

# **Defensive Security Project**

**by: Eric, Heather, Daniel, Danielle, Jaycee**

# Table of Contents

---

This document contains the following resources:

01

**Monitoring  
Environment**

02

**Attack Analysis**

03

**Project Summary  
& Future  
Mitigations**

# Monitoring Environment

# Scenario

---

- SOC analyst at a small company called Virtual Space Industries (VSI). Rumors of a competitor company, JobeCorp, potentially launching cyberattacks to disrupt VSI's business have been going around. Our goal is to utilize past logs to develop baselines, create reports, set alerts and make dashboards to identify and mitigate any potential suspicious events that occur on our administrative webpage, Apache web server and Windows operating system.

# Website Monitoring App

# Website Monitoring

---

- **This app was very easy to use and gave a variety of useful information.**
- **The app is modular and only takes a few minutes to set up**
- **The UI dashboard is clean and easy to understand**
- **Monitor multiple URLs and scan past logs for issues**

# Website Monitoring

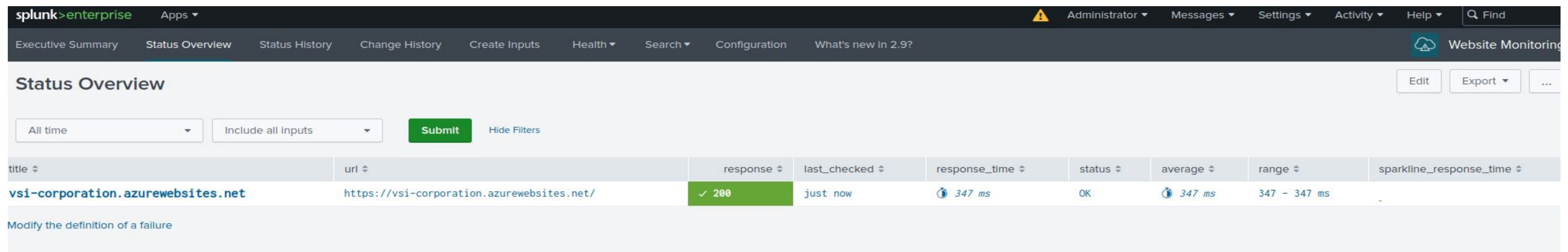
---

- **We chose the add-on application “Website Monitoring” because in March 2020, our adversary JobeCorp, launched an attack to take down our web application.**
- **With the add-on, we now have a dashboard that functions in real time to show us the health and status of our web application.**
- **We can use this to look at performance issues like response times and response codes, detect downtime, and more.**
- **Using this add-on will ensure that if our web application were to go offline again, we would be able to catch it and mitigate the problem quickly.**



# Website Monitoring

- When you click on the “Status Overview” option, it opens a dashboard.
- The dashboard shows the web app URL, HTTP response codes, and response times.
- Below is a normal request that got a 200 response code.



The screenshot shows the Splunk Website Monitoring Status Overview dashboard. The dashboard includes a navigation bar with options like Executive Summary, Status Overview, Status History, Change History, Create Inputs, Health, Search, Configuration, and What's new in 2.9?. Below the navigation bar, there's a section for Status Overview with filters for All time and Include all inputs, a Submit button, and a Hide Filters link. The main content area displays a table with the following data:

title	url	response	last_checked	response_time	status	average	range	sparkline_response_time
vsi-corporation.azurewebsites.net	https://vsi-corporation.azurewebsites.net/	✓ 200	just now	347 ms	OK	347 ms	347 - 347 ms	

Below the table, there is a link to Modify the definition of a failure.



# Website Monitoring

- When the response time is slow.
  - We tried accessing our web application and the response time was slower than average (4415ms vs the previous 347ms).
  - If you click on the red text box, it opens a detailed dashboard.

Status Overview

Edit

Export ▾

...

All time ▾

Include all inputs ▾

Submit

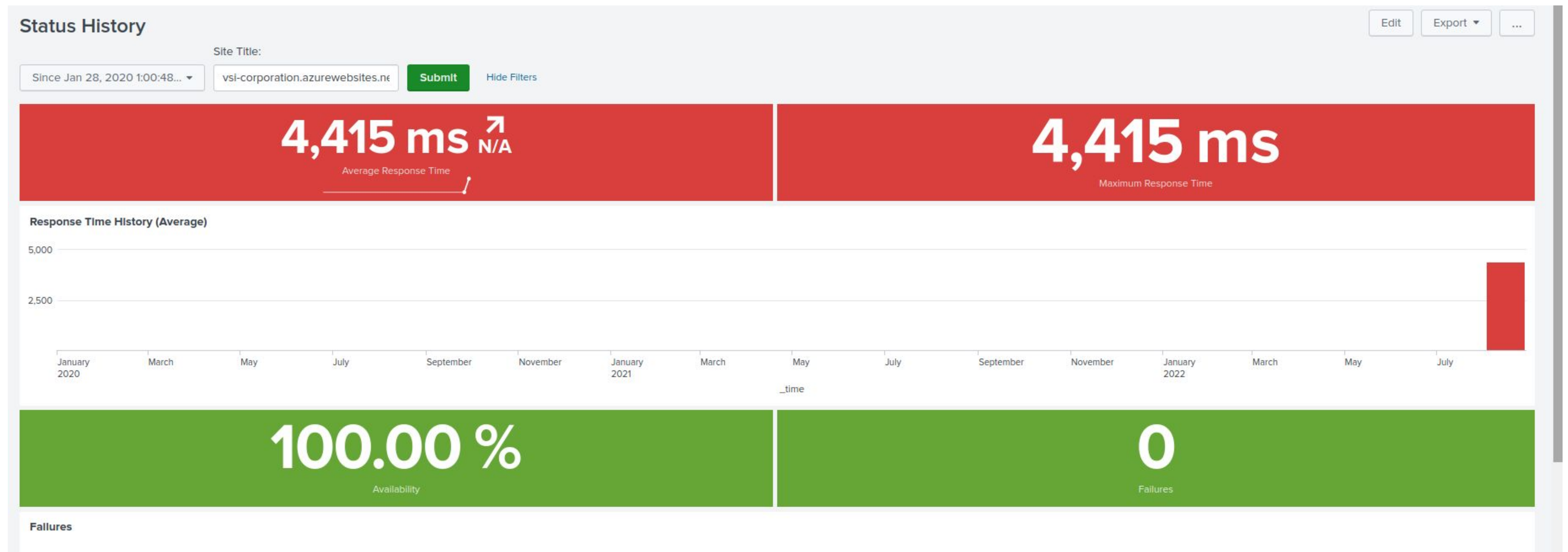
Hide Filters

title ⬆ ⬆	url ⬆ ⬆	response ⬆ ⬆	last_checked ⬆ ⬆	response_time ⬆ ⬆	status ⬆ ⬆	average ⬆ ⬆	range ⬆ ⬆	sparkline_response_time ⬆ ⬆
vsi-corporation.azurewebsites.net	https://vsi-corporation.azurewebsites.net/	✓ 200	just now	⚠ 4415 ms	Failed	⚠ 4415 ms	4415 - 4415 ms	-

Modify the definition of a failure

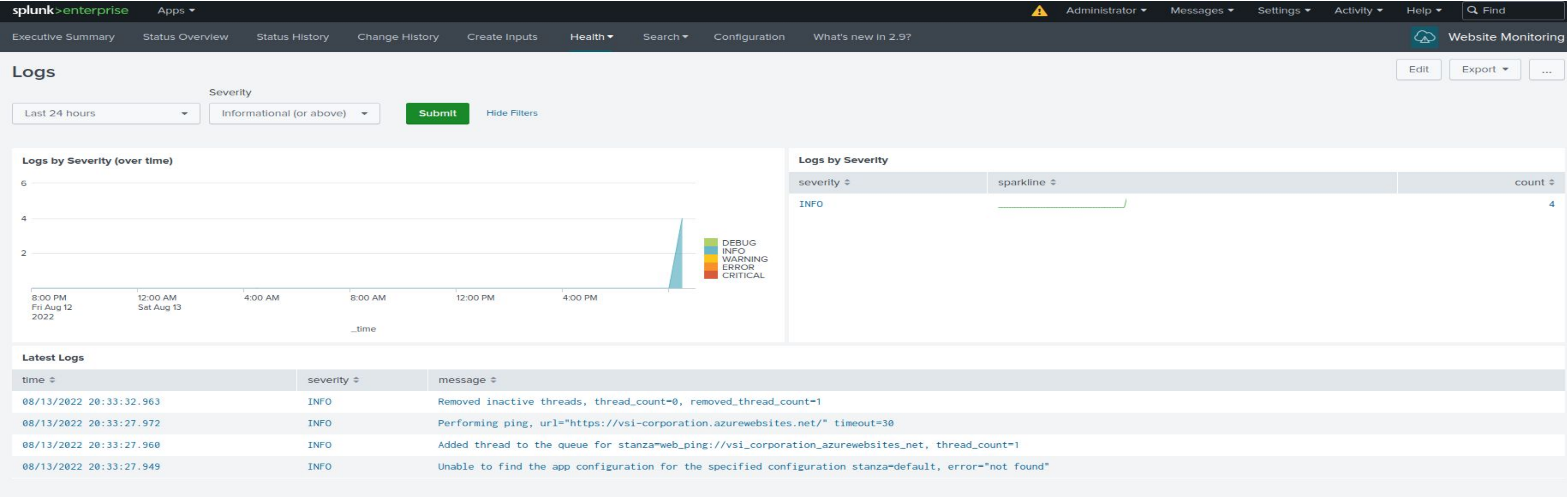
# Website Monitoring

- The detailed dashboard shows a timeline for average and max response times, availability, and failures.



