Defensive Security Project

by: Kelly Hale, Rebecca Gonzalez, & Sam Heaps

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- In this scenario, our group will analyze reports indicative of attacks made against VSI’s Windows and Apache servers. These servers are crucial to VSI’s everyday business practices and need more secure protection against threats.
- Using Splunk, our team will develop a Dashboard to showcase numerous different alerts, reports, and graphs developed all as a part of our monitoring solution for VSI.
- Through the analysis of several report packets, our team is successful in identifying several instances of attacks launched against the network.
- Analyzing these threats and creating the proper alerts to trigger for them will help protect VSI in the future. Building a Dashboard will allow our team to demonstrate how graphical analysis can provide better visualization for assessing threats and how they specifically target areas of the network.
- This report will analyze several logs containing proof of malicious acts launched against VSI’s network and will demonstrate the tools and techniques necessary for identifying and neutralizing threats against their servers.

WhoisXML and Website Monitoring

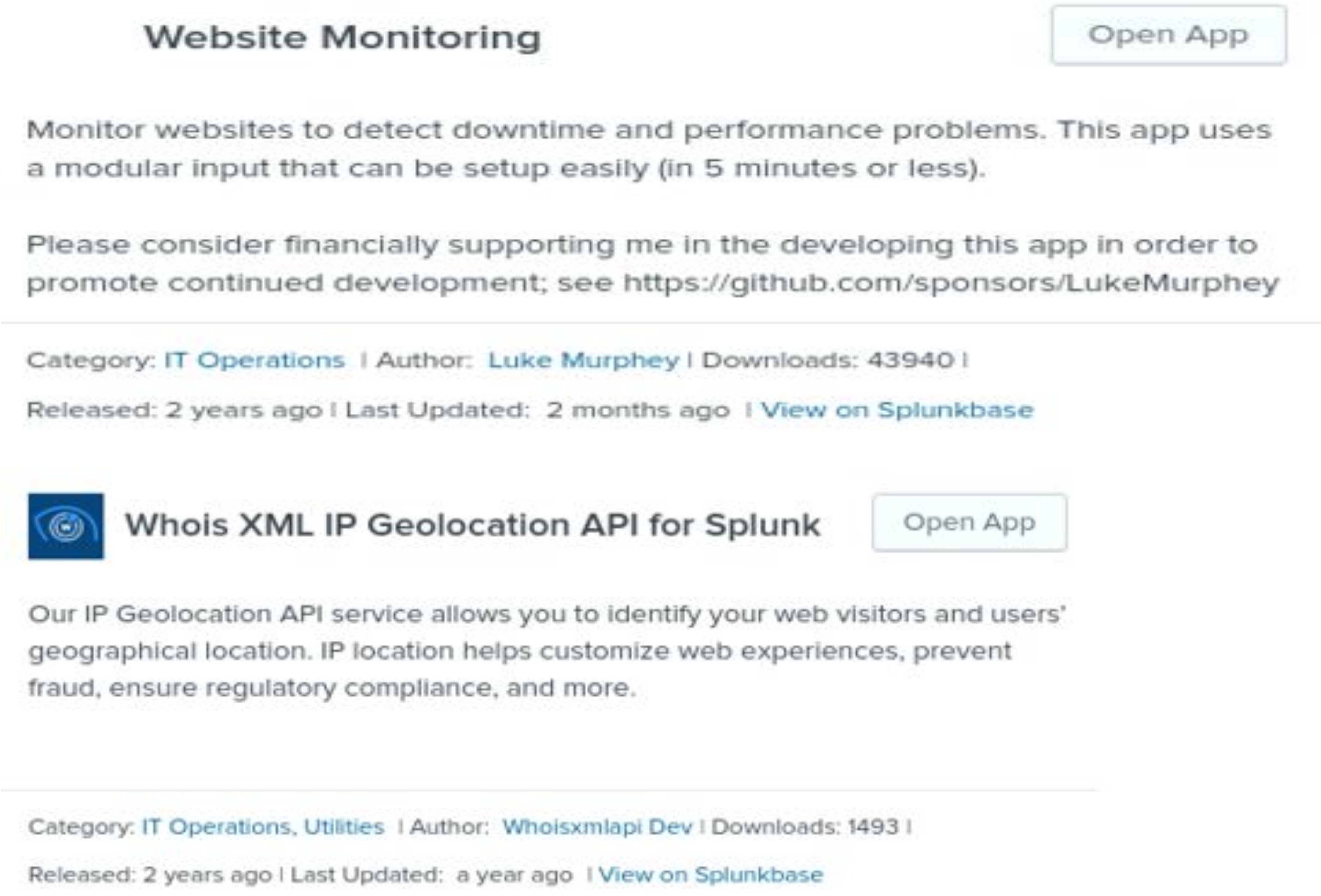
Whois XML and Website Monitoring

For our monitoring solution, our group chose to incorporate two addons to help provide better malicious activity monitoring for VSI’s network. The addons Web Monitoring and WHOis XML were chosen to help better identify threats against the network in specific ways.

Website Monitoring is a free Splunk addon that can be used to better analyze key network performance indicators like upload speeds, latency, and site uptime. For our purposes, we will implement Website Monitoring to more accurately assess site downtimes. This is crucial for VSI in that site downtime or other performance issues directly impacts the customer experience in a variety of negative ways, and should be properly scanned and analyzed as thoroughly as possible.

WHOis XML can be used to better identify IP addresses by providing geographical locations for them.

Website Monitoring and Whois XML for Splunk



Website Monitoring

Monitor websites to detect downtime and performance problems. This app uses a modular input that can be setup easily (in 5 minutes or less).

Please consider financially supporting me in the developing this app in order to promote continued development; see https://github.com/sponsors/LukeMurphey

Category: IT Operations | Author: Luke Murphey | Downloads: 43940 |

Released: 2 years ago | Last Updated: 2 months ago | View on Splunkbase

Whois XML IP Geolocation API for Splunk

Our IP Geolocation API service allows you to identify your web visitors and users' geographical location. IP location helps customize web experiences, prevent fraud, ensure regulatory compliance, and more.

Category: IT Operations, Utilities | Author: Whoisxmlapi Dev | Downloads: 1493 |

Released: 2 years ago | Last Updated: a year ago | View on Splunkbase

Logs Analyzed

1

Windows Logs

Our team discovered numerous instances of failed activities on the network. We also discovered an unusual amount of successful logins.

User accounts being locked out and unsuccessful password reset attempts present a clear threat against VSI.

After successfully gathering and analyzing this data, our team can use Splunk to visualize these occurrences.

2

Apache Logs

These logs provide further proof of attacks made against the network.

We have discovered more concrete details on the perpetrator of this attack based on data retrieved. Through Splunk, we can provide further visualized details on the attacks performed against the site.

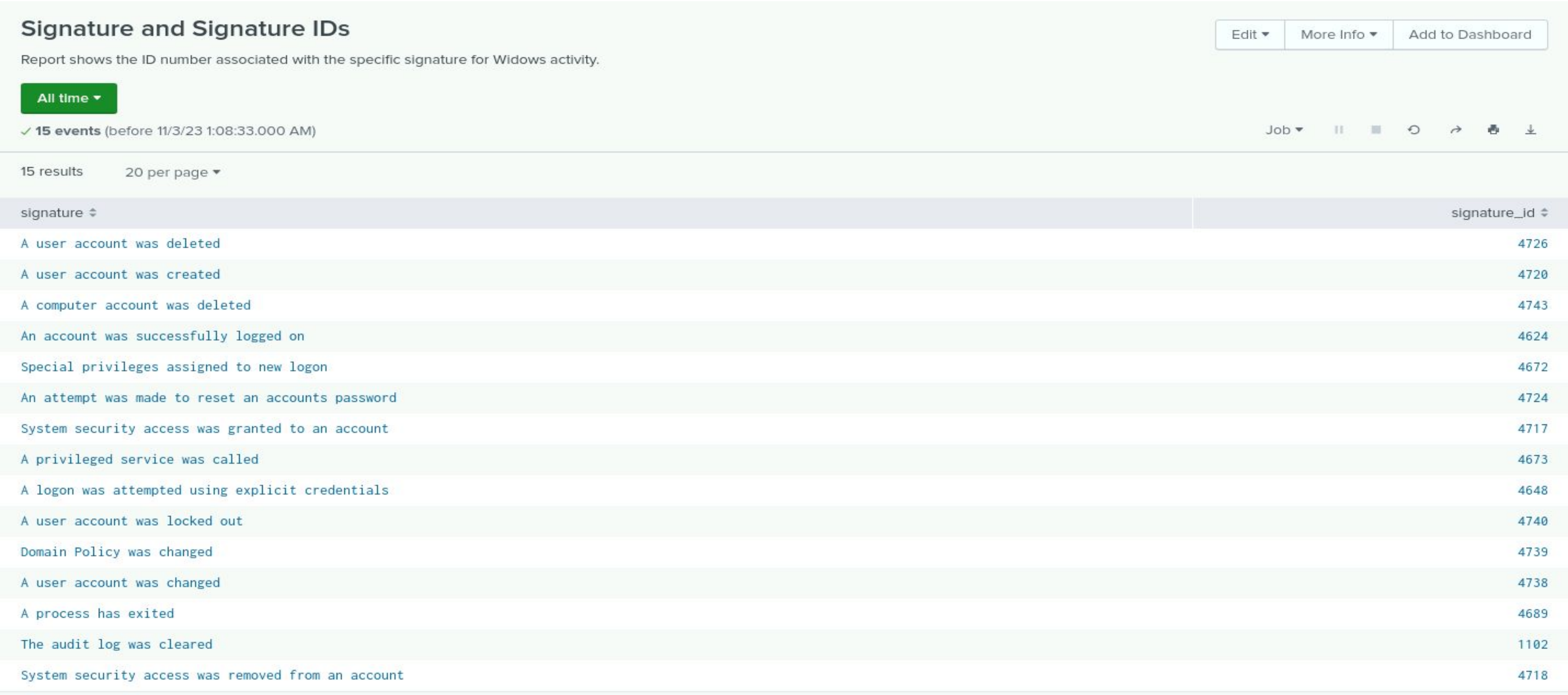
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signature and Signature IDs Report	Displays the ID number associated with the specific signature for Windows activity.
Severity, Count, and Percentage Report	Displays the severity level and count, along with the percentage of each.
Success and Failure of Windows activities	Provides a comparison between the success and failure of Windows activities.

