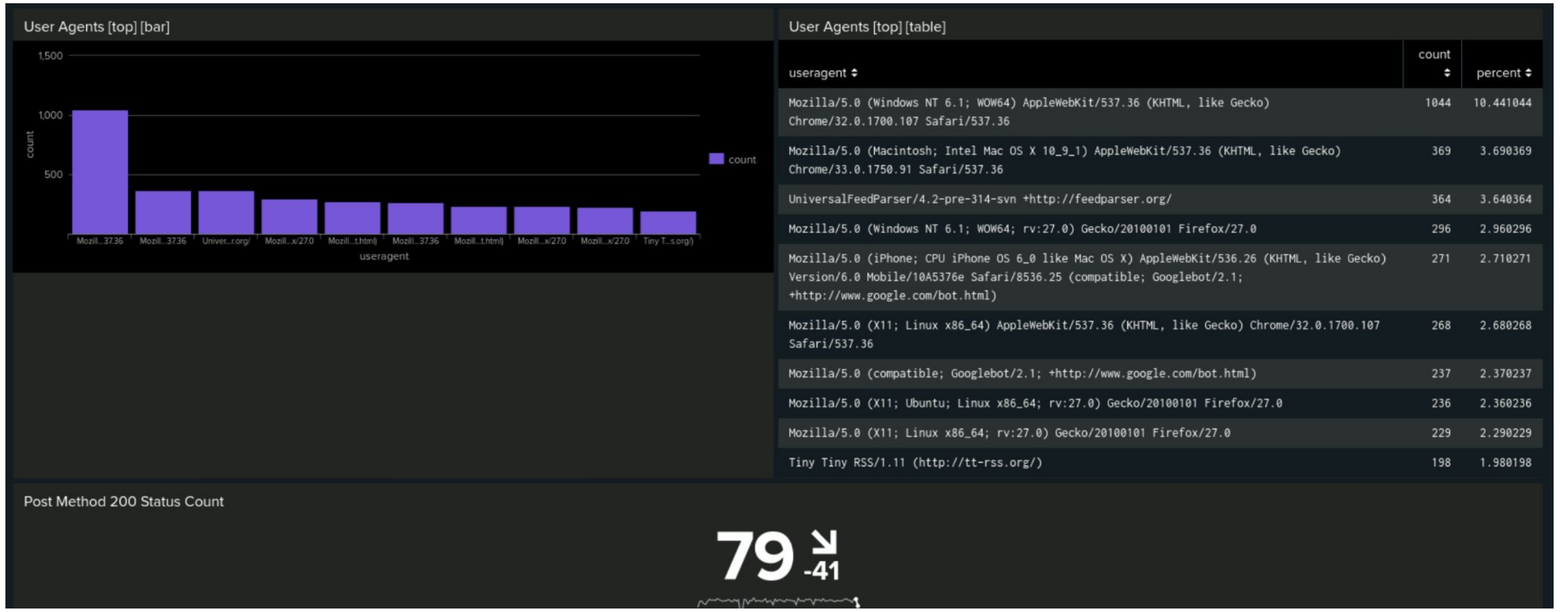
Apache Web Server Monitoring Dashboard





Dashboard - continued





Windows Logs
[post attack dashboard analysis]

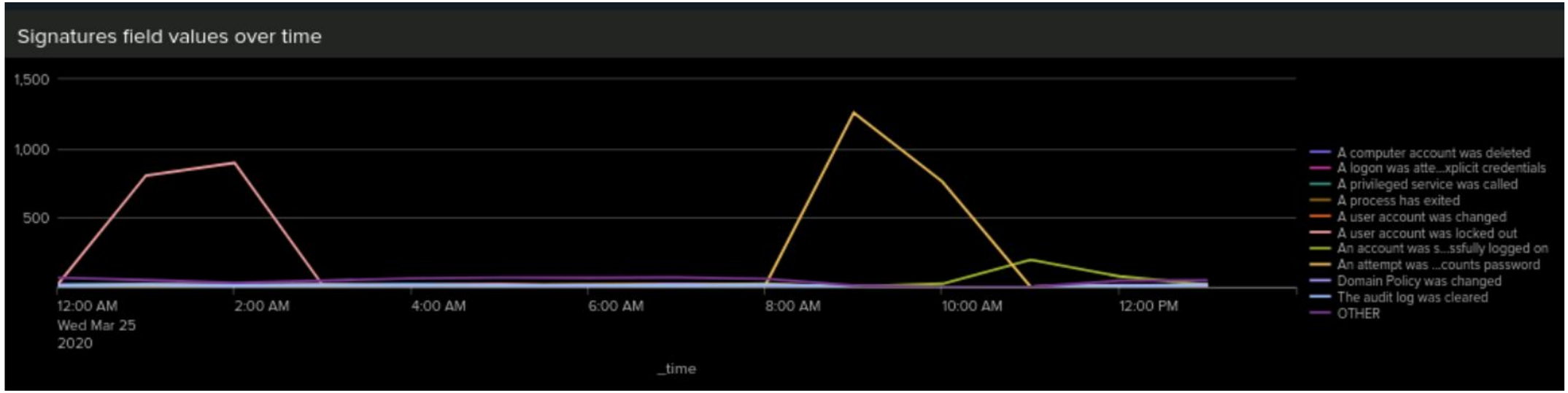
Signature field values over time—Windows Dashboards

From the results, we can identify that there were two primary signatures that peaked within the attack logs

- “An attempt was made to reset an accounts password” - between 12:00 am and 03:00 am
- “A user account was locked out” - between 08:00 am and 11:00 am

“An account was successfully logged on” saw a spike between 10:00 am and 1:00 pm

This potentially points towards a brute force attack, due to the nature of the corresponding signatures. This is especially evident in relation to “an account was successfully logged on”, signifying that the brute force attack may have been sucessful.



User and Signature Counts

From the results, we can identify that:

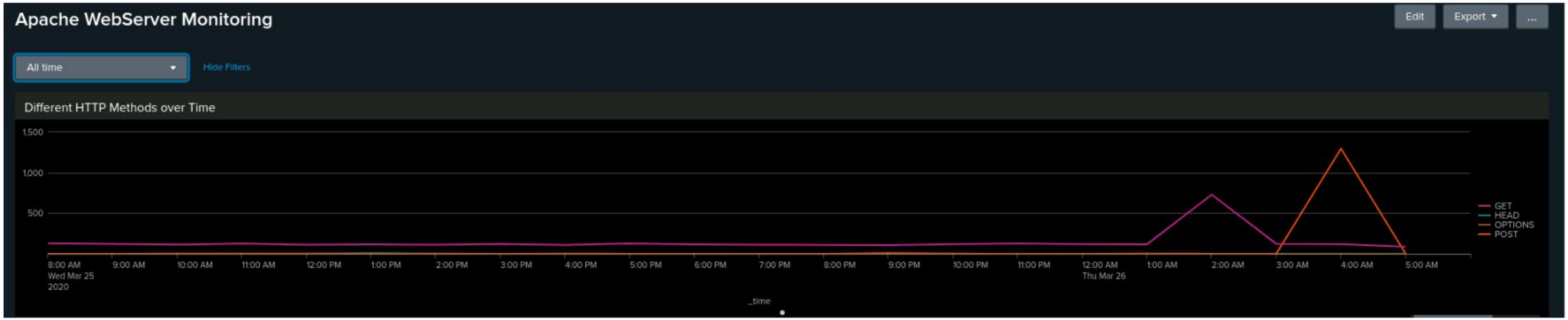
- user_a and user_k had increased levels of activity during the attack.
- Various signatures saw a spike in activity:
  - “A user account was locked out”
  - An attempt was made to reset an accounts password”

This again points towards a brute force attack, with user_a and user_k either having involvement or their accounts were potentially exploited and used during the malicious operation.