# Website Monitoring

- The below logs show events captured and level of severity from <https://vsi-corporation.azurewebsites.net/> by the Website Monitoring Application installed on Splunk





# Logs Analyzed

---

1

## Windows Logs

Windows Logs contain information as below:

- Account User types
- Account User Activity(Signatures)
- Severity level of security activity
- Windows Activity(Success/Failure)

By analyzing this logs, we could identify suspicious user activity patterns, set-up alerts that would promptly notify the SOC team.

2

## Apache Logs

Apache HTTP server logs contain information as below:

- Logs request methods Get and Post
- Which resources were accessed
- When they were accessed
- who accessed them

By analyzing this log, we could identify Request being made to the server. What was accessed, who did it and when it happened, allowing us to set-up alerts that would promptly notify the SOC team of suspicious activity.

# Windows Logs

# Reports—Windows

---

Designed the following Reports:

Report Name	Report Description
VSI Signatures and Signature IDs	Shows the ID number associated with the specific signature for Windows activity
Severity of Windows logs being viewed	Gives a quick view of severity level for Windows logs being viewed
VSI Success and Failure Activities on the Server	This report shows if there is a suspicious level of failed activities on the VSI Server



# Images of Reports—Windows

VSI Signatures and Signature IDs

All time

✓ 15 events (before 8/12/22 2:41:35.000 AM)

15 results50 per page

signature

signature\_id

A user account was deleted4726

A user account was created4720

A computer account was deleted4743

An account was successfully logged on4624

Special privileges assigned to new logon4672

An attempt was made to reset an accounts password4724

System security access was granted to an account4717

A privileged service was called4673

A logon was attempted using explicit credentials4648

A user account was locked out4740

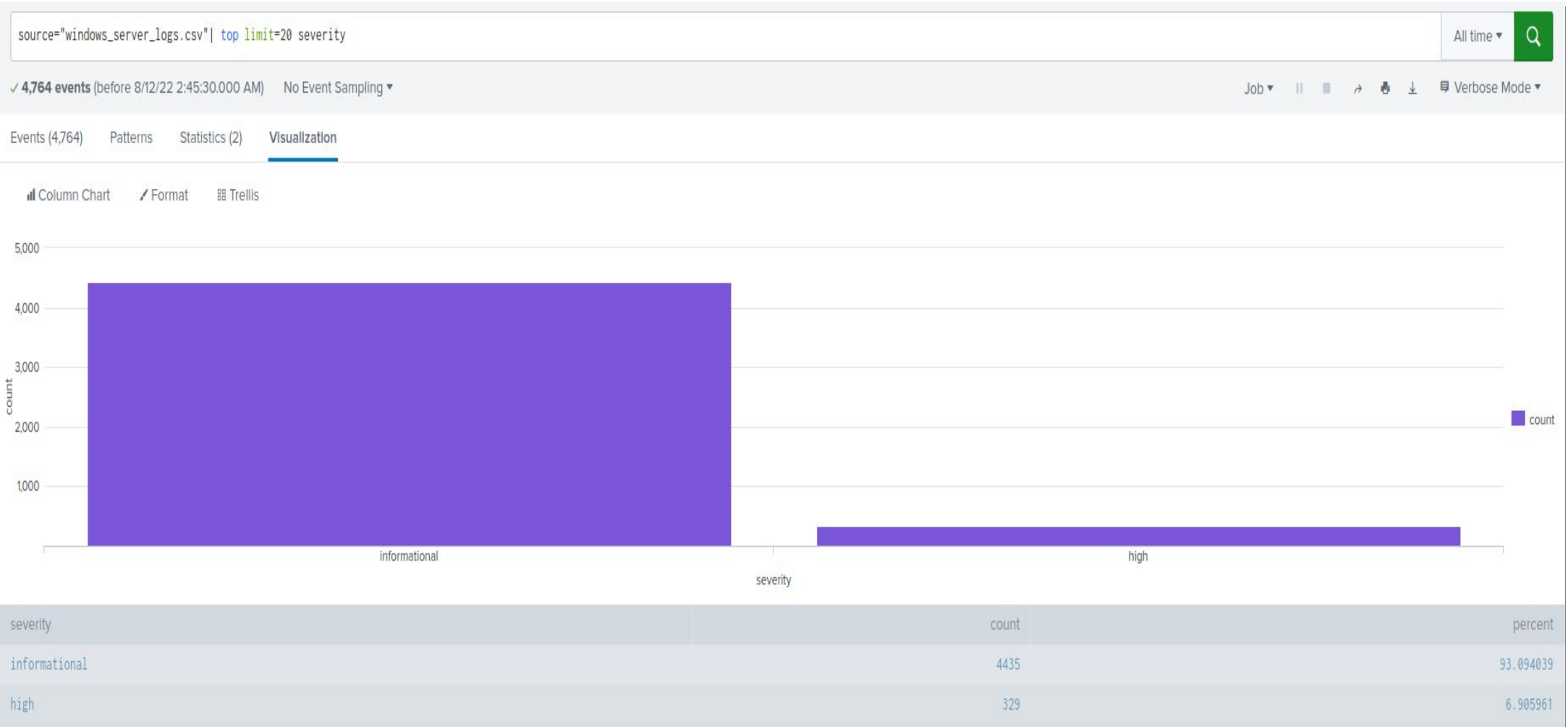
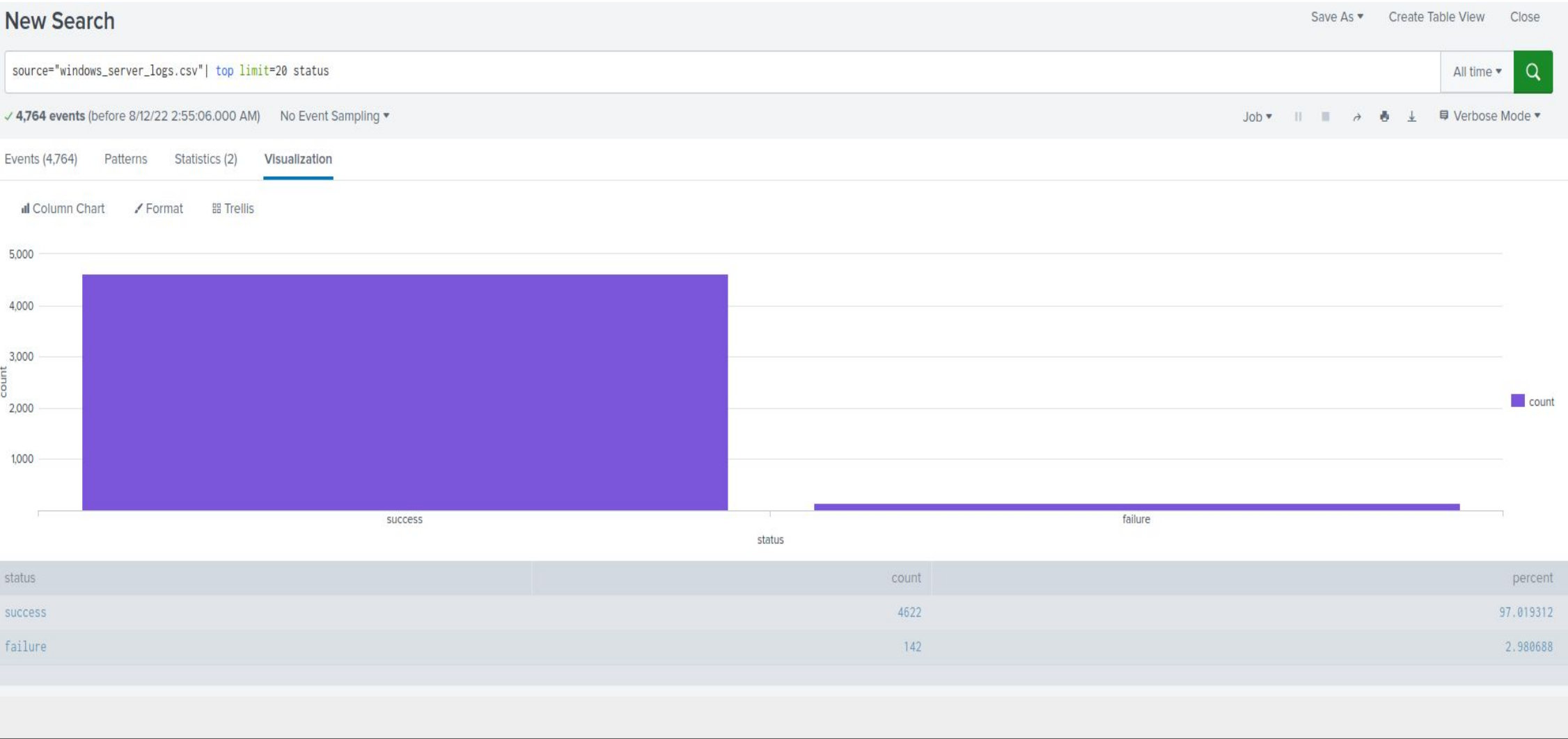
Domain Policy was changed4739

A user account was changed4738

A process has exited4689

The audit log was cleared1102

System security access was removed from an account4718



# Alerts—Windows

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	This alerts notifies SOC team if there are certain numbers of failed attempt in an hour	7	If 15 or more per hour

**JUSTIFICATION:** If we log failed Windows activity, we can look out for unusually high levels. This would alert us to attempts being made by bad actors to infiltrate our systems. The baseline/average was about 7 failed activities per hour. To decrease the number of false positives, while still catching unusual activity, we set our alert threshold to 15 or more failed activities per hour.