Images of Reports—Windows



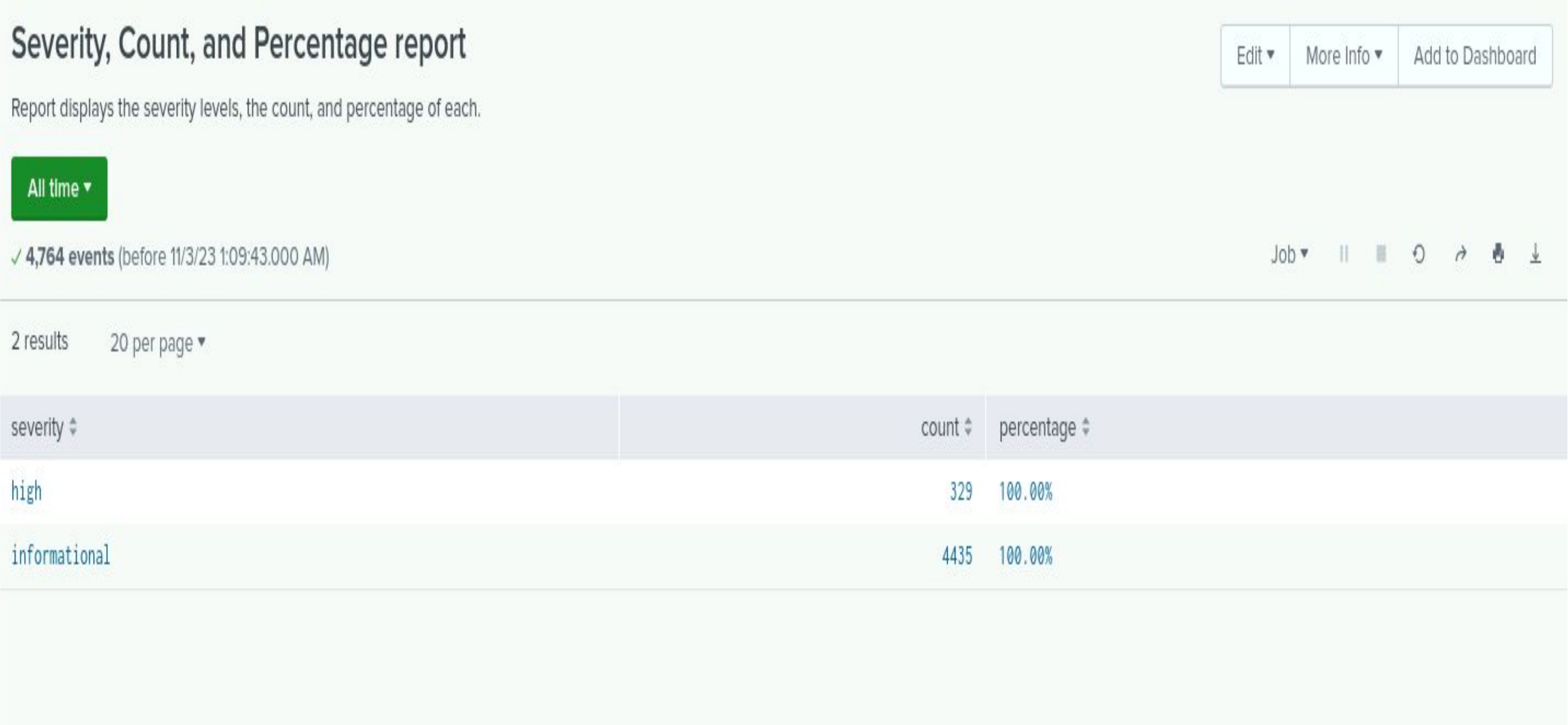
Signature and Signature IDs

Report shows the ID number associated with the specific signature for Widows activity.

✓ **15 events** (before 11/3/23 1:08:33.000 AM)

15 results 20 per page ▾

signature	signature_id
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718



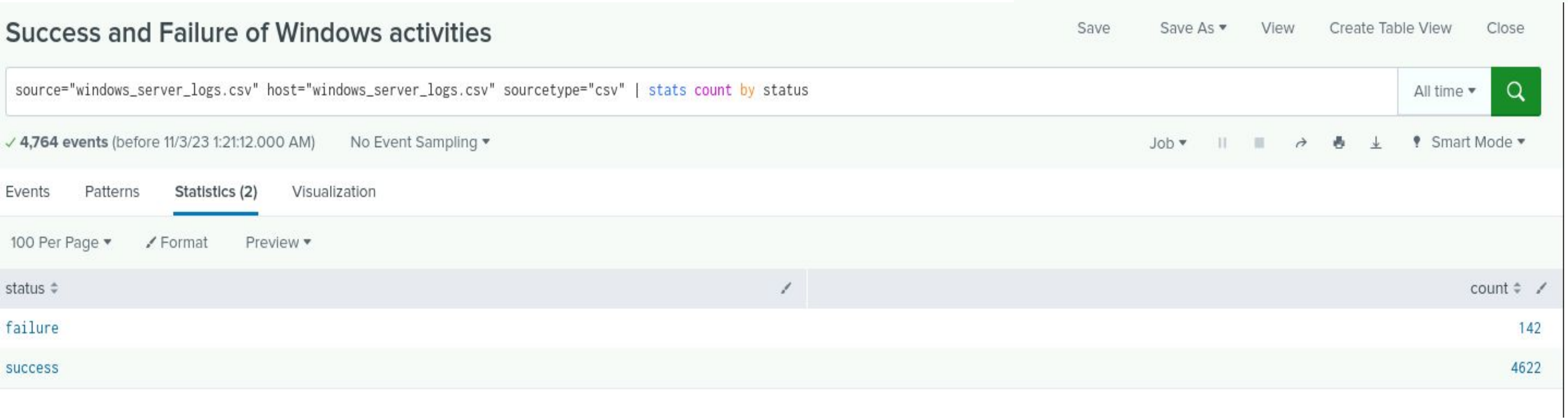
Severity, Count, and Percentage report

Report displays the severity levels, the count, and percentage of each.

✓ **4,764 events** (before 11/3/23 1:09:43.000 AM)

2 results 20 per page ▾

severity	count	percentage
high	329	100.00%
informational	4435	100.00%



Success and Failure of Windows activities

```
source="windows_server_logs.csv" host="windows_server_logs.csv" sourcetype="csv" | stats count by status
```

All time ▾

✓ **4,764 events** (before 11/3/23 1:21:12.000 AM) No Event Sampling ▾

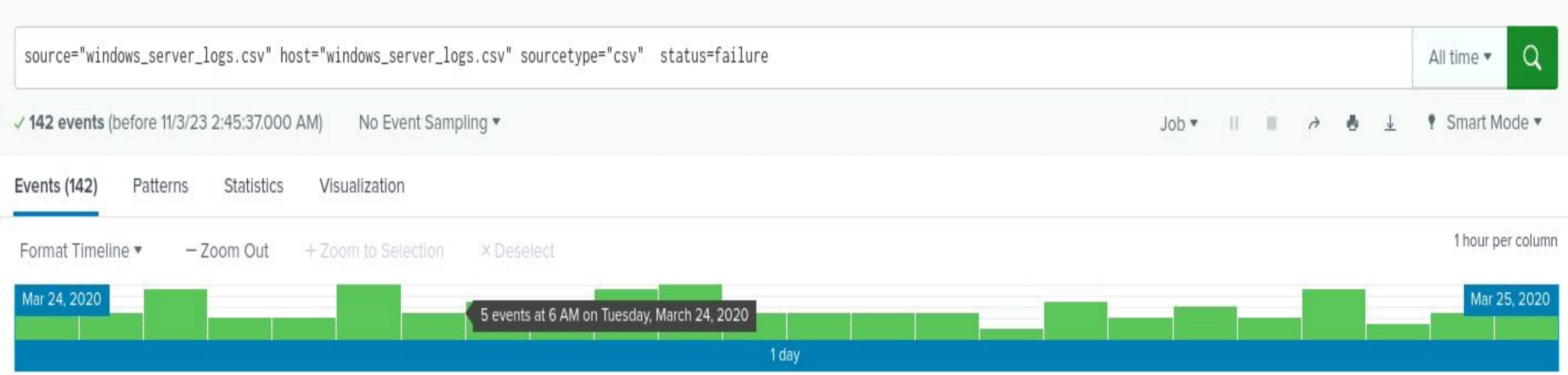
status	count
failure	142
success	4622

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity Alert -4724	Triggered when >8 failed activities are reached.	5 per hour	8 per hour

