The Splunkings

Defensive Security Project by:

Alex Bourjau, Travis Meyer, Mohsen Rezaei,
Nicholas Spencer, Cameron Whitford

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Scenario

- Working in the SOC for Virtual Space Industries (VSI).
- Tasked to build a monitoring solution with Splunk after rumors that JobeCorp (a competing company) may launch disruptive cyberattacks.
- Monitoring VSI's Apache web server hosting an administrative web page, as well as a Windows server running back-end operations.
- VSI then experienced cyber attacks that took down several systems, targeting the Apache and Windows servers.
- Analysed logs from during the attack to determine what happened, whether our monitoring solution was effective and guide further mitigation strategies.

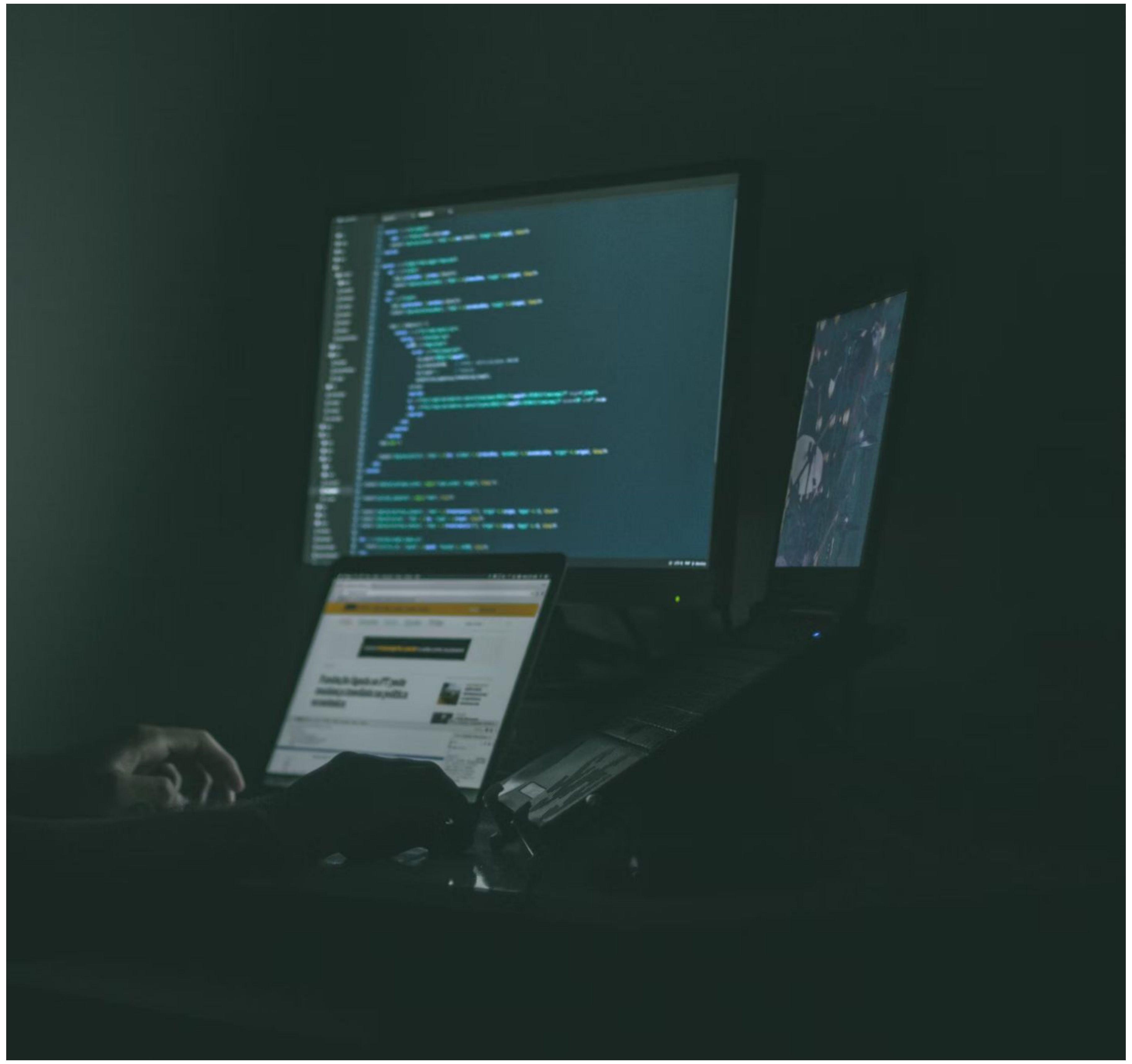
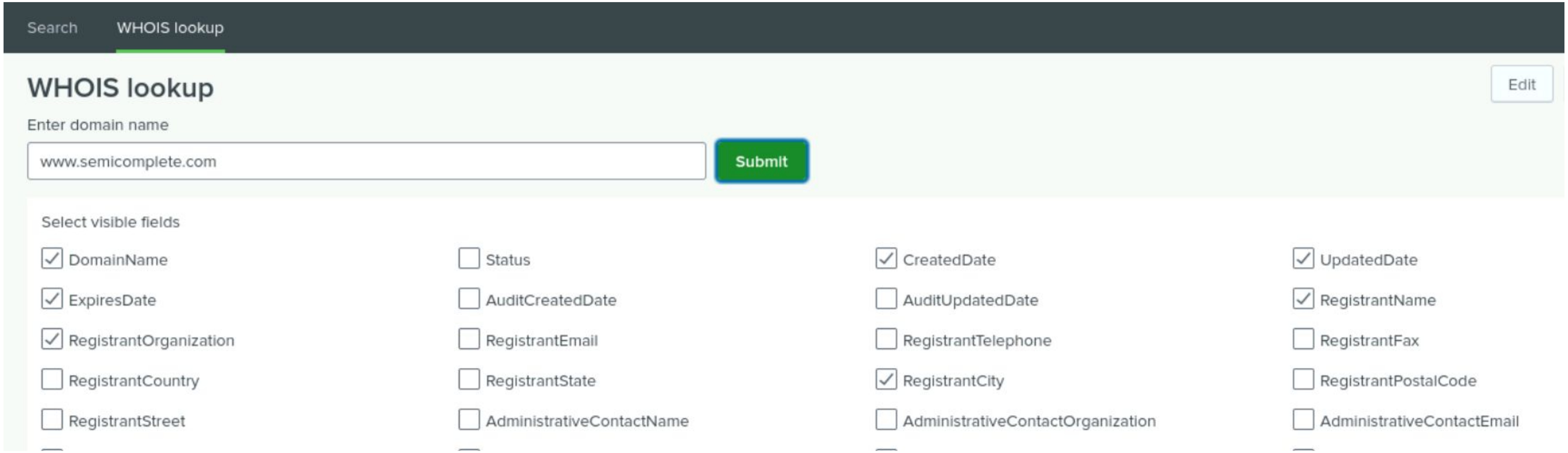