Apache Logs
[post attack dashboard analysis]

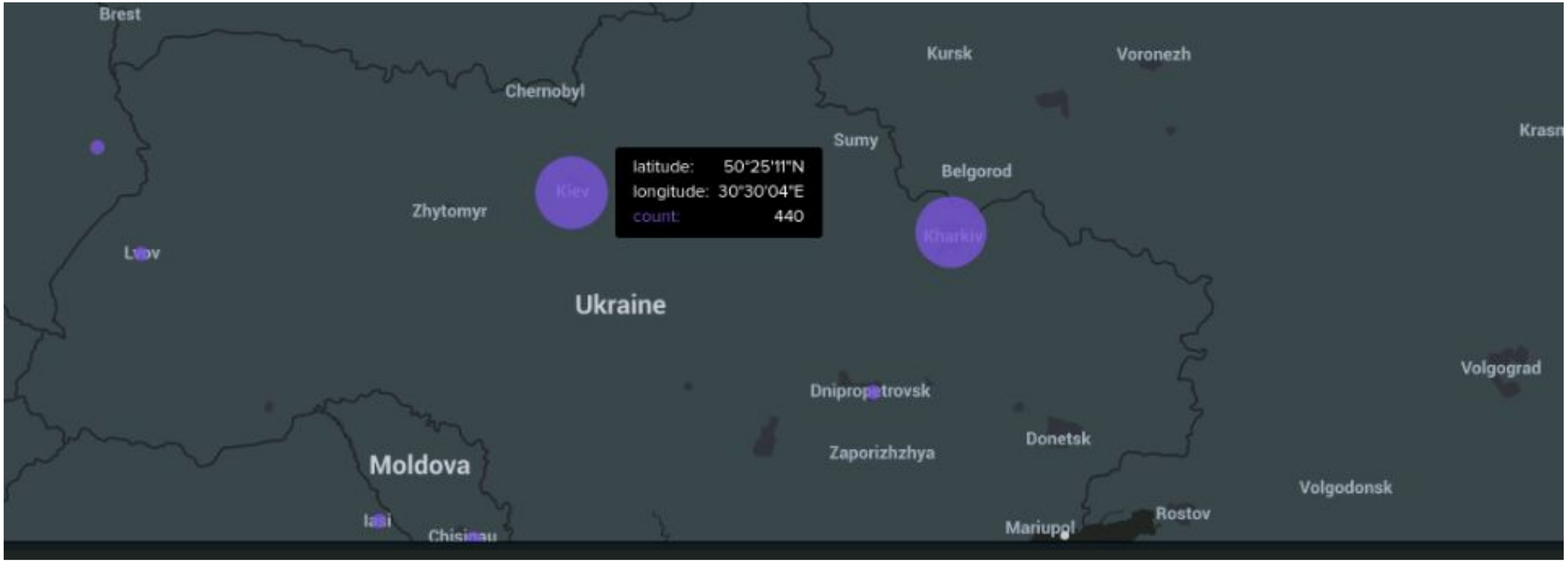
HTTP Methods over time

- Suspicious activity was identified using both GET and POST methods
- GET: Started at 1am on Thursday 26th March 2020 and stopped at 3am on Thursday 26th March 2020.
  - GET: Peak count during the attack was 729
- POST: Started at 3am on Thursday 26th March 2020 and stopped at 5am on Thursday 26th March 2020.
  - POST: Peak count during the attack was 1296



Client IP by Geolocation

- There was suspicious activity in the country of Ukraine, specifically in the cities of Kiev and Kharkiv.
- The city of Kiev, Ukraine had a high volume of activity.
  - Kiev: Count of 440
- The city of Kharkiv, Ukraine had a high volume of activity.
  - Kharkiv: Count of 432.

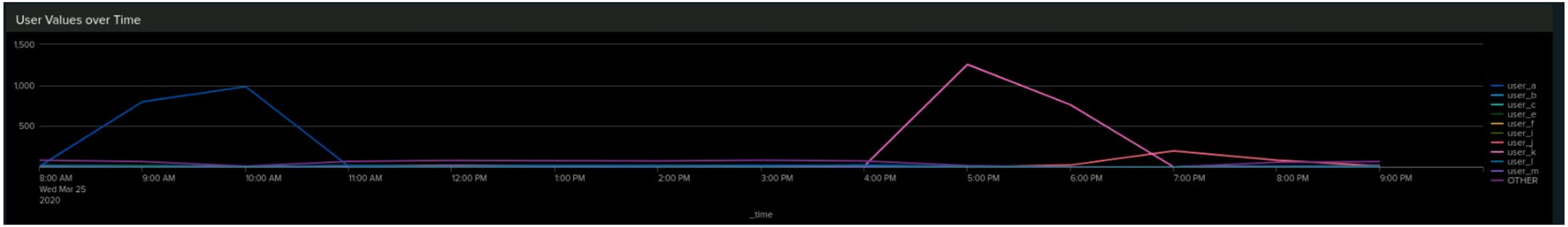


Pie chart of different URI counts—Apache

User Values over time — Apache

From the data below, we can see an increase in activity by two users in particular:

- user_a
  - Started at 12:00 am and stopped at 03:00 am 25th March
  - Peak count of 984
- user_k
  - Started at 08:00 am and stopped at 11:00 am 25th March
  - Peak count of 1256

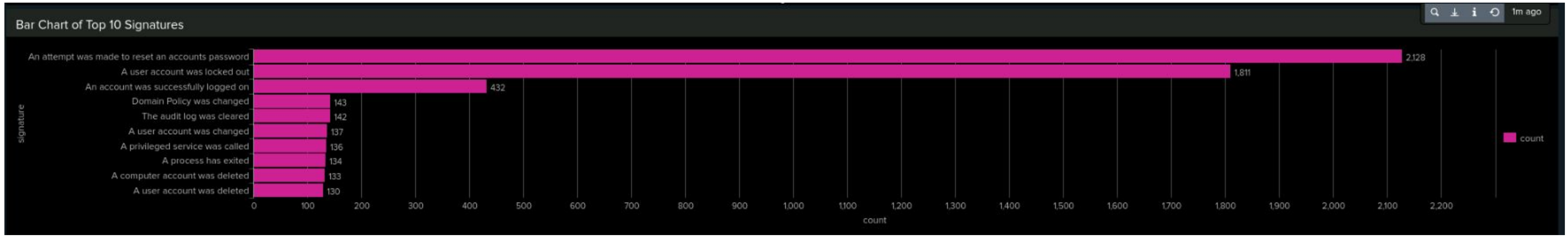


Bar chart of top signatures—Apache

From the results, we can identify that:

- “An attempt was made to reset an accounts password” had a count of 2128
- “A user account was locked out” had a count of 1811

This potentially points towards a brute force attack, due to the nature of the corresponding signatures