JUSTIFICATION: We chose threshold of 8 failed Windows activities in an hour because the baseline is 5/hr. Greater than 8 failures will alert to notify of possible malicious intent.



```
source="windows_server_logs.csv" host="windows_server_logs.csv" sourcetype="csv"  status=failure
```

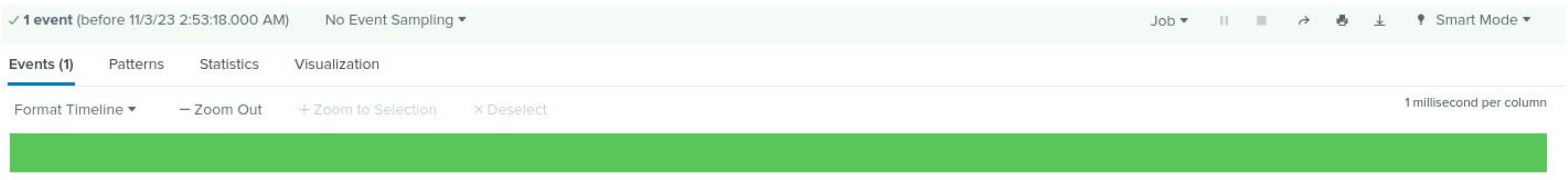
✓ 142 events (before 11/3/23 2:45:37.000 AM)

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account was Successfully Logged on -4624	Triggered when threshold greater than 3 successful logons are reached	1 per hour	3 per hour

JUSTIFICATION: We selected a threshold of 3 because the report shows 1 login is baseline.



✓ **1 event** (before 11/3/23 2:53:18.000 AM)

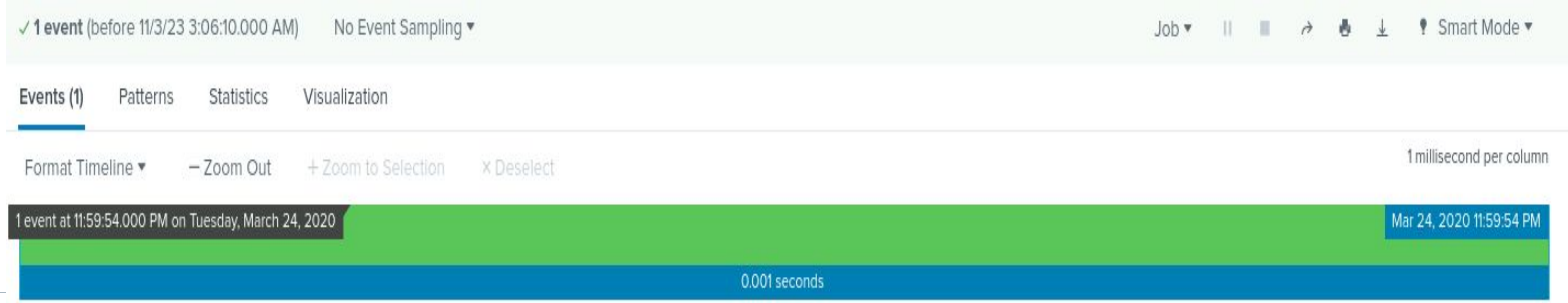
1 millisecond per column

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deleted Alert - 4726	Triggered when the threshold of 3 has been reached	1 per hour	3 per hour

JUSTIFICATION: We selected a threshold of 3 because baseline in the report is 1.



✓ 1 event (before 11/3/23 3:06:10.000 AM)

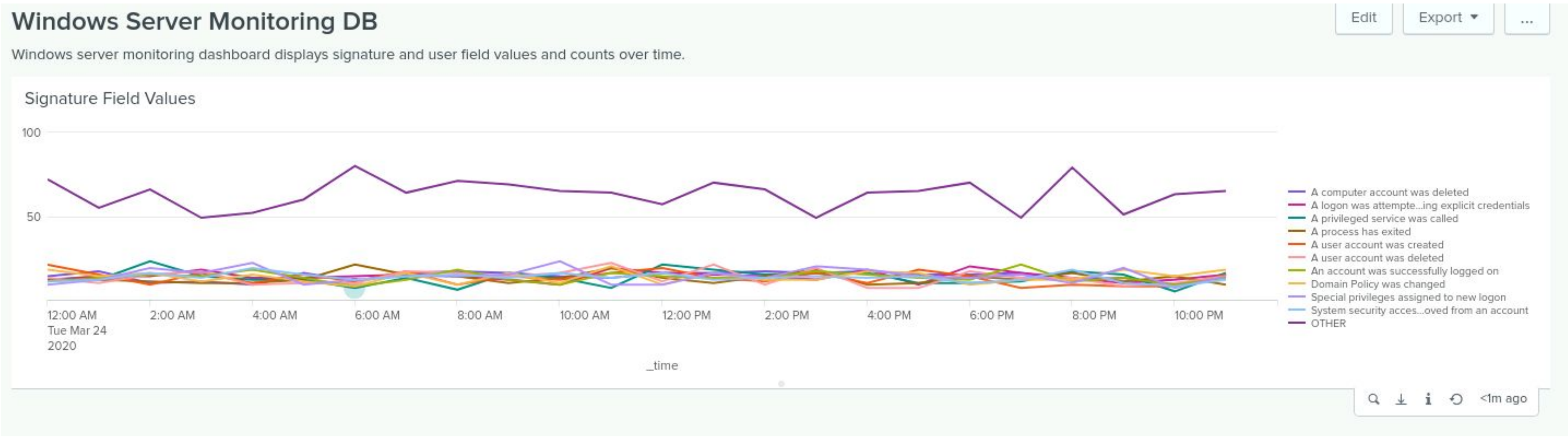
1 millisecond per column

1 event at 11:59:54.000 PM on Tuesday, March 24, 2020

Mar 24, 2020 11:59:54 PM

0.001 seconds

Dashboards—Windows

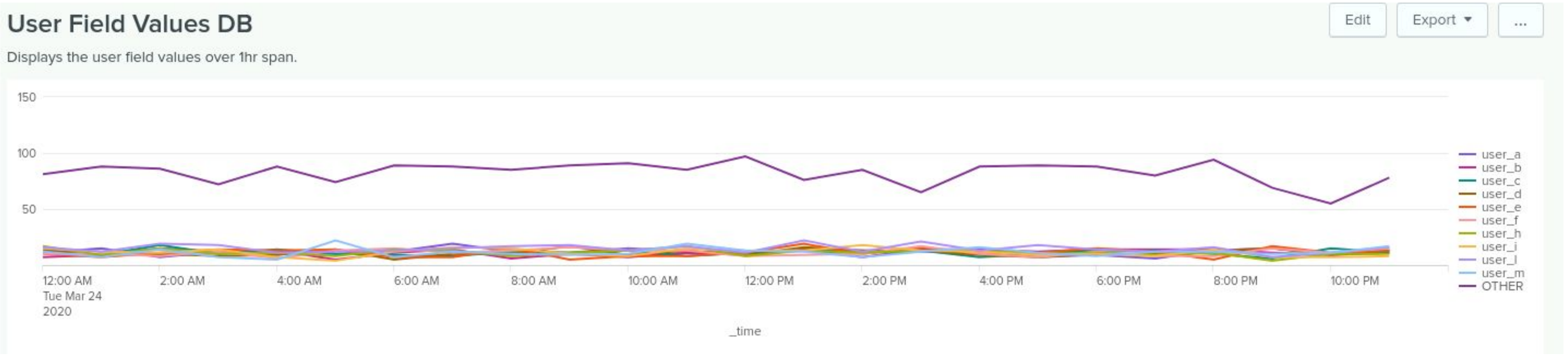


Windows Server Monitoring DB

Windows server monitoring dashboard displays signature and user field values and counts over time.

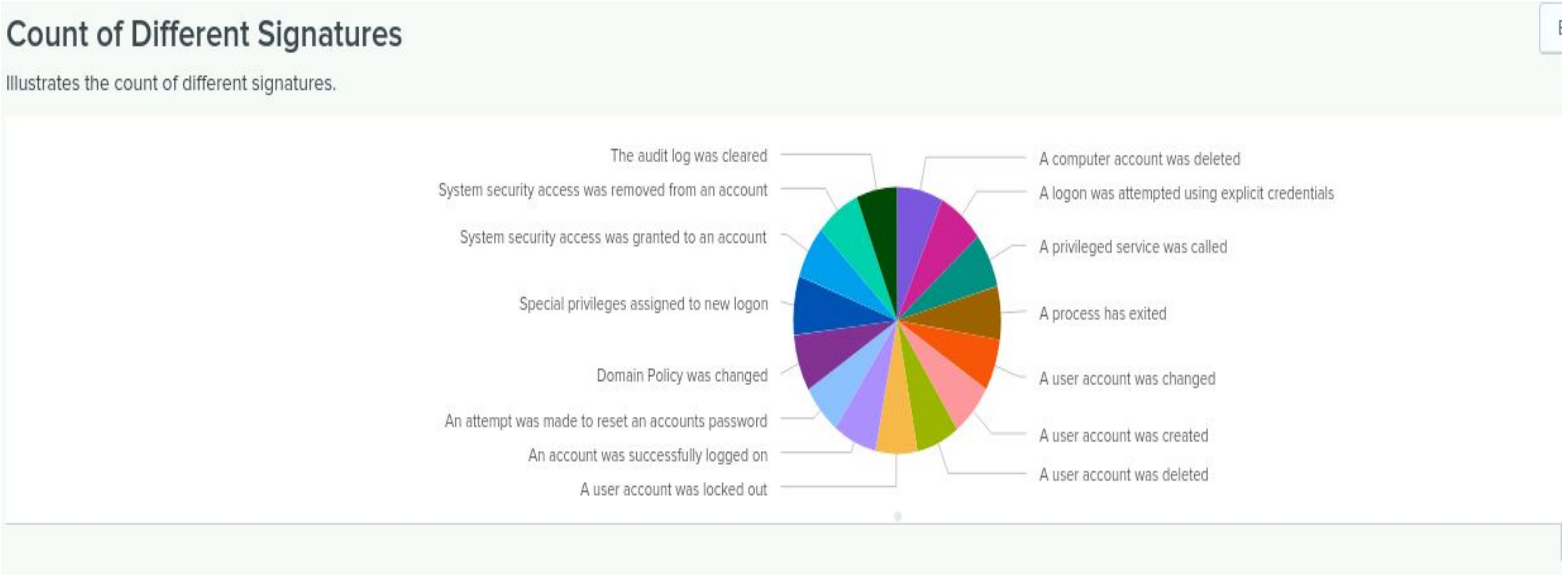
Signature Field Values

Edit
Export ▾
...
100
50
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was attempte...ing explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security acces...oved from an account
OTHER
<1m ago