# Alerts—Windows

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of Signatures with Successful Logons	This alert notifies the SOC team if there is a certain number of signatures with successful logons within an hour.	15	Greater than 35

**JUSTIFICATION:** The reason we look at successful logons per hour is to make sure there are not a massive increase or decrease in our baseline. We set our baseline to about 15 successful logons per hour from studying typical trends. To avoid too many false positives but still capture an attack, we set to be alerted whenever there were 35 or more successful logins.

# Alerts—Windows

---

Designed the following alerts:

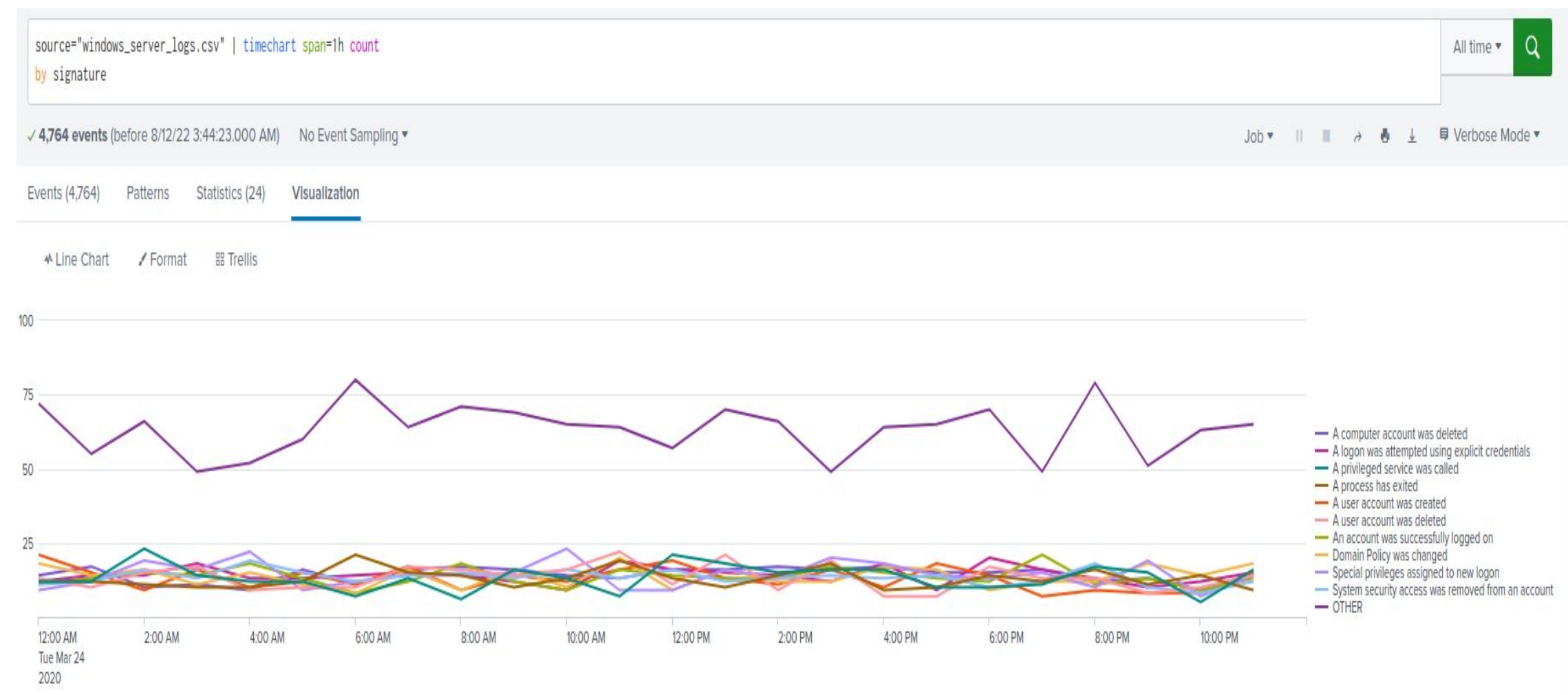
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted User Accounts	This alerts notifies SOC team if there are certain numbers of deleted accounts in an hour	16	Greater than 30.

**JUSTIFICATION:** Logging deleted user accounts can show us unusual activity like mass amounts of deleted users within one hour or lack of activity. The alert baseline was 16. To avoid too many false positives but still capture a mass deleted user spree, we set our alert threshold to greater than 30 deleted accounts in one hour.

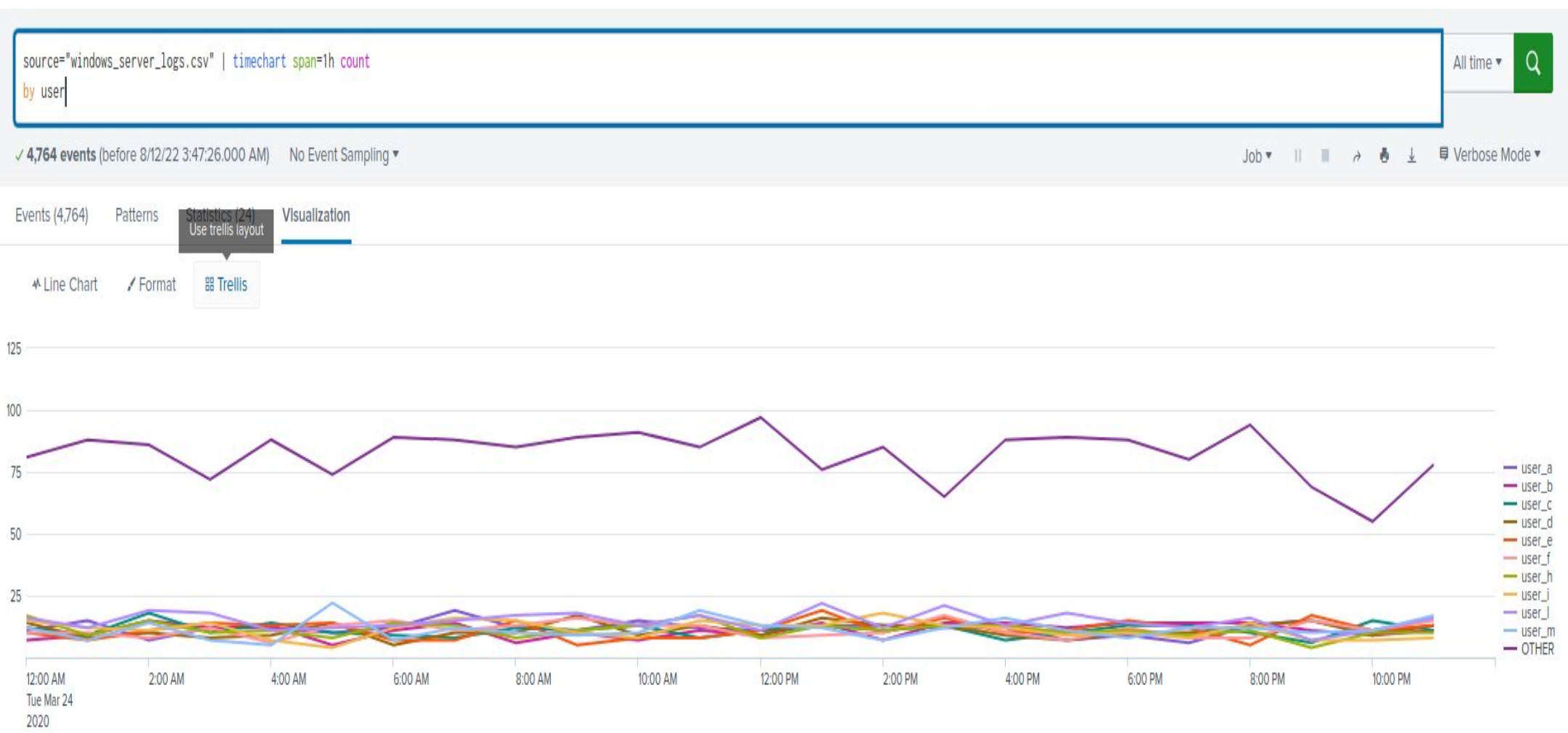


# Dashboards—Windows

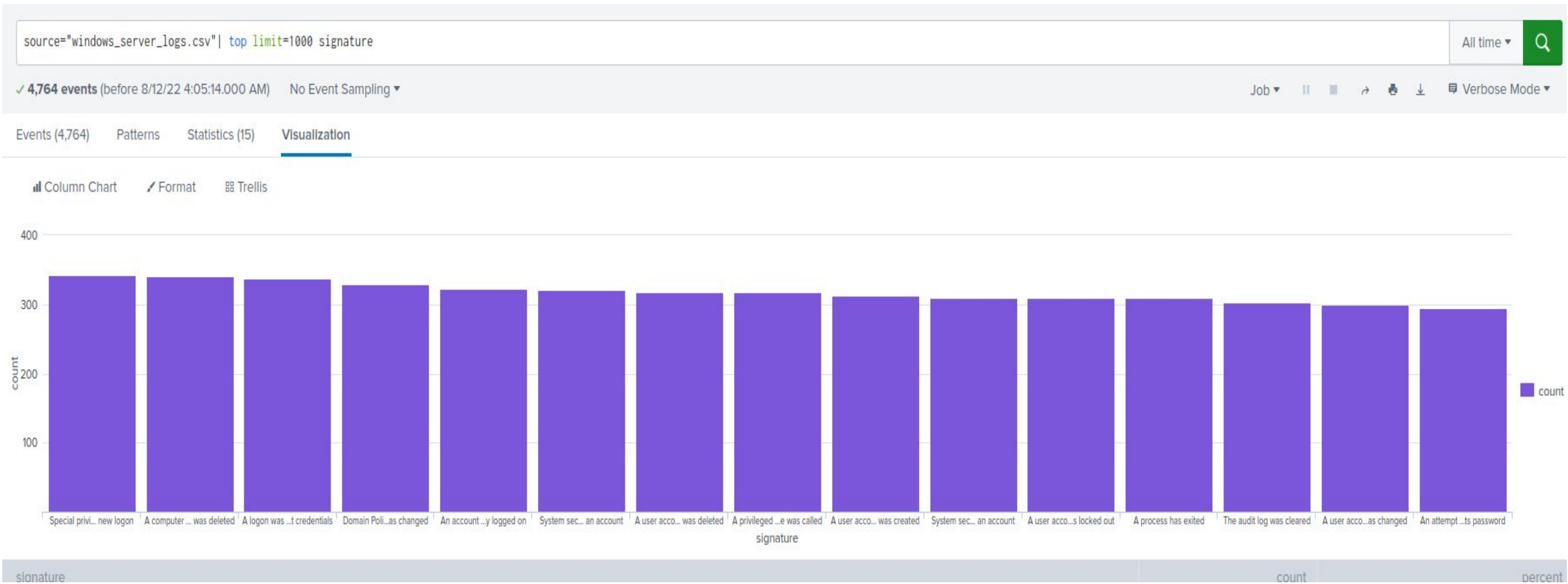
Different Signature Field Values Over Time