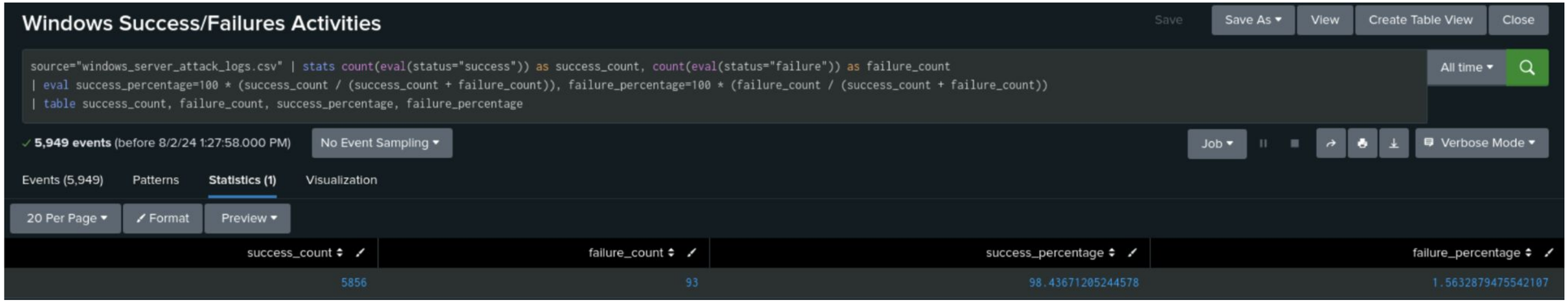


Attack Analysis

Attack Summary — Windows Reports

Windows Success/Failures Activities Report

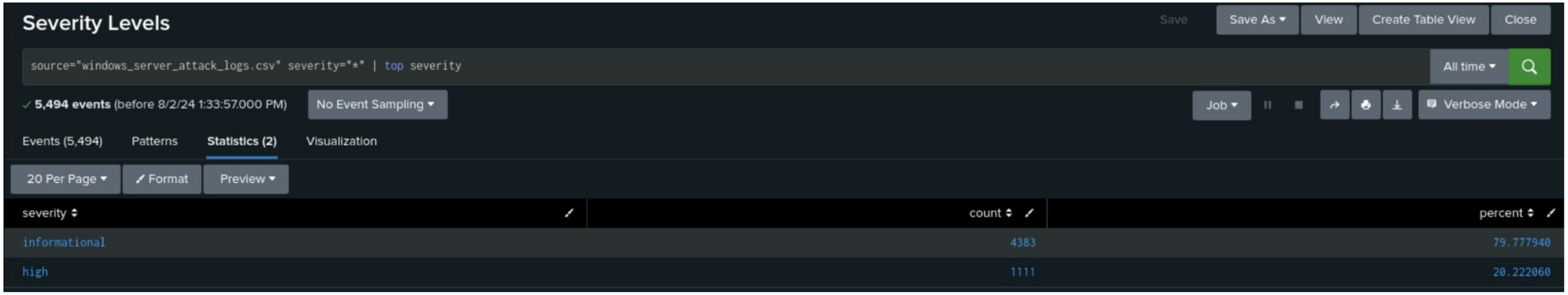
- There was evidence of suspicious failed activities.
- Success count increased to a total of 5856, with a percentage of 98.43
- Failure count decreased to 93, with a percentage of 1.56%



Attack Summary — Windows Reports

Severity Levels Report

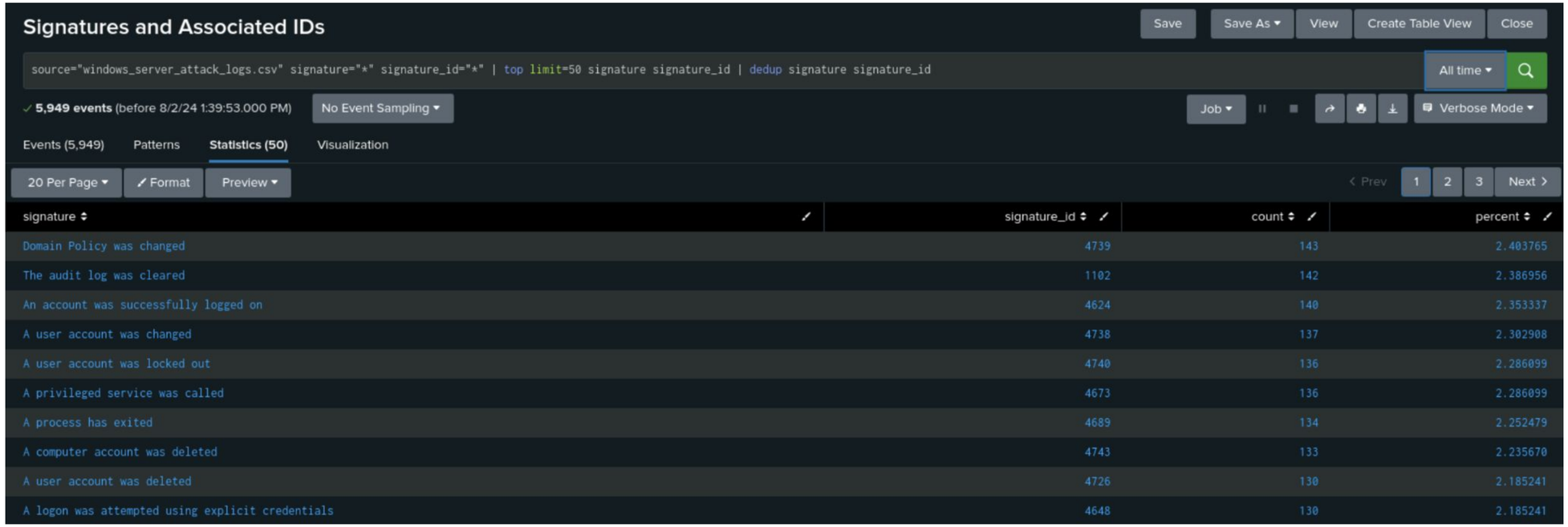
- Results indicate a increase in high severity events, with a count of 1111 in comparison to a normal event count of 329
- High severity events increased from 6.9% to 20.2%



Attack Summary — Windows Reports

Signature and Signature IDs Report

- Various new signatures and corresponding IDs identified, combination of said signature indicates that attackers have potentially gain unauthorized access into VSI systems
- On the other hand, current employees may be co-conspiring and aiding in the attack from the inside
- Various new signatures identified, including:
  - “Domain Policy was changed” with a count of 143
  - “The audit log was cleared” with a count of 142



signature	signature_id	count	percent
Domain Policy was changed	4739	143	2.403765
The audit log was cleared	1102	142	2.386956
An account was successfully logged on	4624	140	2.353337
A user account was changed	4738	137	2.302908
A user account was locked out	4740	136	2.286099
A privileged service was called	4673	136	2.286099
A process has exited	4689	134	2.252479
A computer account was deleted	4743	133	2.235670
A user account was deleted	4726	130	2.185241
A logon was attempted using explicit credentials	4648	130	2.185241

Attack Summary — Windows Alerts

Were the thresholds for corresponding alerts correct?

Failed Windows Activity

- Identified a spike in events, totalling at 35 at 08:00 am 25th March
- Alert was reviewed and the decision was made that no improvements were needed to be added to the alert as it was functioning properly and was triggered.

