Cybersecurity Defense at Virtual Space Industries

by: Joy Dada

Cybersecurity Defense at Virtual Space Industries (VSI)

Objective:

As a SOC analyst, our primarily goal is to build a secure monitoring system that keeps VSI’s digital asset safe against potential cyber threats by JobeCorp, our competitor. We will utilize Splunk’s capabilities to analyze and interpret security logs from Windows and Apache servers.

Cybersecurity Defense at Virtual Space Industries (VSI)

3 Phases involved in project

01

Monitoring Environment

02

Attack Analysis

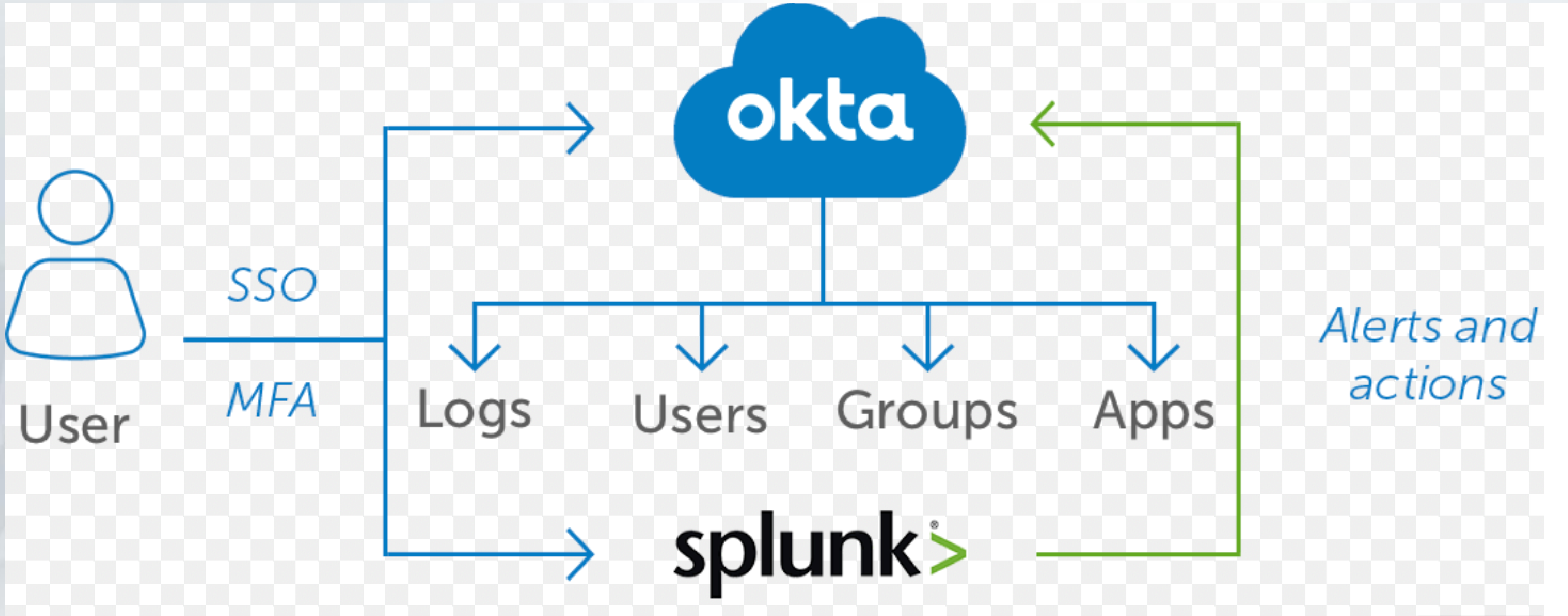
03

Project Summary & Future Mitigations

Monitoring: Okta Identity Cloud Add-on for Splunk

Okta is an identity management service that provides identity and access management (IAM) solutions.

- Integrates Okta logs with Splunk for improved monitoring.
- Enhances detection of security threats and anomalies.
- Supports compliance and audit processes.
- Mitigates identity-related risks.
- Essential for security analytics and identity management.



Proactive Security with Okta Add-on at VSI

Scenario:

VSI needs to secure its virtual-reality programs from cyber threats by JobeCorp without the challenge of managing an expanding number of services.

Solution: Integration of the Okta Identity Cloud add-on with Splunk to boost monitoring and control over authentication and user activities.

Outcomes:

- Threat Detection
- Streamlined Compliance
- Refined Access Permissions
- Immediate Incident Response

Logs Analyzed

1 Windows Logs

- Severity Changes: Noted for potential issues.
- Failed Activities: Spike in failed logins suggesting an attack.
- Successful Logins: Unusual high activity indicating potential unauthorized access.
- Deleted Accounts: No suspicious activity exceeded the threshold.
- Signatures: Suspicious activities included locked out accounts and password reset attempts.