Displays the Different User Field Values Over Time

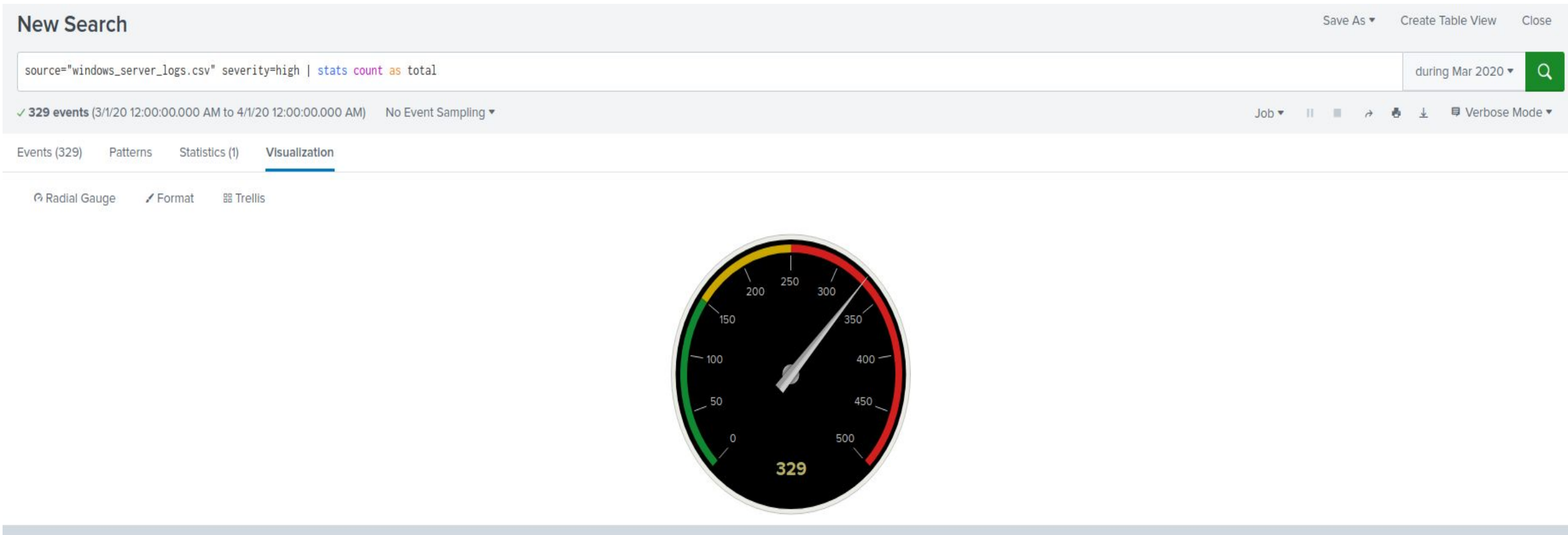


Count of Different Signatures

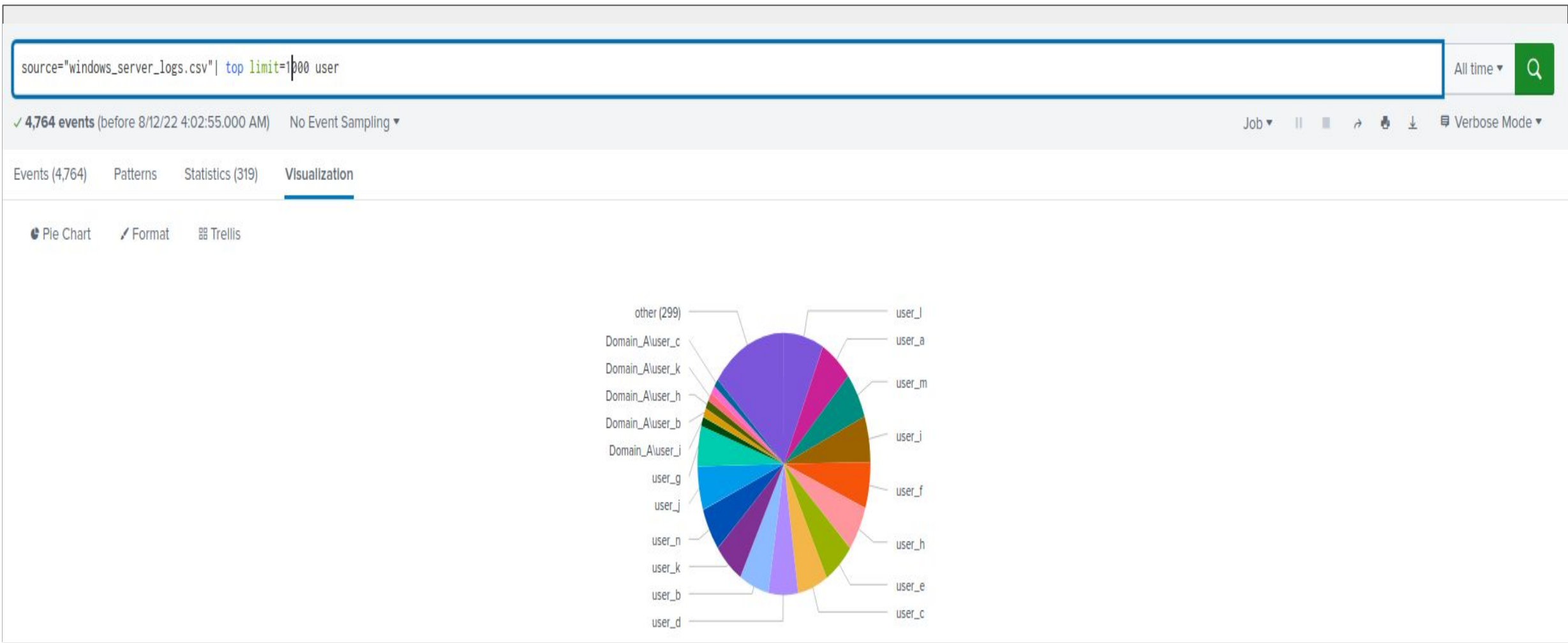


# Dashboards—Windows

## Number of High Severity Events



## Illustrates the count of different users





# Apache Logs

# Reports—Apache

---

Designed the following reports:

Report Name	Report Description
HTTP Methods Count	A table that shows the count and percentage of the total for each HTTP method (GET, POST, HEAD, OPTIONS). We can analyze this for suspicious changes to the percentages of methods.
Top 10 Referrer Domains	A table that shows the count and percentage of the total for the top 10 referrer domains. We can analyze this for suspicious changes in the top 10 domains.
HTTP Response Code Counts	A table that shows the count of different HTTP response codes. We can analyze this for suspicious levels of HTTP responses.

# Images of Reports—Apache

HTTP methods Count Table

All time

✓ 10,000 events (before 8/16/22 12:38:39.000 AM)

Edit

More Info

Add to Dashboard

Job

||

4 results20 per page

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

Top 10 Referer Domains

All time

✓ 4,497 events (before 8/16/22 12:40:20.000 AM)

Edit

More Info

Add to Dashboard

Job

||

10 results20 per page

referer_domain	count	percent
http://www.semicomplete.com	764	49.22680
http://semicomplete.com	572	36.85567
http://www.google.com	37	2.38402
https://www.google.com	25	1.61082
http://stackoverflow.com	15	0.96649
https://www.google.com.br	6	0.38659
https://www.google.co.uk	6	0.38659
http://tuxradar.com	6	0.38659
http://logstash.net	6	0.38659
http://www.google.de	5	0.32216

HTTP Response Code Counts

All time

✓ 10,000 events (before 8/16/22 12:43:18.000 AM)

Edit

More Info

Add to Dashboard

Job

||

8 results20 per page

status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

# Alerts—Apache

---

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity From Any Country besides the US	This alert notifies SOC team if there is certain amount of activity from other countries besides the US in an hour.	75	Greater than 100.

**JUSTIFICATION:** We want to be alerted to suspicious activity coming from outside the US. The baseline/average activity during normal business was about 75 non-US clients during 1 hour. To decrease the number of false positives to avoid alert fatigue, but still be notified in the event of an attack, we set our threshold to greater than 100 Non-US clients per hour.