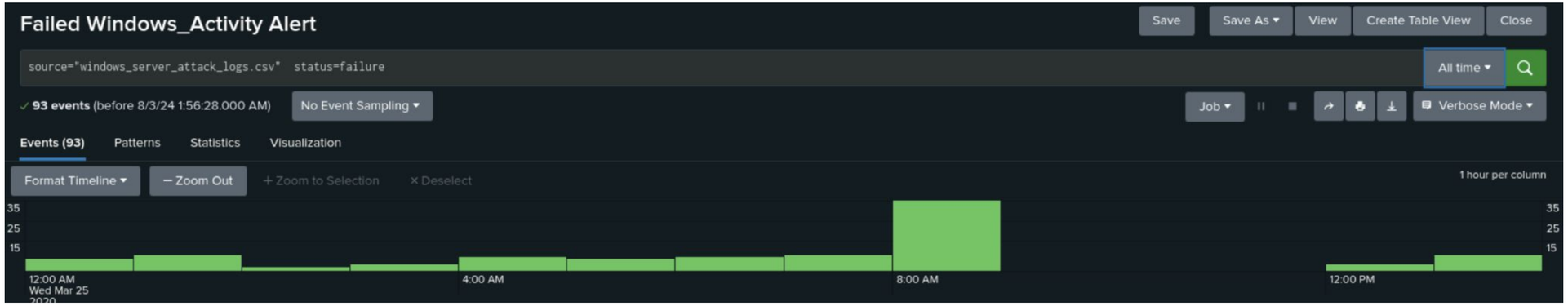
Account Successful Logins

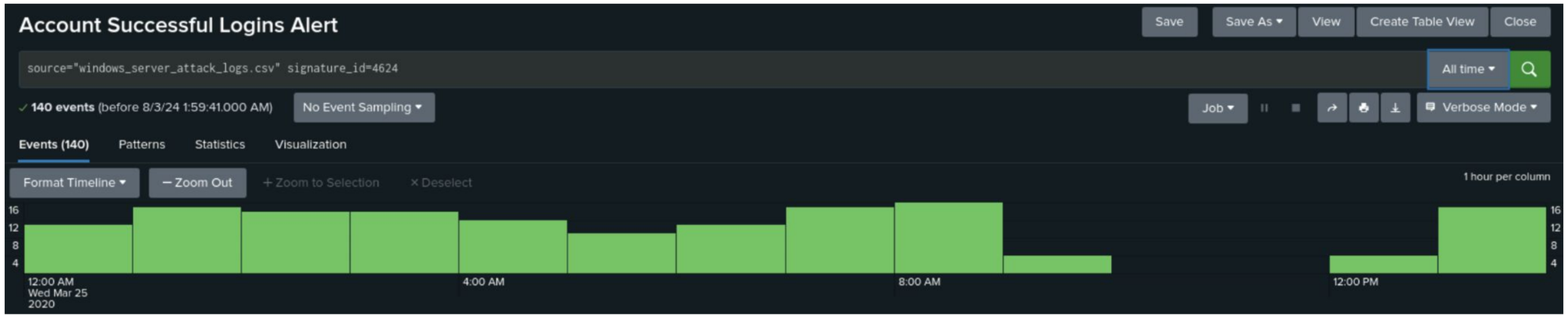
- Alert was triggered, as event count fell under threshold target, with lowest event count being recorded between 10:00 am 12:00 pm, totalling 0 events.
- Alert provided a suitable threshold which identified when suspicious activity occurred, therefore no further configuration was required.

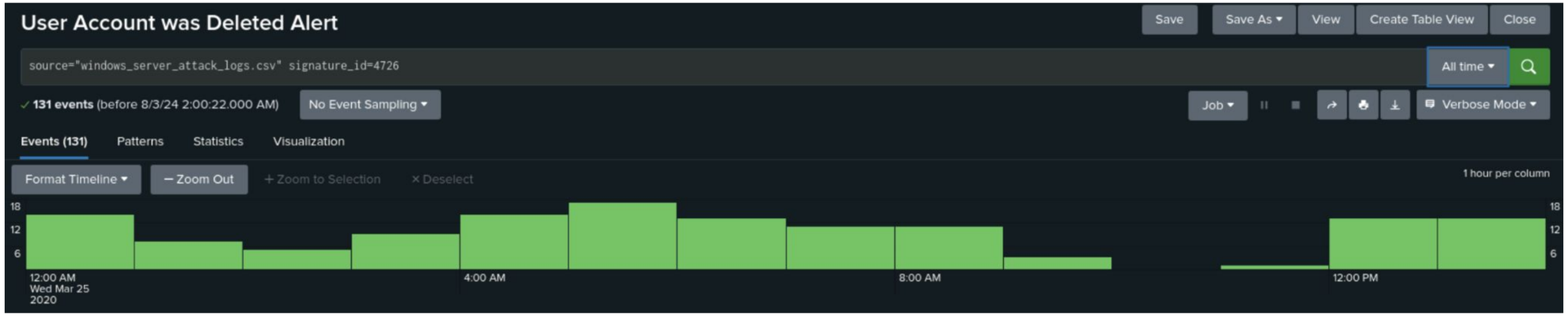
User Account Was Deleted

- Between 10:00 am and 11:00 am we identified a count of 0 events, signifying that the alert had been configured to trigger if events went over a threshold value instead of under, which would have been more appropriate.
- Alert did not operate as intended therefore no alert was received. In order to mitigate against this in the further, the threshold for the alert would be reconfigured to trigger once events went below 5 counts per hour.

Alert Reults







Attack Summary — Windows Dashboards

From the results compiled it points towards a possible brute force-attack due to the increased high level of events that is related to user login and failed logins that occurred within such a short period.

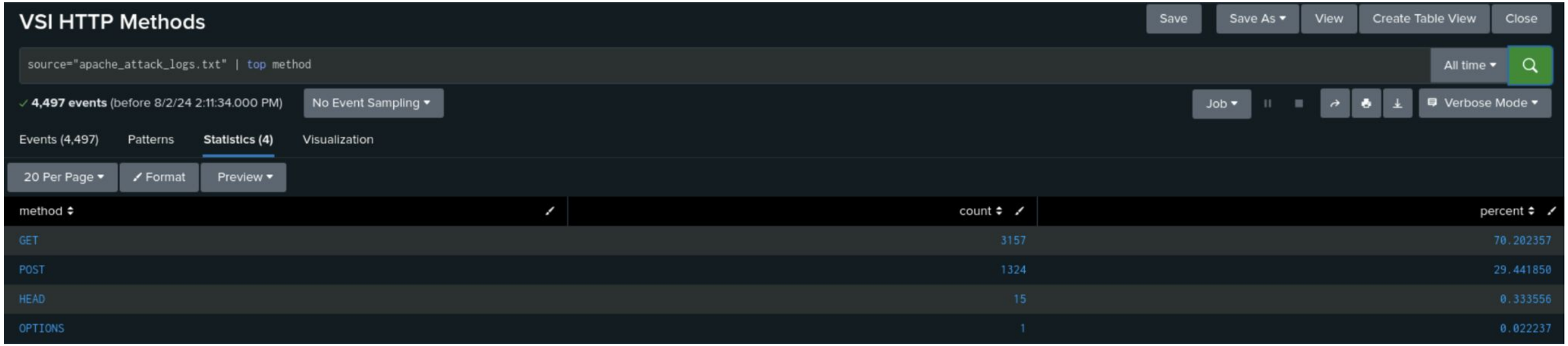
Attempts and change of password requests noticeably decreased as the incline of successful login attempts increased, suggesting that attackers had potentially gained access into VSIs system.