User Field Values DB

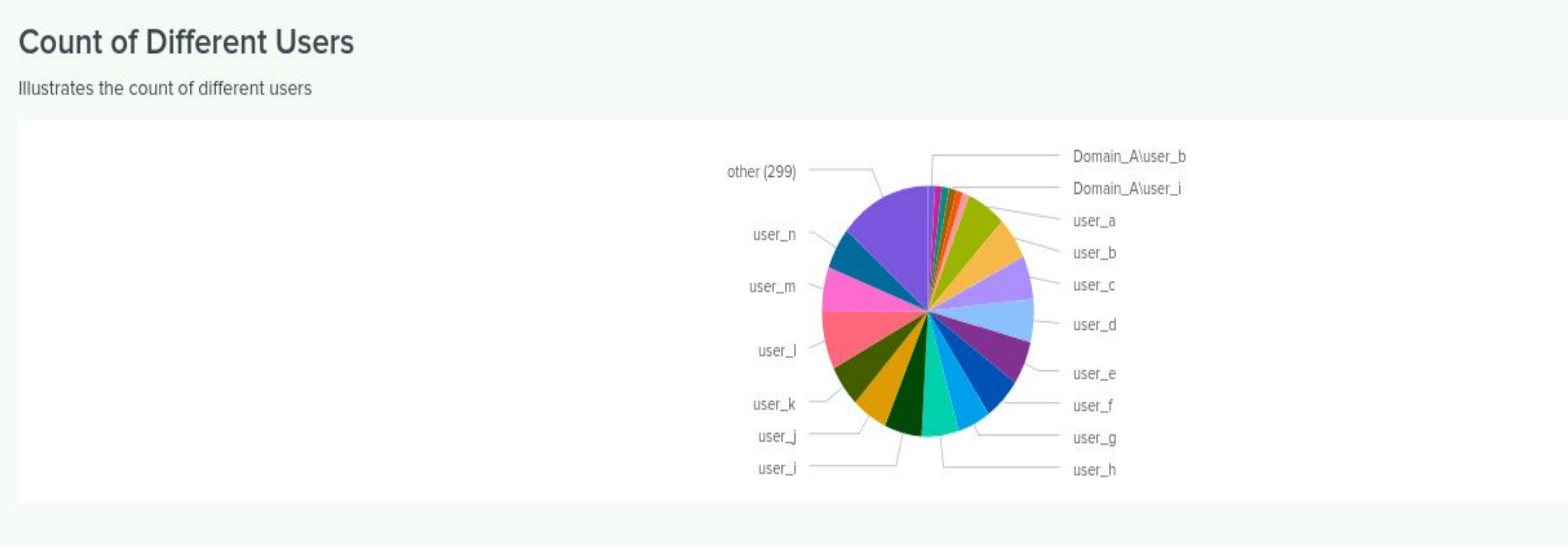
Displays the user field values over 1hr span.



Count of Different Signatures

Illustrates the count of different signatures.

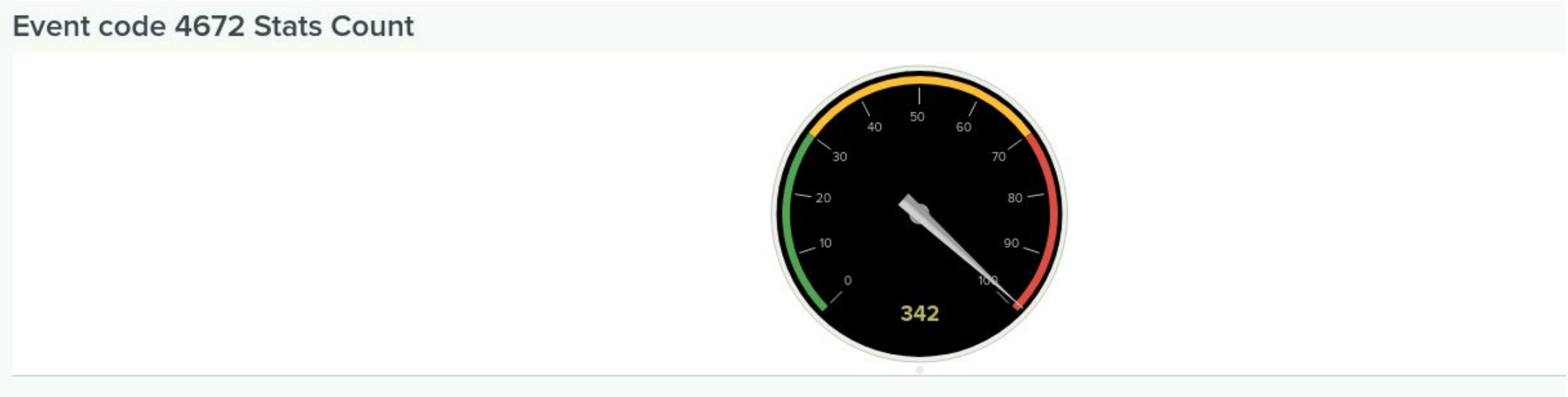
The audit log was cleared
System security access was removed from an account
System security access was granted to an account
Special privileges assigned to new logon
Domain Policy was changed
An attempt was made to reset an accounts password
An account was successfully logged on
A user account was locked out
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 created
A user account was deleted