# Alerts—Apache

---

Designed the following alerts:

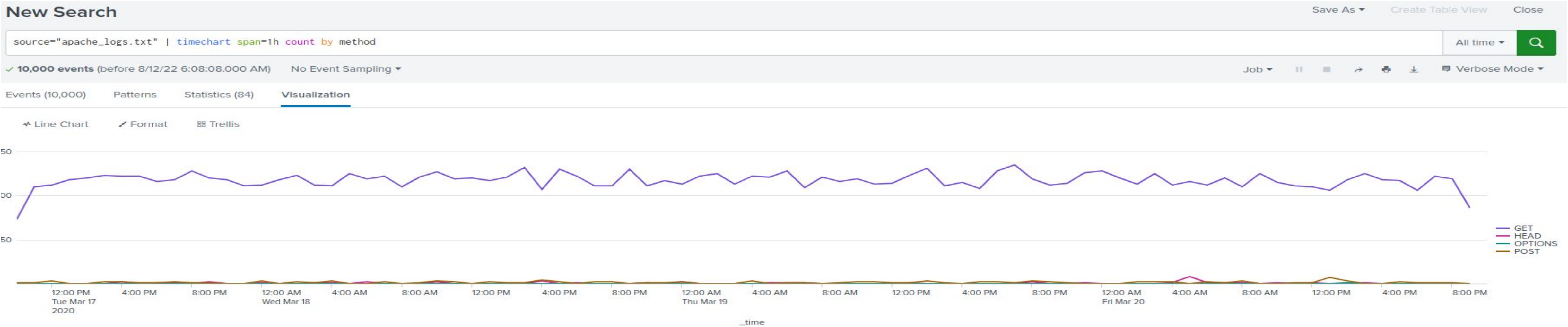
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Number of HTTP Post method by hour	To alert SOC when a higher than usual amount of HTTP POST method requests are being performed in an hour	3	>10

**JUSTIFICATION:** When looking over a 3 day period to find a baseline the average amount of HTTP Post method requests, we found that in any given hour you might see as little as 0 requests to as many as 7. To avoid false positives and alert fatigue we set our baseline at 3 and determined a threshold of >10 would be appropriate.

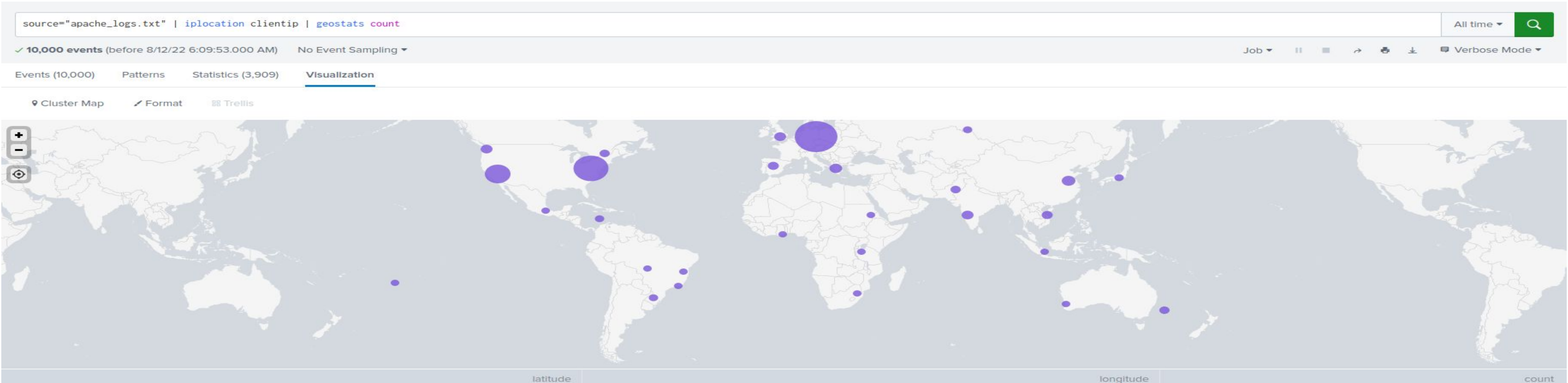


# Dashboards—Apache

HTTP method field values over time



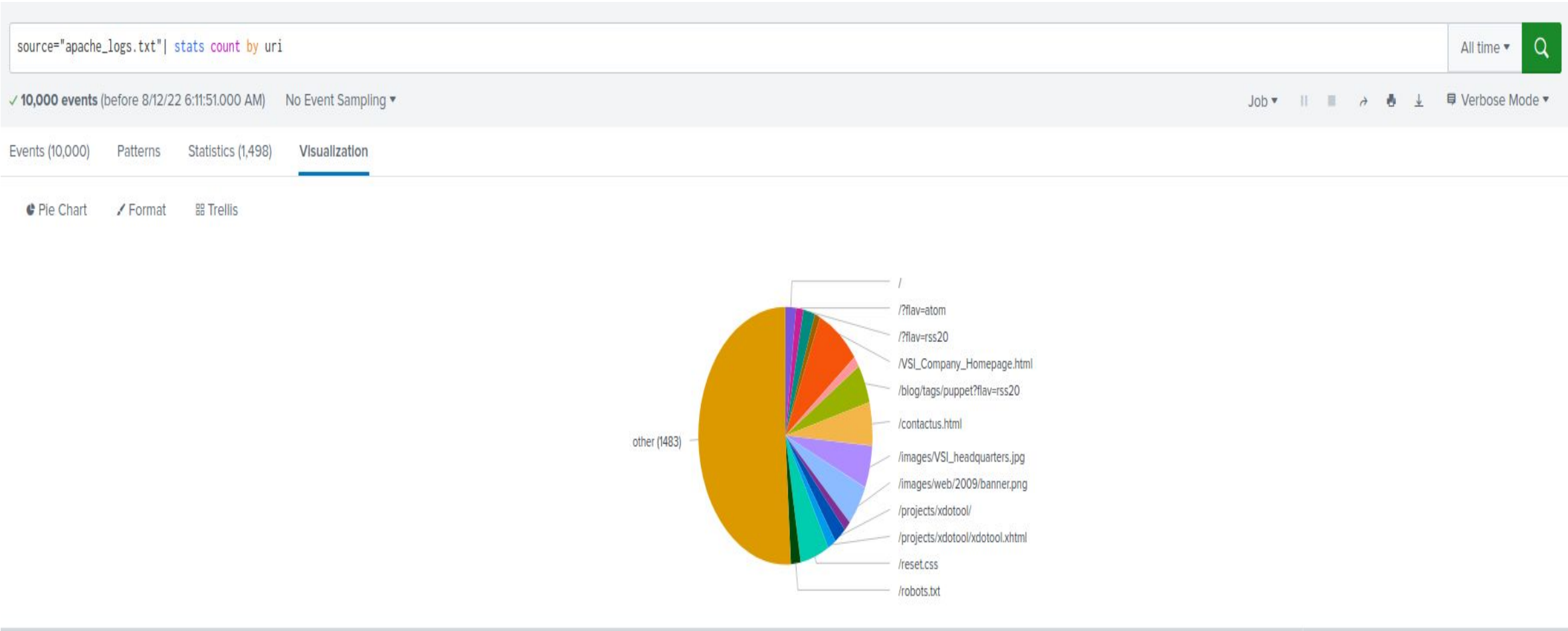
Geographical map showing the location based on the “clientip” field