- The following signatures stood out:
  - “A user account was locked out” between 12:00 am and 02:30 am, with a peak event count of 896
  - “An attempt was made to reset an accounts password” between 08:00 am and 11:00 am, with a peak count of 1258
  - “An account was successfully logged on” between 10:00 am and 12:30 pm, with a peak count of 196 events
- Increased user activities
  - user_a
  - user_k

Attack Summary — Apache Reports

VSI HTTP Methods

- Significant increases in POST requests during the attack period
- Since the POST method is used for submitting data to the server, the increase in events indicates potential exploitation attempts through the use of brute forcing.
  - POST method increased to 1324 events from 106
  - GET method decreased from 9851 events to 3157

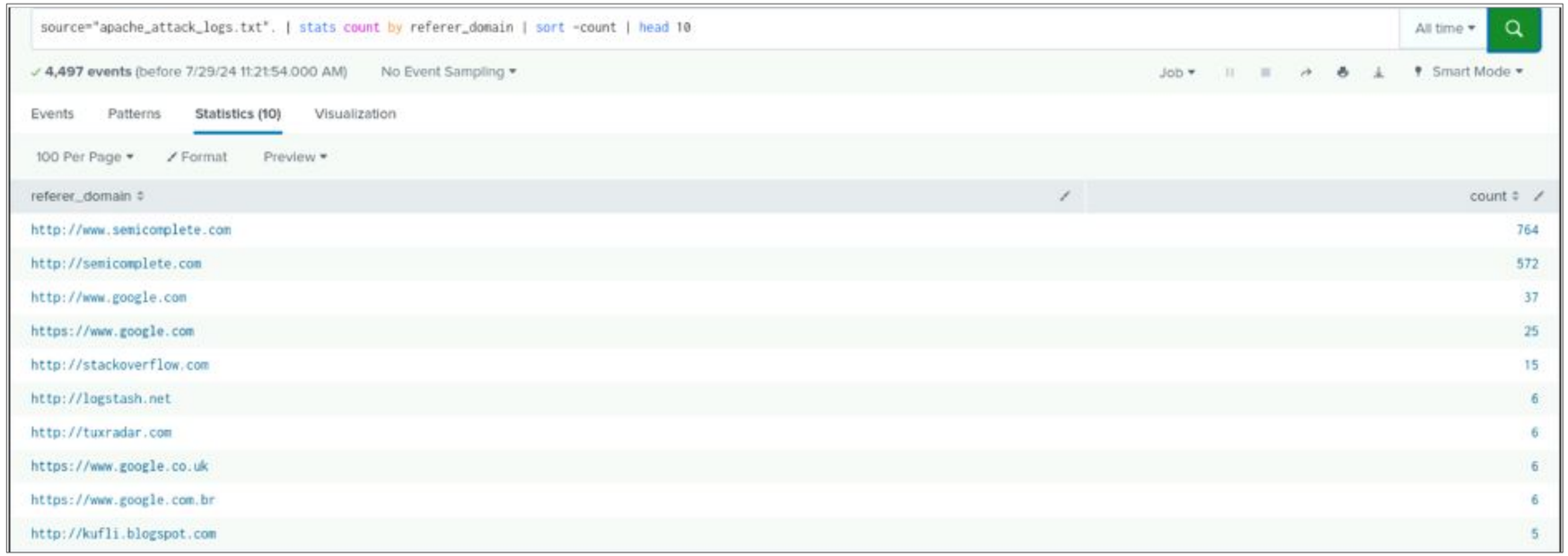


method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

Attack Summary — Apache Reports

VSI Top Domain Referred

- New referrer domains such as http://turxradar.com, https://www.google.com.br, and http://kufli.blogspot.com appeared in the attack logs.
- The appearance of these new domains suggests potential new sources of malicious traffic targeting the server.



referer_domain	count
http://www.semicomplete.com	764
http://semicomplete.com	572
http://www.google.com	37
https://www.google.com	25
http://stackoverflow.com	15
http://logstash.net	6
http://tuxradar.com	6
https://www.google.co.uk	6
https://www.google.com.br	6
http://kufli.blogspot.com	5

Attack Summary — Apache Reports

VSI HTTP Responses Codes

- There was a significant increase in 404 (not found responses) as well as a decrease in successful response (200, 206, 301, 304).
- The increase in 404 errors suggests that many requests were made to non-existent resources, indicating probing or vulnerability scanning activities
- The results are as follows:
  - 200 code had a maximum count of 3746
  - 404 code had a maximum count of 679

status	count
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

Attack Summary — Apache (Alerts)

