Defensive Security Project by: [Jayden R Garcia]

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

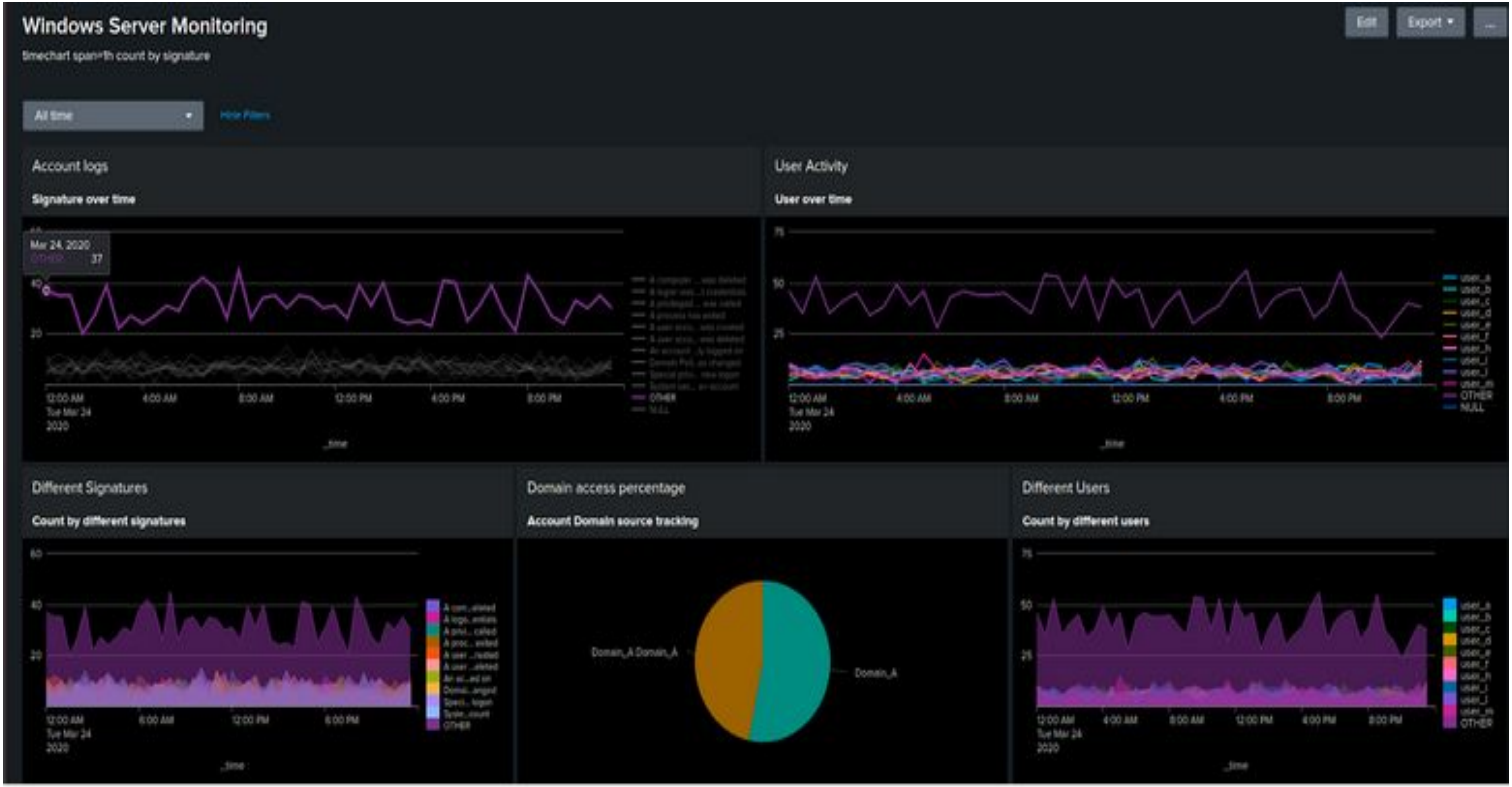
Project Summary & Future Mitigations

Monitoring Environment

Scenario

- I was notified by my manager that VSI recently experienced several cyber attacks, likely from their adversary Jobecorp. Unfortunately, this attack took down several of VSI’s systems. Fortunately, i’ve set up several monitoring solutions to help VSI quickly identify what was attacked. The attack that occurred targeted several systems specifically, Windows & Apache servers, which are fountatley monitoring. Management has quickly provided me with more logs from those same servers. These new logs cover the time period during which the attack occurred.]

Windows Server Monitoring



Windows Server Monitoring

timechart span=1h count by signature

All time ▾ Hide Filters

Account logs

Signature over time

User Activity

User over time

Different Signatures

Count by different signatures

Domain access percentage

Account Domain source tracking

Different Users

Count by different users

Logs Analyzed

1 Windows Logs

[windows_server_logs.csv
windows_server_attack_logs.csv]
o signature
o signature_id
o user
o status
o severity

2 Apache Logs

[apache.logs.txt
apache_attack_logs_txt]
o method
o referrer_domain
o status
o clientip
o useragent

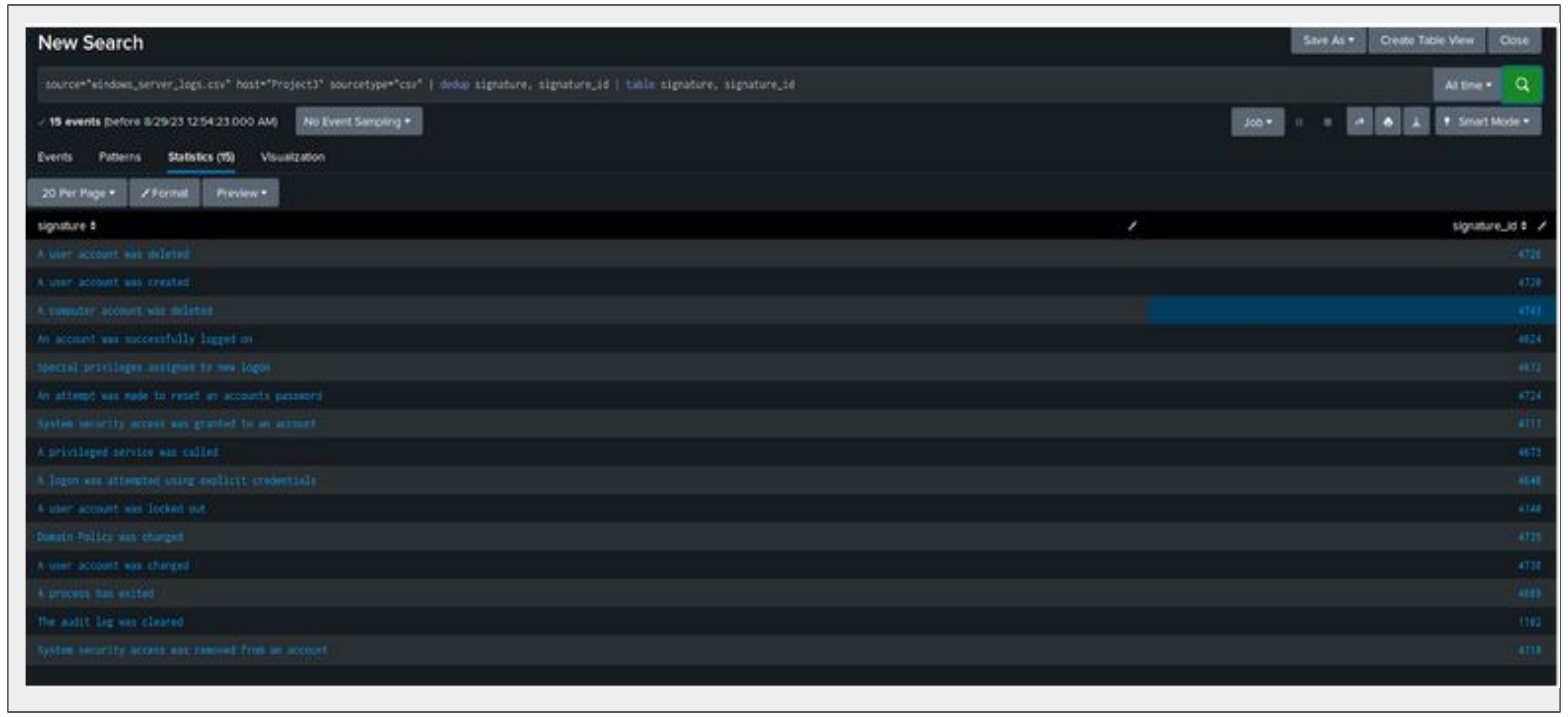
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
[signature_id]	[source="windows_server_attack_logs.csv" host="Linux_Server" sourcetype="csv" | dedup signature, signature_id | table signature, signature_id]
[sig & sig id]	[source="windows_server_attack_logs.csv” host”project3” sourcetype=”csv” |dedup signature, signature_id | table signature, signature_id]
[sig & sig id]	[source=”windows_server_logs.csv” host-’project3” sourcetype=”csv”| top limit=20 severity]

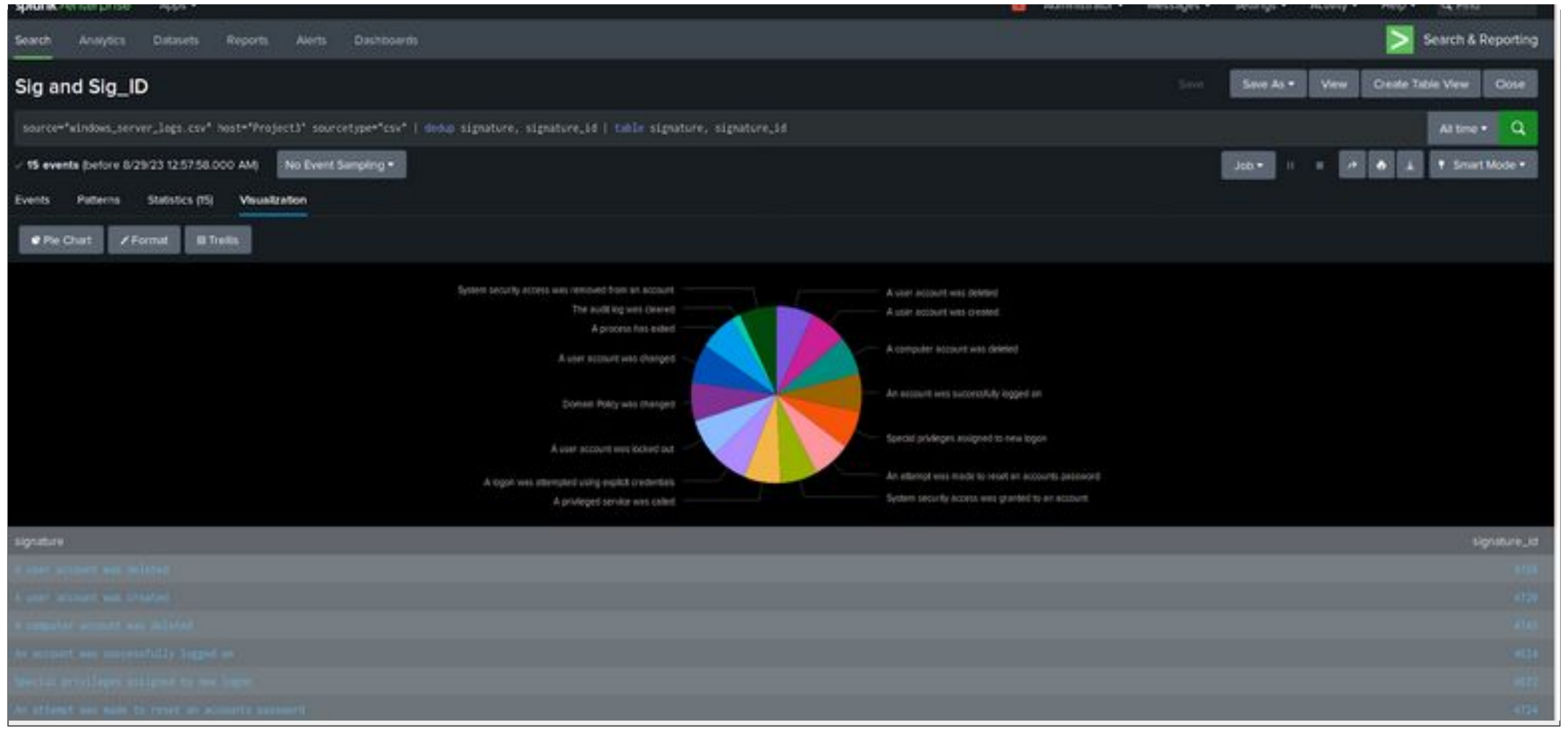
Images of Reports—Windows



```
source="windows_server_logs.csv" host="Project3" sourcetype="csv" | dedup signature, signature_id | table signature, signature_id
```

✓ 15 events (before 8/29/23 12:54:23.000 AM)

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

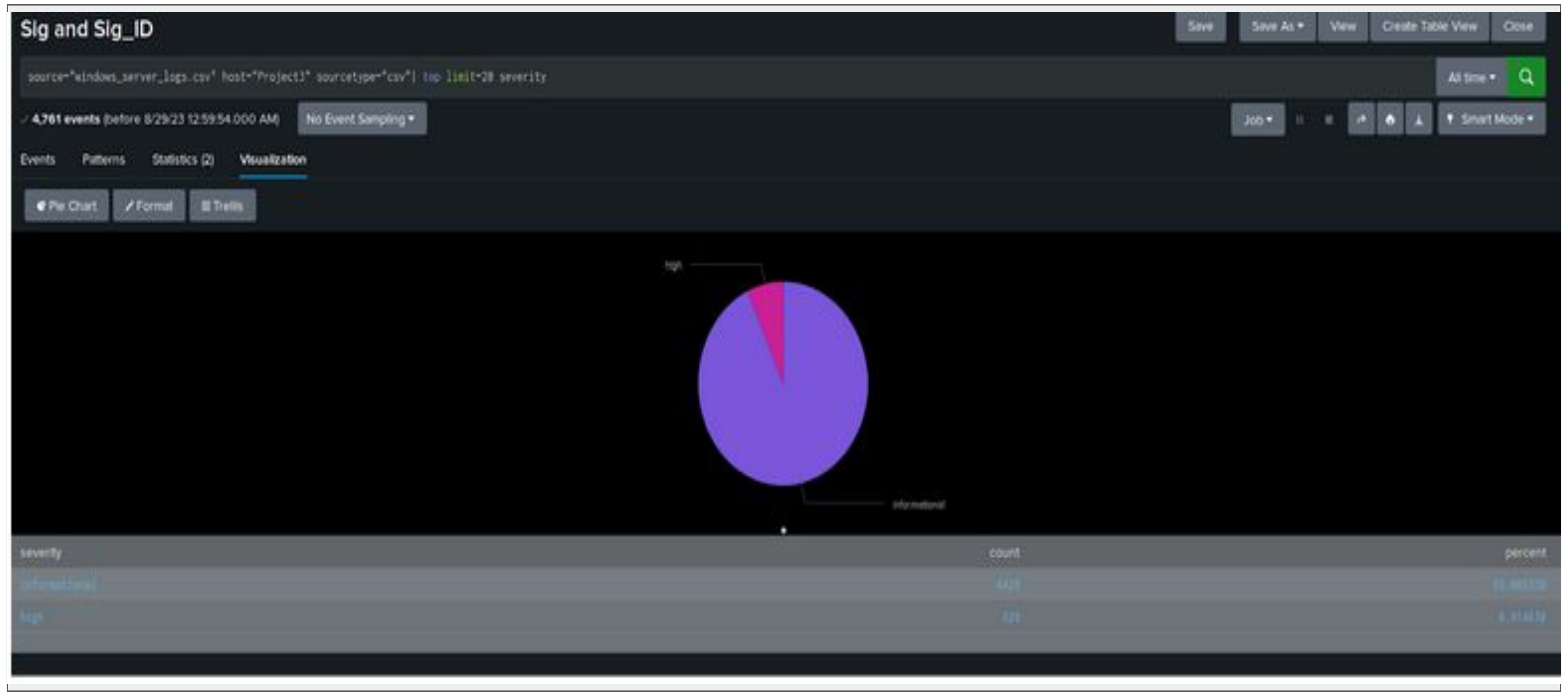


splunk>enterprise
Apps ▾
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Sig and Sig_ID
Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (15)
Visualization
Pie Chart
Format
Trellis
System security access was removed from an account
The audit log was cleared
A process has exited
A user account was changed
Domain Policy was changed
A user account was locked out
A logon was attempted using explicit credentials
A privileged service was called
A user account was deleted
A user account was created
A computer account was deleted
An account was successfully logged on
Special privileges assigned to new logon
An attempt was made to reset an accounts password
System security access was granted to an account

```
source="windows_server_logs.csv" host="Project3" sourcetype="csv" | dedup signature, signature_id | table signature, signature_id
```