Photo by Jefferson Santos on Unsplash

WHOIS “Add-On” App

Whois XML History API

- Splunk Add-On app “Whois XML History API”.
- Required installing the app, registering with the WHOIS provider and configuring the API key.
- Allows integrated searching of current and historical domain WHOIS information within Splunk.
- Performing a WHOIS lookup of a domain name can provide information about the domain registration details, potentially including contact details.



WHOIS lookup

Enter domain name

www.semicomplete.com

Select visible fields

☑ DomainName	□ Status	☑ CreatedDate	☑ UpdatedDate
☑ ExpiresDate	□ AuditCreatedDate	□ AuditUpdatedDate	☑ RegistrantName
☑ RegistrantOrganization	□ RegistrantEmail	□ RegistrantTelephone	□ RegistrantFax
□ RegistrantCountry	□ RegistrantState	☑ RegistrantCity	□ RegistrantPostalCode
□ RegistrantStreet	□ AdministrativeContactName	□ AdministrativeContactOrganization	□ AdministrativeContactEmail

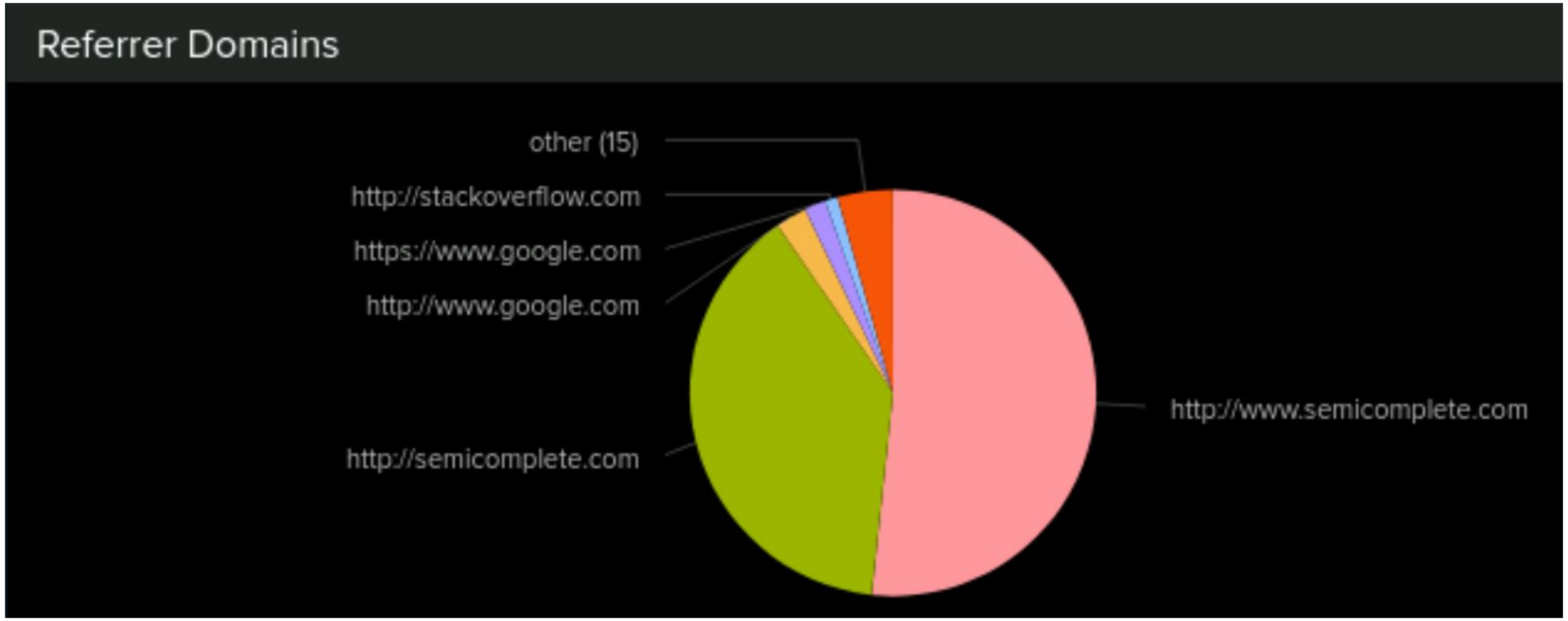
Whois XML History API

Usage Scenario

An analyst looking at referrer domains in a web server log may notice an unusual spike in requests referred from a specific domain.
This suspicious domain could then be analysed using the WHOIS add-on to determine useful information such as:

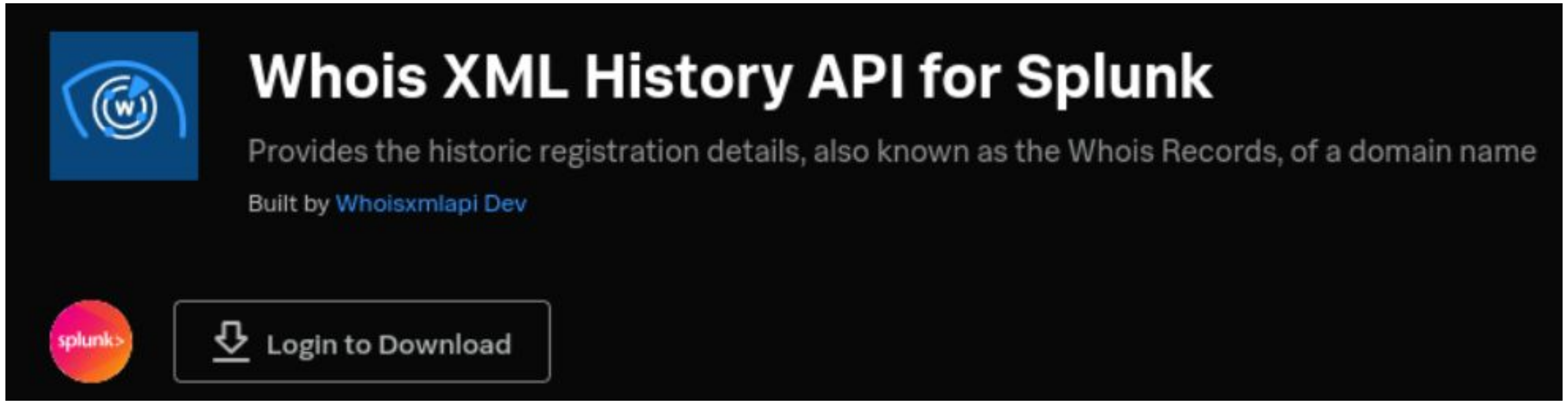
- Domain age
- Registration location
- Registrar details
- Potential registrant details

This could help an analyst to determine if the unusual traffic is malicious.



Whois XML History API - Installation

Download from Splunkbase.