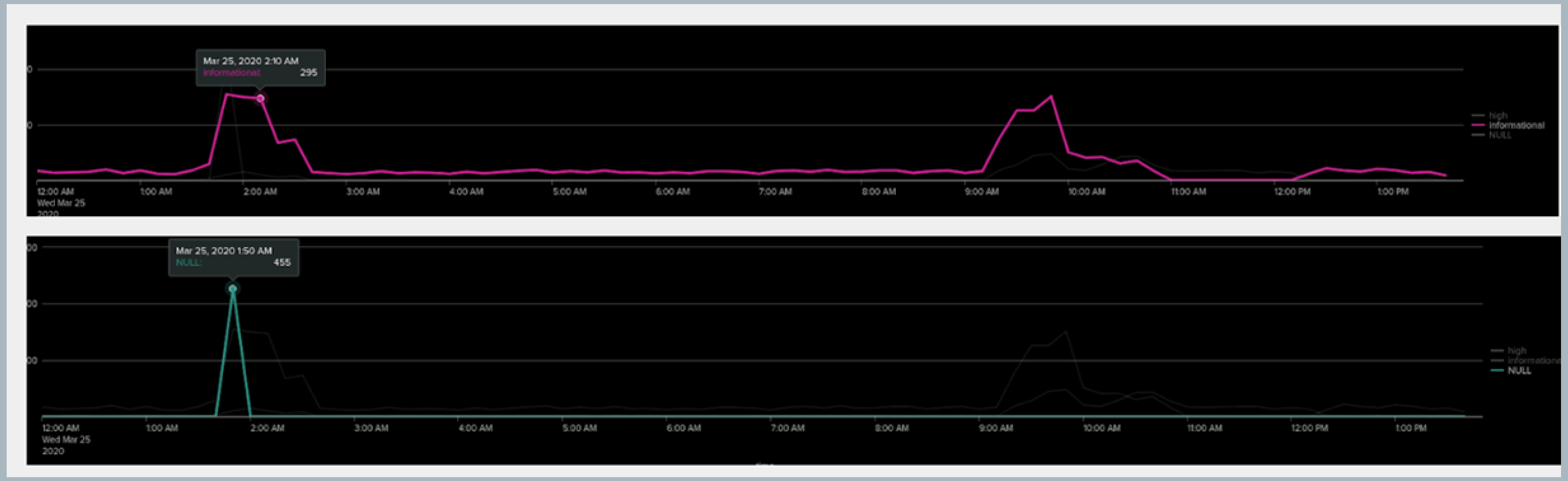
2 Apache Logs

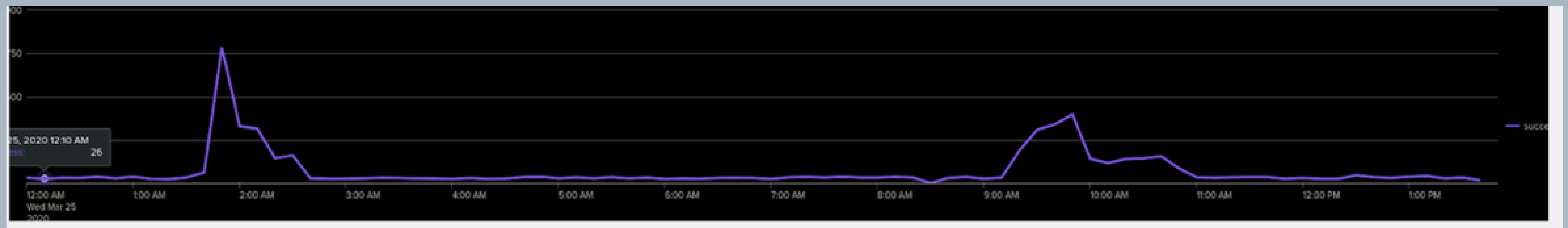
- HTTP Methods: GET and POST methods flagged for suspicious activities.
- Referrer Domains: "Null" referrer domains indicating potential threats.
- HTTP Response Codes: Unusual patterns suggesting probing or attacks.
- International Activity: High activity from Ukraine indicating cyber threats.
- HTTP POST Activity: Significant volume hinting at potential brute force attacks or exploits.
- Specific Concerns: Notable activity from specific locations and a frequently hit URI suggesting targeted unauthorized access attempts.

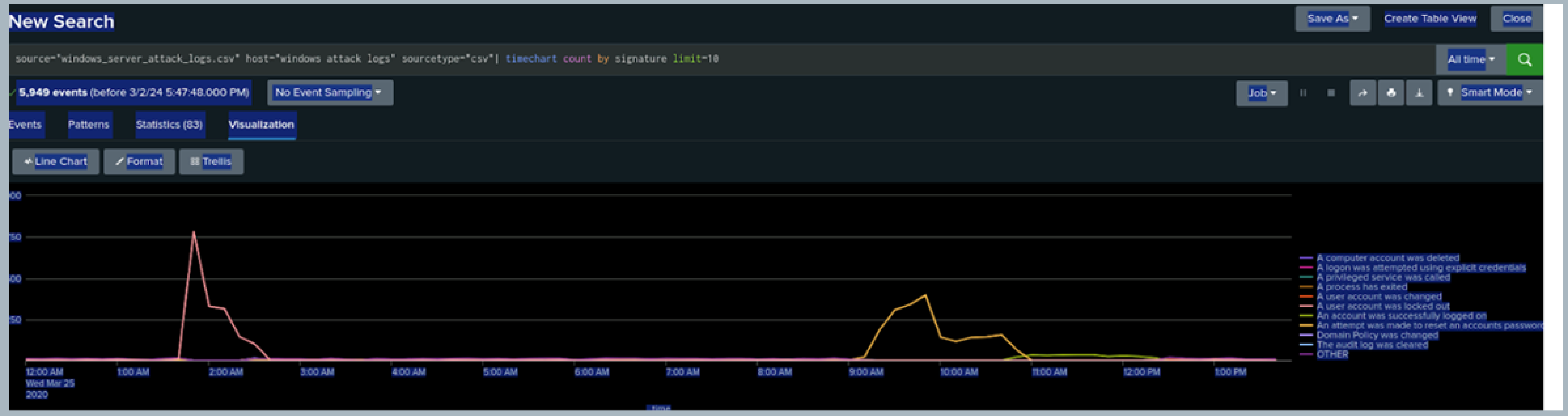
Reports—Windows Logs

Report Name	Report Description
Sever Attack Report	Identifies trends and anomalies in event severity levels
Failed Login Attempts	Tracks failed login attempts to detect possible brute force attacks/unauthorized access
Successful Logins	Monitors all successful logins events to detect unusual activity
Account Activity Monitoring	Tracks the creation ,modification and deletion of users accounts to identify any unusual or unauthorized changes.

Images of Reports—Windows







```
source="windows_server_attack_logs.csv" host="windows attack logs" sourcetype="csv"| timechart count by signature limit=10
```

✓ 5,949 events (before 3/2/24 5:47:48.000 PM)

- A computer account was deleted
- A logon was attempted using explicit credentials
- A privileged service was called
- A process has exited
- A user account was changed
- A user account was locked out
- An account was successfully logged on
- An attempt was made to reset an accounts passwor
- Domain Policy was changed
- The audit log was cleared
- OTHER

Alerts—Windows

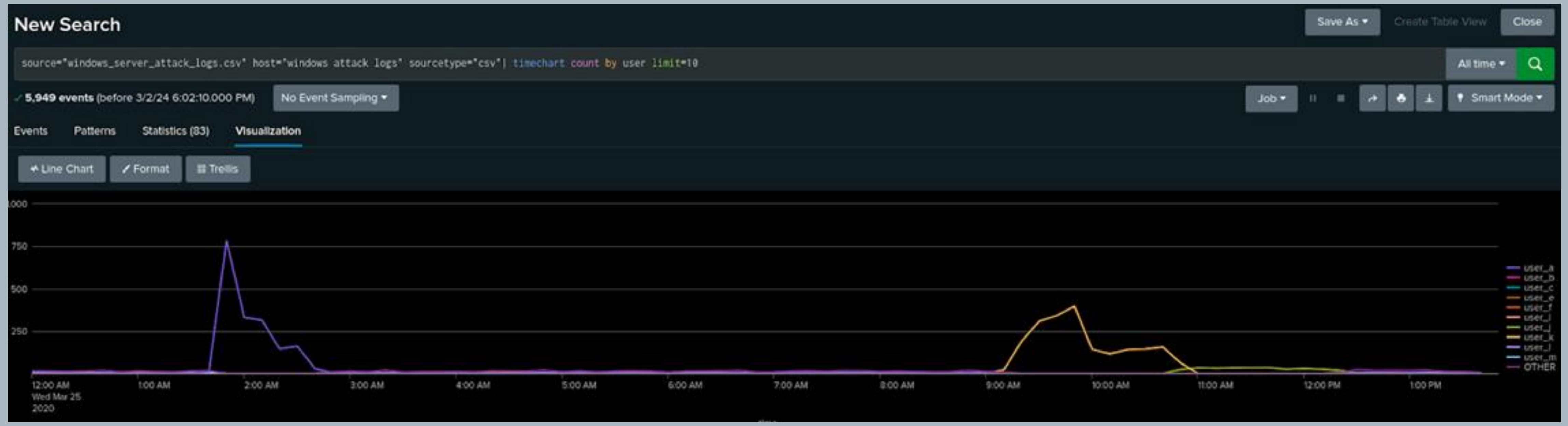
Alert Name	Alert Description	Alert Baseline	Alert Threshold
A user account was deleted	16 or more user account was deleted from the domain	8	16

JUSTIFICATION: 8 user account being deleted is the norm whereas 16 or more is an unusual number of accounts being deleted.