✓ 15 events (before 8/29/23 12:57:58.000 AM)

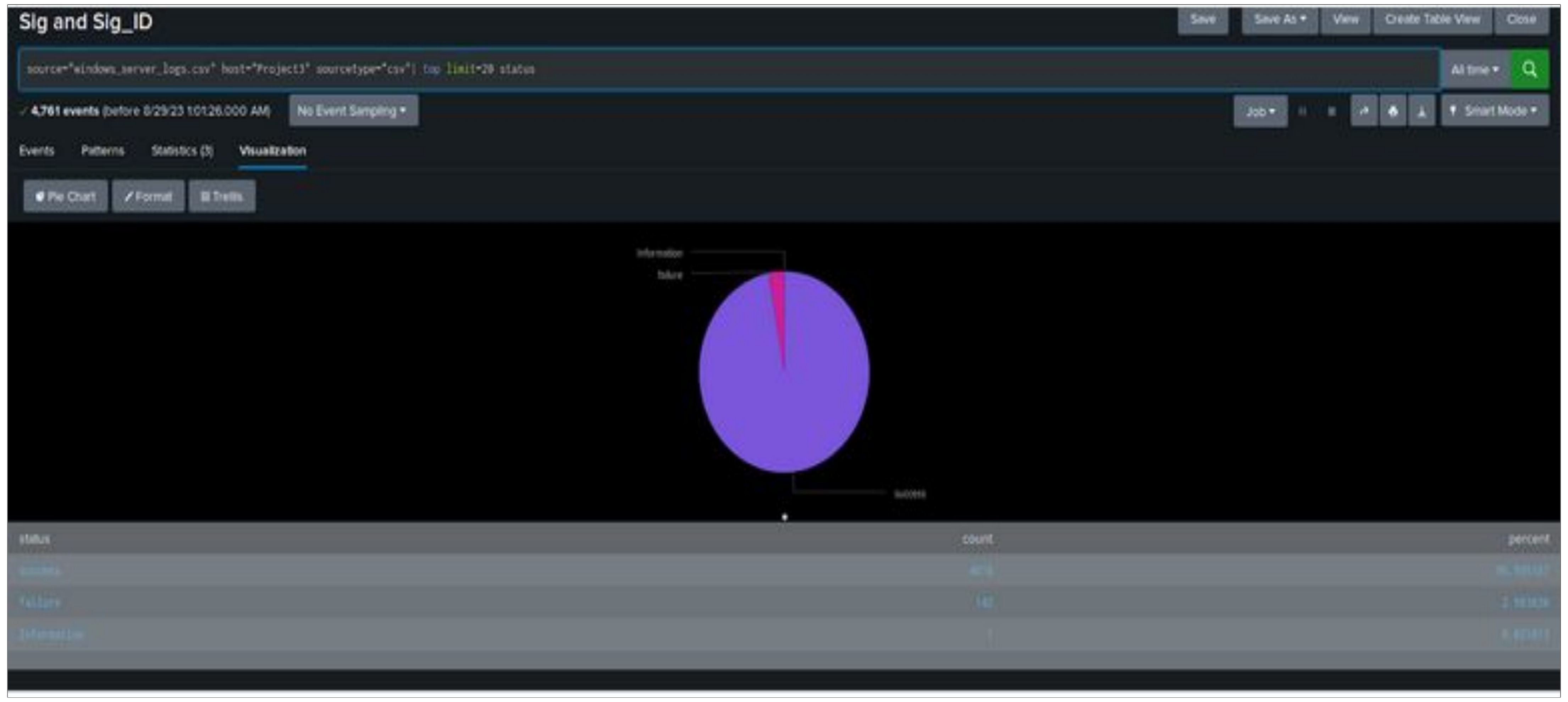
signature	signature_id
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724



```
source="windows_server_logs.csv" host="Project3" sourcetype="csv"| top limit=20 severity
```

✓ 4,761 events (before 8/29/23 12:59:54.000 AM)

severity	count	percent
informational	4435	[illegible]
high	326	[illegible]



```
source="windows_server_logs.csv" host="Project3" sourcetype="csv"| top limit=20 status
```

✓ 4,761 events (before 8/29/23 1:01:26.000 AM)

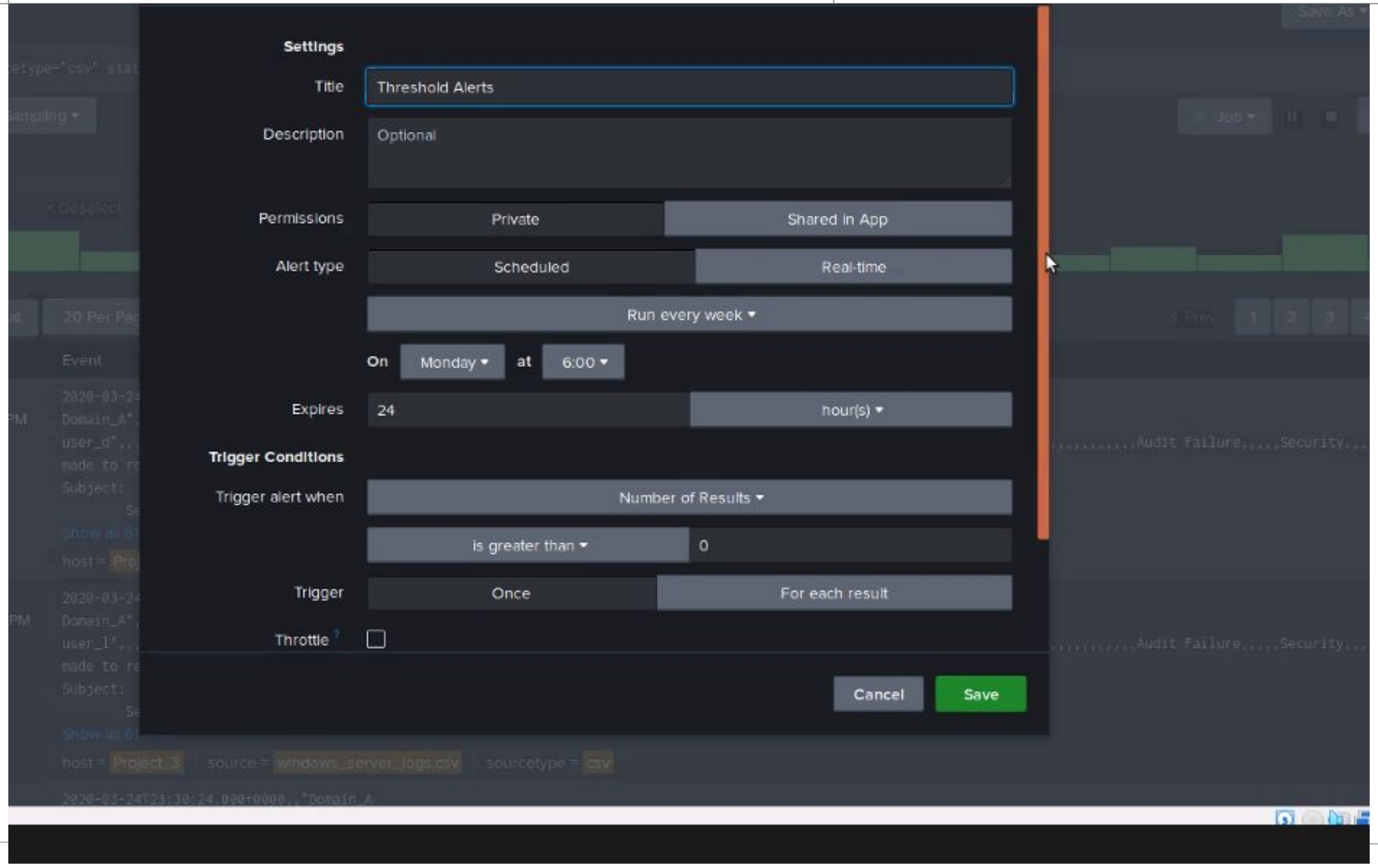
status	count	percent
success	4618	[illegible]
failure	142	[illegible]
information	1	[illegible]

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Threshold alert]	[alarm triggered when number of results are greater than 18.]	[for each result]	[18]

JUSTIFICATION:



Settings

Title: Threshold Alerts

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every week

On Monday at 6:00

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

is greater than: 0

Trigger: Once | For each result

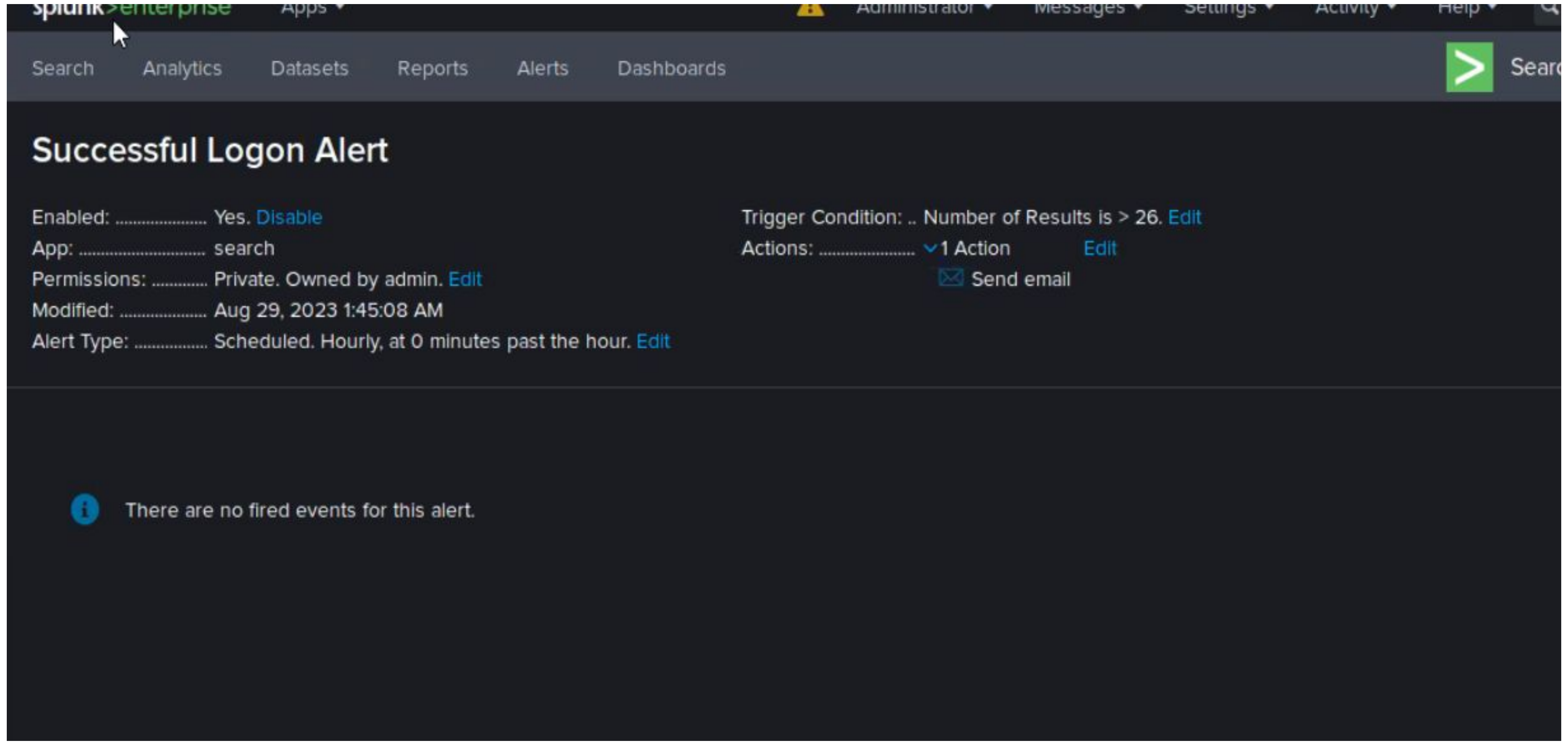
Throttle ☐

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Successful Logon Alert]	[scheduled alert type triggered if number of results are greater than 26]	[Baseline]	[26]

JUSTIFICATION:



Successful Logon Alert

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 29, 2023 1:45:08 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 26. Edit
Actions: .... 1 Action Edit
Send email

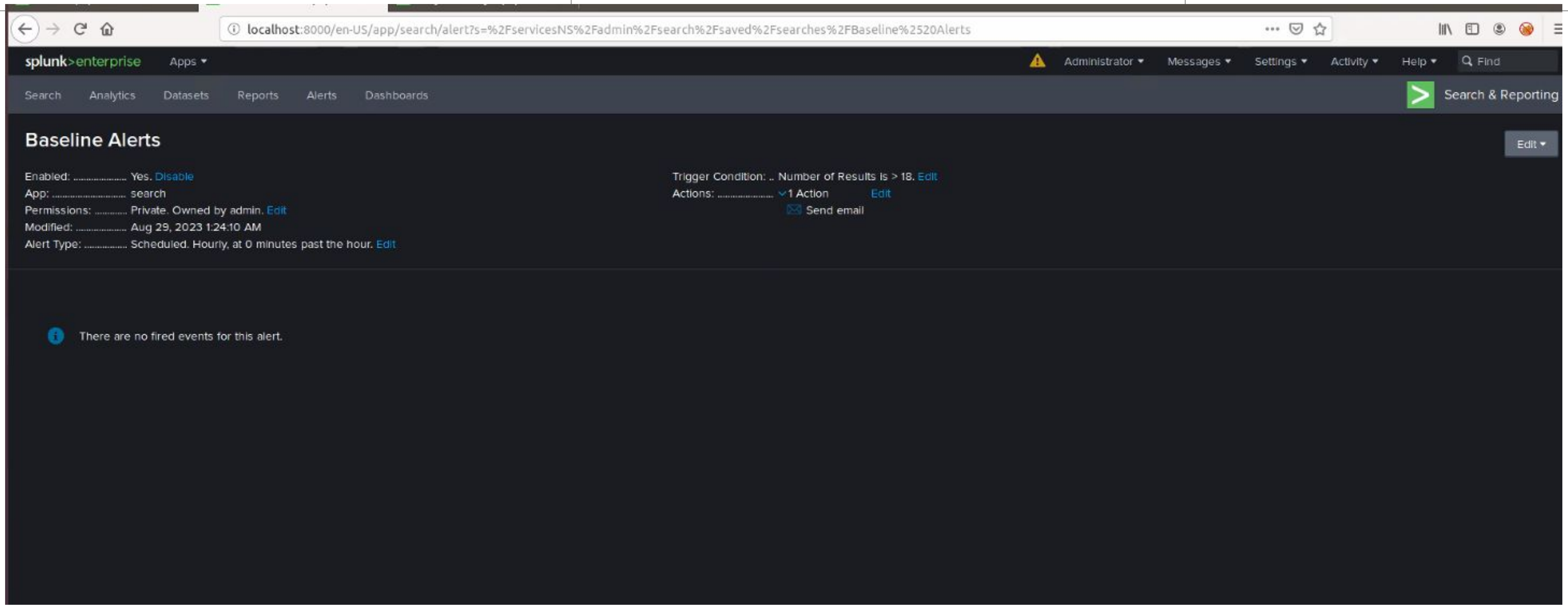
There are no fired events for this alert.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Baseline Alert]	[scheduled hourly trigger condition greater than 18]	[Baseline]	[Greater than 18]