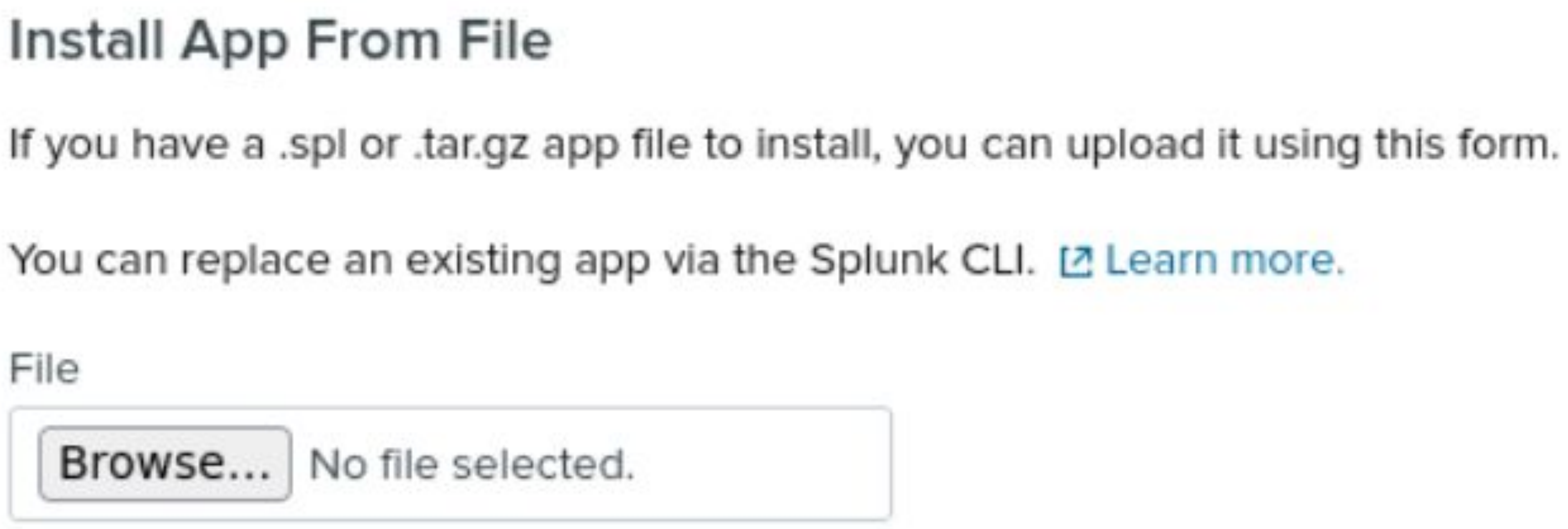


Whois XML History API for Splunk

Provides the historic registration details, also known as the Whois Records, of a domain name

Built by Whoisxmlapi Dev

Install from file.



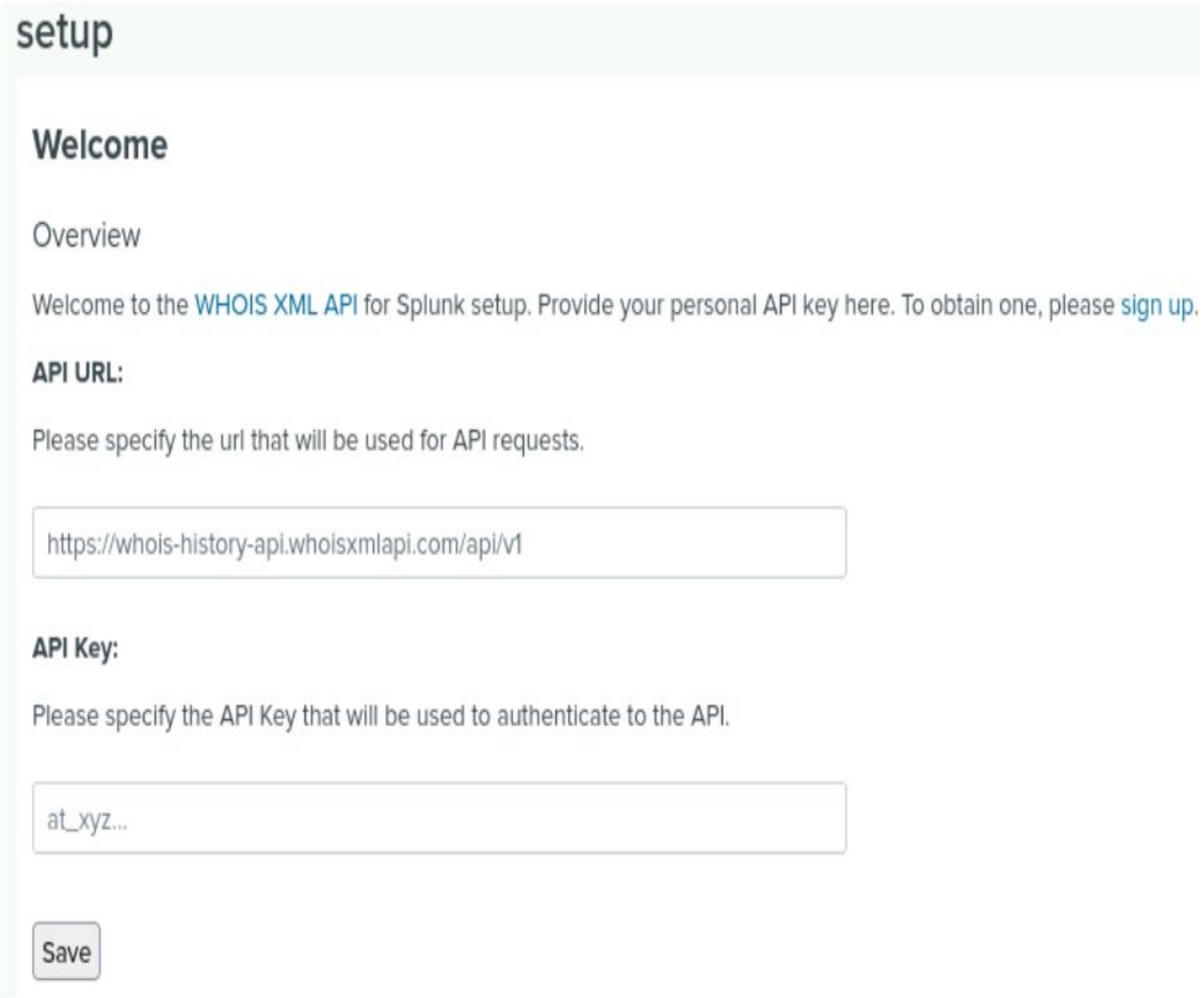
Install App From File

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File

Configure API Key (requires signup).



setup

Welcome

Overview

Welcome to the WHOIS XML API for Splunk setup. Provide your personal API key here. To obtain one, please sign up.