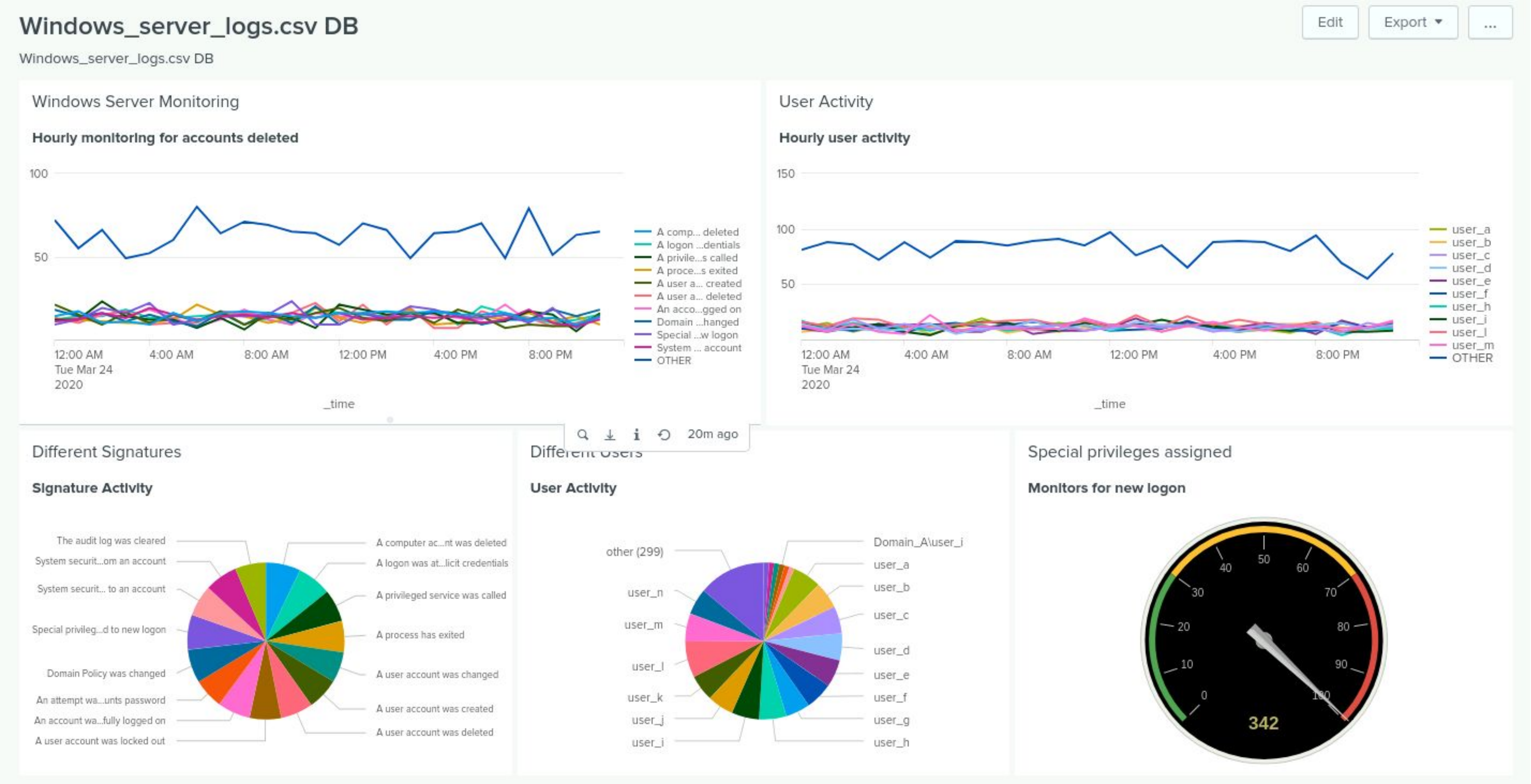


Count of Different Users

Illustrates the count of different users

Dashboards—Windows


Event code 4672 Stats Count


Windows_server_logs.csv DB

Windows_server_logs.csv DB

Windows Server Monitoring

Hourly monitoring for accounts deleted

User Activity

Hourly user activity

Different Signatures

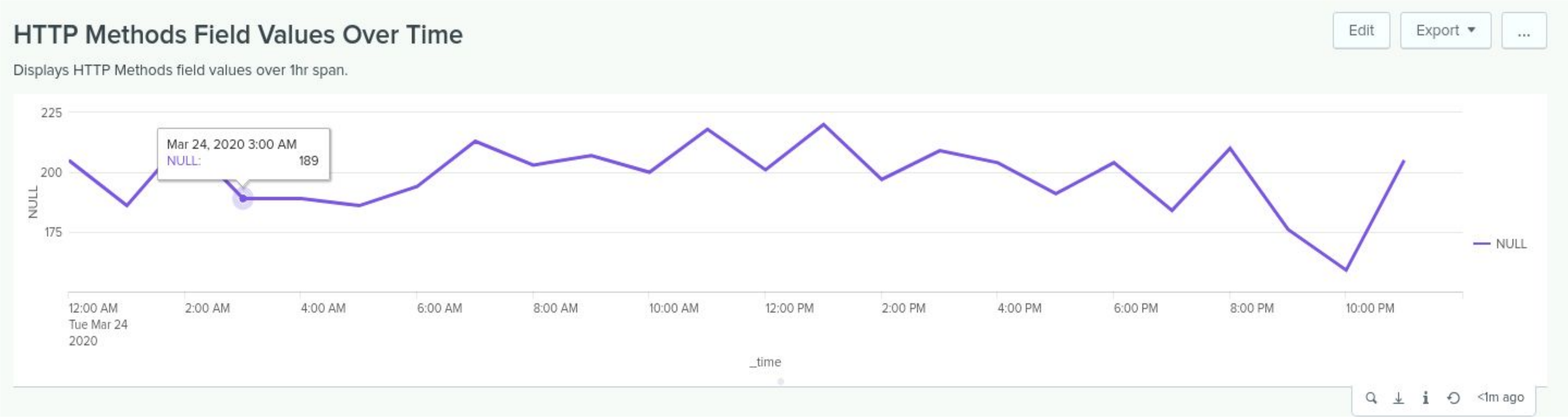
Signature Activity

Different Users

User Activity

Special privileges assigned

Monitors for new logon


HTTP Methods Field Values Over Time

Displays HTTP Methods field values over 1hr span.

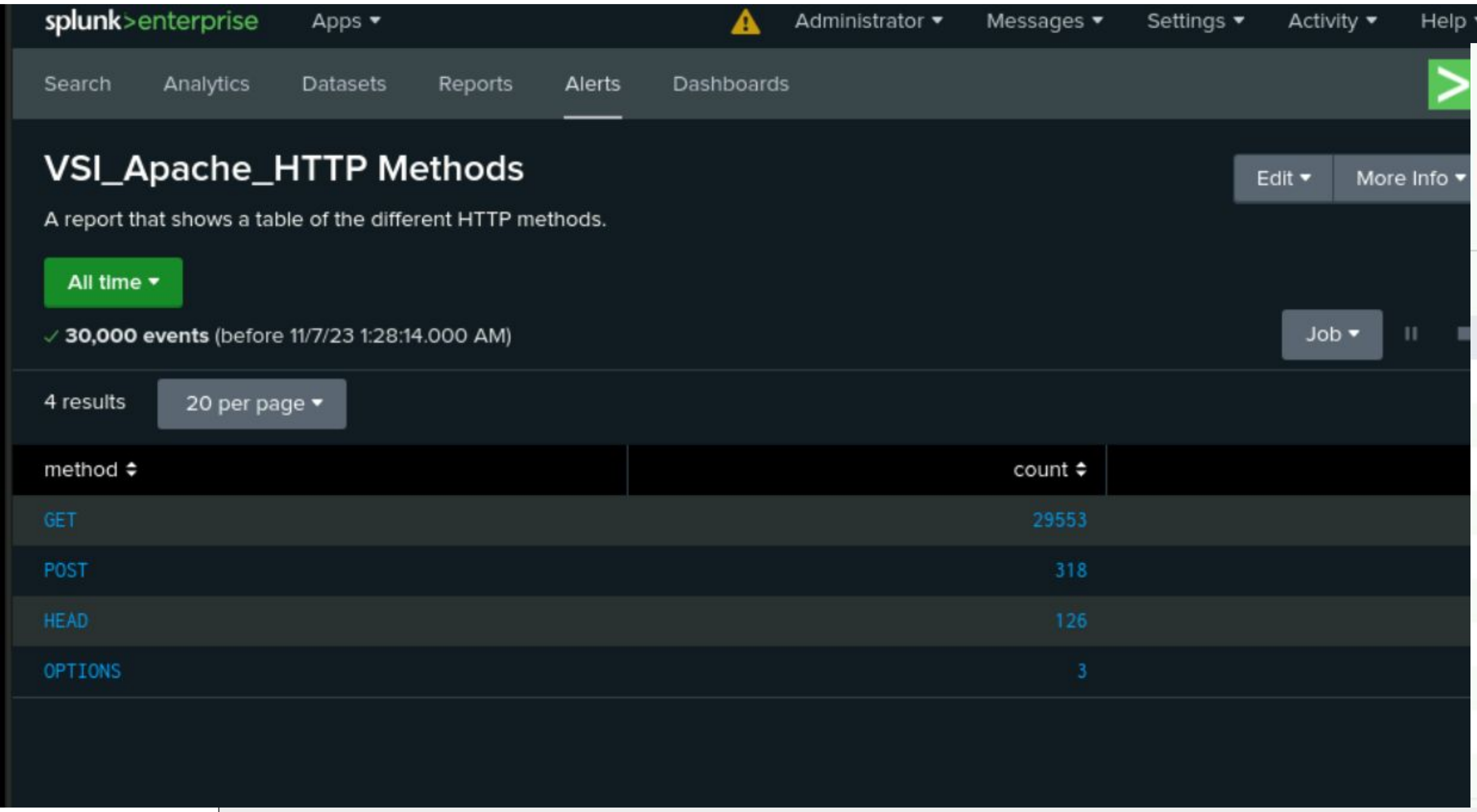
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	This report shows the top HTTP methods used against the server.
Top Domains	This report shows the most domains referred.
HTTP Response Codes	This report shows the various HTTP response codes and their counts.

Images of Reports—Apache



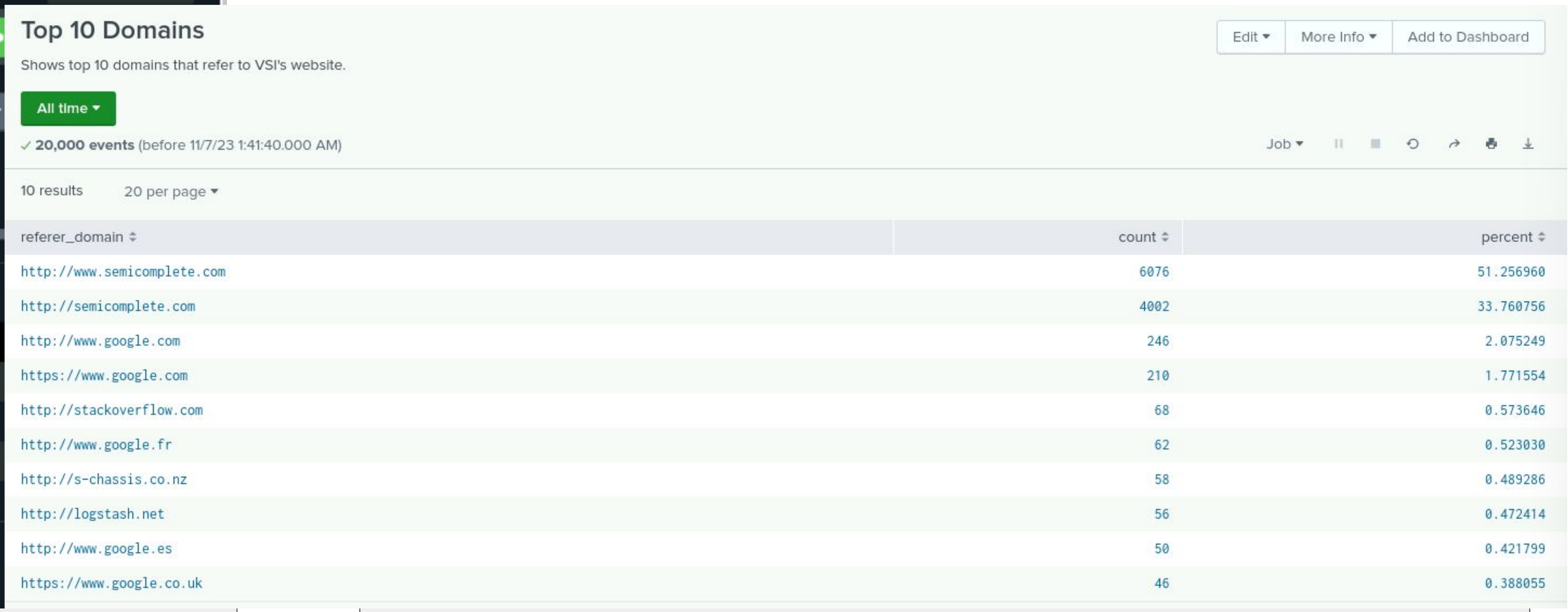
VSI_Apache_HTTP Methods

A report that shows a table of the different HTTP methods.