JUSTIFICATION:



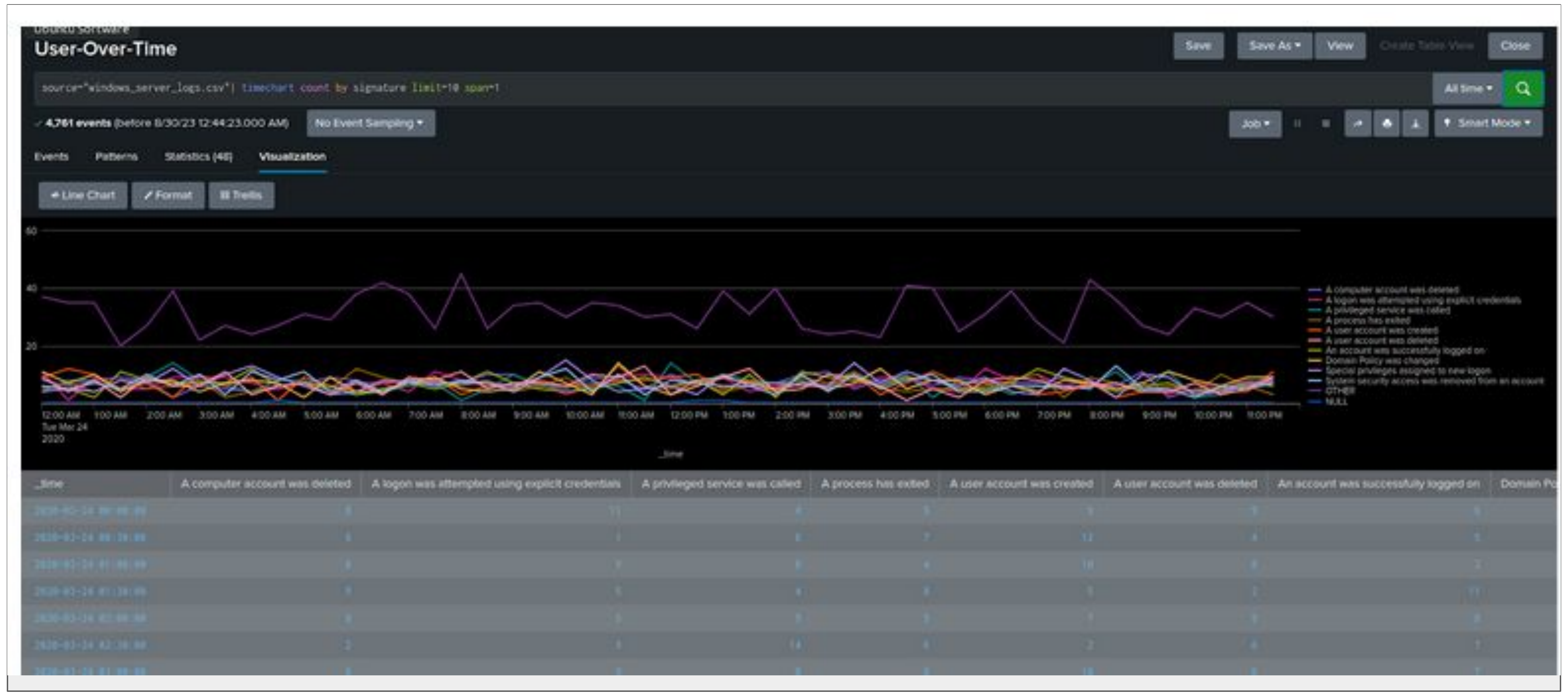
Baseline Alerts

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 29, 2023 1:24:10 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 18. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

Dashboards—Windows



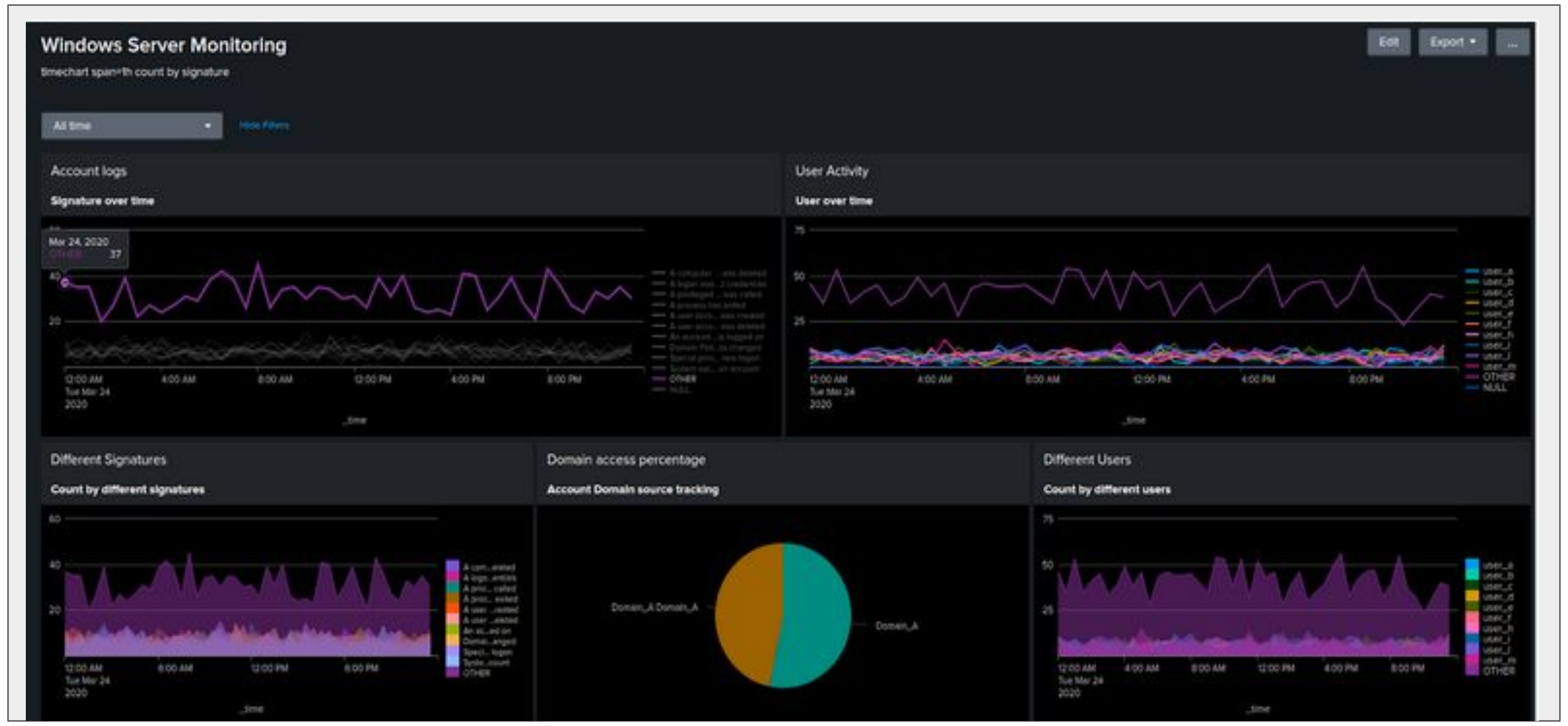
User-Over-Time

```
source="windows_server_logs.csv"| timechart count by signature limit=10 span=1
```

✓ 4,761 events (before 8/30/23 12:44:23.000 AM)

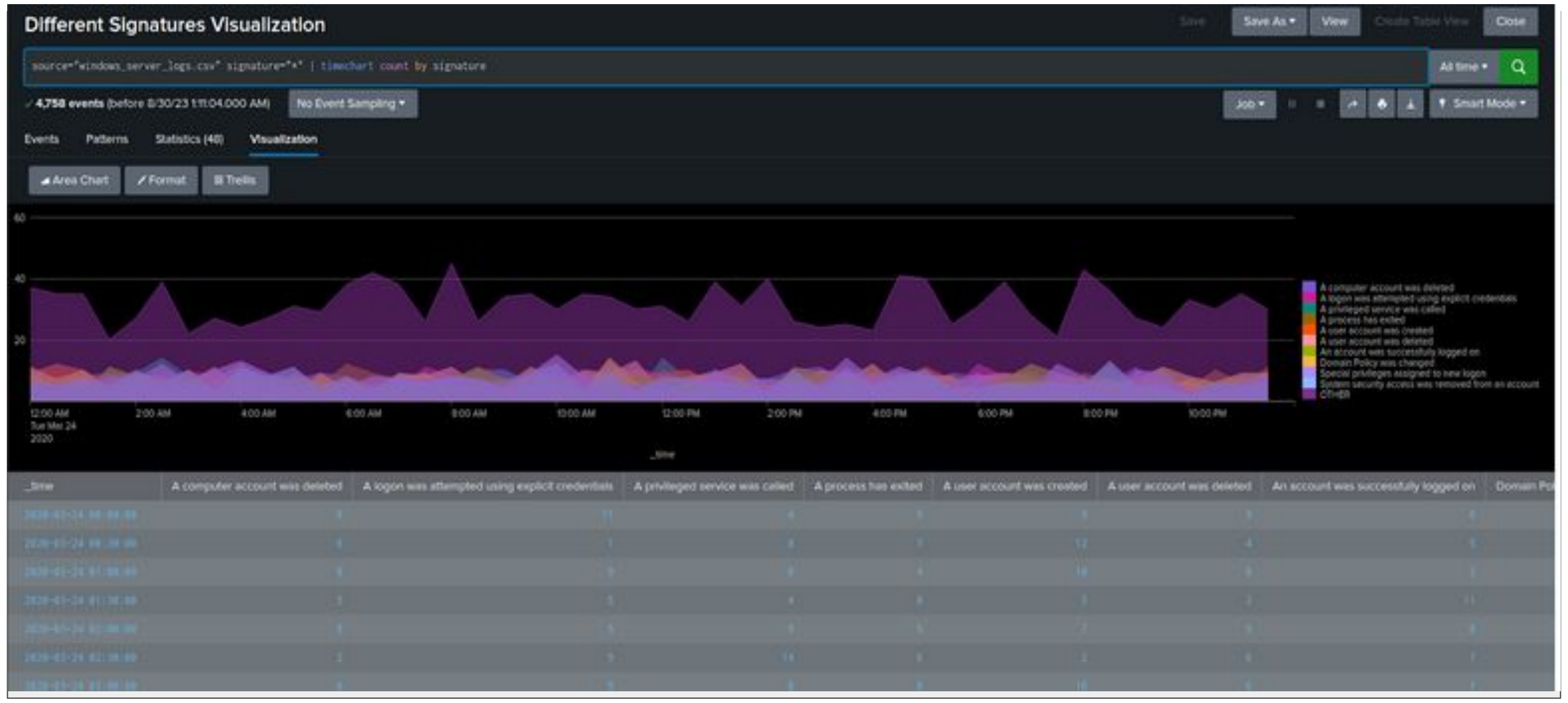
Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (48)
Visualization
Line Chart
Format
Trellis
60
40
20
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
NULL
12:00 AM
Tue Mar 24
2020
_time

_time	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 created	A user account was deleted	An account was successfully logged on	Domain Po
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	



Windows Server Monitoring

timechart span=1h count by signature



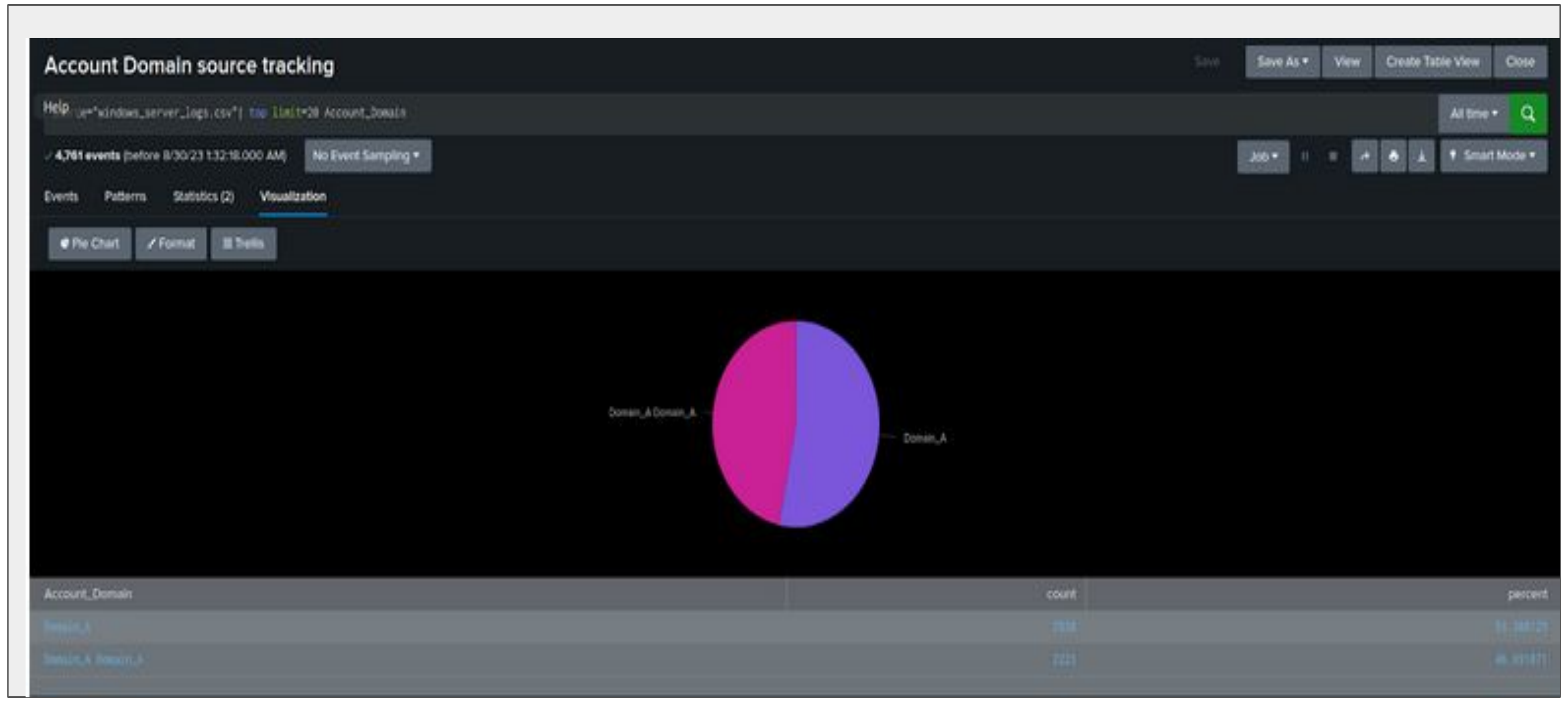
Different Signatures Visualization

```
source="windows_server_logs.csv" signature="*" | timechart count by signature
```