API URL:

Please specify the url that will be used for API requests.

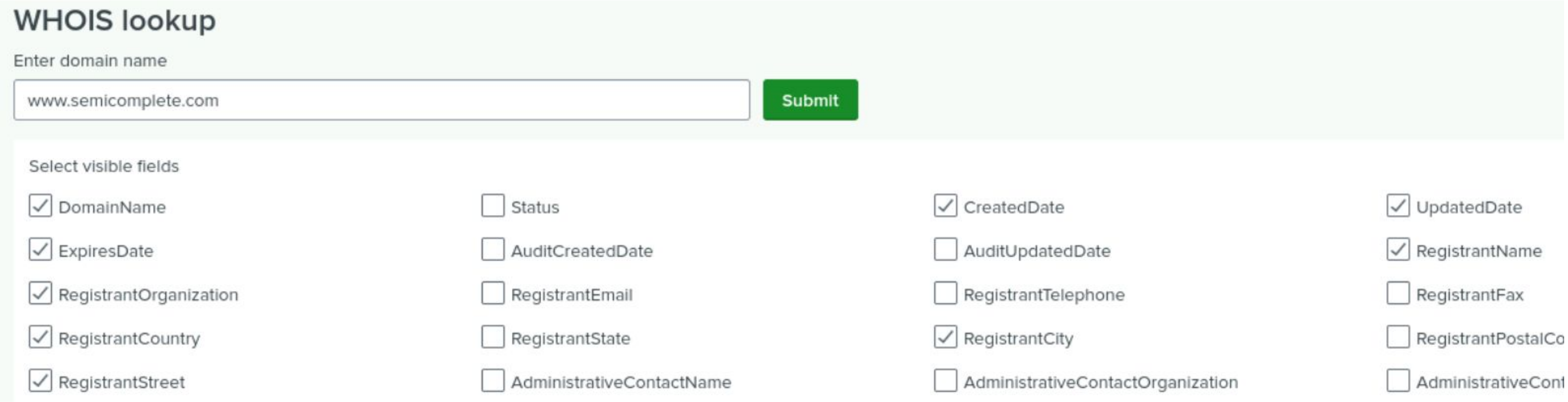
https://whois-history-api.whoisxmlapi.com/api/v1

API Key:

Please specify the API Key that will be used to authenticate to the API.

at_xyz...

Whois XML History API - Domain Information



WHOIS lookup

Enter domain name

www.semicomplete.com

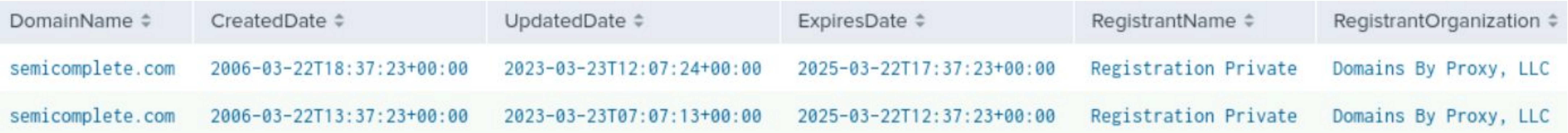
Select visible fields

☑ DomainName
☑ ExpiresDate
☑ RegistrantOrganization
☑ RegistrantCountry
☑ RegistrantStreet

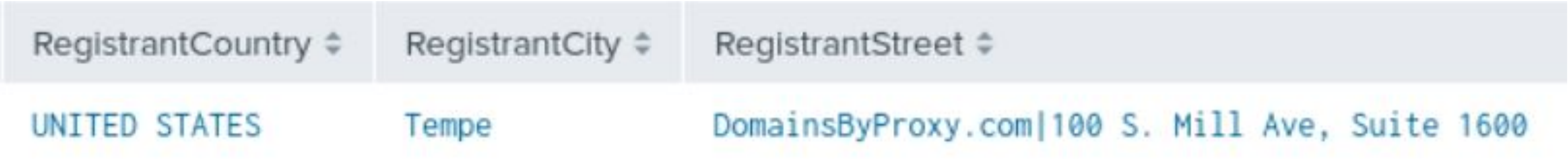
☐ Status
☐ AuditCreatedDate
☐ RegistrantEmail
☐ RegistrantState
☐ AdministrativeContactName

☑ CreatedDate
☐ AuditUpdatedDate
☐ RegistrantTelephone
☑ RegistrantCity
☐ AdministrativeContactOrganization