✓ **30,000 events** (before 11/7/23 1:28:14.000 AM)

4 results

method	count
GET	29553
POST	318
HEAD	126
OPTIONS	3



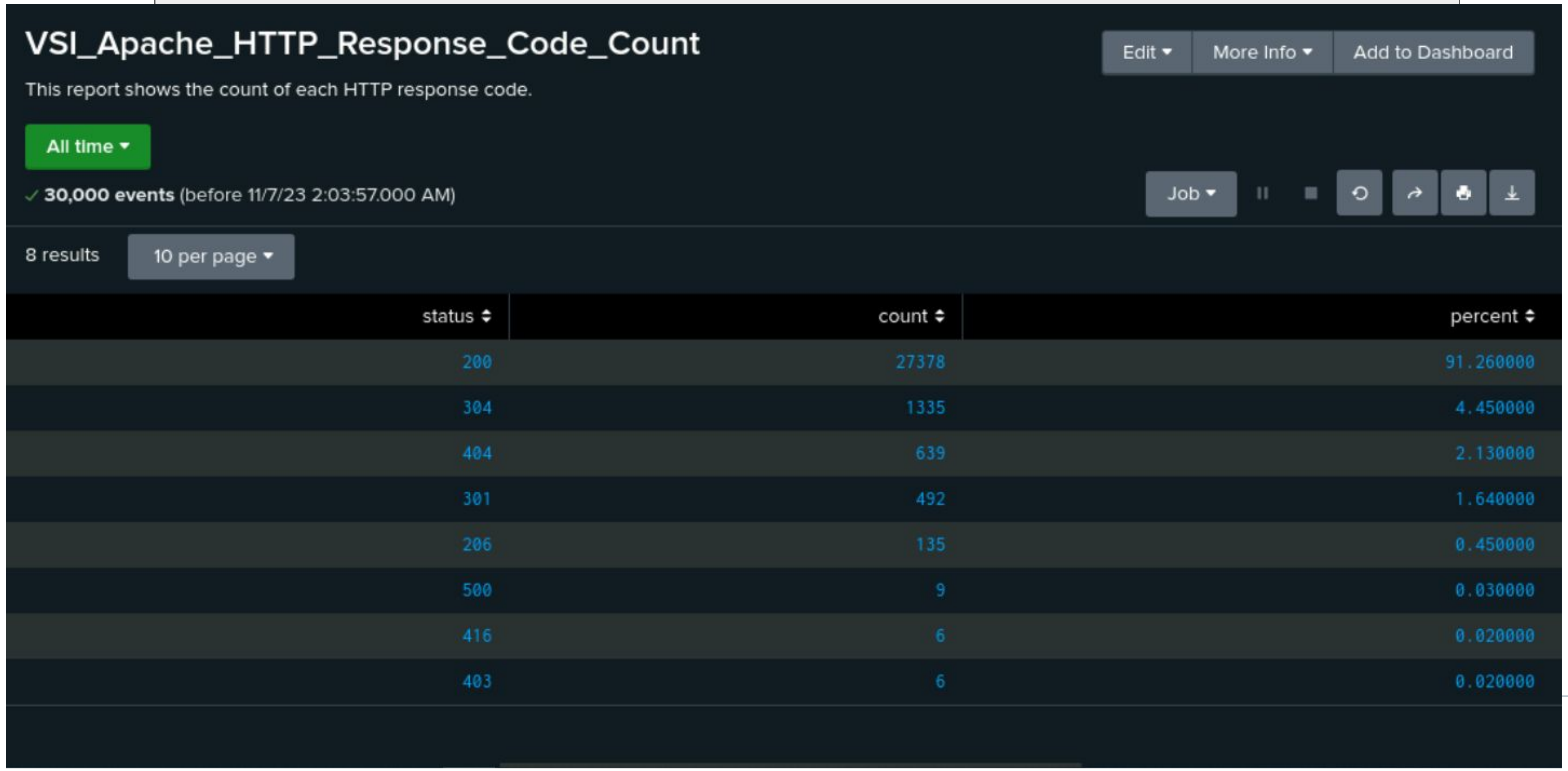
Top 10 Domains

Shows top 10 domains that refer to VSI's website.

✓ **20,000 events** (before 11/7/23 1:41:40.000 AM)

10 results

referer_domain	count	percent
http://www.semicomplete.com	6076	51.256960
http://semicomplete.com	4002	33.760756
http://www.google.com	246	2.075249
https://www.google.com	210	1.771554
http://stackoverflow.com	68	0.573646
http://www.google.fr	62	0.523030
http://s-chassis.co.nz	58	0.489286
http://logstash.net	56	0.472414
http://www.google.es	50	0.421799
https://www.google.co.uk	46	0.388055



VSI_Apache_HTTP_Response_Code_Count

This report shows the count of each HTTP response code.

✓ **30,000 events** (before 11/7/23 2:03:57.000 AM)

8 results

status	count	percent
200	27378	91.260000
304	1335	4.450000
404	639	2.130000
301	492	1.640000
206	135	0.450000
500	9	0.030000
416	6	0.020000
403	6	0.020000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Suspicious International Activity	A suspicious volume of international activity was observed.	15	20

JUSTIFICATION: We selected 15 as baseline and 20 Threshold because it was the average in the report.

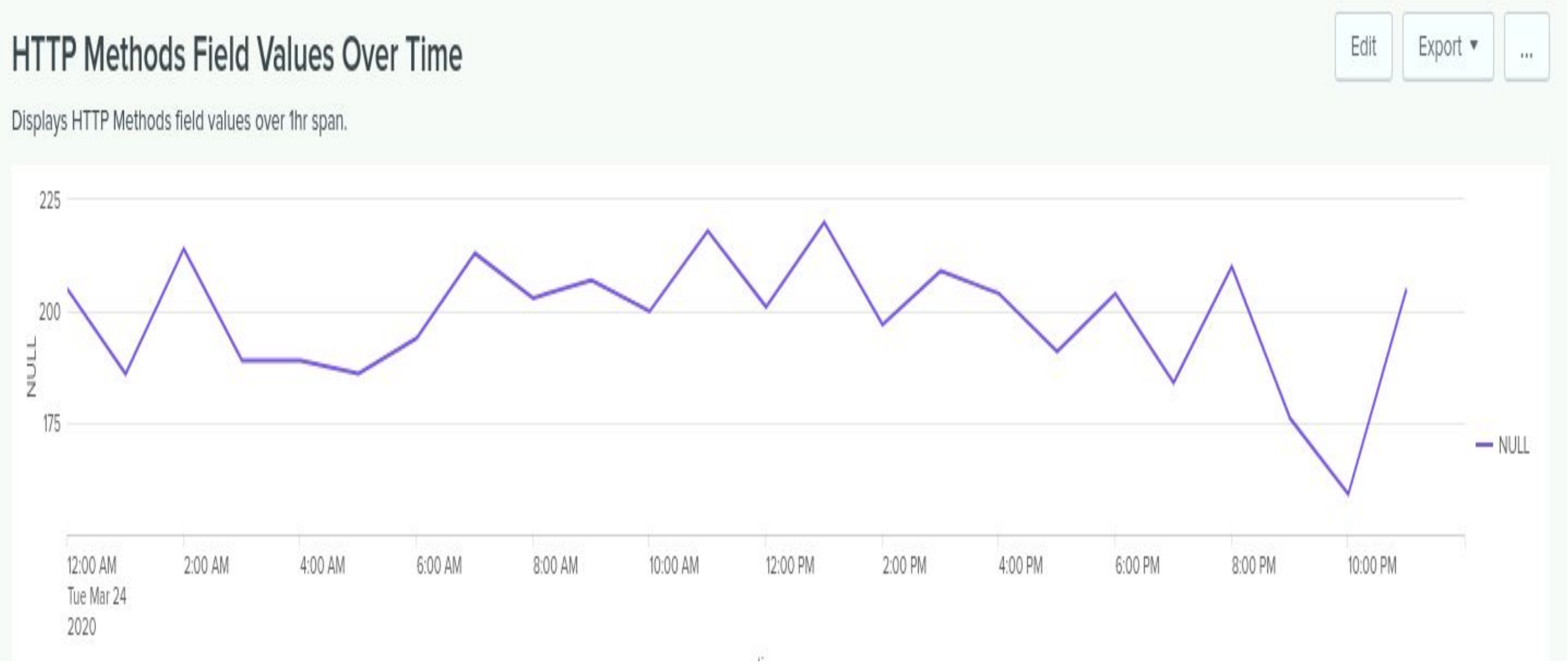
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Suspicious HTTP activity	Deviations in HTTP response codes were recognized.	15	20