✓ 4,758 events (before 8/30/23 1:11:04.000 AM)

Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (48)
Visualization
Area Chart
Format
Trellis
60
40
20
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 created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
12:00 AM
Tue Mar 24
2020
_time

_time	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 created	A user account was deleted	An account was successfully logged on	Domain Po
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	



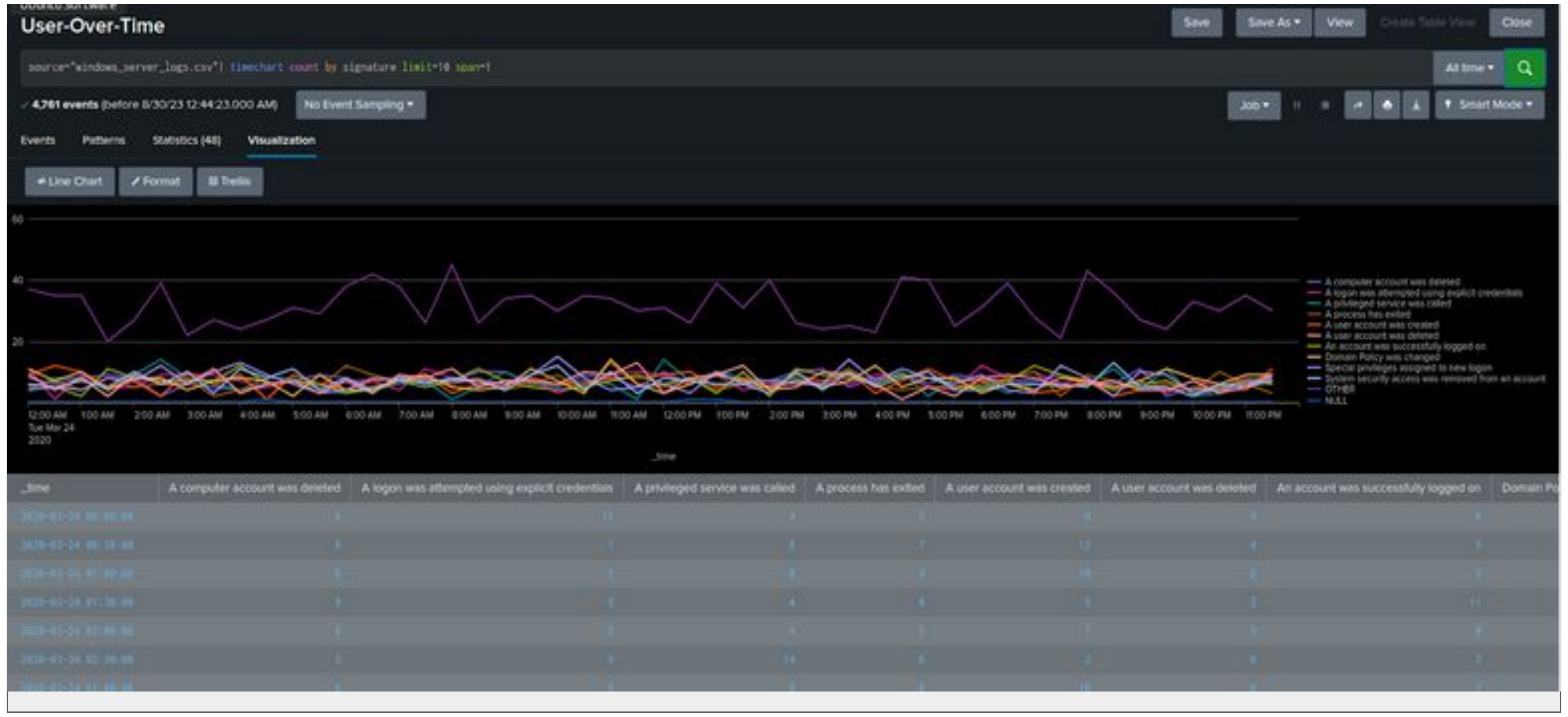
Account Domain source tracking

```
ce="windows_server_logs.csv"| top limit=20 Account_Domain
```

✓ 4,761 events (before 8/30/23 1:32:18.000 AM)

Account_Domain	count	percent
Domain_A	[illegible]	[illegible]
Domain_A Domain_A	[illegible]	[illegible]

Dashboards—Windows

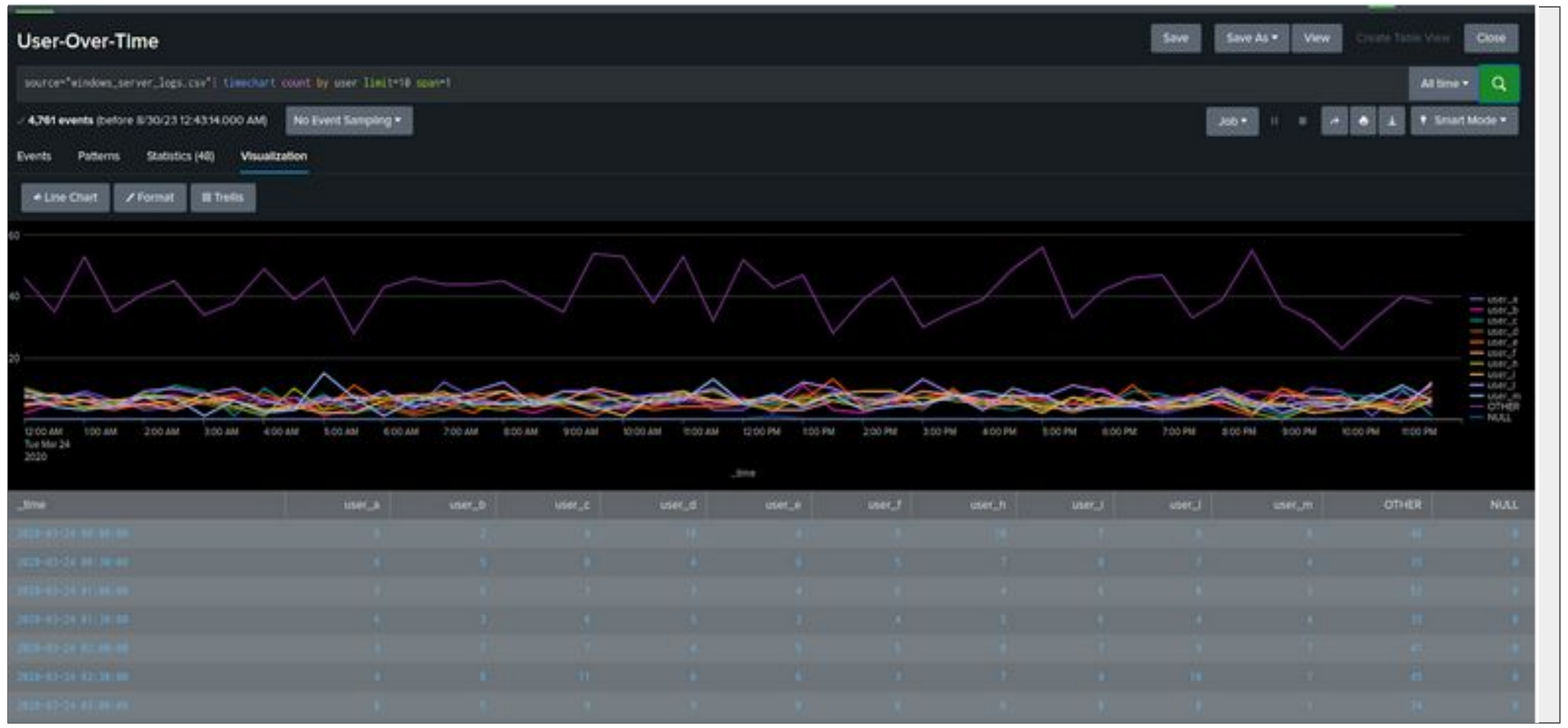


User-Over-Time

```
source="windows_server_logs.csv"| timechart count by signature limit=10 span=1
```

✓ 4,761 events (before 8/30/23 12:44:23.000 AM)

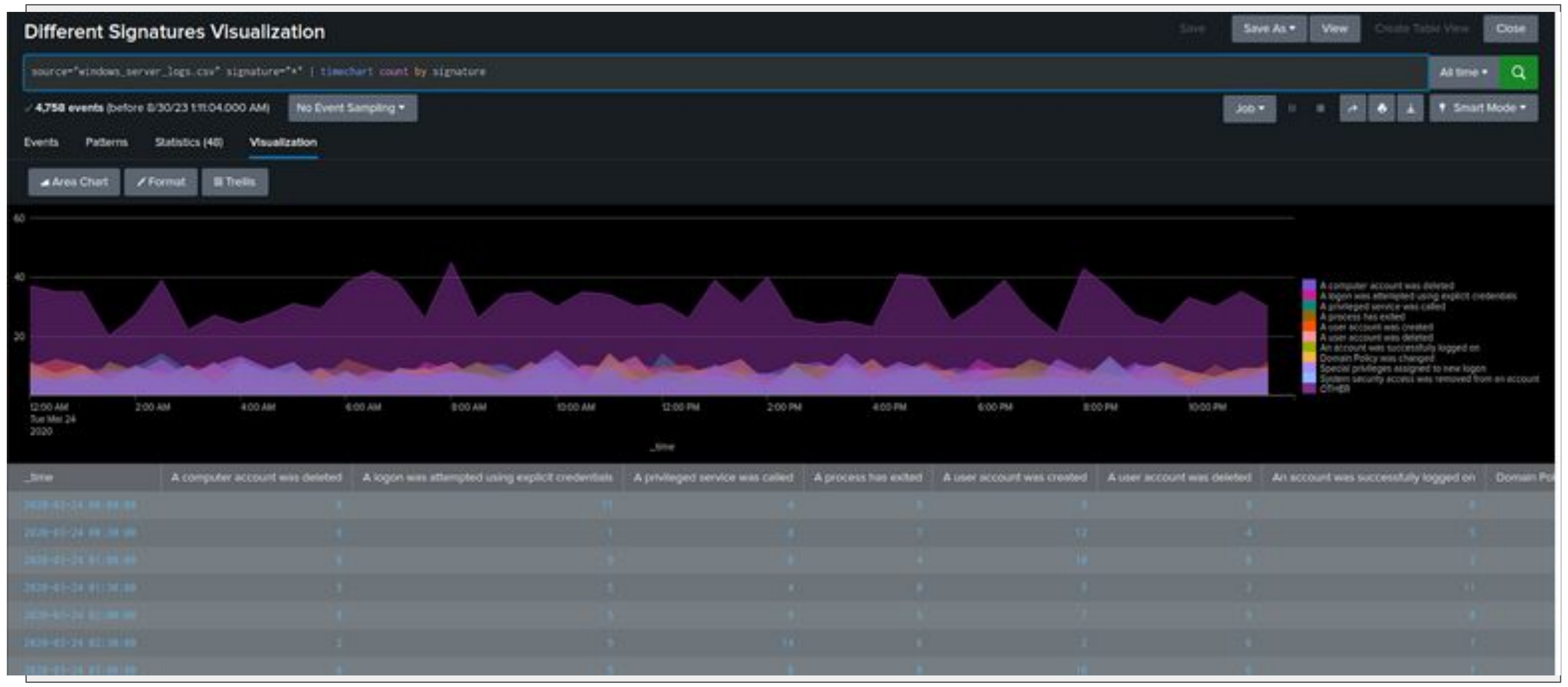
Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (48)
Visualization
Line Chart
Format
Trellis
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
NULL
_time
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 created
A user account was deleted
An account was successfully logged on
Domain Po



User-Over-Time

```
source="windows_server_logs.csv"| timechart count by user limit=10 span=1
```

✓ 4,761 events (before 8/30/23 12:43:14.000 AM)

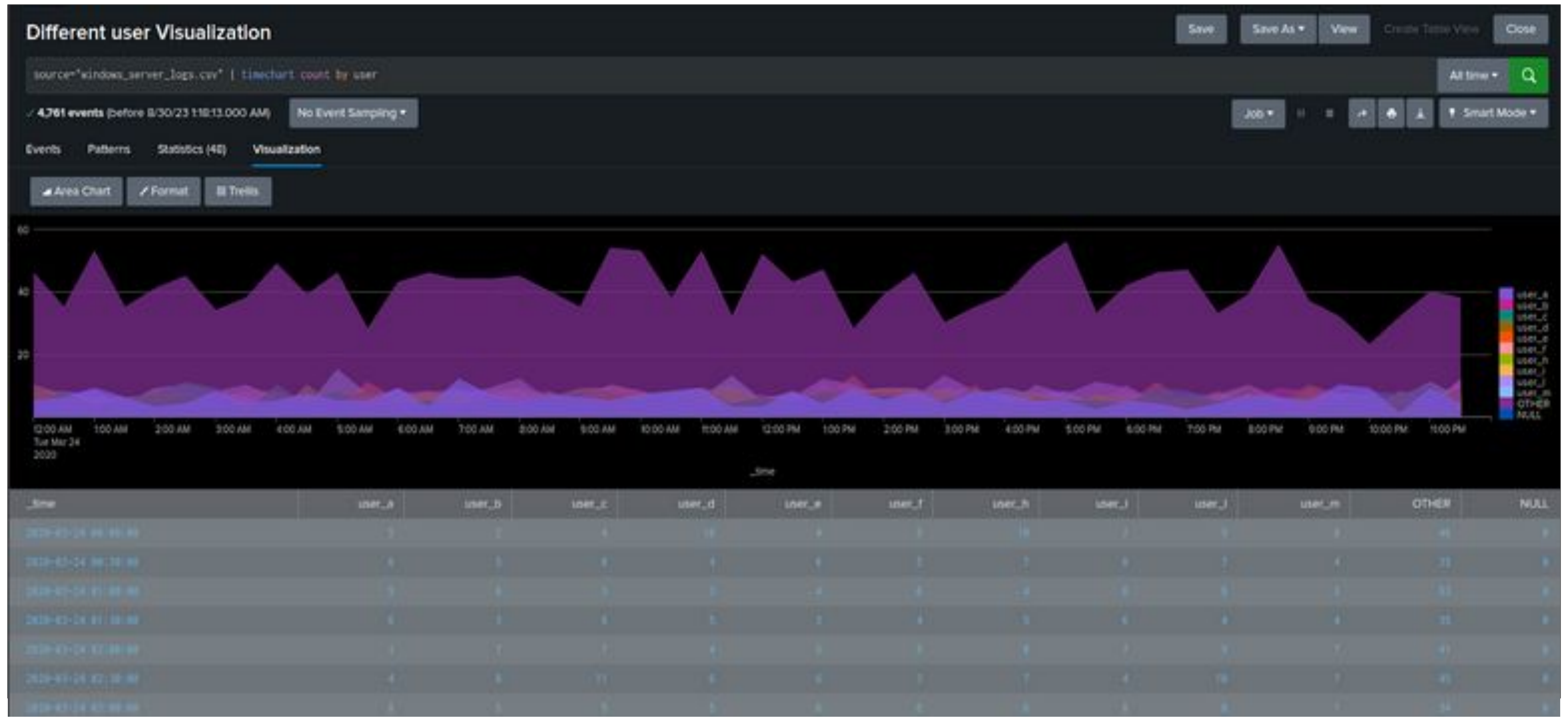


Different Signatures Visualization

```
source="windows_server_logs.csv" signature="*" | timechart count by signature
```

✓ 4,758 events (before 8/30/23 1:11:04.000 AM)

Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (48)
Visualization
Area Chart
Format
Trellis
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 created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER
_time
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 created
A user account was deleted
An account was successfully logged on
Domain Po