☑ UpdatedDate
☑ RegistrantName
☐ RegistrantFax
☐ RegistrantPostalCo
☐ AdministrativeCont

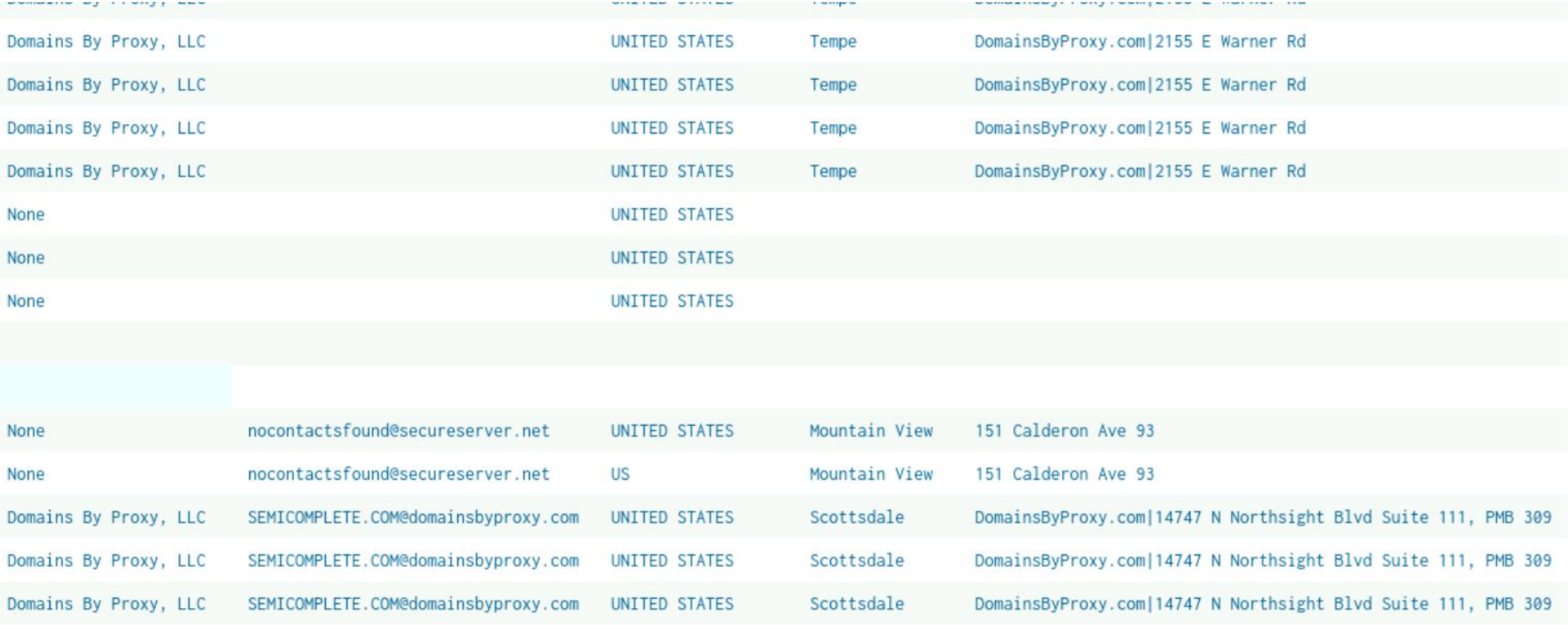


DomainName	CreatedDate	UpdatedDate	ExpiresDate	RegistrantName	RegistrantOrganization
semicomplete.com	2006-03-22T18:37:23+00:00	2023-03-23T12:07:24+00:00	2025-03-22T17:37:23+00:00	Registration Private	Domains By Proxy, LLC
semicomplete.com	2006-03-22T13:37:23+00:00	2023-03-23T07:07:13+00:00	2025-03-22T12:37:23+00:00	Registration Private	Domains By Proxy, LLC



RegistrantCountry	RegistrantCity	RegistrantStreet
UNITED STATES	Tempe	DomainsByProxy.com|100 S. Mill Ave, Suite 1600

Whois XML History API - Historical Data



Domains By Proxy, LLC		UNITED STATES	Tempe	DomainsByProxy.com|2155 E Warner Rd
Domains By Proxy, LLC		UNITED STATES	Tempe	DomainsByProxy.com|2155 E Warner Rd
Domains By Proxy, LLC		UNITED STATES	Tempe	DomainsByProxy.com|2155 E Warner Rd
Domains By Proxy, LLC		UNITED STATES	Tempe	DomainsByProxy.com|2155 E Warner Rd
Domains By Proxy, LLC		UNITED STATES	Tempe	DomainsByProxy.com|2155 E Warner Rd
None		UNITED STATES		
None		UNITED STATES		
None		UNITED STATES		
None	nocontactsfound@secureserver.net	UNITED STATES	Mountain View	151 Calderon Ave 93
None	nocontactsfound@secureserver.net	US	Mountain View	151 Calderon Ave 93
Domains By Proxy, LLC	SEMICOMPLETE.COM@domainsbyproxy.com	UNITED STATES	Scottsdale	DomainsByProxy.com|14747 N Northsight Blvd Suite 111, PMB 309
Domains By Proxy, LLC	SEMICOMPLETE.COM@domainsbyproxy.com	UNITED STATES	Scottsdale	DomainsByProxy.com|14747 N Northsight Blvd Suite 111, PMB 309
Domains By Proxy, LLC	SEMICOMPLETE.COM@domainsbyproxy.com	UNITED STATES	Scottsdale	DomainsByProxy.com|14747 N Northsight Blvd Suite 111, PMB 309