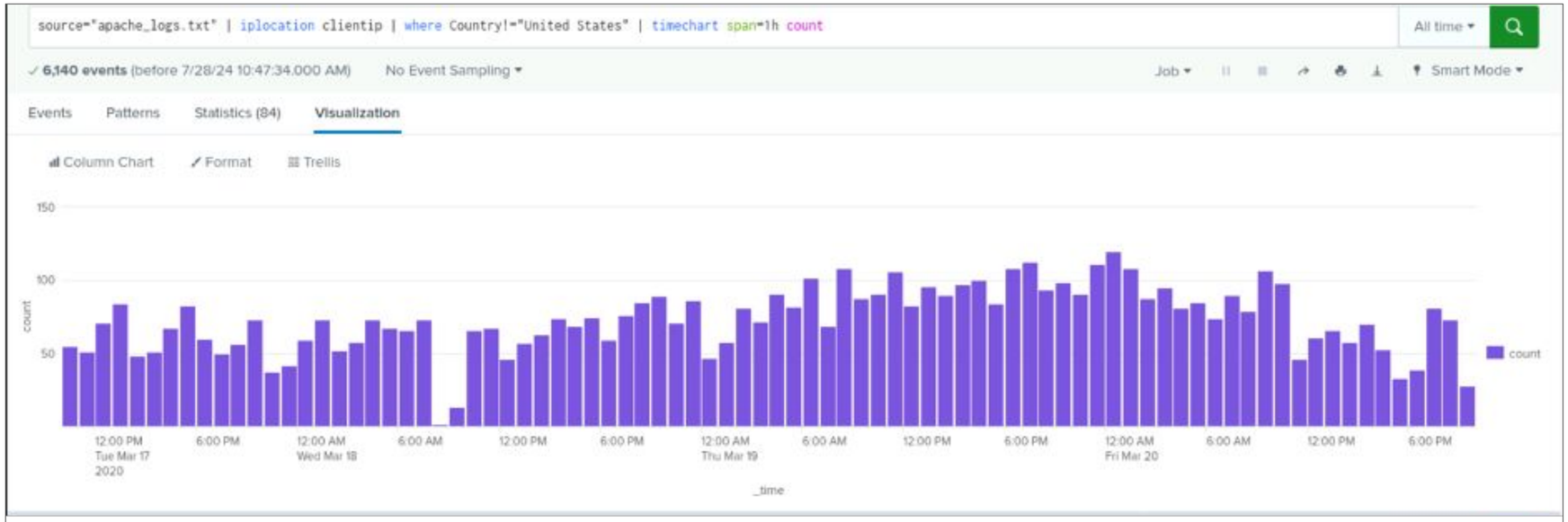
VSI Non-US Activity

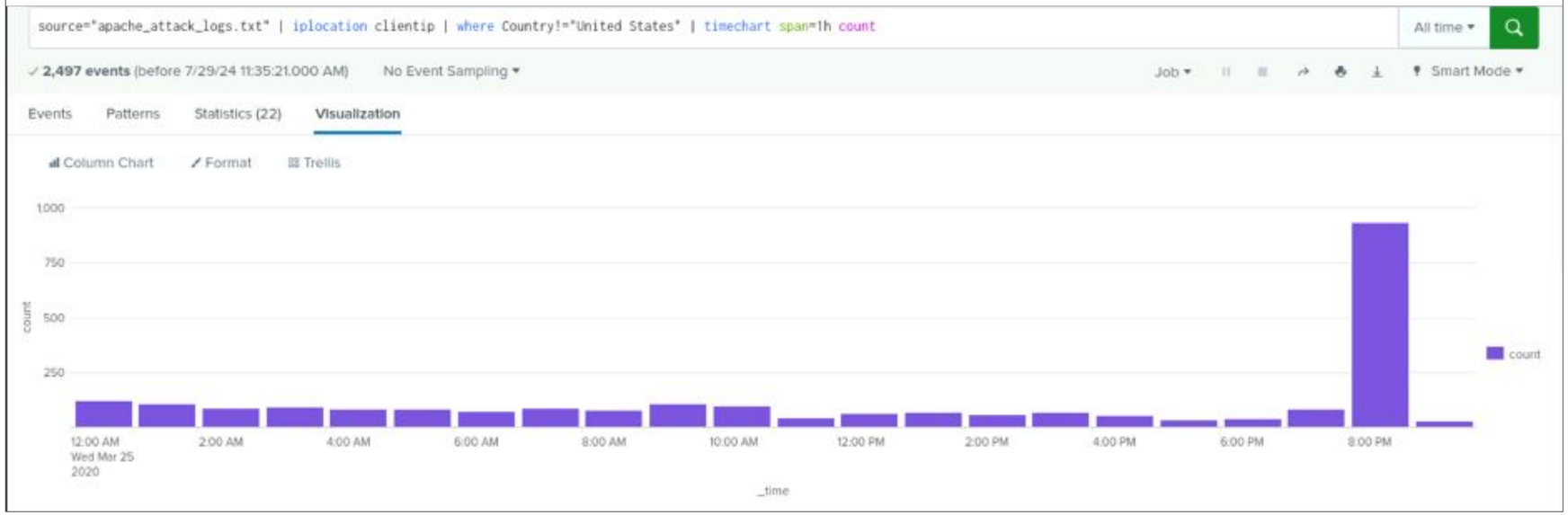
- There was a suspicious volume of activity from Ukraine, with 877 events at 4:00 AM on March 26th
- The threshold was set at 170 which would have triggered the alert indicating that a change in threshold was unnecessary

HTTP Post Activity

- There was a significant spike in POST requests with a count of 1296 at 8:00 PM on March 25th
- The threshold was set at 11 which would have triggered the alert indicating that a change in threshold was unnecessary