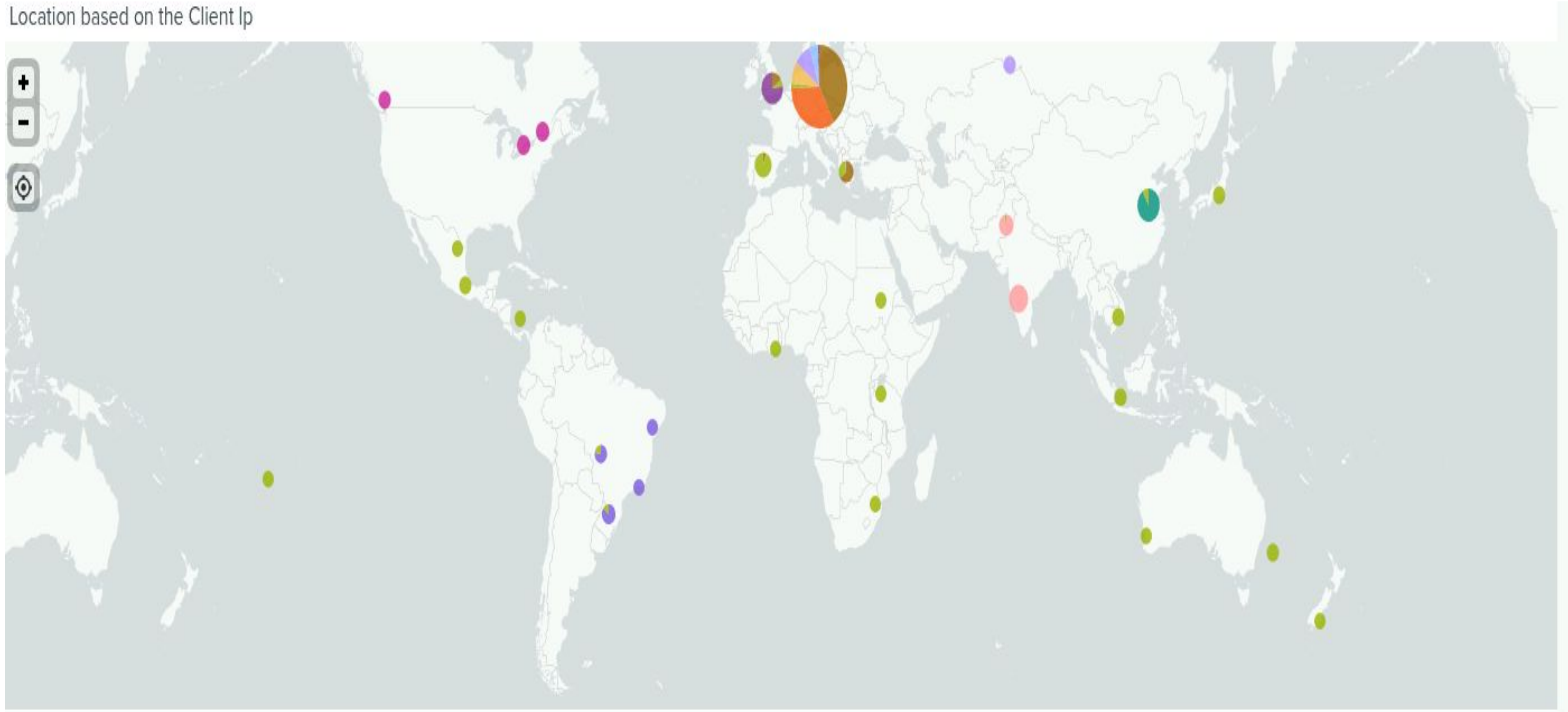
JUSTIFICATION: This baseline and threshold was also reflective of averages in our reporting after data analysis.

Dashboards—Apache

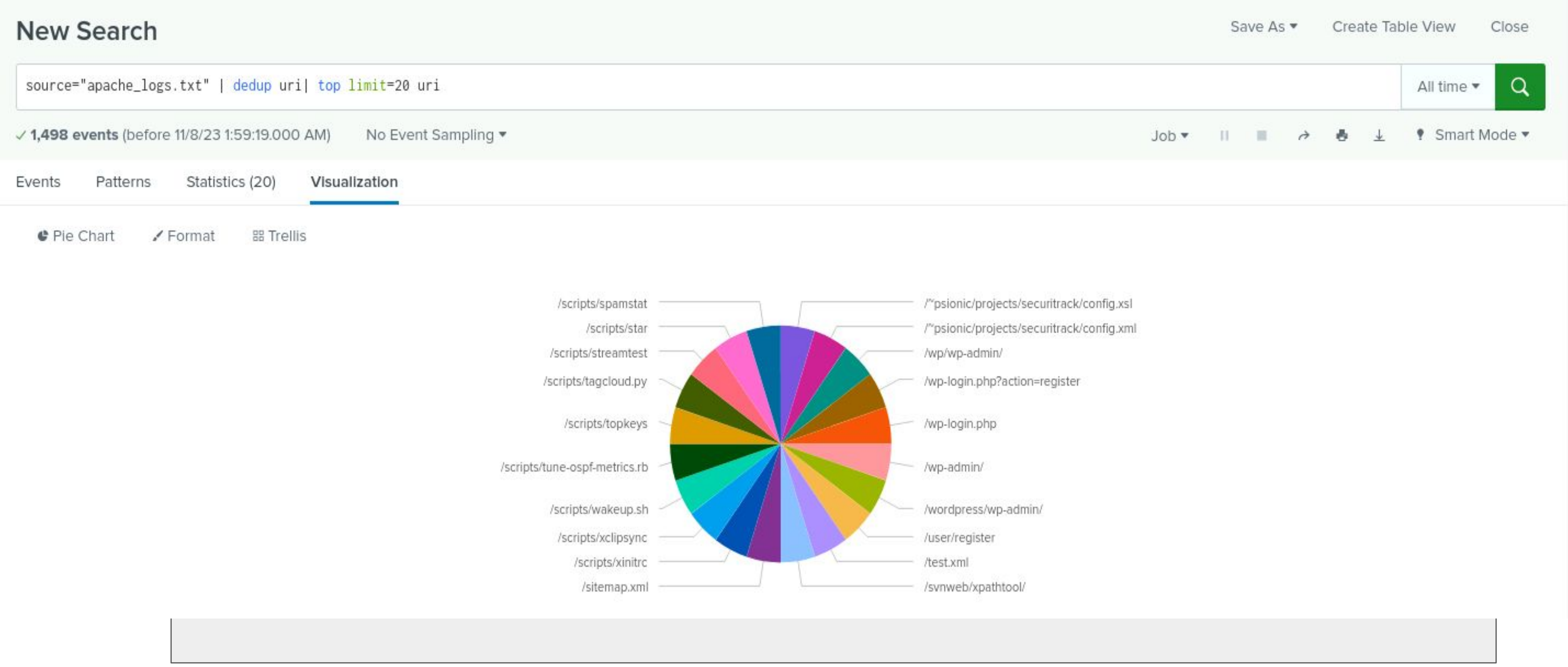


HTTP Methods Field Values Over Time

Displays HTTP Methods field values over 1hr span.