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account was successfully logged on	Monitors for an unusual spike in successful login attempts, could indicate credential stuffing or compromise.	7	14

JUSTIFICATION: Based on this analysis, a normal hour sees up to 7 successful logins. The Threshold is set at 14 to help detect double the average volume, which can help indicate potential unauthorized access.

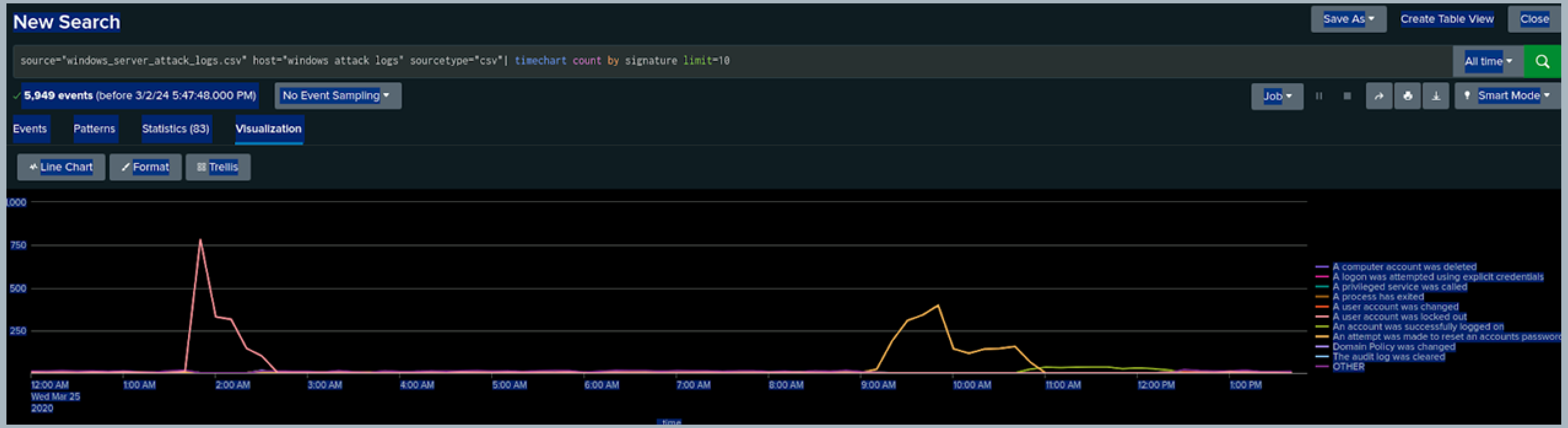
Dashboards—Windows



New Search

```
source="windows_server_attack_logs.csv" host="windows attack logs" sourcetype="csv"| timechart count by user limit=10
```

✓ 5,949 events (before 3/2/24 6:02:10.000 PM)