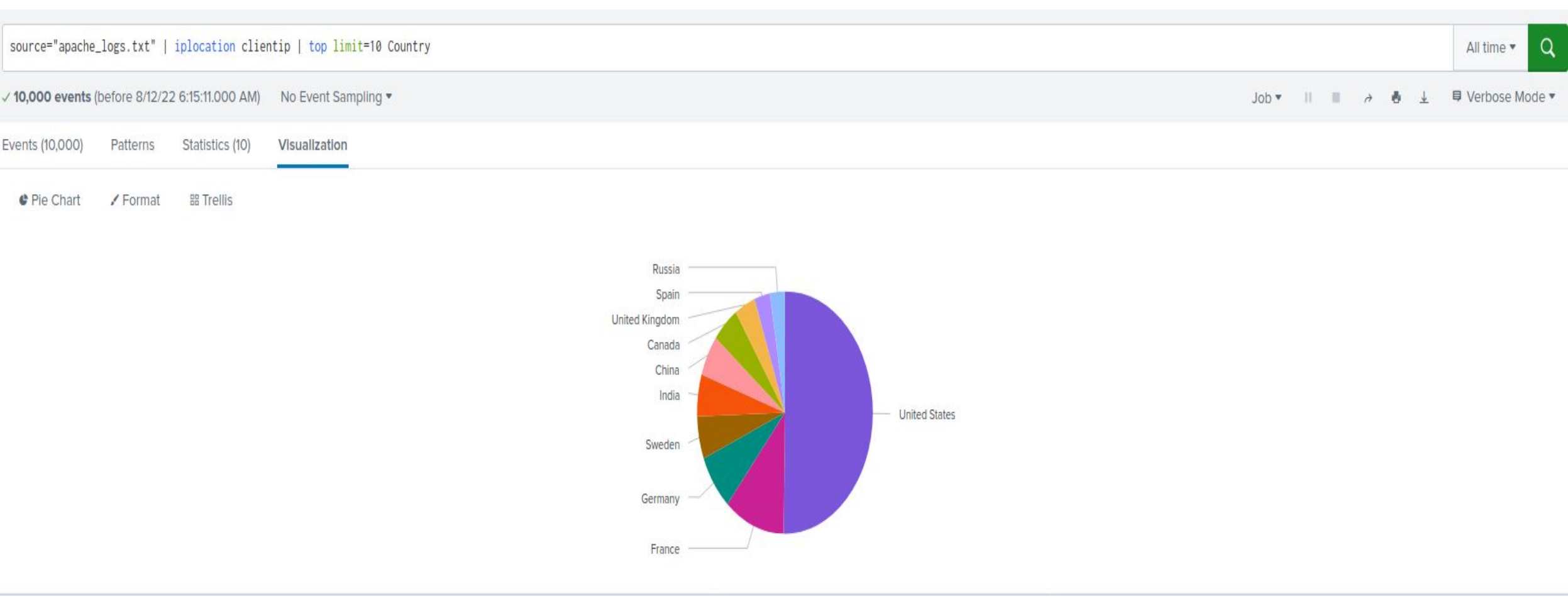


# Dashboards—Apache

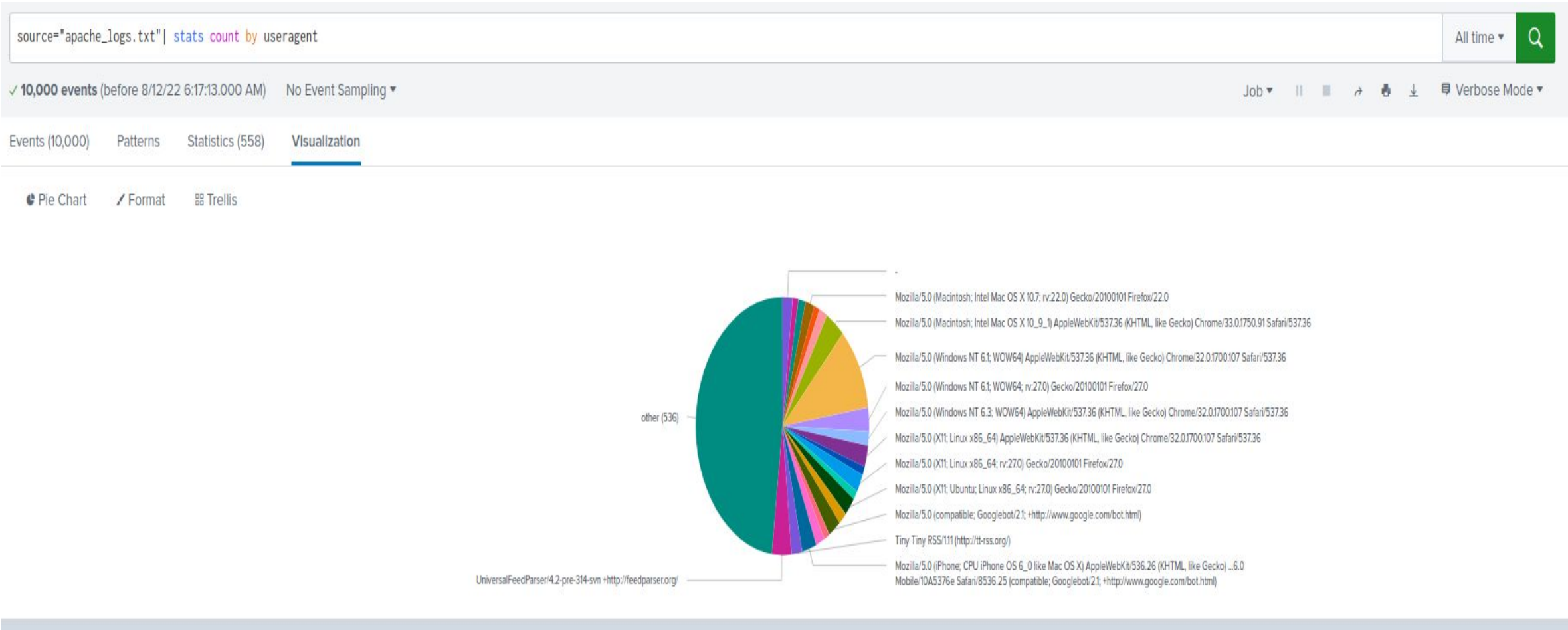
## Number of different URIs



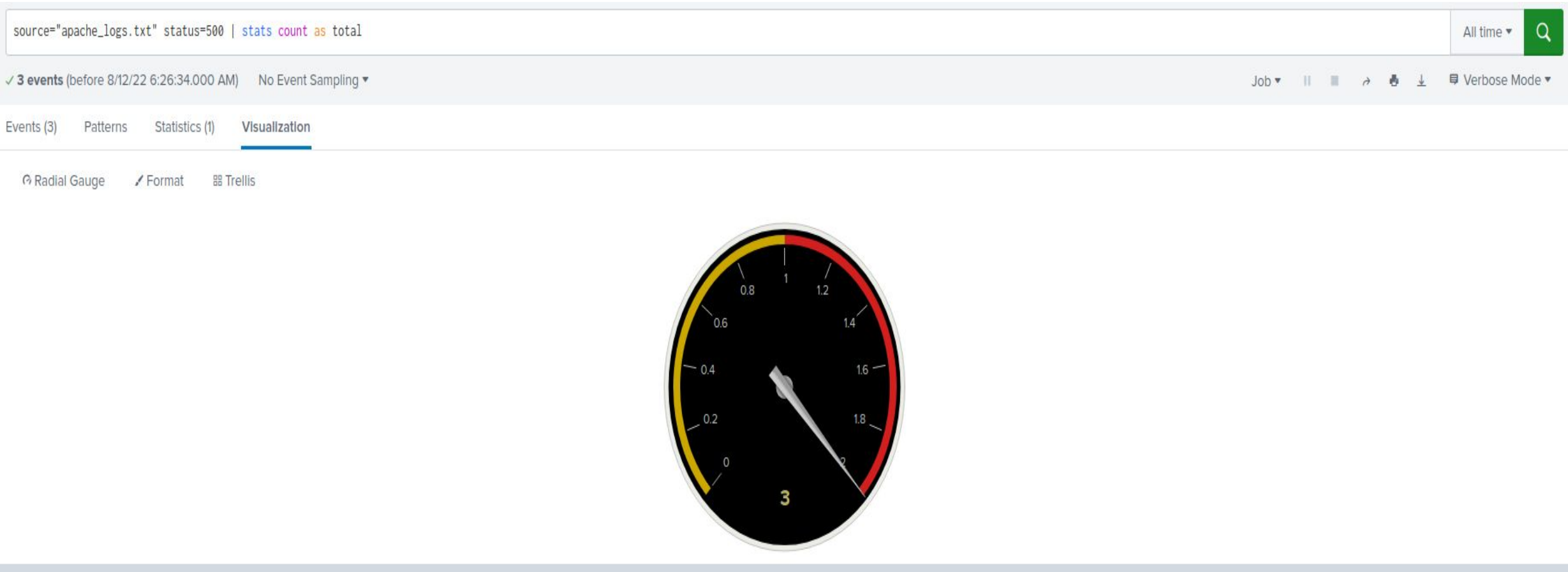
## Displays the count of the top 10 countries that appear in the log



## Count of different user agents



## By Response Code 500



# Attack Analysis

# Attack Summary—Windows

---

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

- On the **Severity Report**, we noticed the informational level severity alerts percentage dropped from 93% at our normal traffic to 79.8% during the attack. More importantly, the high level severity percentage rose from 7% during normal traffic to 20.2% during the attack. This is a significant increase in high severity levels.
- On the **Failed Activities Report**, we noticed that there was a decrease in failed activities during the attack. Before the attack, we had 2.98% failed activities on our Windows server. During the attack, we had 1.56% failed activities on our Windows server. This could be because their attack was successful and created more successful activities. However, it wasn't a significant change in percentage. The traffic was increased during the attack (5856 successes during the attack vs 4622 successes during normal times), which is more significant of a change.



# Attack Summary—Windows

---

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

- The **Failed Activity Alert** was triggered because during the attack there were 35 failed events during the hour between 8am and 9am. Our alert was set to trigger for 15 or more failed activities. Our threshold was correct and we wouldn't make changes to it.
- The **Successful Logins Alert** was not triggered. We set our alert to notify us for unusually high levels of successful logins (35 or more). However, the unusual activity was that during the hours between 9am and 10am, there was no successful logins. Also, between 11am and 12pm as well as 12pm to 1pm, there were only 4 successful logins. We should have set a lower limit to notify us if there were less than 7 successful logins during an hour. This would help us catch a system outage.
- The **Deleted Accounts Alert** had an unusually low amount of deleted accounts between 9am and 12pm. We would change our alert to also have a floor to alert us, for example, when deleted accounts is less than 5, send an alert. This would show if the servers were offline.