Different user Visualization

```
source="windows_server_logs.csv" | timechart count by user
```

✓ 4,761 events (before 8/30/23 1:18:13.000 AM)

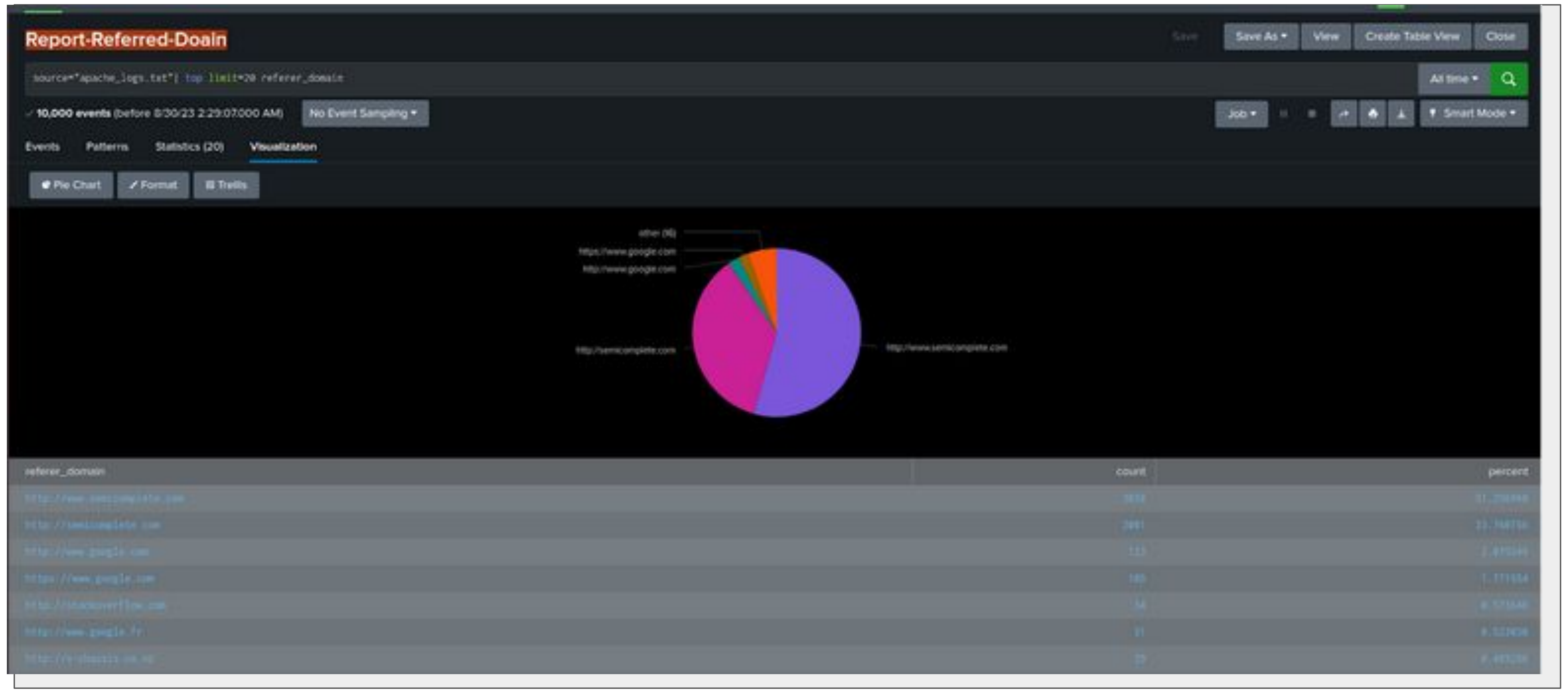
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
[Method]	[Analyzes the percent & count of various method]
[Referer Domain]	[Analyzes the different referrer domains]
[Http Response Code]	[Analyzes the different http reponse code]
[Http Post Activity]	[Setting up alerts for suspicious activity & volume of Http Post Activity]

Images of Reports—Apache

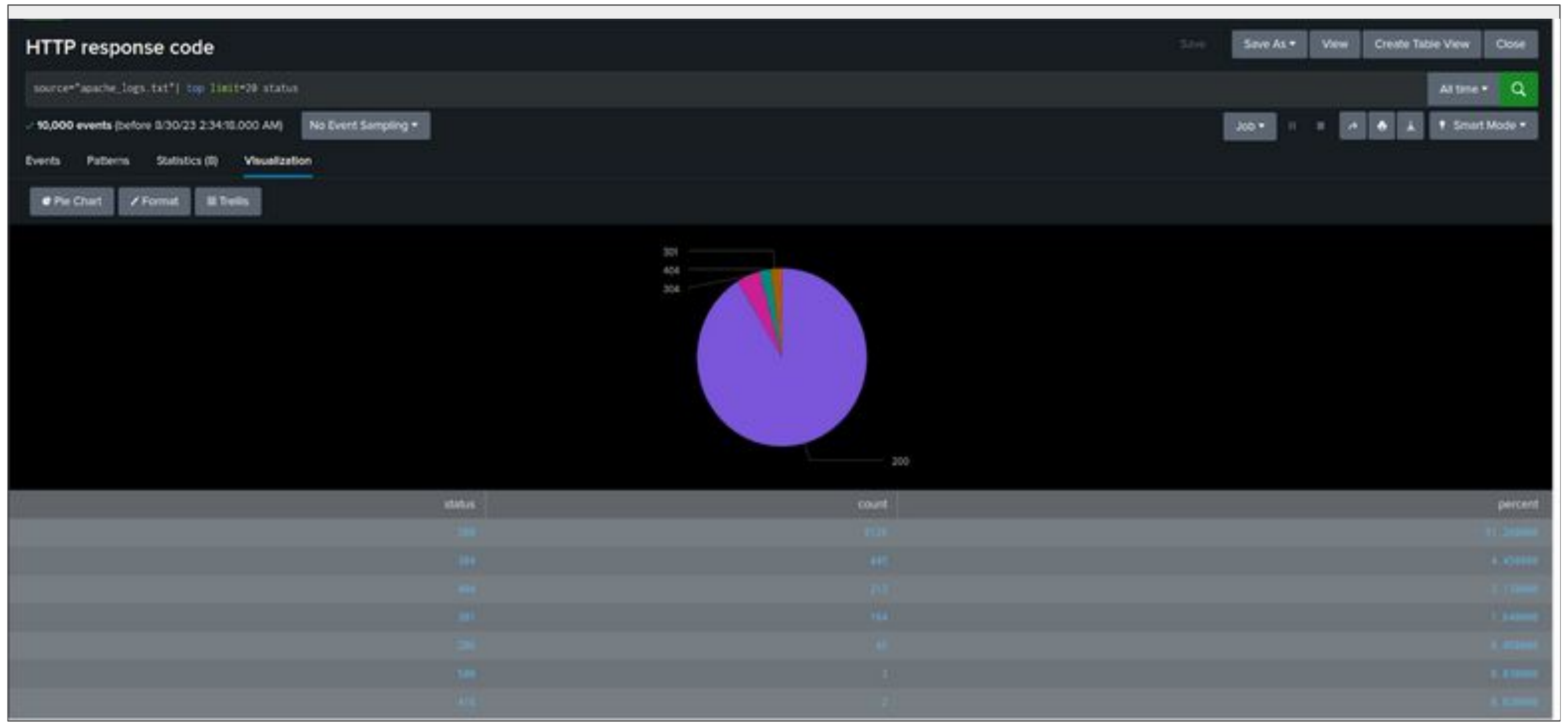


Report-Referred-Doain

```
source="apache_logs.txt"| top limit=20 referer_domain
```

✓ 10,000 events (before 8/30/23 2:29:07.000 AM)

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256940
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

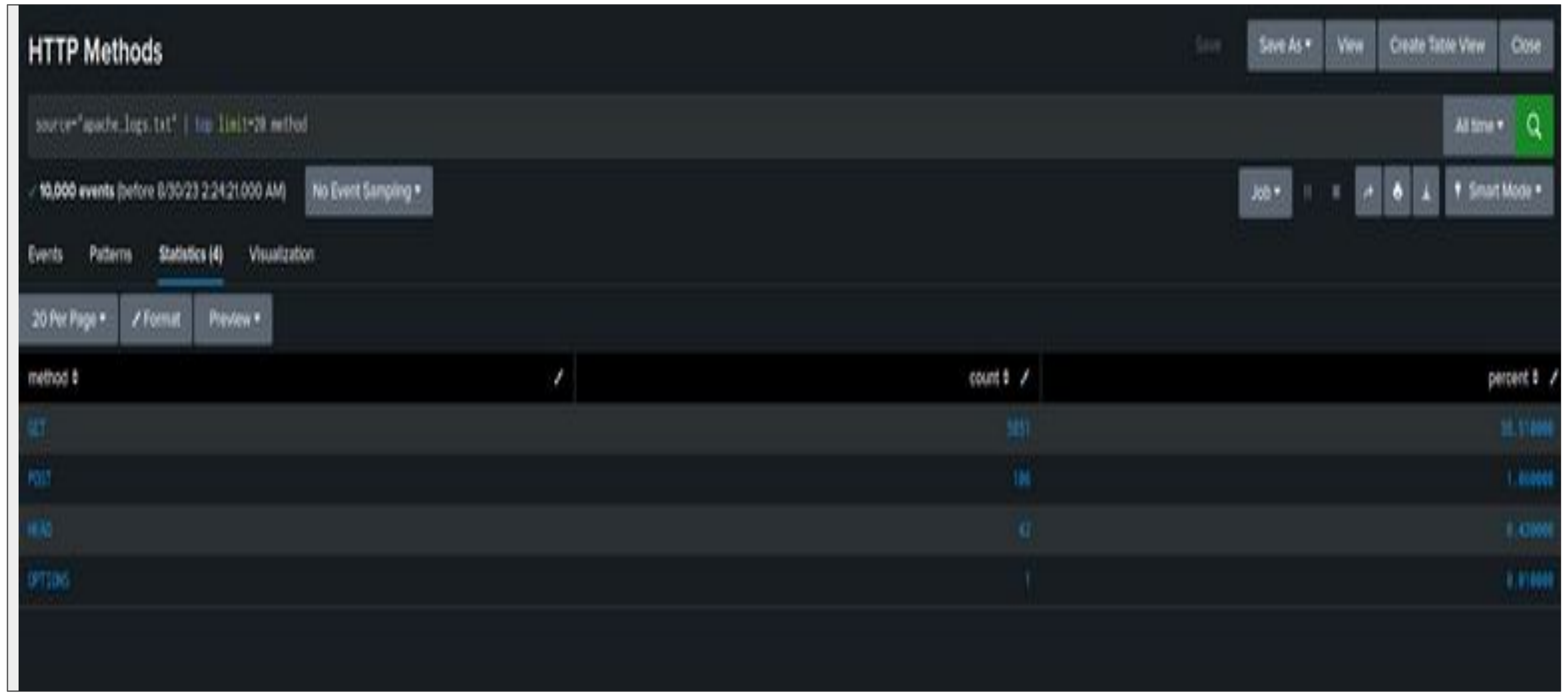


HTTP response code

```
source="apache_logs.txt"| top limit=20 status
```

✓ 10,000 events (before 8/30/23 2:34:18.000 AM)

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

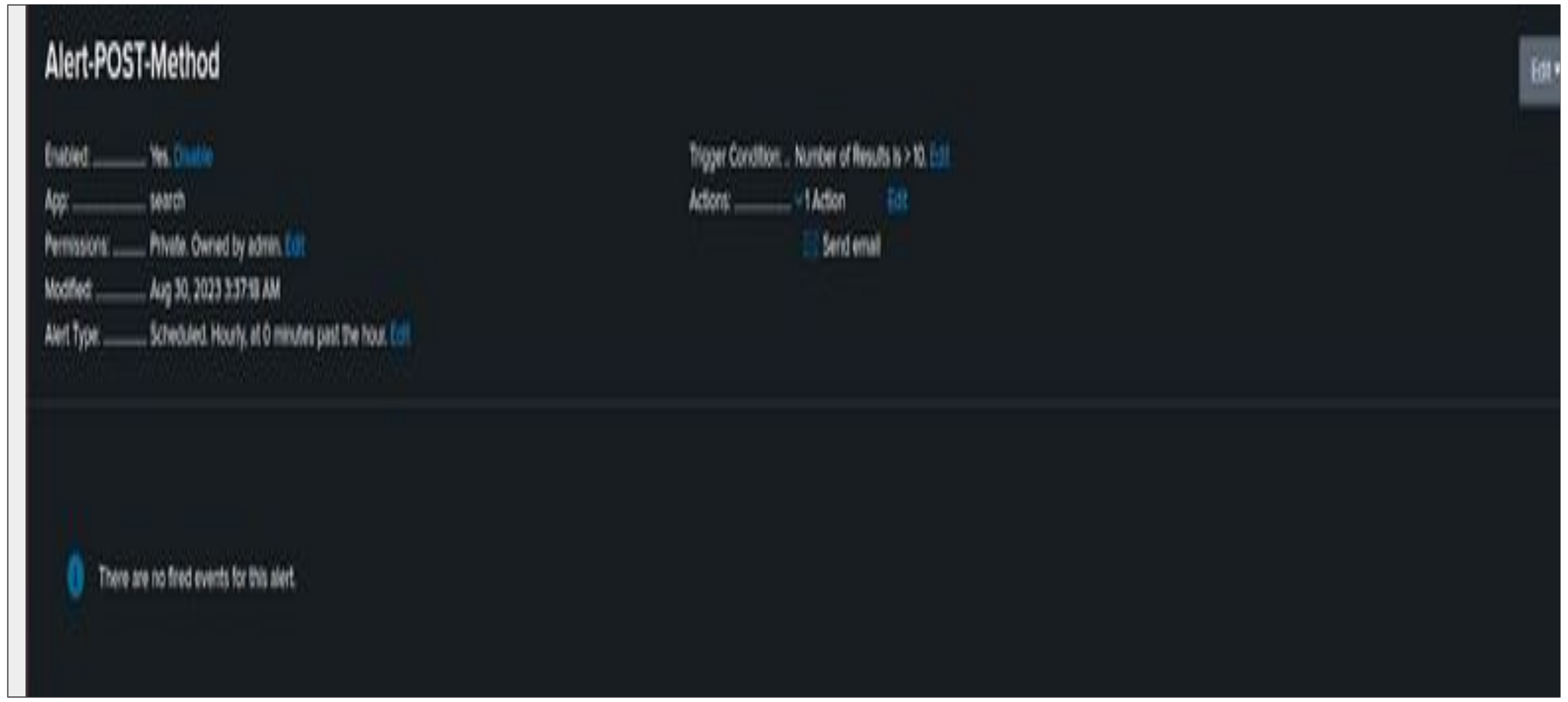


HTTP Methods

```
source="apache_logs.txt" | top limit=20 method
```

✓ 10,000 events (before 8/30/23 2:24:21.000 AM)

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



Alert-POST-Method

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 30, 2023 3:37:18 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 10. Edit
Actions: .... ✓1 Action Edit
Send email

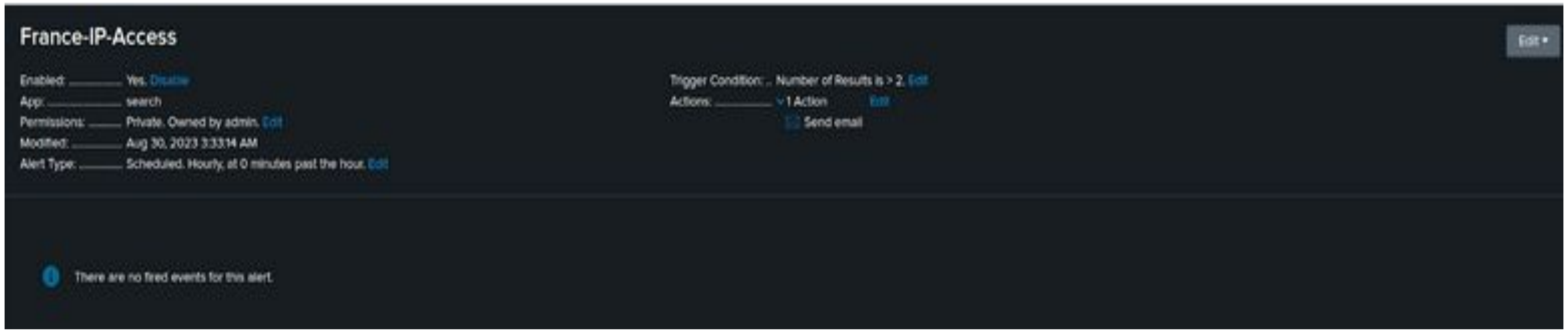
There are no fired events for this alert.