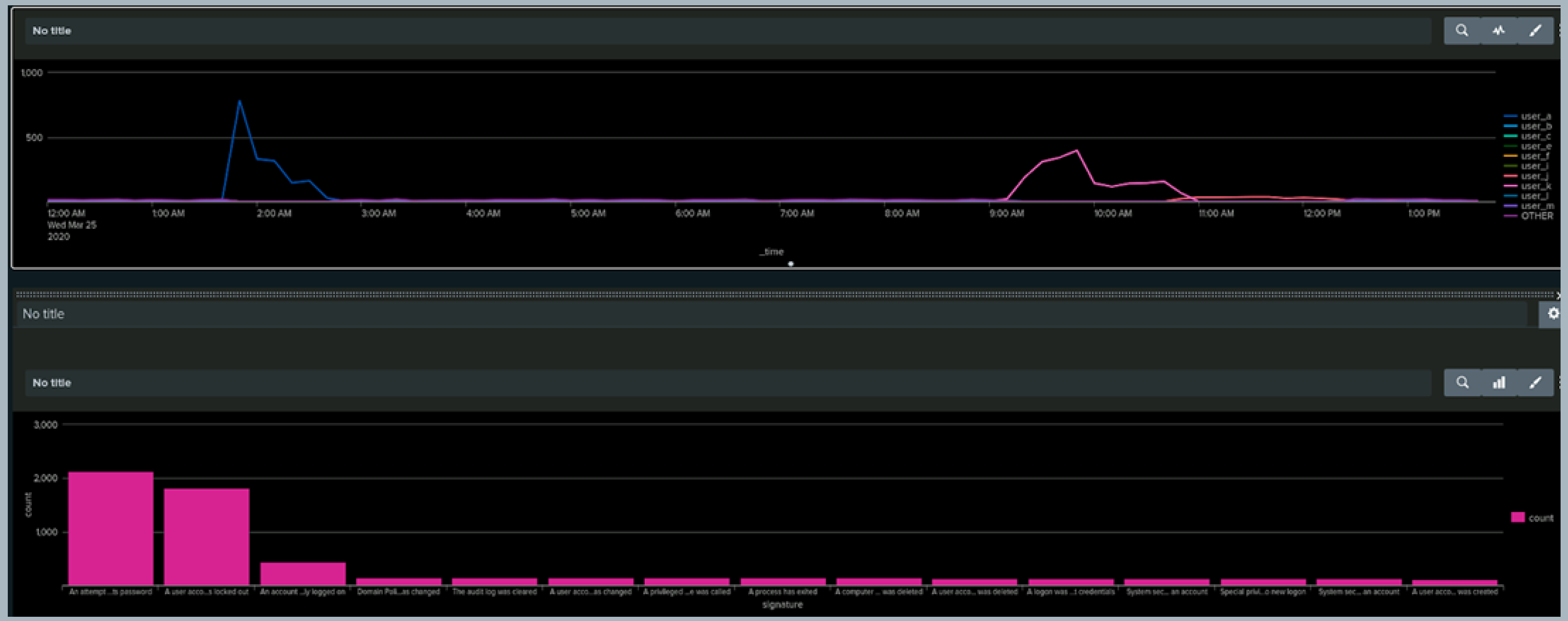


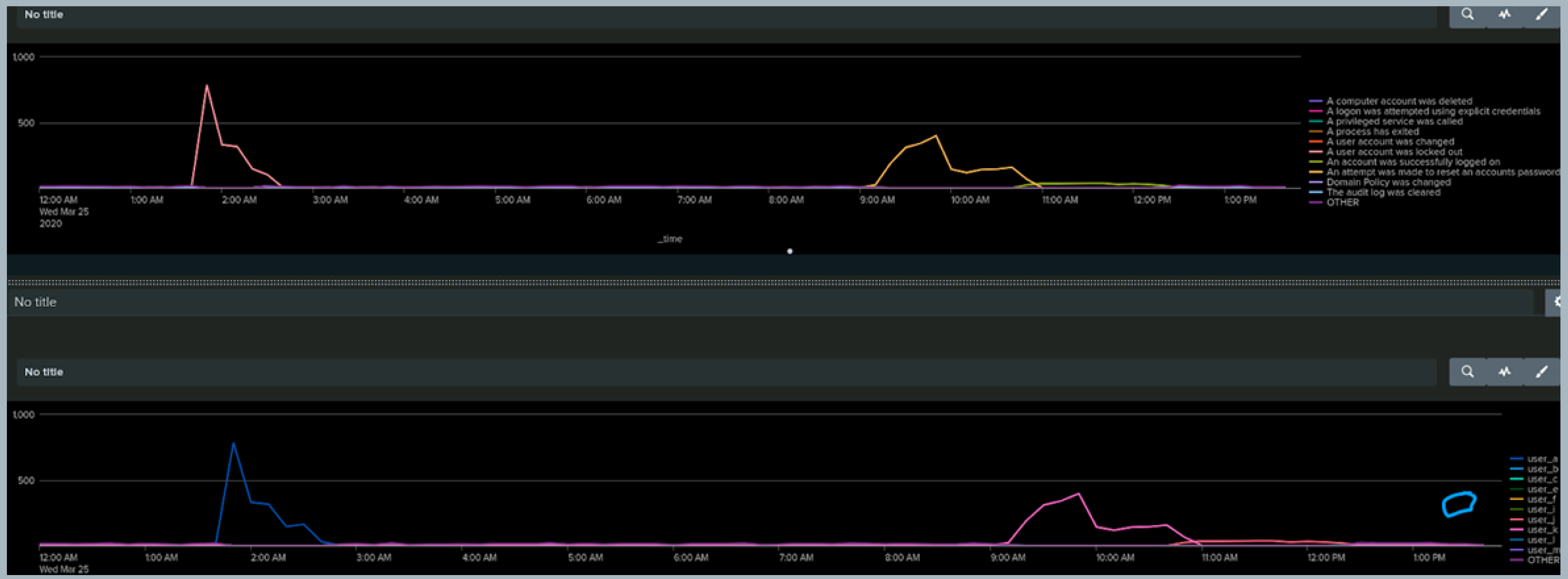
New Search

```
source="windows_server_attack_logs.csv" host="windows attack logs" sourcetype="csv"| timechart count by signature limit=10
```

✓ 5,949 events (before 3/2/24 5:47:48.000 PM)

Save As
Create Table View
Close
All time
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (83)
Visualization
Line Chart
Format
Trellis
1,000
750
500
250
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER

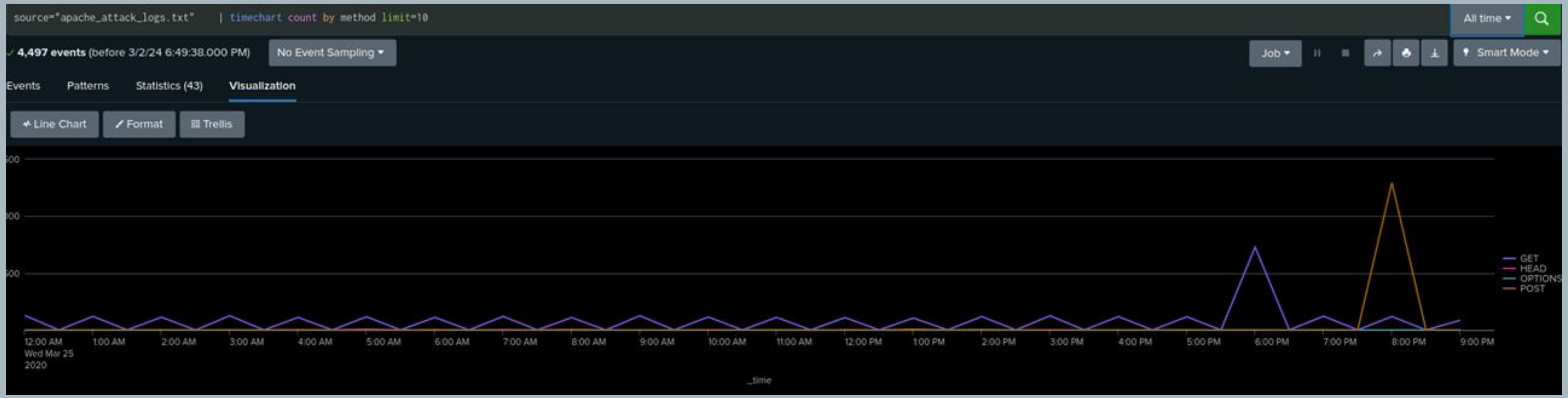




Reports—Apache

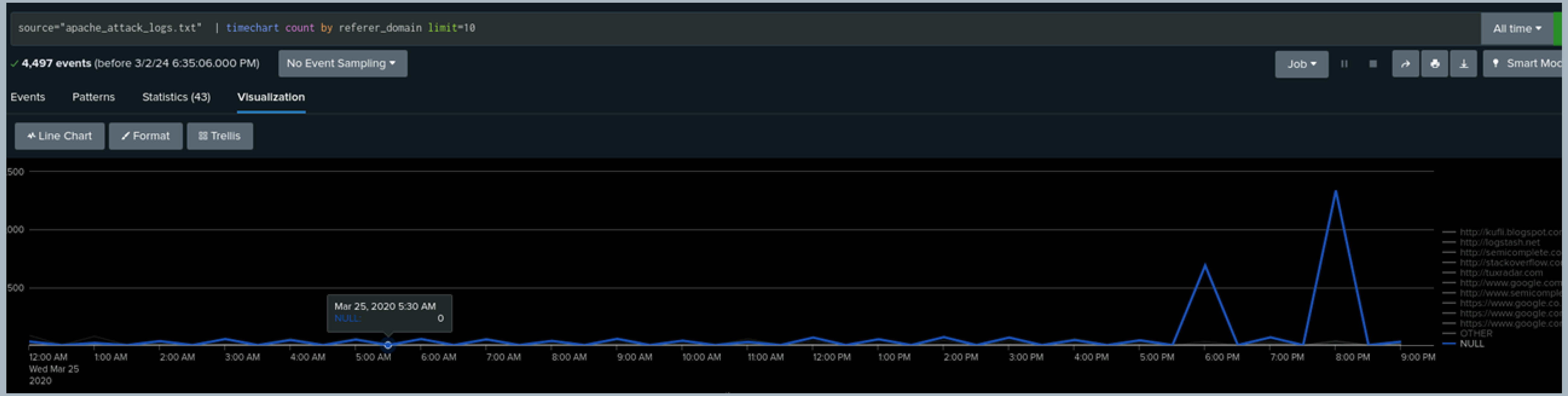
Report Name	Report Description
HTTP methods	Represents all the get post and delete methods.
HTTP Response	Gives us all the response code.(200’s 404’s,301’s)
Pie Chart- Top 10 URI_Path	Represents top of the website that was accessed.
Top 10 domains	Top 10 domains