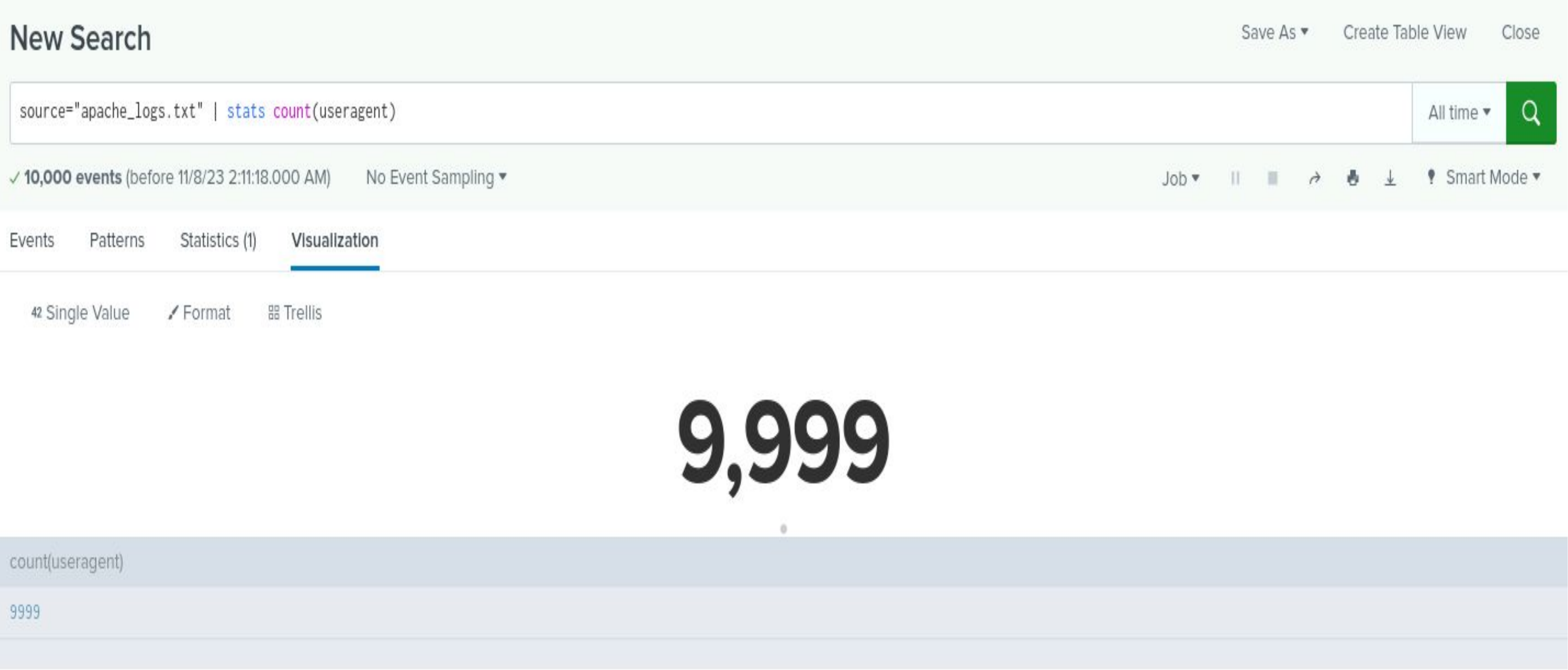
Location based on the Client Ip



New Search

```
source="apache_logs.txt" | dedup uri| top limit=20 uri
```

✓ 1,498 events (before 11/8/23 1:59:19.000 AM) No Event Sampling ▾



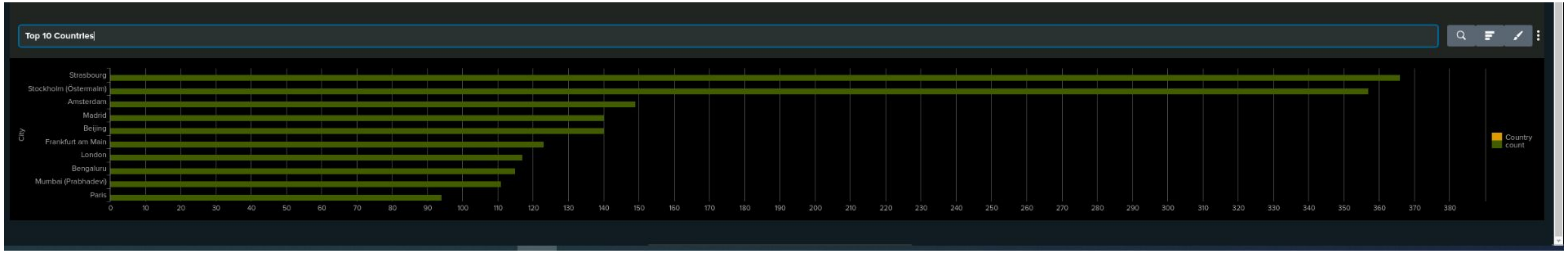
New Search

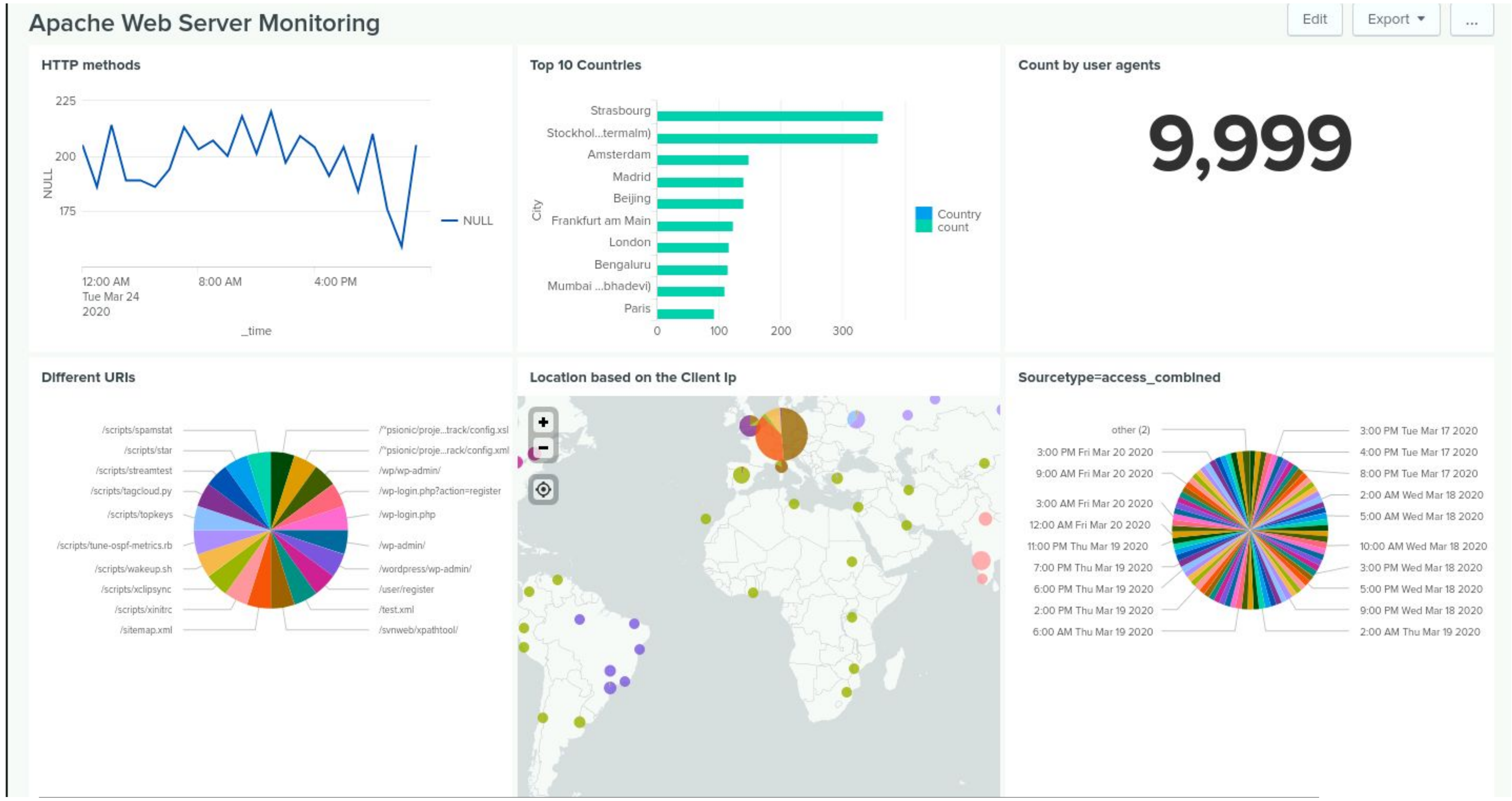
```
source="apache_logs.txt" | stats count(useragent)
```

✓ 10,000 events (before 11/8/23 2:11:18.000 AM) No Event Sampling ▾

count(useragent)
9999

Dashboards—Apache





Attack Analysis

Attack Summary—Windows

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

- After analyzing the attack data, our team was able to successfully identify and visualize attacks against VSI. We were also able to identify which users in particular were the most active against the server, and where those IPs originated.
- Atypical amounts of successful logins, failed windows activity, abnormal HTTP request activity, and numerous other abnormalities in these reports were properly identified.
- These threats identify threats made against the network and provide insight into where VSI needs to strengthen their security to prevent denial of service through things like DDoS.

Attack Summary—Windows

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

- We are confident in our thresholds. Establishing a proper baseline, we were able to confidently provide an adequate threshold for alerts to trigger adequately.
- These reports allow us to identify which users in particular were acting against the server.
- Utilizing more data collected over larger periods of time will help establish more accurate baselines for trigger alerts, but the current thresholds are accurate given the data we have on hand.

Attack Summary—Windows

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

- Our dashboards visualize which attack vectors were discovered in our report, and how these affect VSI's network in particular.
- These dashboards display which users and which activities are being flagged. This data provides insight on how the attacker may be attempting to breach the system. It also shows us where their IPs originate from, and when the attacks happen.
- These dashboards identify why it is crucial to set the proper thresholds so that alerts trigger when abnormalities against the server do happen.

Attack Summary—Apache

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

- Our team was successful in identifying malicious activity against the Apache server.
- Analyzing these logs, we can determine the geolocation of the most problematic IPs in addition to which attack vectors (DDoS, BFA) are being used.
- Our reports, alerts, and dashboards demonstrate the methods bad actors used against VSI’s apache server. We are able to properly identify which users in particular are acting against the network, and are provided further proof of the exploits they used to achieve this.

Attack Summary—Apache

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

- There was suspicious international activity from Ukraine. Suspicious GET and POST. 200 and 404 response codes were flagged. There was a decrease in 200 while 404 responses increased. There was a slight decrease in referrer domains.

Attack Summary—Apache

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

- Analyzing the Apache records comes up with some interesting findings.

  We can conclude that suspicious activity is coming from two cities in Ukraine, Kiev and Kharkiv.
- Analyzing URI data, our group found instances of scripts being used, indicating the possibility of brute force attacks being launched against the logon page.

Summary and Future Mitigations

Project 3 Summary

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

Our group has deduced that VSI is receiving attacks from rival corporation Jobecorp. Screenshots and data provided in this report deduce that users A and K were acting maliciously against the network using DDoS and brute force attacks.

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

Stronger passwords should be implemented for all users on the network. Work should be done to lockout users once too many instance so failed activity are recognized. VSI should continue to work to better test their networks in the future through proper penetration testing and having an educated security staff to address threats. The implementation of security keys is also advised.