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[France IP Access]	[Scheduled alert type trigger condition greater than 2]	[Baseline]	[Greater than 2]

JUSTIFICATION:



France-IP-Access

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 30, 2023 3:33:14 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 2. Edit
Actions: .... 1 Action Edit
Send email

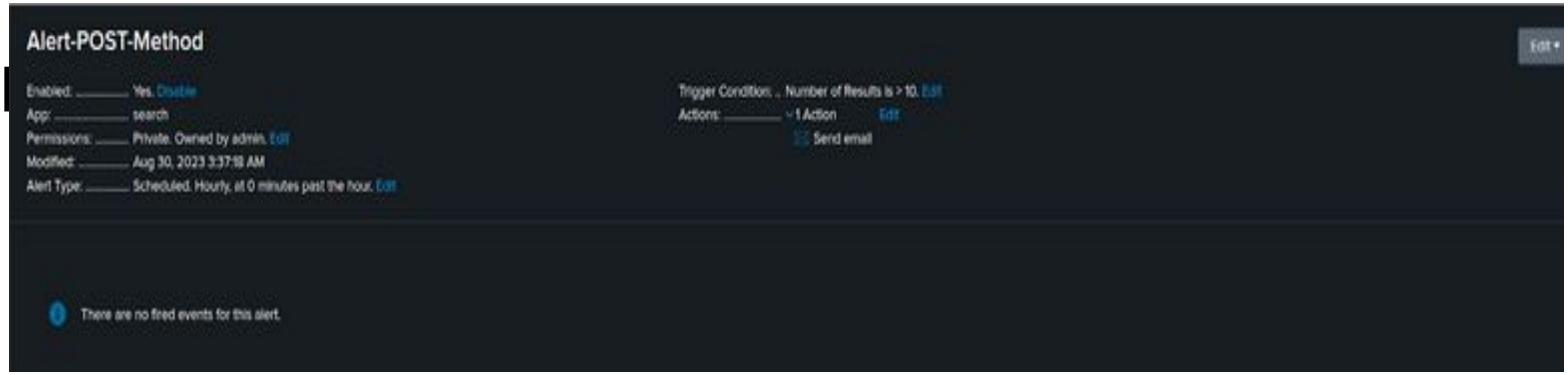
There are no fired events for this alert.

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
[Alert Post Method]	[Scheduled alert trigger condition greater than 10]	[Baseline]	[Greater than 10]

JUSTIFICATION: [



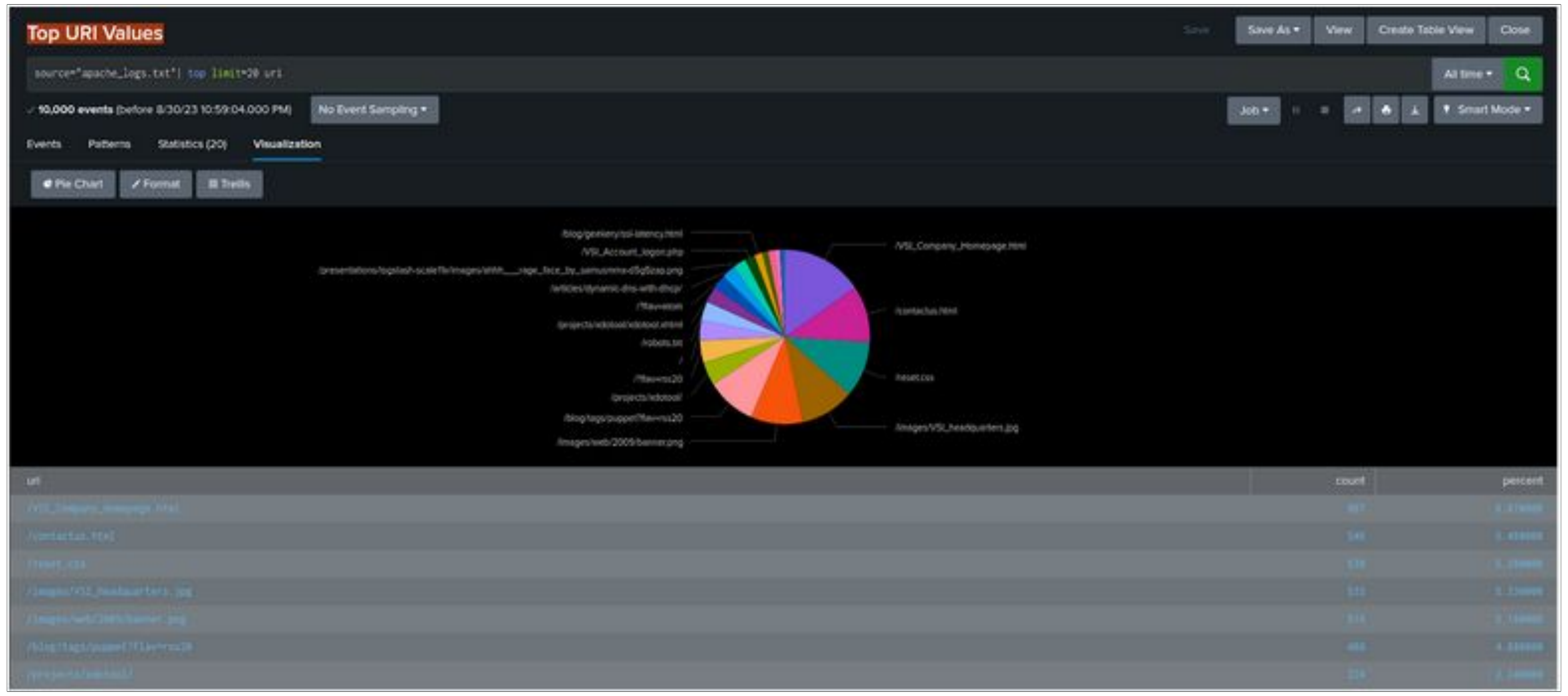
Alert-POST-Method

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 30, 2023 3:37:18 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 10. Edit
Actions: .... ⌄1 Action Edit
Send email

There are no fired events for this alert.

Dashboards—Apache



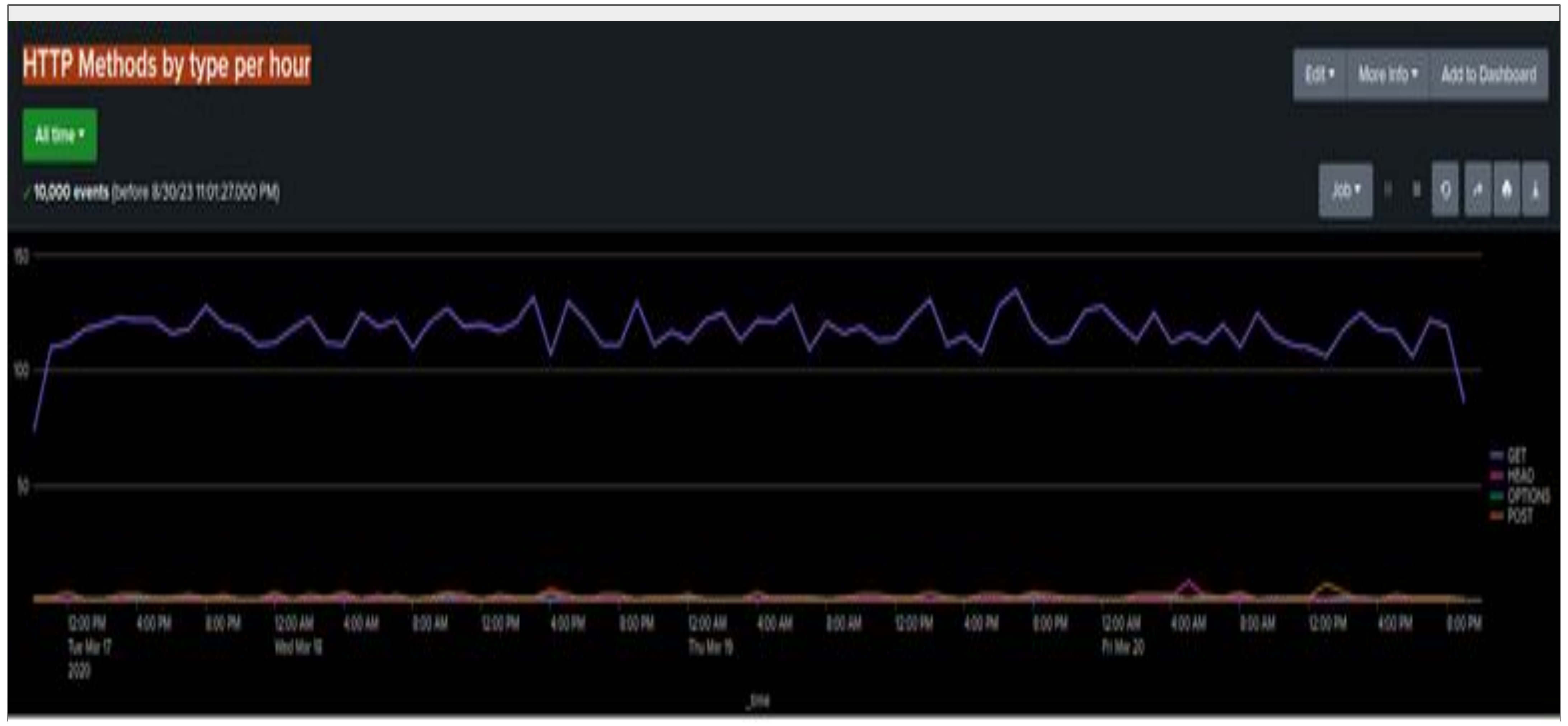
Top URI Values

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

✓ 10,000 events (before 8/30/23 10:59:04.000 PM)

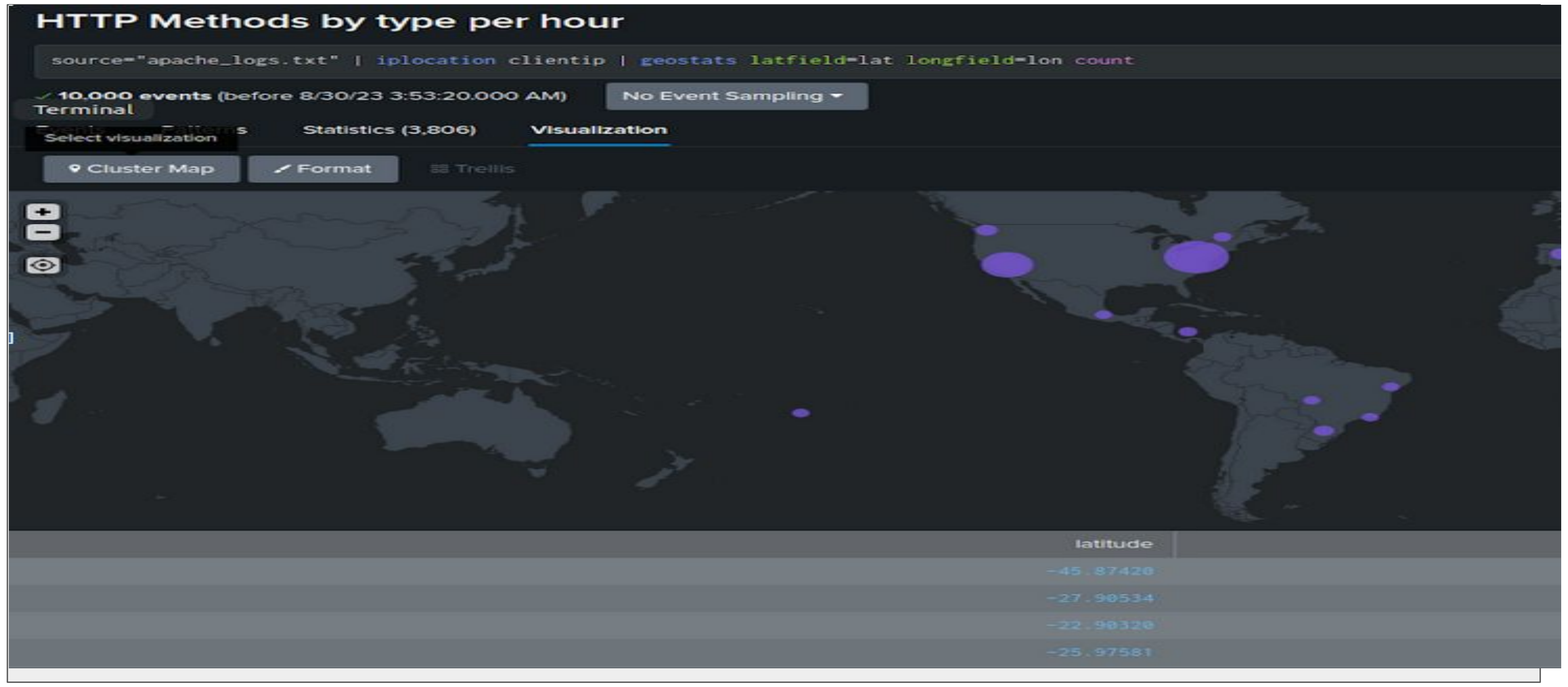
Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (20)
Visualization
Pie Chart
Format
Trellis
/blog/geekery/ssl-latency.html
/VSI_Account_logon.php
/presentations/logstash-scale11x/images/ahhh___rage_face_by_samusmmx-d5g5zap.png
/articles/dynamic-dns-with-dhcp/
/?flav=atom
/projects/xdotool/xdotool.xhtml
/robots.txt
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg

uri	count	percent
/VSI_Company_Homepage.html	[illegible]	[illegible]
/contactus.html	[illegible]	[illegible]
/reset.css	[illegible]	[illegible]
/images/VSI_headquarters.jpg	[illegible]	[illegible]
/images/web/2009/banner.png	[illegible]	[illegible]
/blog/tags/puppet?flav=rss20	[illegible]	[illegible]
/projects/xdotool/	[illegible]	[illegible]



HTTP Methods by type per hour

✓ 10,000 events (before 8/30/23 11:01:27.000 PM)