Images of Reports—Apache



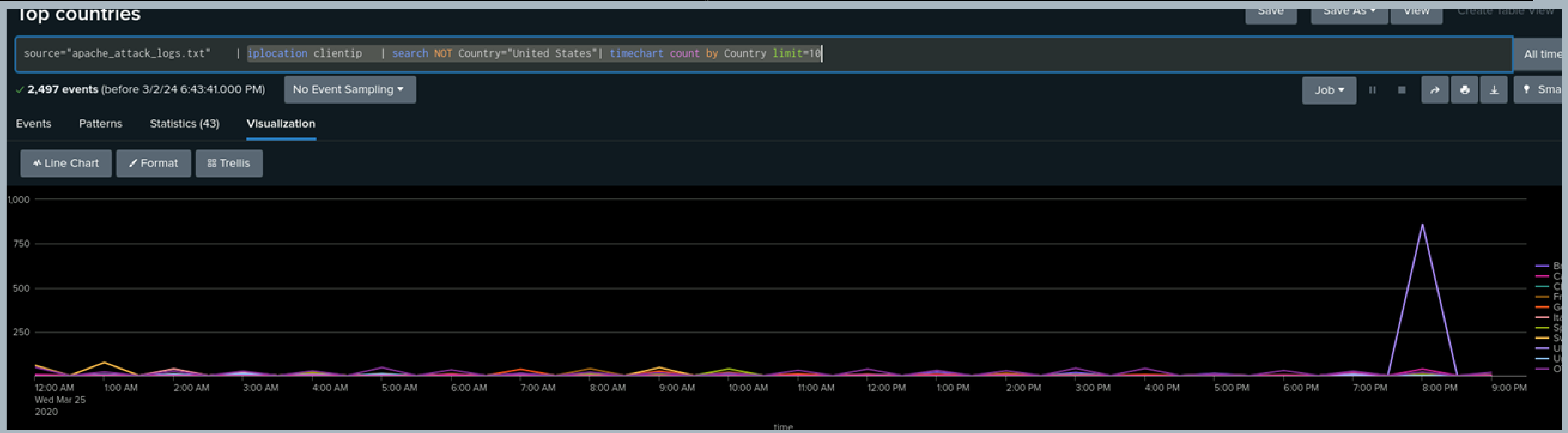
```
source="apache_attack_logs.txt"    | timechart count by method limit=10
```

✓ 4,497 events (before 3/2/24 6:49:38.000 PM)



```
source="apache_attack_logs.txt"  | timechart count by referer_domain limit=10
```

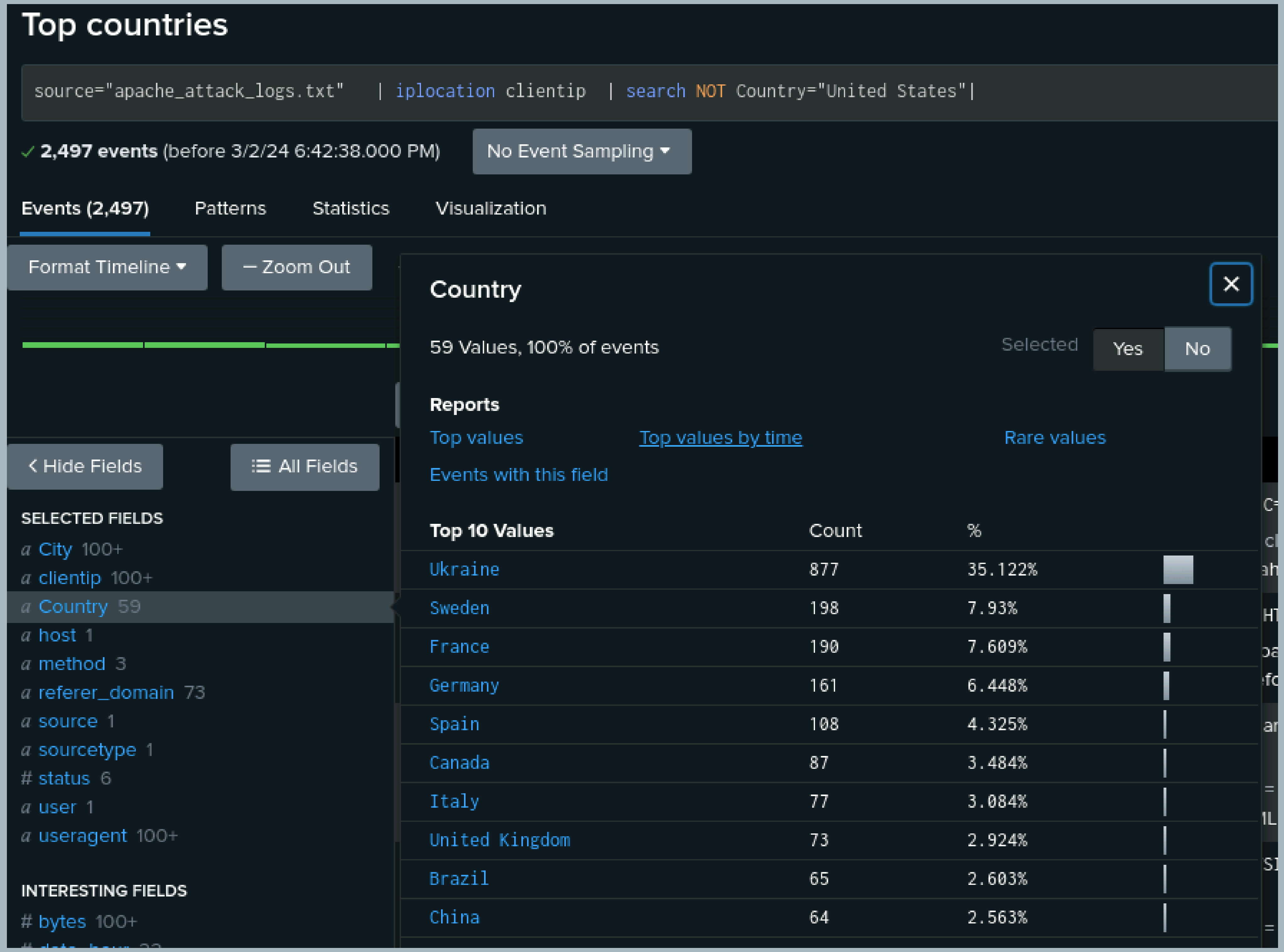
✓ 4,497 events (before 3/2/24 6:35:06.000 PM)



Top countries

```
source="apache_attack_logs.txt"    | iplocation clientip   | search NOT Country="United States"| timechart count by Country limit=10
```

✓ 2,497 events (before 3/2/24 6:43:41.000 PM)



Top countries

```
source="apache_attack_logs.txt"    | iplocation clientip   | search NOT Country="United States"|
```

✓ 2,497 events (before 3/2/24 6:42:38.000 PM)

SELECTED FIELDS

- a City 100+
- a clientip 100+
- a Country 59
- a host 1
- a method 3
- a referer_domain 73
- a source 1
- a sourcetype 1
- # status 6
- a user 1
- a useragent 100+