International Activity Comparison

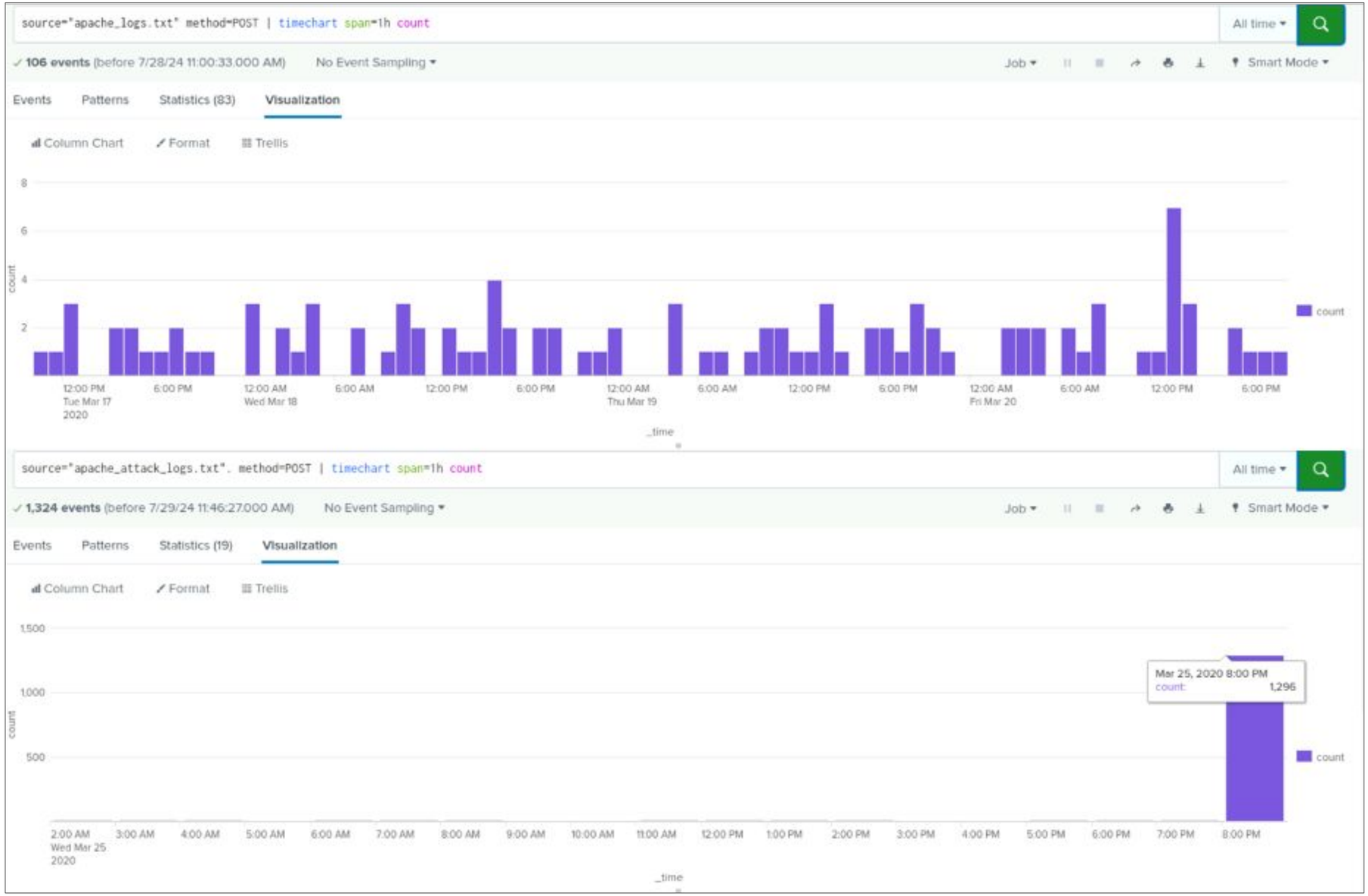




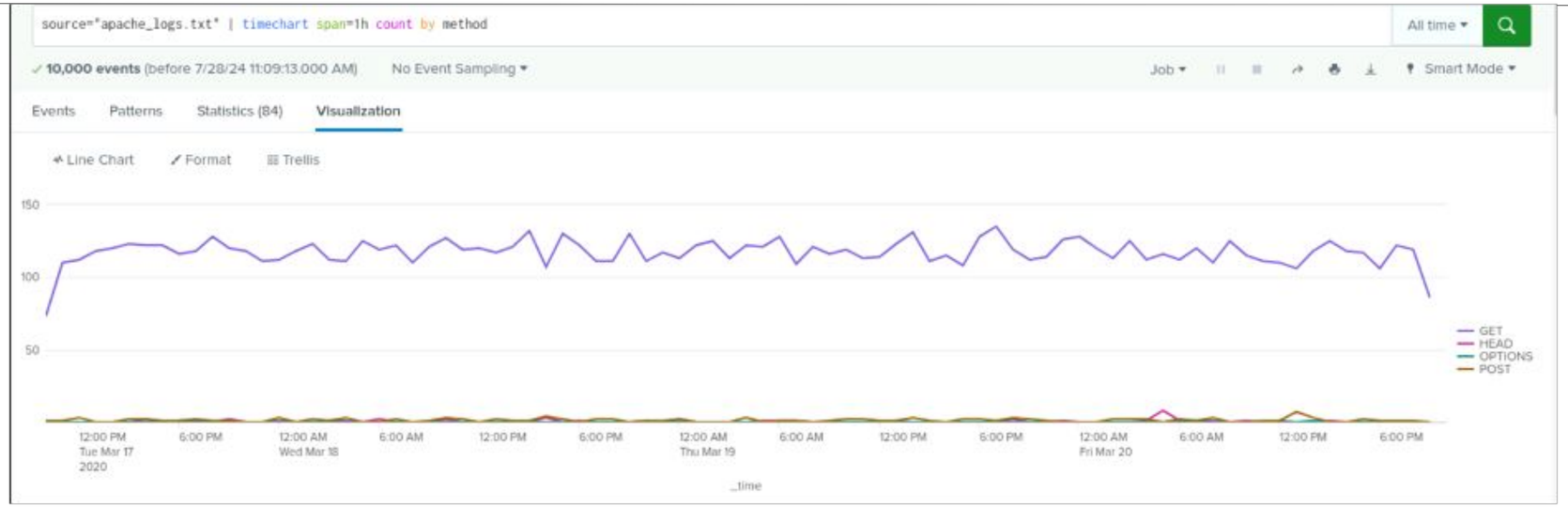
VSI Non-US Activity, Post Attack Results

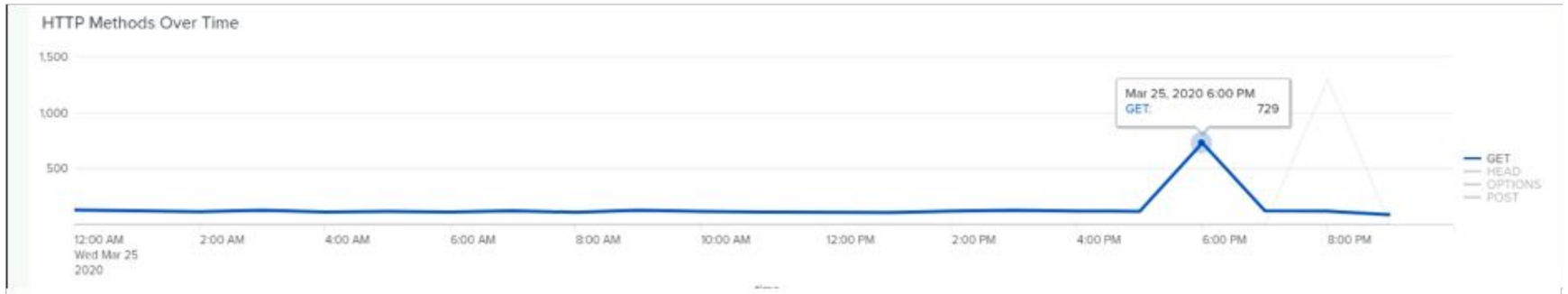
Top 10 Values	Count	%
Ukraine	877	35.122%
Sweden	198	7.93%
France	190	7.609%
Germany	161	6.448%
Spain	108	4.325%
Canada	87	3.484%
Italy	77	3.084%
United Kingdom	73	2.924%
Brazil	65	2.603%
China	64	2.563%