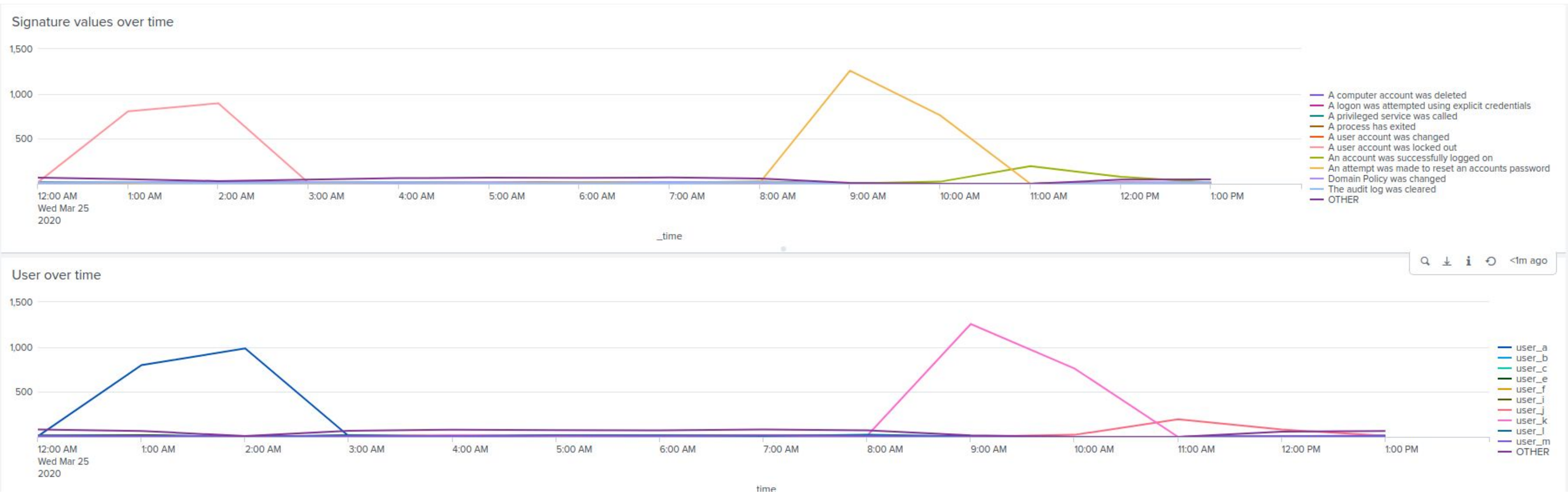
# Attack Summary—Windows

---

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

- User A (984 activities in one hour), User J (196 activities/hr), and User K (1256 activities/hr) all had unusually high levels of activity during the attack on our Windows server.
- There were also 3 particular activity signatures that were found in unusually high levels during the attack period: a user account was locked out (1811 times), an attempt was made to reset an accounts password (2128 times), and an account was successfully logged in (432 times).
- After analyzing the time stamps of the user activity and the activity signatures, we concluded User A was probably responsible for the locked out accounts, User K was responsible for the reset passwords, and User J was responsible for the successful logins (see screenshots on next slide).

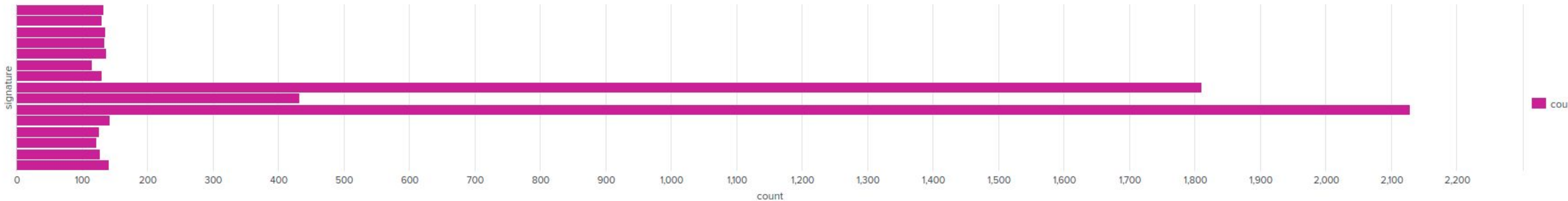
# Screenshots of Attack Logs



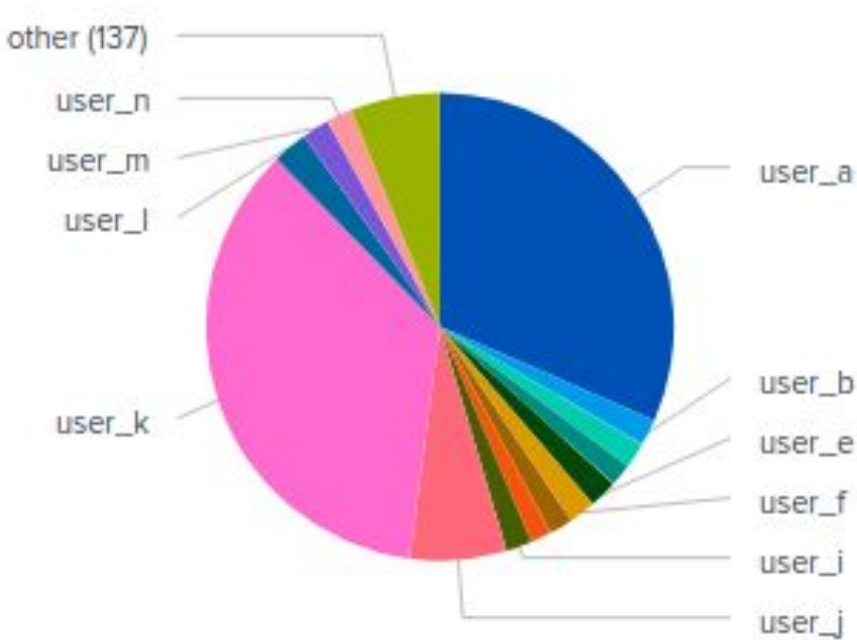


# Screenshots of Attack Logs

Signature Counts



User Count



High Severity Gauge



# Attack Summary—Apache

---

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

- On the **HTTP Methods Report**, there was a significant drop in GET (5pm-7pm) methods (98.51% to 70.20% during the attack) and the POST(7pm-9pm) increased substantially (1.06% to 29.44% during the attack).
- On the **Top 10 Referers Domain Report**, all the referrer domain counts dropped by about 75%.
- On the **HTTP Response Code Report**, the number of response code 200 dropped about 8%. Response code 404 increased significantly (213 preattack to 679 during the attack).

# Attack Summary—Apache

---

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

- For the **Non-US client Alert**, there was 939 Non-US client requests from the hour of 8pm to 9pm. This was extremely high compared to our baseline of 75 per hour from normal business. Our alert threshold of over 100 per hour was triggered and we were alerted to the attack. We could have increased our threshold slightly to about 135 to decrease the number of false positives.
- The **HTTP POST Alert** was also triggered. At 8pm there was a large spike in HTTP POST activity. We had 1296 HTTP POST activities during the attack. Our threshold of greater than 10 was definitely met and our alert was triggered. We wouldn't change the threshold on this alert.

# Attack Summary—Apache

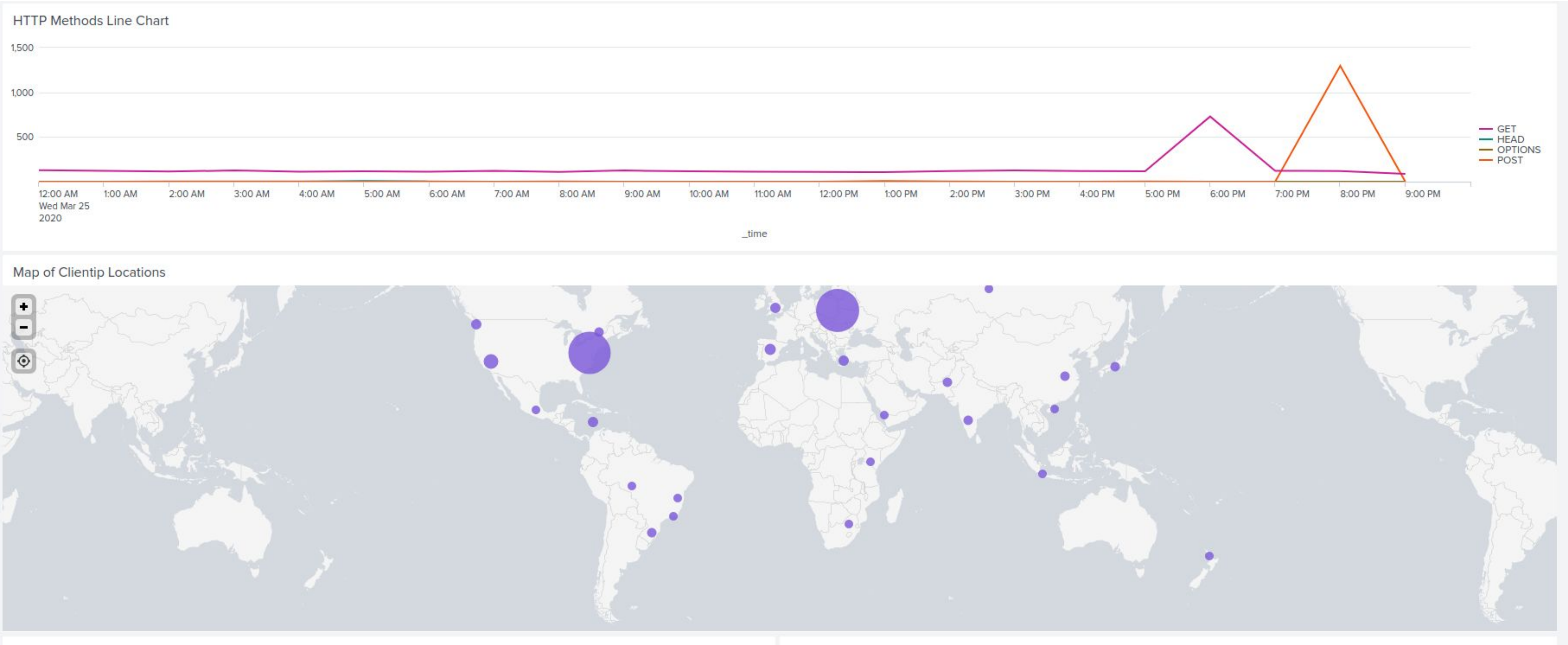
---

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

- Our Apache Web Server dashboard showed us suspicious activity of HTTP Methods over a time chart. There were two large spikes in GET method and POST method around 5pm and 7pm, respectively. This shows the attack of bad actors trying to post to our web server.
- The cluster map on our dashboard showed a large amount of traffic coming from Ukraine. We were able to zoom in to see that most of the traffic was coming specifically from Kiev, Ukraine and Kharkiv, Ukraine. This is where our attackers IP addresses were from.
- We noticed that the top 2 URI's were /VSI\_Account\_logon.php and /files/logstash-1.3.2-monolithic.jar, which both increased substantially during the attack. The most hit was the the /VSI\_Account\_logon.php page. This shows that they were trying to log in to our web server.