INTERESTING FIELDS

- # bytes 100+

Country

59 Values, 100% of events

Selected Yes [✓ No]

Reports

Top values Top values by time Rare values

Events with this field

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%

Alerts—Apache

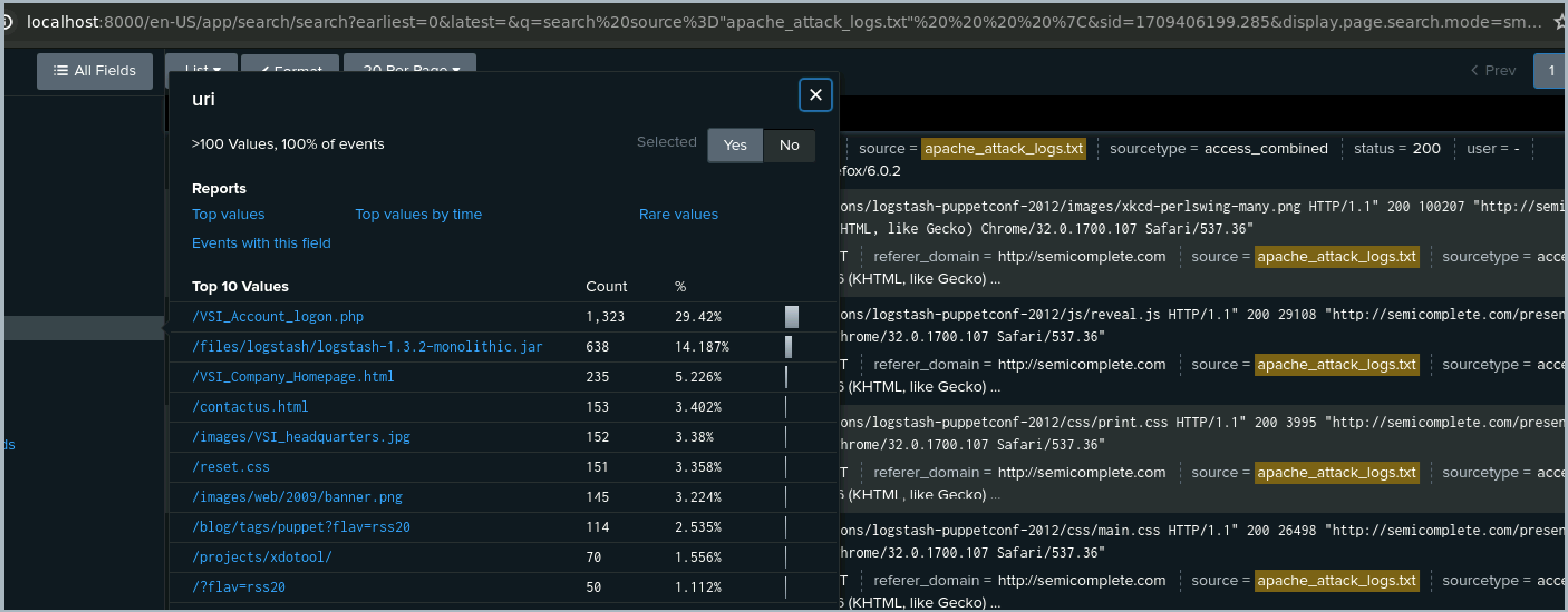
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Top Countries	Flags unexpected high traffic from other countries, hinting at possible cyber threats.	50	100

JUSTIFICATION: Set to flag unexpected spikes in foreign traffic after the baseline is set at 50, this will help identify targeted attacks from specific regions without over-alerting.

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Post HTTP methods	Flags unusually high Post request volumes	3	6

JUSTIFICATION: Chosen to spot undual form submissions indicating potential attacks, balancing between normal activity alert baseline 3 and possible threats that can be an alert threshold over 6.

Dashboards—Apache



localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search%20source%3D"apache_attack_logs.txt"%20%20%20%20%7C&sid=1709406199.285&display.page.search.mode=sm...

uri

>100 Values, 100% of events

Selected: Yes | No

Reports

Top values — Top values by time — Rare values

Events with this field

Top 10 Values	Count	%
/VSI_Account_logon.php	1,323	29.42%
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187%
/VSI_Company_Homepage.html	235	5.226%
/contactus.html	153	3.402%
/images/VSI_headquarters.jpg	152	3.38%
/reset.css	151	3.358%
/images/web/2009/banner.png	145	3.224%
/blog/tags/puppet?flav=rss20	114	2.535%
/projects/xdotool/	70	1.556%
/?flav=rss20	50	1.112%

```
source = apache_attack_logs.txt | sourcetype = access_combined | status = 200 | user = - |
fox/6.0.2
ons/logstash-puppetconf-2012/images/xkcd-perlswing-many.png HTTP/1.1" 200 100207 "http://semi
HTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
T | referer_domain = http://semicomplete.com | source = apache_attack_logs.txt | sourcetype = acce
5 (KHTML, like Gecko) ...
ons/logstash-puppetconf-2012/js/reveal.js HTTP/1.1" 200 29108 "http://semicomplete.com/presen
hrome/32.0.1700.107 Safari/537.36"
T | referer_domain = http://semicomplete.com | source = apache_attack_logs.txt | sourcetype = acce
5 (KHTML, like Gecko) ...
ons/logstash-puppetconf-2012/css/print.css HTTP/1.1" 200 3995 "http://semicomplete.com/presen
hrome/32.0.1700.107 Safari/537.36"
T | referer_domain = http://semicomplete.com | source = apache_attack_logs.txt | sourcetype = acce
5 (KHTML, like Gecko) ...
ons/logstash-puppetconf-2012/css/main.css HTTP/1.1" 200 26498 "http://semicomplete.com/presen
hrome/32.0.1700.107 Safari/537.36"
T | referer_domain = http://semicomplete.com | source = apache_attack_logs.txt | sourcetype = acce
5 (KHTML, like Gecko) ...
```

Attack Summary—Windows

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

- **After analyzing the Windows logs we notices that there was a marked increase in severity around 1:50 am with 455 nulls severities and significant informational count at 295. Also, there was a sharp spike in failed login attempts that occurred at 8am with 28 counts, which shows a potential attack.**
- **Moreover, we also analyzed that there were high volumes of successful logins coming from User A and User K, which shows us potential unauthorized access and attack attempts.**