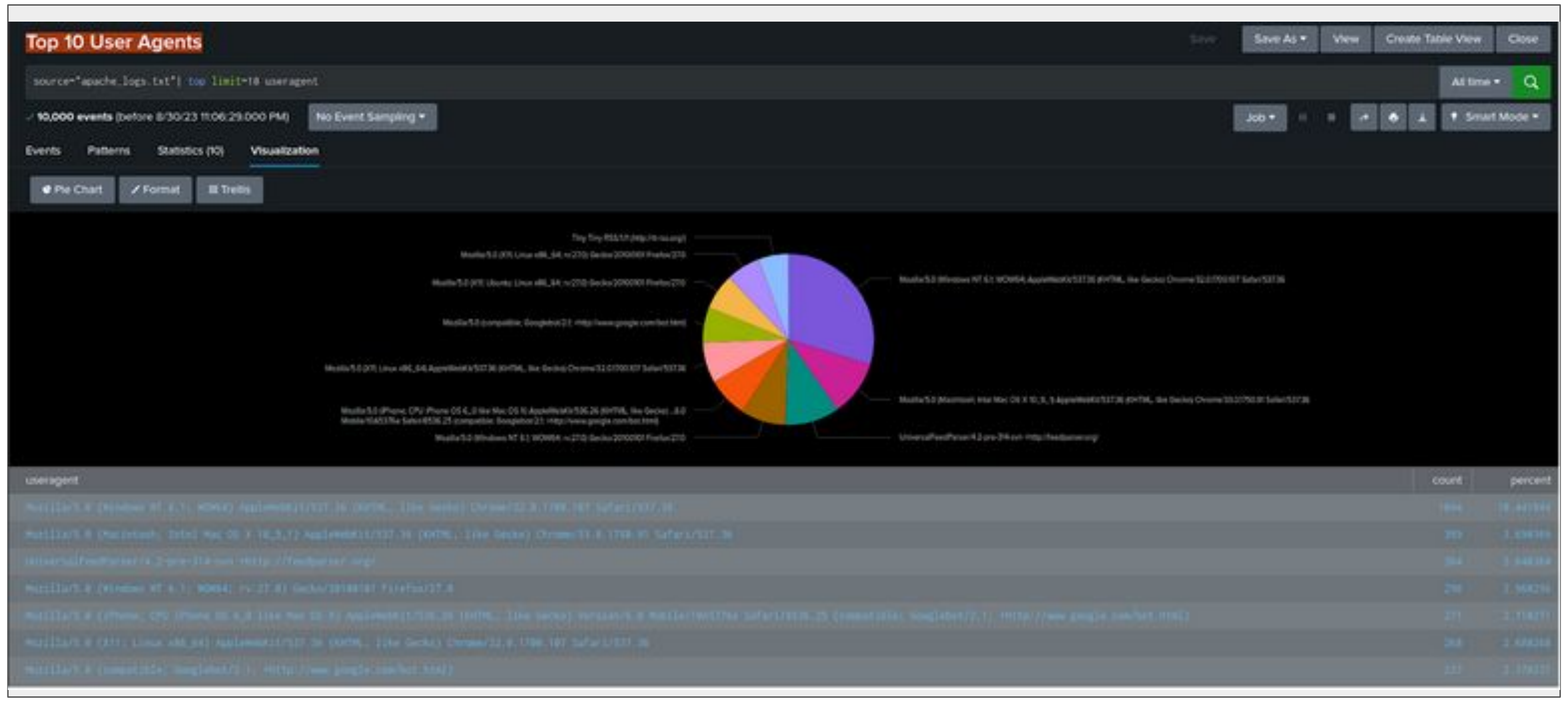


HTTP Methods by type per hour

```
source="apache_logs.txt" | iplocation clientip | geostats latfield=lat longfield=lon count
```

✓ 10,000 events (before 8/30/23 3:53:20.000 AM)

latitude
-45.87420
-27.98534
-22.90320
-25.97581



Top 10 User Agents

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

✓ 10,000 events (before 8/30/23 11:06:29.000 PM)

Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (10)
Visualization
Pie Chart
Format
Trellis
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) ...6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/

useragent	count	percent
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	[illegible]	[illegible]
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36	[illegible]	[illegible]
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	[illegible]	[illegible]
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	[illegible]	[illegible]
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	[illegible]	[illegible]
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	[illegible]	[illegible]
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	[illegible]	[illegible]

Attack Analysis

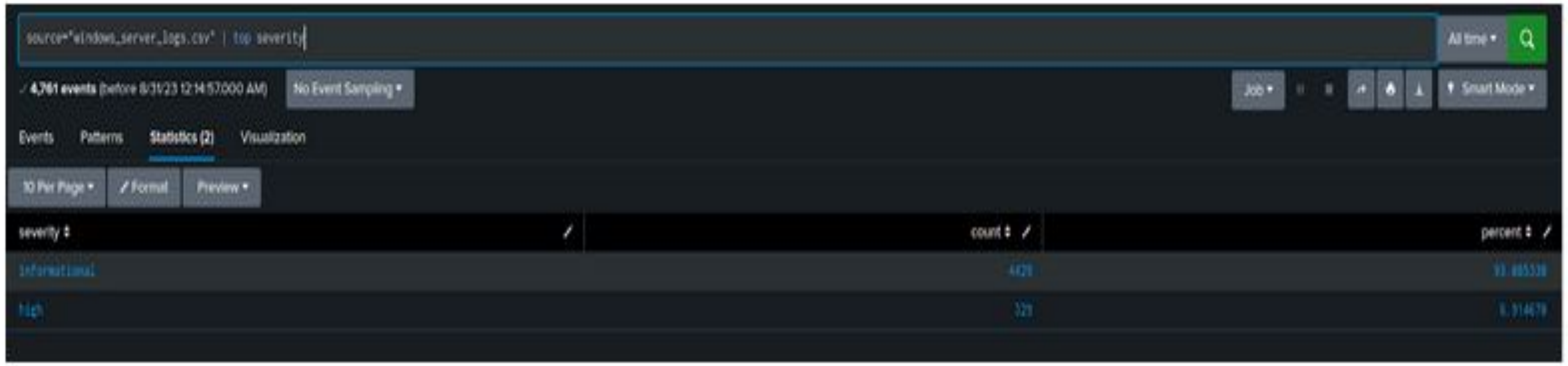
Attack Summary—Windows

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

SPLUNK DAY 2

- —

TOP SEVERITY- LOGS



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

✓ 4,761 events (before 8/31/23 12:14:57.000 AM)

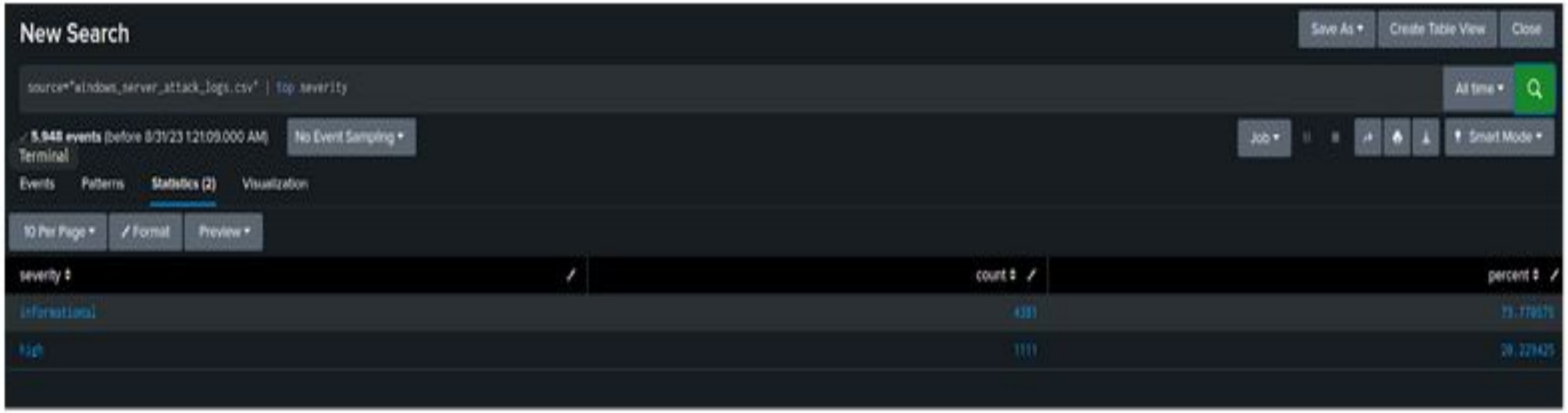
severity	count	percent
informational	4429	93.085330
high	329	6.914670

TOP SEVERITY- ATTACKS

Attack Summary—Windows

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

-



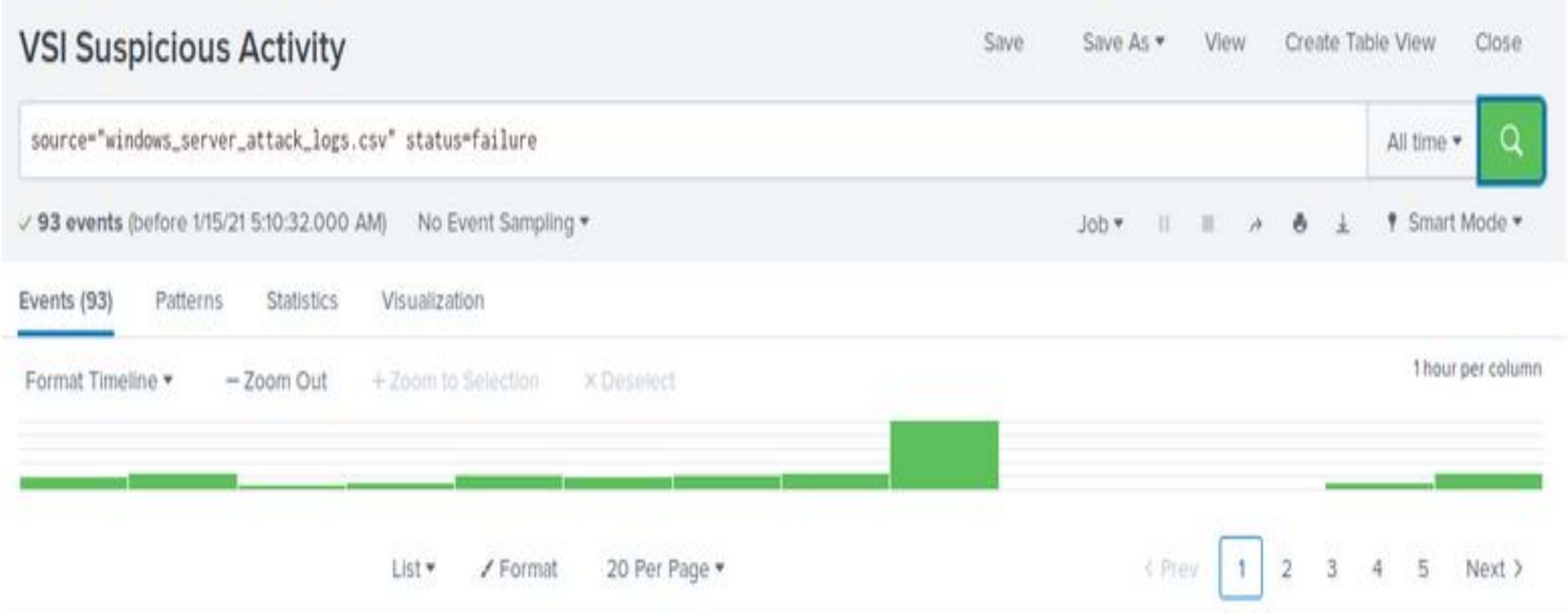
```
source="windows_server_attack_logs.csv" | top severity
```

✓ 5,948 events (before 8/31/23 1:21:09.000 AM)

severity	count	percent
informational	4383	79.778575
high	1111	20.221425

Attack Summary—Windows

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



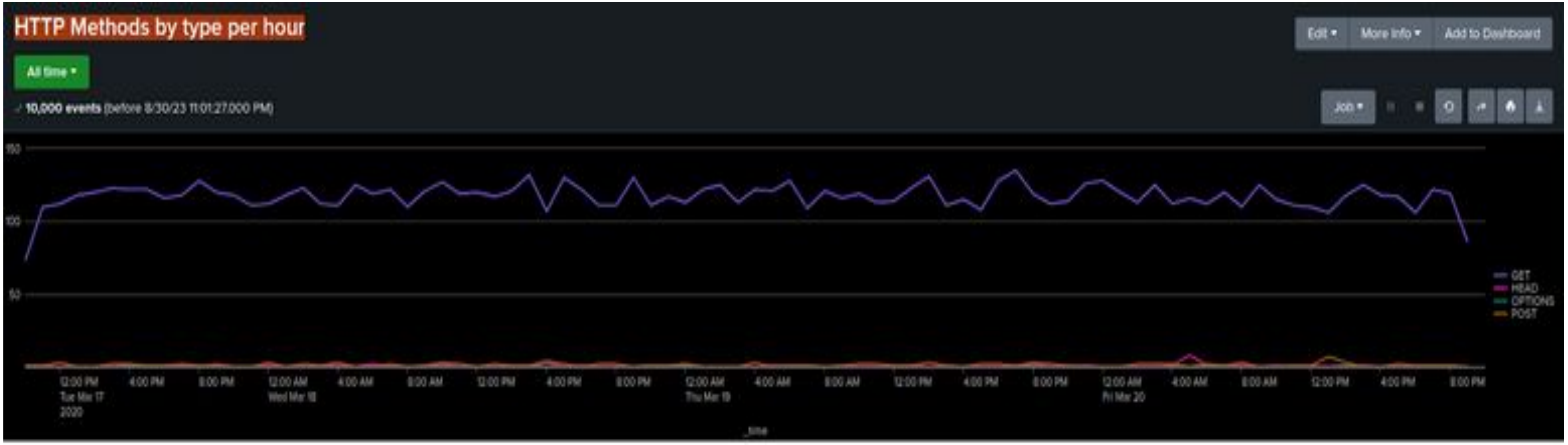
VSI Suspicious Activity

```
source="windows_server_attack_logs.csv" status=failure
```

✓ 93 events (before 1/15/21 5:10:32.000 AM)

Attack Summary—Apache

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

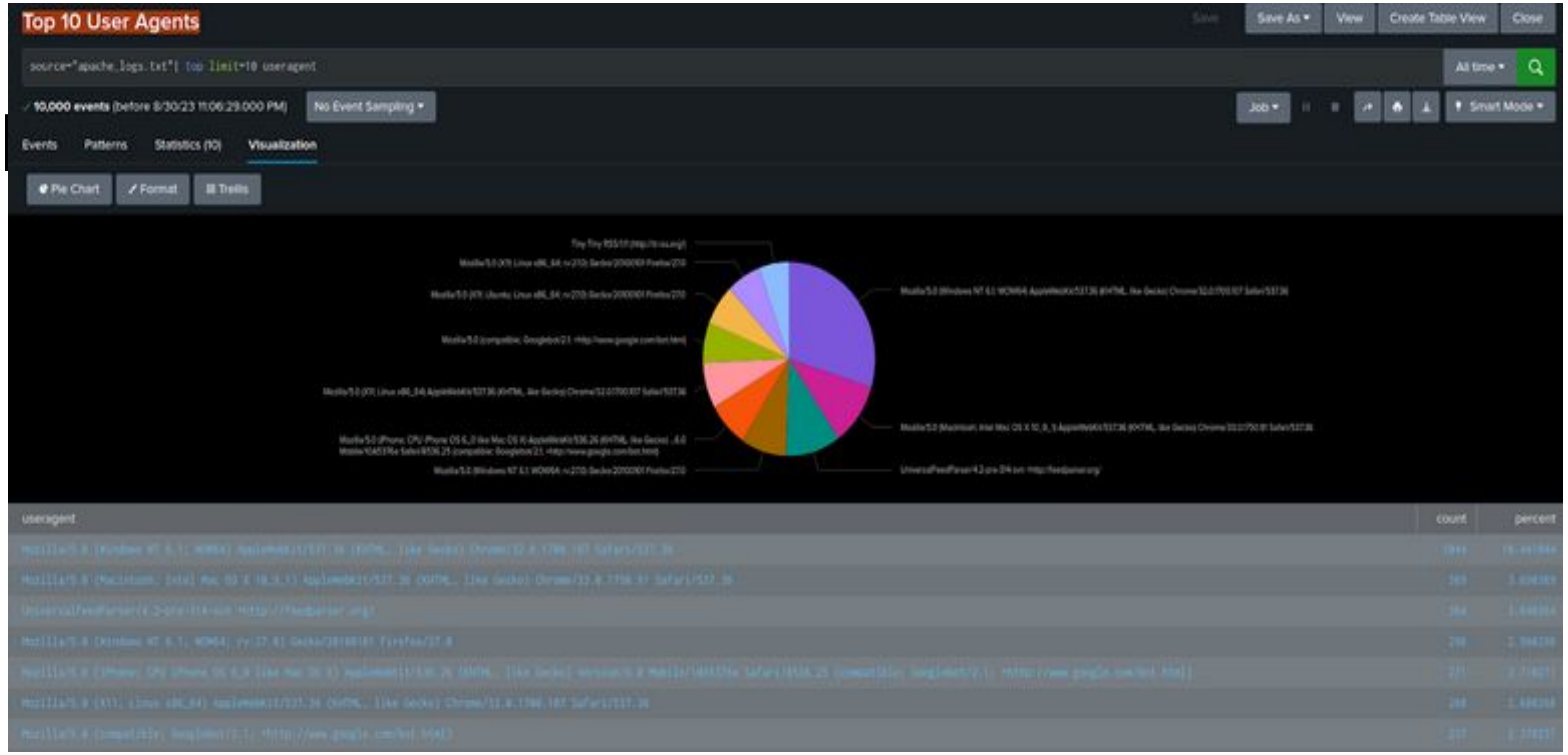
- 

HTTP Methods by type per hour

✓ 10,000 events (before 8/30/23 11:01:27.000 PM)