Windows Logs

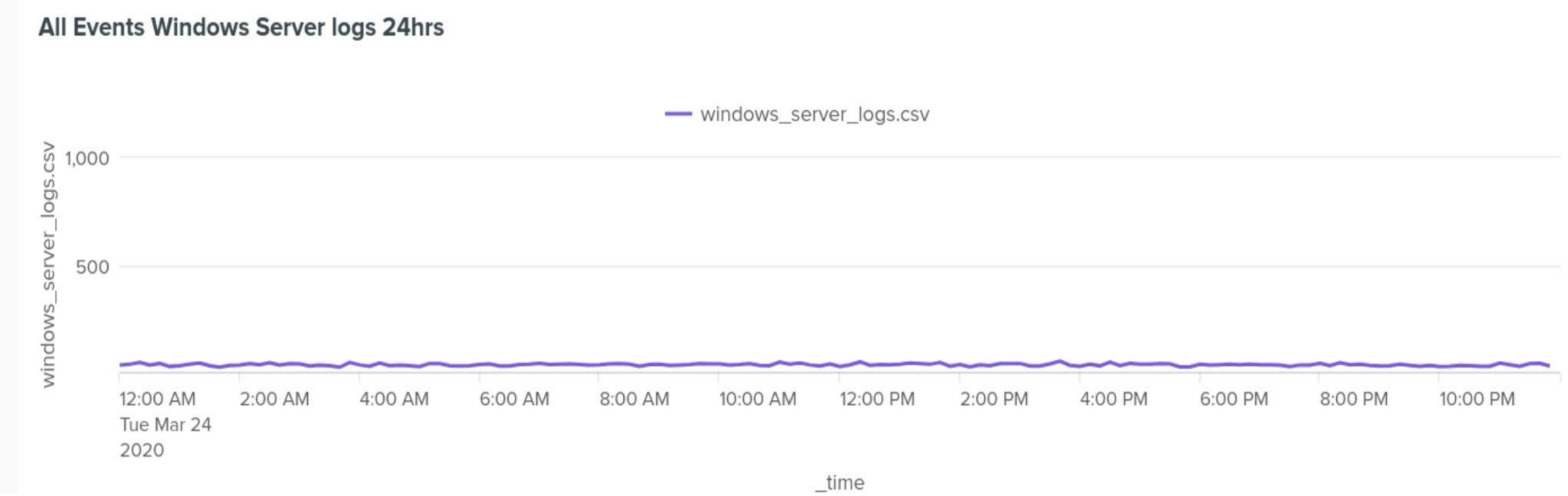
Windows Logs

Windows_Server_Logs.csv

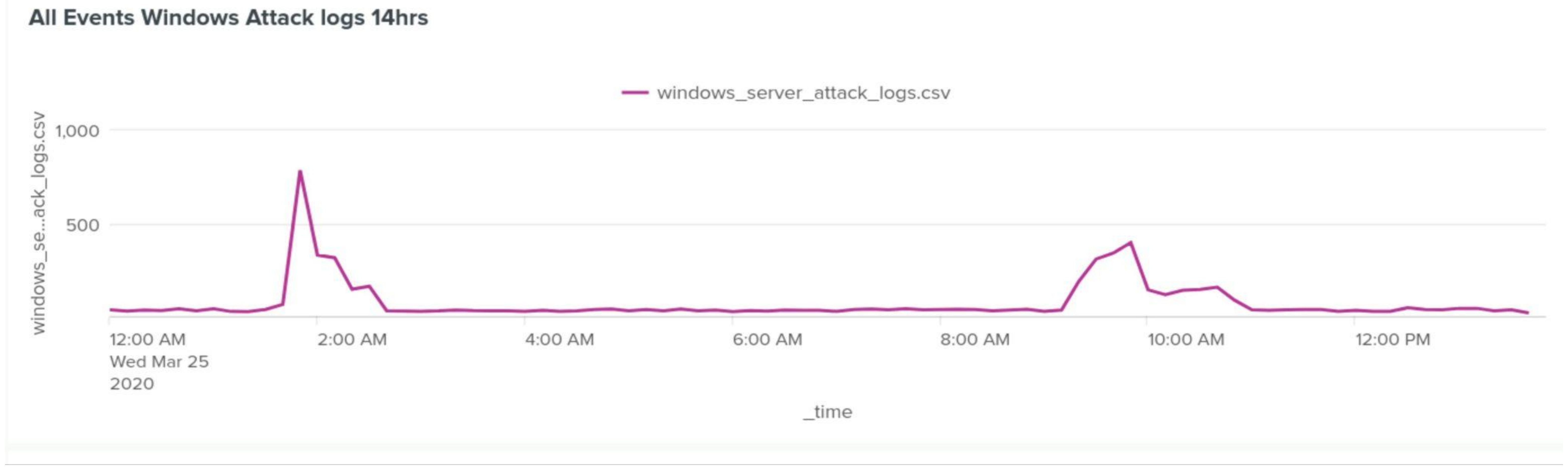
- **Duration:** 24 hrs
- **Date:** 24/25 Mar 2020
- **Events:** 4764