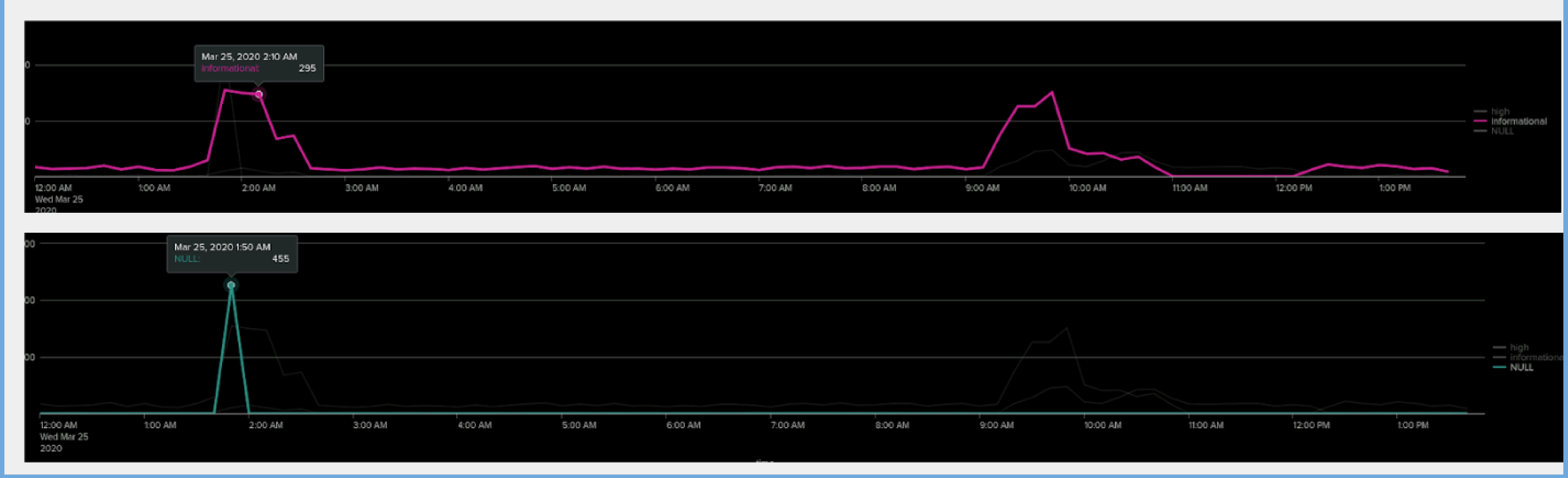
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

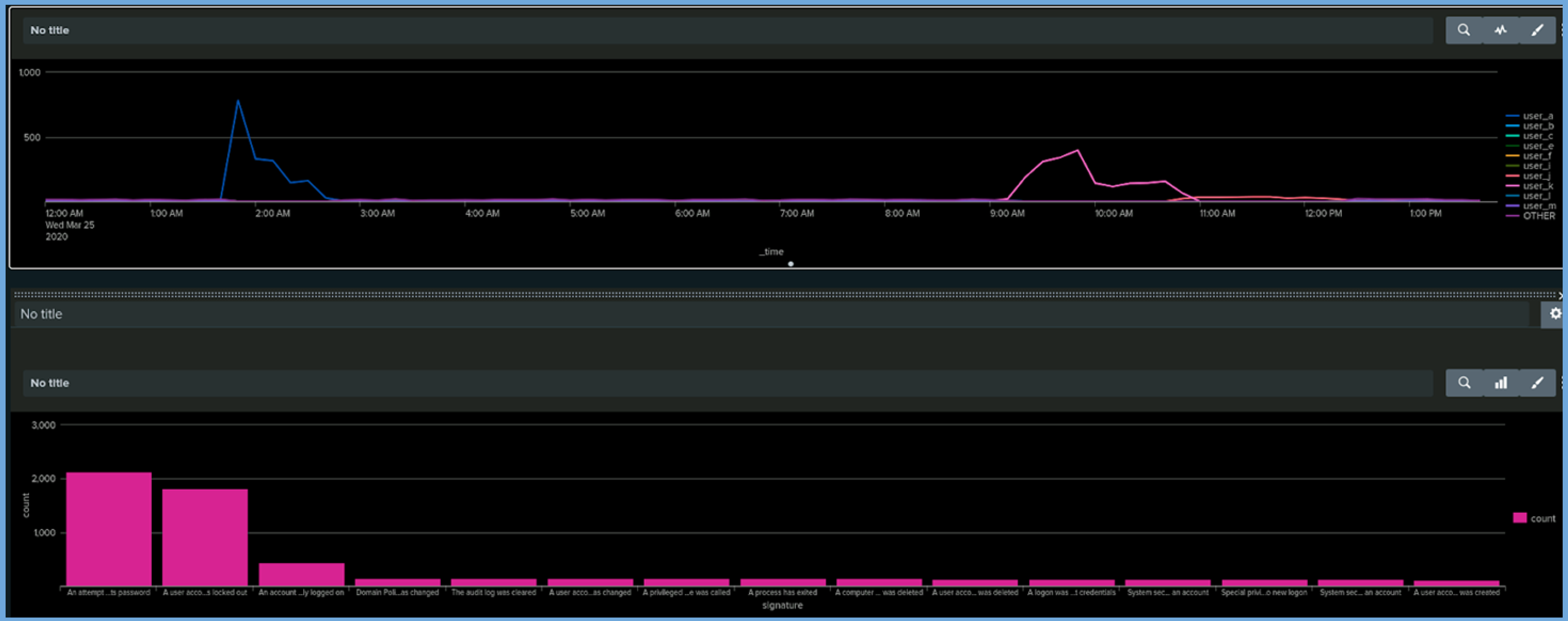
- **These Alerts were set up perfectly because they confirmed abnormal activities, detected all the thresholds were correct and flagged potential security incidents without triggering false positives.**

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

- **The Dashboards clearly showed us the security status, backing up our earlier findings with clear pictures of unusual login attempts and critical security alerts.**

Screenshots of Attack Logs- Windows





Attack Summary—Apache

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

- **For our Apache findings the reports uncovered unusual web activity and resources. For example, we saw a big increase in POST request and a lot of access that came from Ukraine. This suggest attacks trying to guess passwords or force entry, especially targeting the “/VSI_Logon.php”page.**

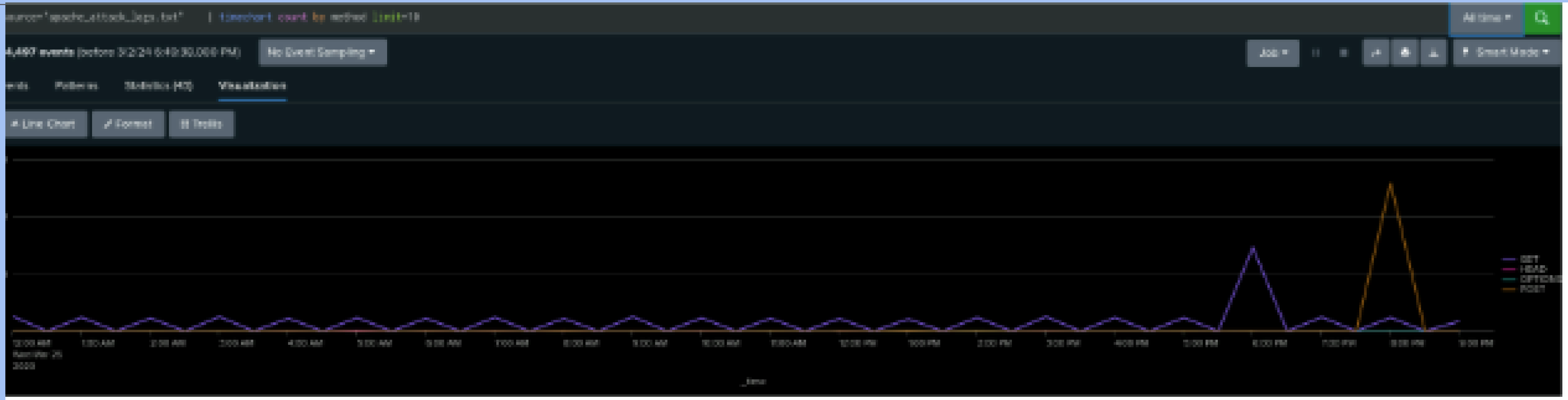
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- **Overall, the alerts helped point out major security risks, with set limits for web form submissions (POST activities) and overseas traffic that caught unusual behavior. These alerts were great at catching true dangers to the organization.**