Attack Summary—Apache

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

- 

Save
Save As ▾
View
Create Table View
Close
All time ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (10)
Visualization
Pie Chart
Format
Trellis
Tiny Tiny RSS/1.11 (http://tt-rss.org/)
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/

Top 10 User Agents

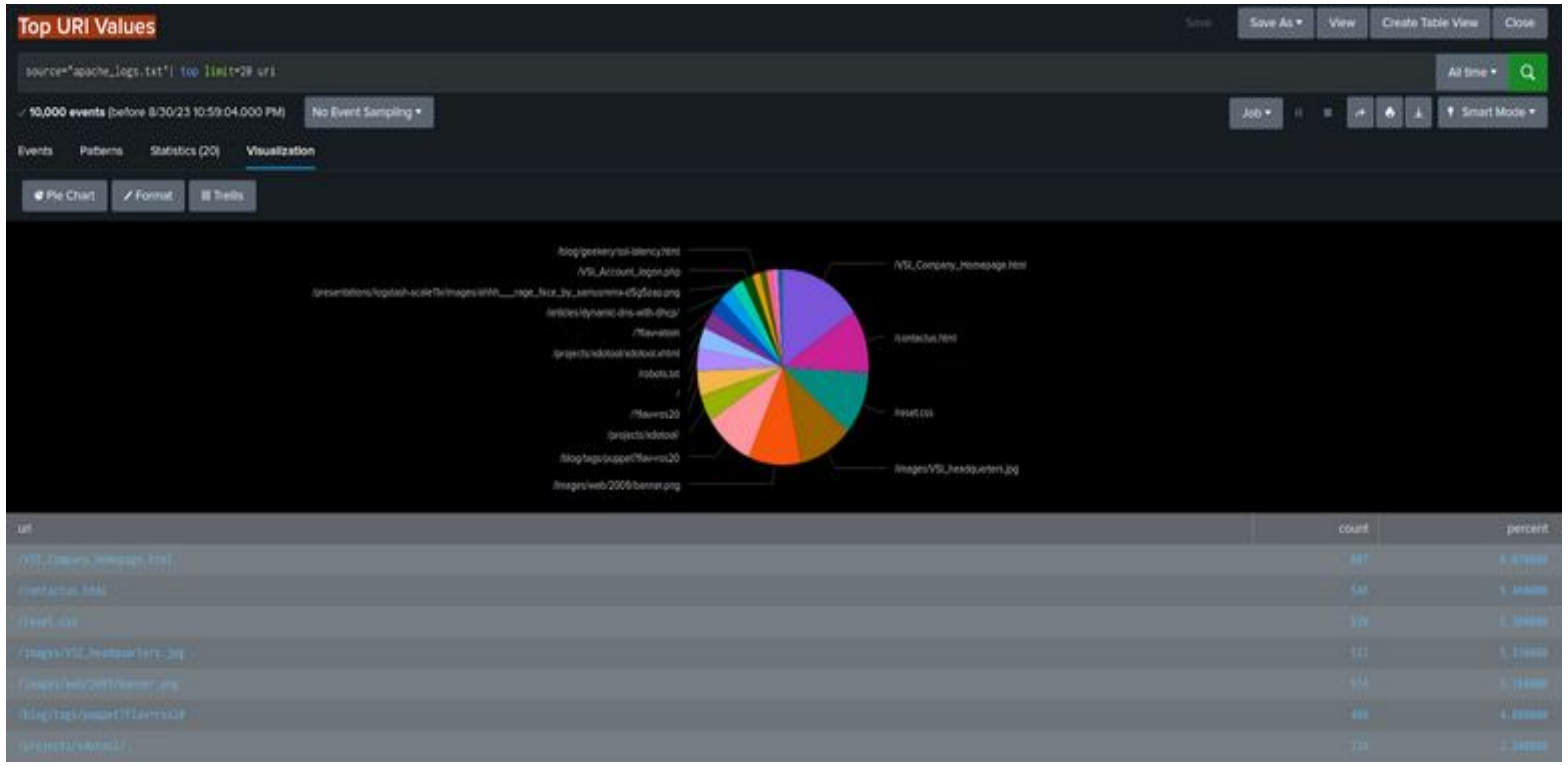
```
source="apache_logs.txt"| top limit=10 useragent
```

✓ 10,000 events (before 8/30/23 11:06:29.000 PM) No Event Sampling ▾

useragent	count	percent
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1044	10.440000
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36	369	3.690000
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364	3.640000
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	298	2.980000
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	271	2.710000
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268	2.680000
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237	2.370000

Attack Summary—Apache

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

- 

Top URI Values

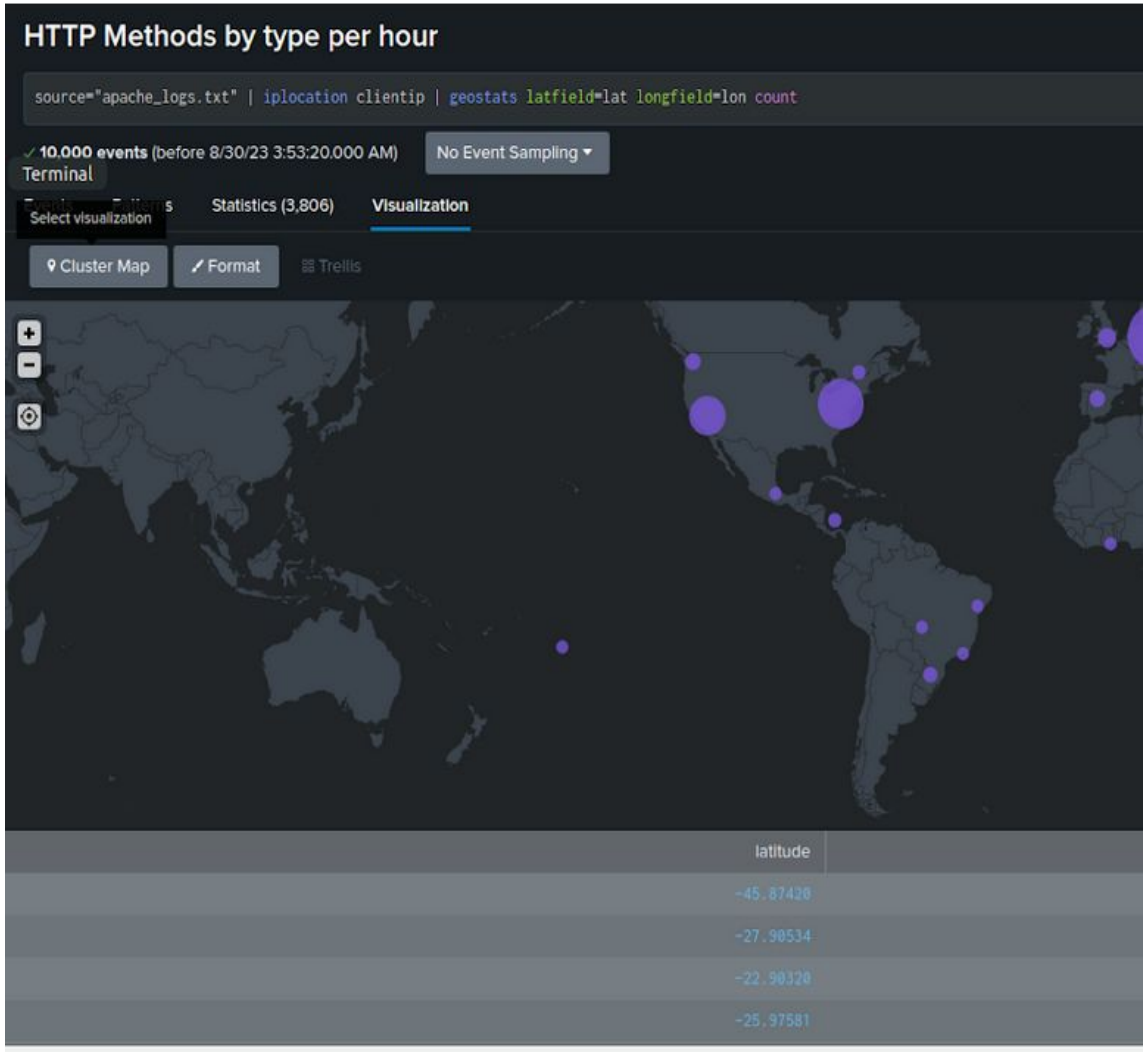
```
source="apache_logs.txt"| top limit=20 uri
```

✓ **10,000 events** (before 8/30/23 10:59:04.000 PM)

Save
Save As ▾
View
Create Table View
Close
All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (20)
Visualization
Pie Chart
Format
Trellis
/blog/geekery/ssl-latency.html
/VSI_Account_logon.php
/presentations/logstash-scale11x/images/ahhh___rage_face_by_samusmmx-d5g5zap.png
/articles/dynamic-dns-with-dhcp/
/?flav=atom
/projects/xdotool/xdotool.xhtml
/robots.txt
/
/?flav=rss20
/projects/xdotool/
/blog/tags/puppet?flav=rss20
/images/web/2009/banner.png
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg

uri	count	percent
/VSI_Company_Homepage.html	[illegible]	[illegible]
/contactus.html	[illegible]	[illegible]
/reset.css	[illegible]	[illegible]
/images/VSI_headquarters.jpg	[illegible]	[illegible]
/images/web/2009/banner.png	[illegible]	[illegible]
/blog/tags/puppet?flav=rss20	[illegible]	[illegible]
/projects/xdotool/	[illegible]	[illegible]

Screenshots of Attack Logs



HTTP Methods by type per hour

```
source="apache_logs.txt" | iplocation clientip | geostats latfield=lat longfield=lon count
```

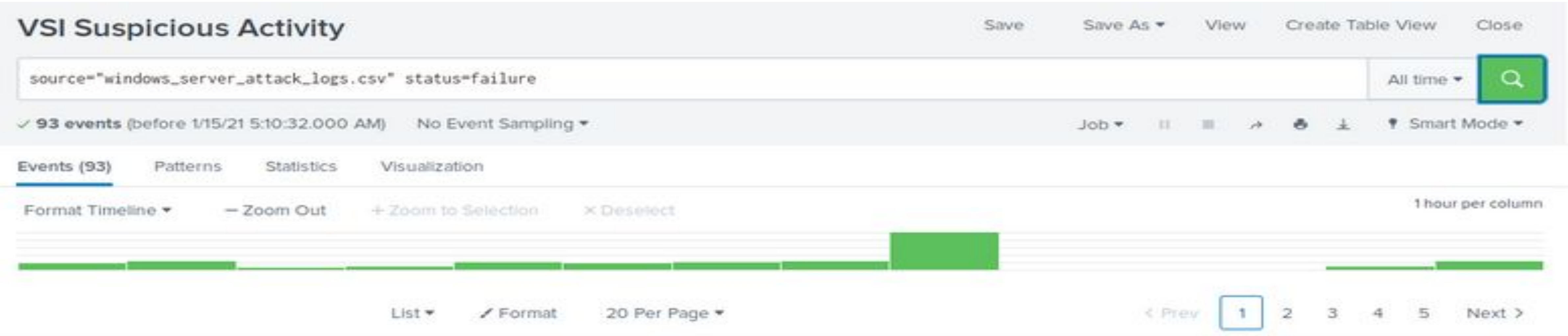
✓ 10,000 events (before 8/30/23 3:53:20.000 AM)

latitude
-45.87420
-27.90534
-22.90320
-25.97581

Summary and Future Mitigations

Project 3 Summary

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



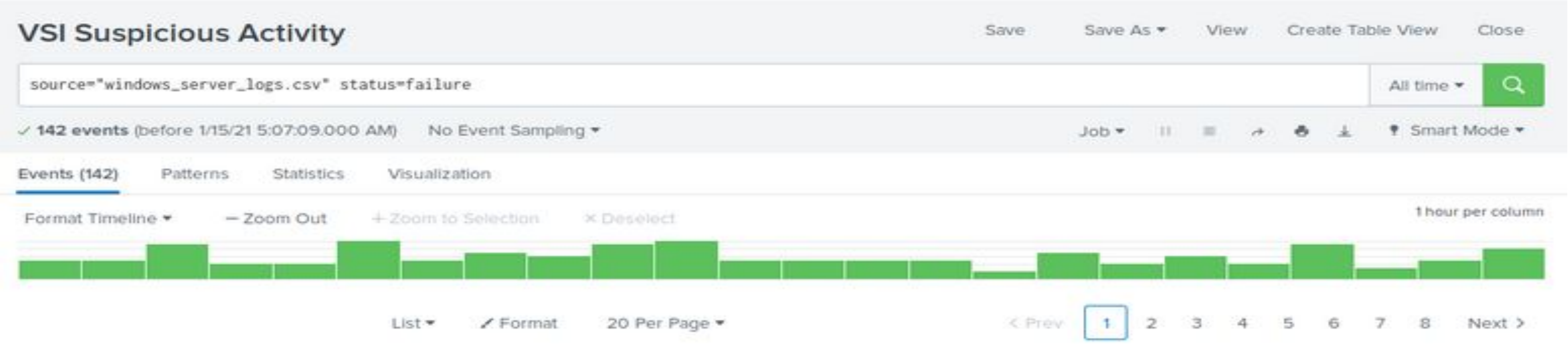
VSI Suspicious Activity

```
source="windows_server_attack_logs.csv" status=failure
```

✓ 93 events (before 1/15/21 5:10:32.000 AM) No Event Sampling ▾

Events (93)

1 hour per column



VSI Suspicious Activity

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

✓ 142 events (before 1/15/21 5:07:09.000 AM) No Event Sampling ▾

Events (142)

1 hour per column

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

  [I would consider raising the thresholds on alerts. Also using statistical charts providing a comprehensive view of identification outliners for unusual activities as they will stand out from typical statistical patterns.]