HTTP Method Activity



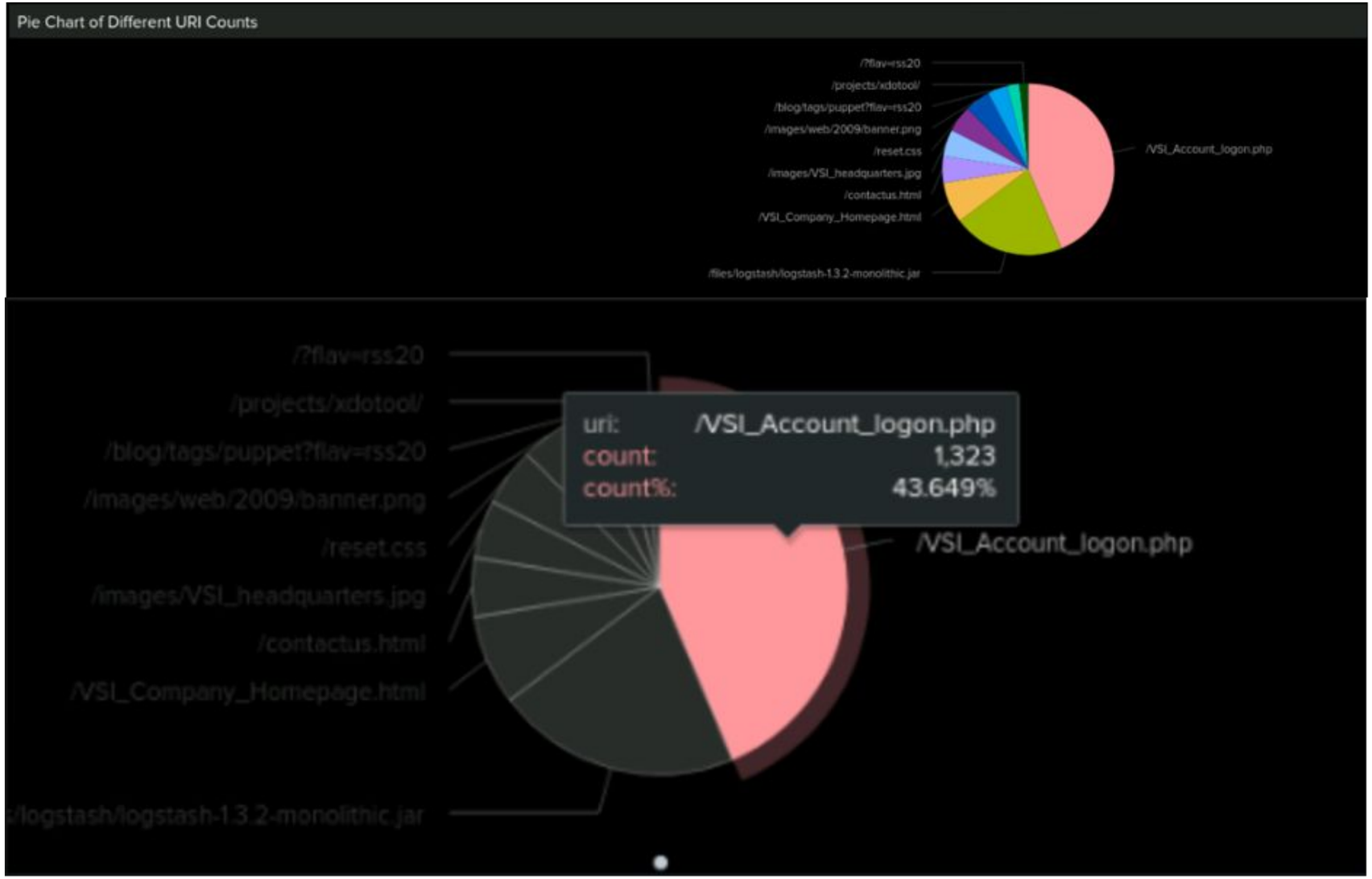
Line Graph of HTTP Methods



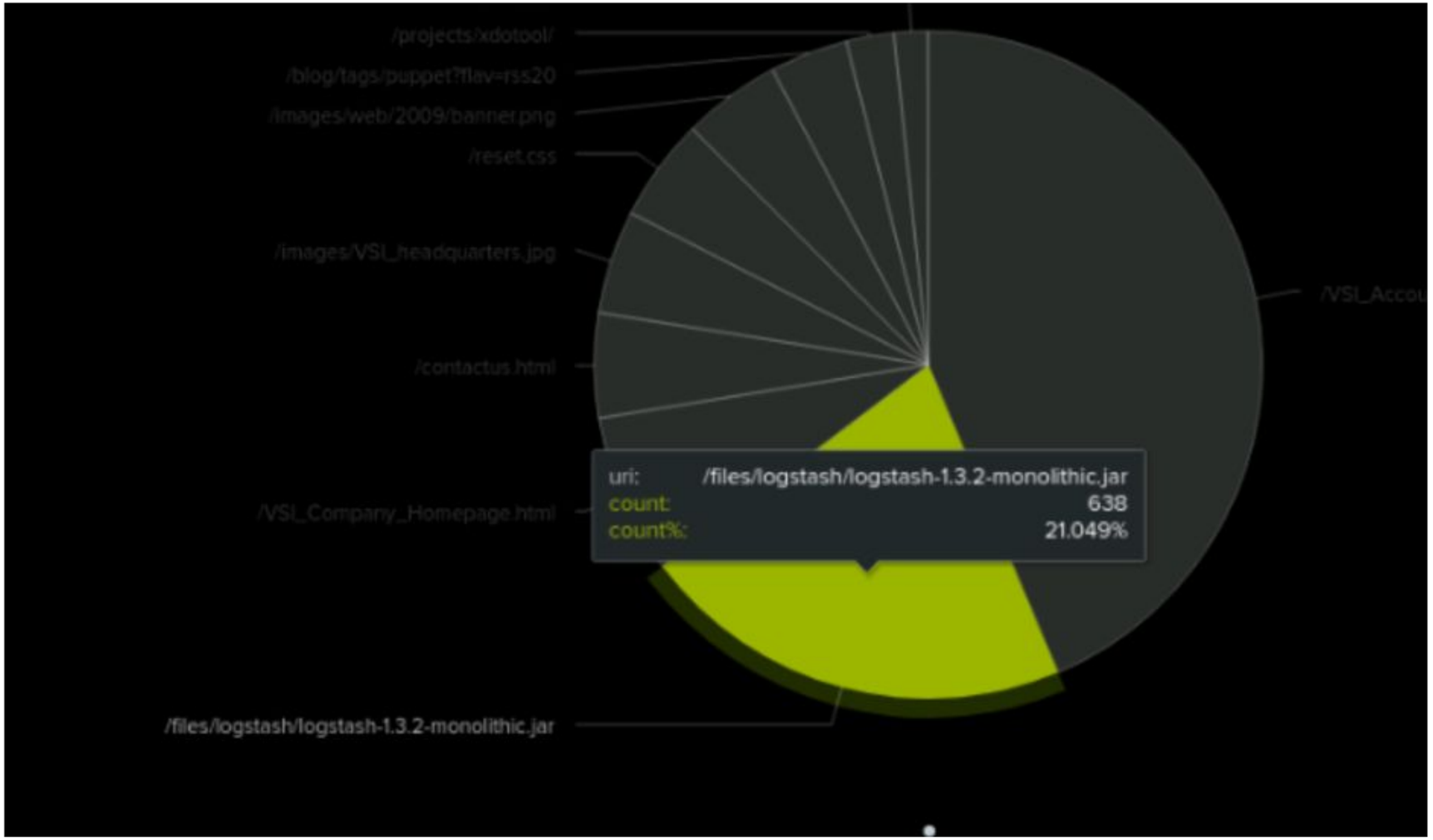


Cluster Map - Post Attack Results

URI Data - Post Attack Results



URI Data - Post Attack Results, continued



Attack Summary—Apache (Dashboards)

Line Graph of HTTP Methods

- Significant spikes in GET and POST requests on March 25, 2020 indicate a coordinated attack most likely a brute force attempt.
- Both GET and POST methods were used, with the POST method showing a higher spike than the GET method
- Attack started around 6:00 PM with GET requests and continued through 8:00 PM with POST requests
- Peak count of GET requests was 729 and for POST requests; 1296.

Cluster Map

- High volume of activity from Kiev and Kharkiv, Ukraine
- Kiev had 440 events and, and Kharkiv had 432 events

URI Data

- The URI “/files/logstash/logstash-1.3.2-monolithic.jar” had 638 counts (21%), and the URI “/VSI_Account_logon.php” had 1323 counts (43.6%).
- The high hit count on “/VSI_Account_logon.php” suggests a brute force attack on the VSI logon page.

Summary and Future Mitigations

Findings - Summary

From our findings were identified that the company suffered 2 significant attacks:

- A DDoS attack which was identified through the Apache logs:
  - We pinpointed unauthorized activity coming out of Ukraine which points to the origin of the attacks.
  - Increase in POST method requests indicate that attackers flooded VSI's webs server in order to compromise the availability and functionality of the site.
  - Additional suspicious/fake domains identified (eg. https://www.google.com.br) which may have been used to fool employees to give away sensitive information such as login credentials or company data.
  - Increased traffic to URI "/VSI_Account_logon.php" indicates possibly of brute-force attacking

- A brute force attack could be seen within the Windows logs:
  - Identified through a spike in various signature fields relating to password resets and failed logins and account lockouts. This data indicates attackers attempted brute-forcing, resulting in accounts lockouts.
  - Increases in high security events signify attackers gained access into VSI systems. Given the access attackers may have had, this would correlate with signatures "Domain Policy was changed" and "The audit log was cleared". This shows attackers were aiming to cover their tracks, escalate privileges for user accounts and establish persistence within VSI systems.
  - Users user_a and user_k identified as culprits within various suspicious activities, which had significant impacts within VSI. Both users could of potentially given attackers initial access, or both user accounts may have had account vulnerabilities (weak passwords), and so were exploited in order to access VSI systems.

Mitigation and Preventative Measures

Windows Server - Mitigation:

- Implement 2FA policies for user accounts and devices
- Establish more effective Splunk add-ons which operate within company servers to identify potential threats
- Coordinate and manage regular training and awareness programs within the workforce to facilitate increased cybersecurity practises.
- Configuration of Intrusion Prevention Systems (IPS)
- Review password policies and take necessary actions to strengthen password rules and lockout settings
- Review and restrict user privileges

Apache Web Server - Mitigation:

- Implementation of network segmentation
- Isolation strategies to mitigate against spikes in activity from countries outside normal activity regions via IP-blocking tools and additional Splunk alerts/add-ons.
- Dedicated DDoS Mitigation Services
- Configuration of Intrusion Prevention Systems (IPS)
- Web Application Firewalls (WAF)
- Coordinate and manage regular training and awareness programs within the workforce to facilitate increased cybersecurity practises.

Thank you for watching