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

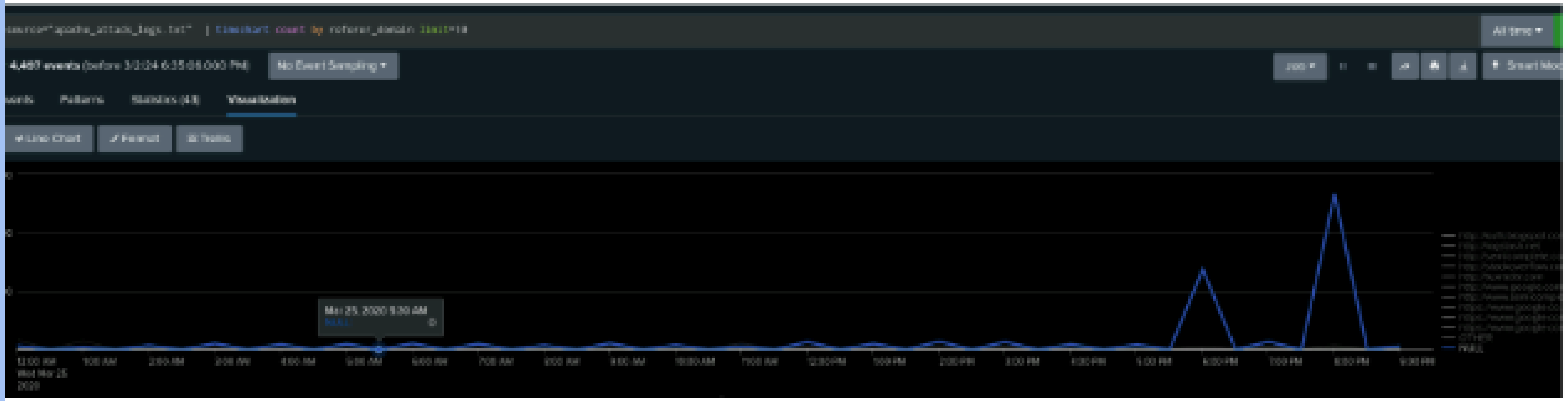
- **The Dashboards gave a straightforward view of how attacks happened, using maps and charts to show where attacks came from and how they were carried out, adding to what we learned from reports and alerts.**

Screenshots of Attack Logs- Apache



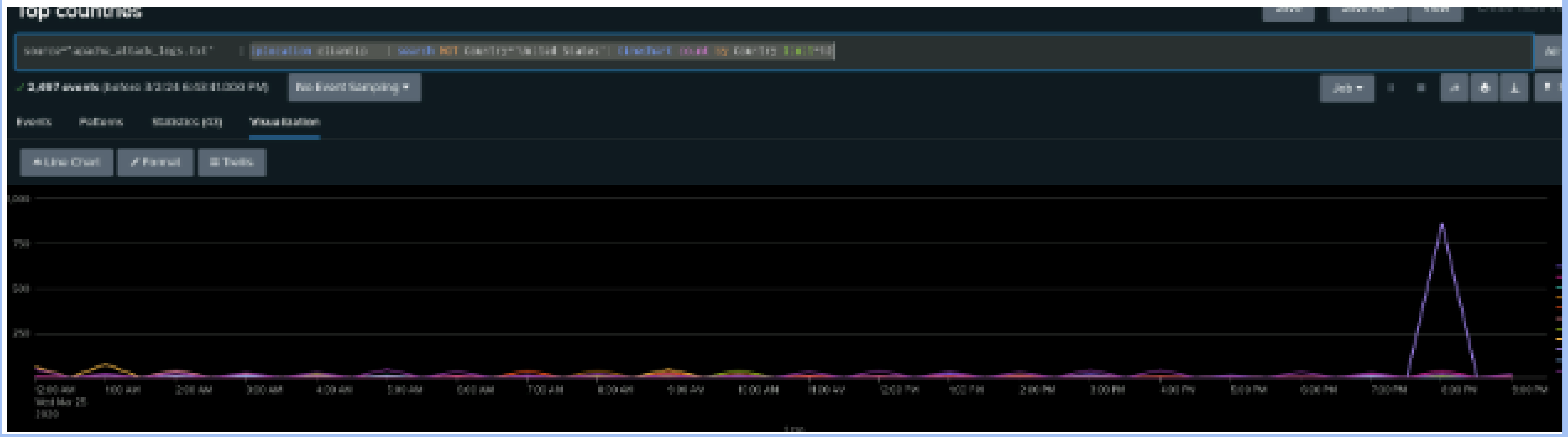
```
source="apache_attack_logs.txt"   | timechart count by method limit=10
```

4,497 events (before 3/2/24 6:40:30.000 PM)



```
source="apache_attack_logs.txt"  | timechart count by referer_domain limit=10
```

4,497 events (before 3/2/24 6:35:08.000 PM)



Top countries

```
source="apache_attack_logs.txt"   | iplocation clientip   | search NOT Country="United States"| timechart count by Country limit=10
```

✓ 3,497 events (before 3/2/24 6:53:41.000 PM)

Summary and Future Mitigations

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

- Based on the URI access and Post request the attacker can potentially be requesting a Brute force attack and its coming from Ukraine.

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

- Setting up account lockout policies , require 2FA (Two factor Authentication) to stop Brute force attacks. Lastly, we recommend continuing utilizing Okta for future monitoring.

Resources

Cybersecurity Specialist. (2021). Cybersecurity fundamentals: Understanding modern information and system protection technology and strategies. Retrieved from https://www.coursera.org

MITRE. (n.d.). MITRE ATT&CK®. Retrieved from https://attack.mitre.org/

Okta. (n.d.). Okta documentation. Retrieved from https://help.okta.com/

OpenAI. (2024). Cybersecurity project discussion on Windows and Apache log analysis. ChatGPT.

OpenAI. (2024). Discussion on the benefits of the Okta Identity Cloud add-on for Splunk. ChatGPT session.

OWASP. (n.d.). OWASP. The Open Web Application Security Project. Retrieved from https://owasp.org/

SANS Institute. (n.d.). Reading Room. SANS Institute. Retrieved from https://www.sans.org/reading-room

Splunk. (n.d.). Splunk documentation. Retrieved from https://docs.splunk.com/

The Apache Software Foundation. (n.d.). Apache HTTP Server Documentation. Apache HTTP Server Project. Retrieved from https://httpd.apache.org/docs/