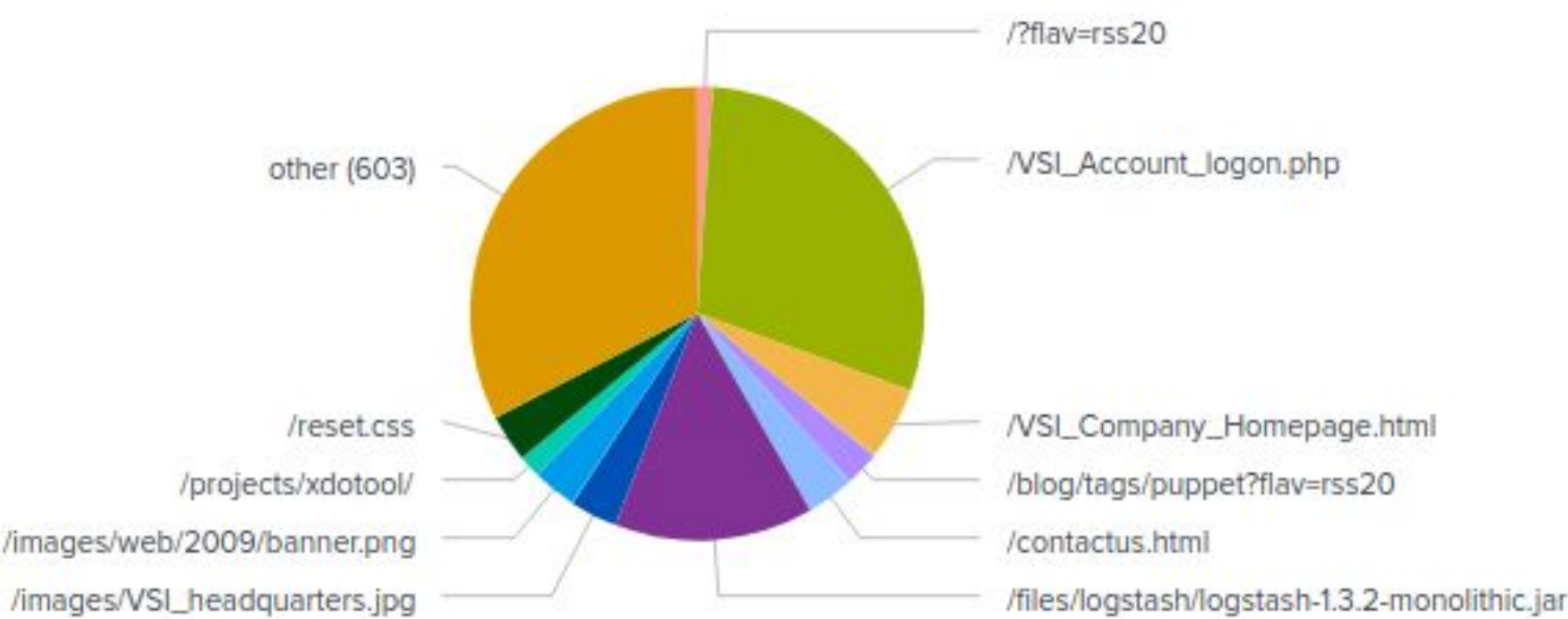
# Screenshots of Attack Logs



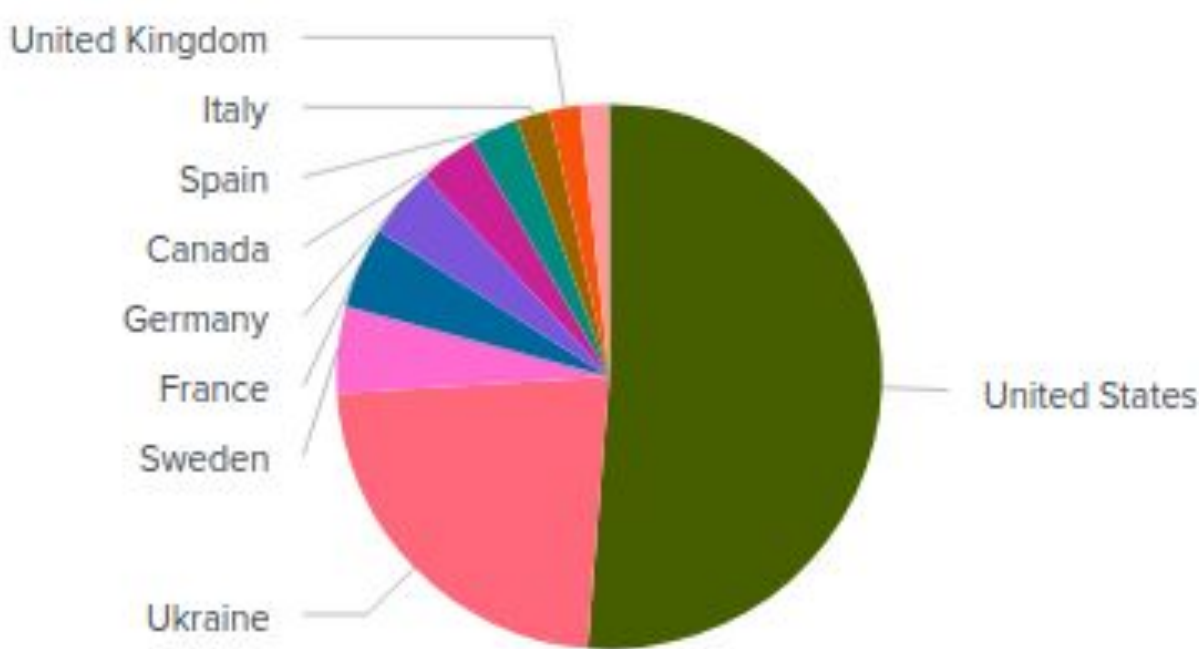


# Screenshots of Attack Logs

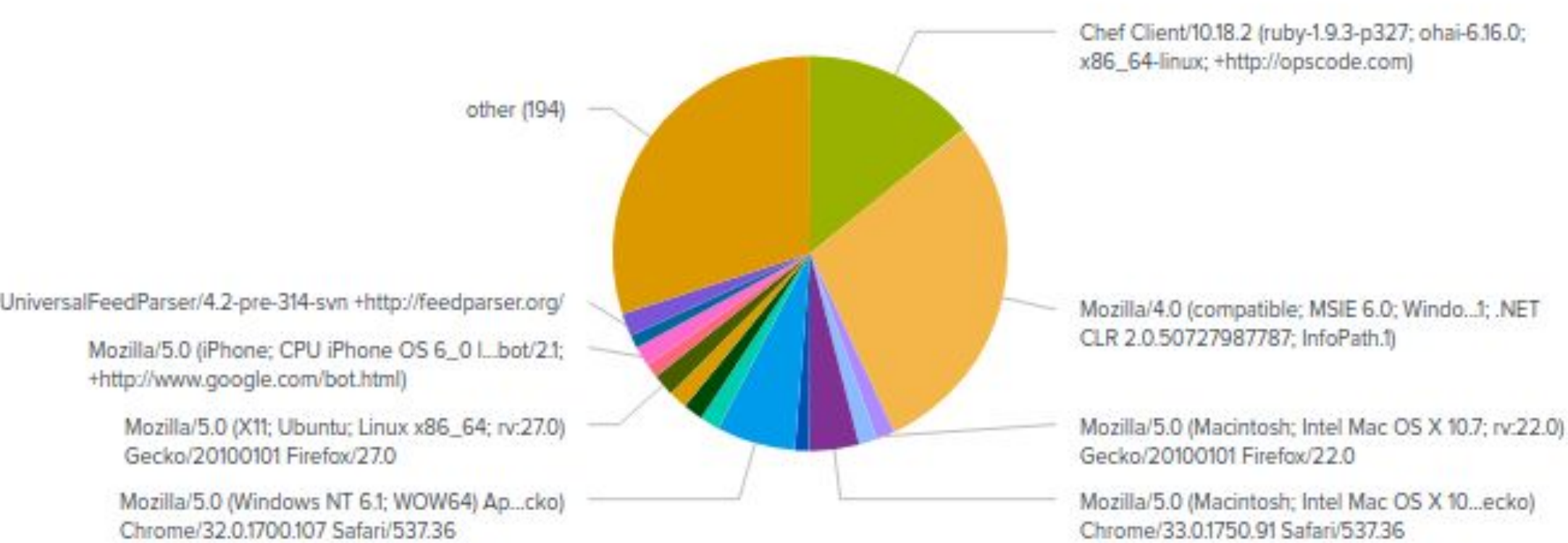
Different URI Counts



Top 10 Country IPs



Useragent Counts



HTTP Status 500 Gauge



# Summary and Future Mitigations

# Project 3 Summary

---

- What were your overall findings from the attack that took place?
- ❖ On the Windows server, there were 3 specific users (User A, User K, and User J) who were mainly responsible for the attack on our Windows server. There were unusually high numbers of accounts being locked out, attempts to reset passwords, and successful logins associated with these users' timestamps to activity.
- ❖ On the Apache web server, there were unusually high numbers of GET and POST requests. Most of the activity during the attack was coming from Ukraine. The attackers were trying to access a login page, which shows they were trying to gain access to our web server/app.
  - To protect VSI from future attacks, what future mitigations would you recommend?
- ❖ Better monitoring through the use of a SIEM or SOAR.
- ❖ Adjust thresholds for alerts to better capture attack activity.
  - Add in floor and ceiling thresholds. You want to capture excessive traffic along with lack of traffic.
- ❖ Block IPs that have unusually high traffic.