Windows_attack_Logs.csv

- **Duration:** 14 hrs
- **Date:** 25 Mar 2020
- **Events:** 5949



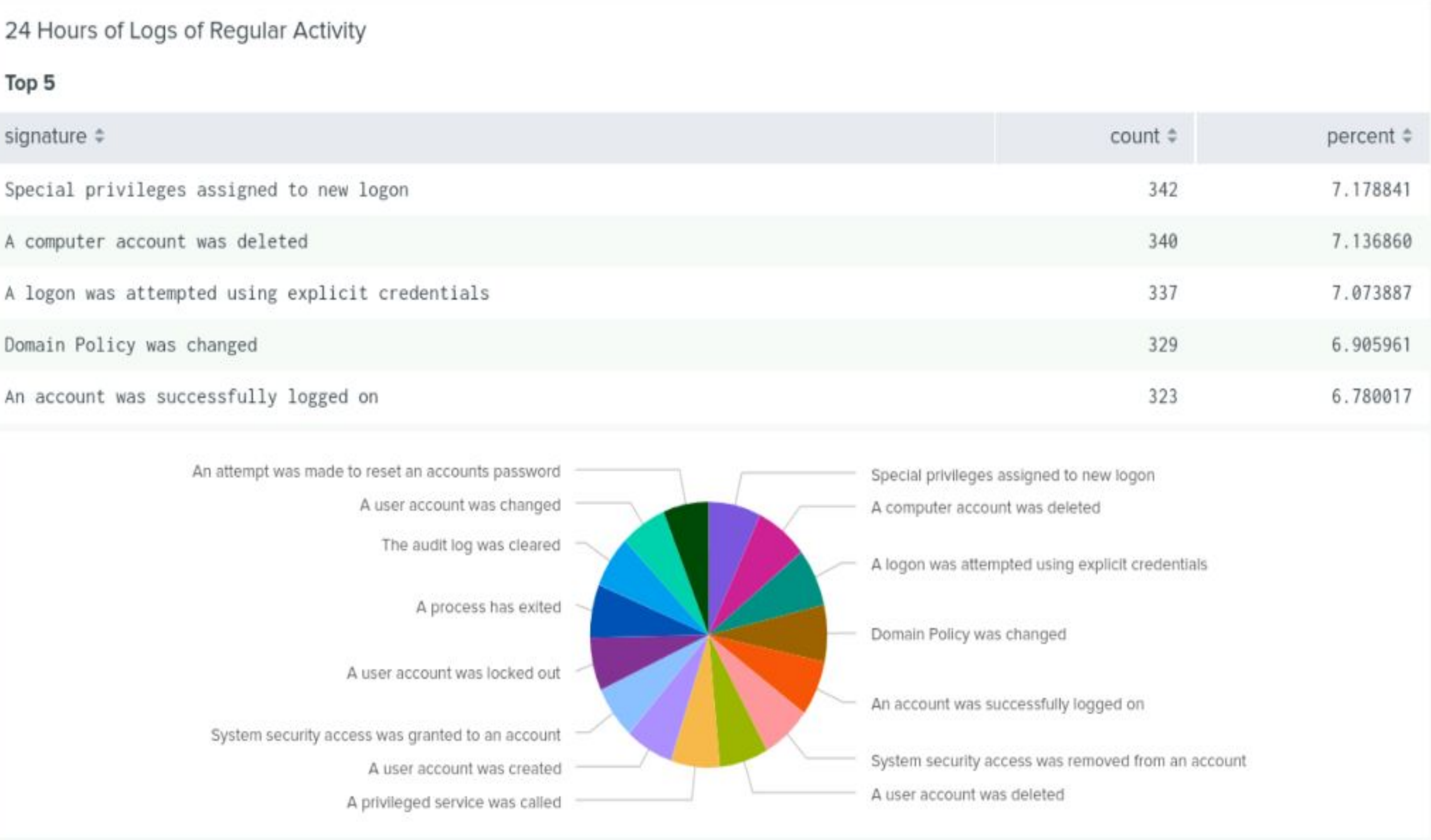
All Events Windows Server logs 24hrs



All Events Windows Attack logs 14hrs

Reports—Windows Security event by Signature

Description	Analysis
This is a report showing the number of events sorted by the signatures. We have displayed the percentage of each signature in a pie chart.	- Large increases to “An attempt was made to reset an account password” & “A user account was locked out” - Also an increase to “An account was successfully logged on”

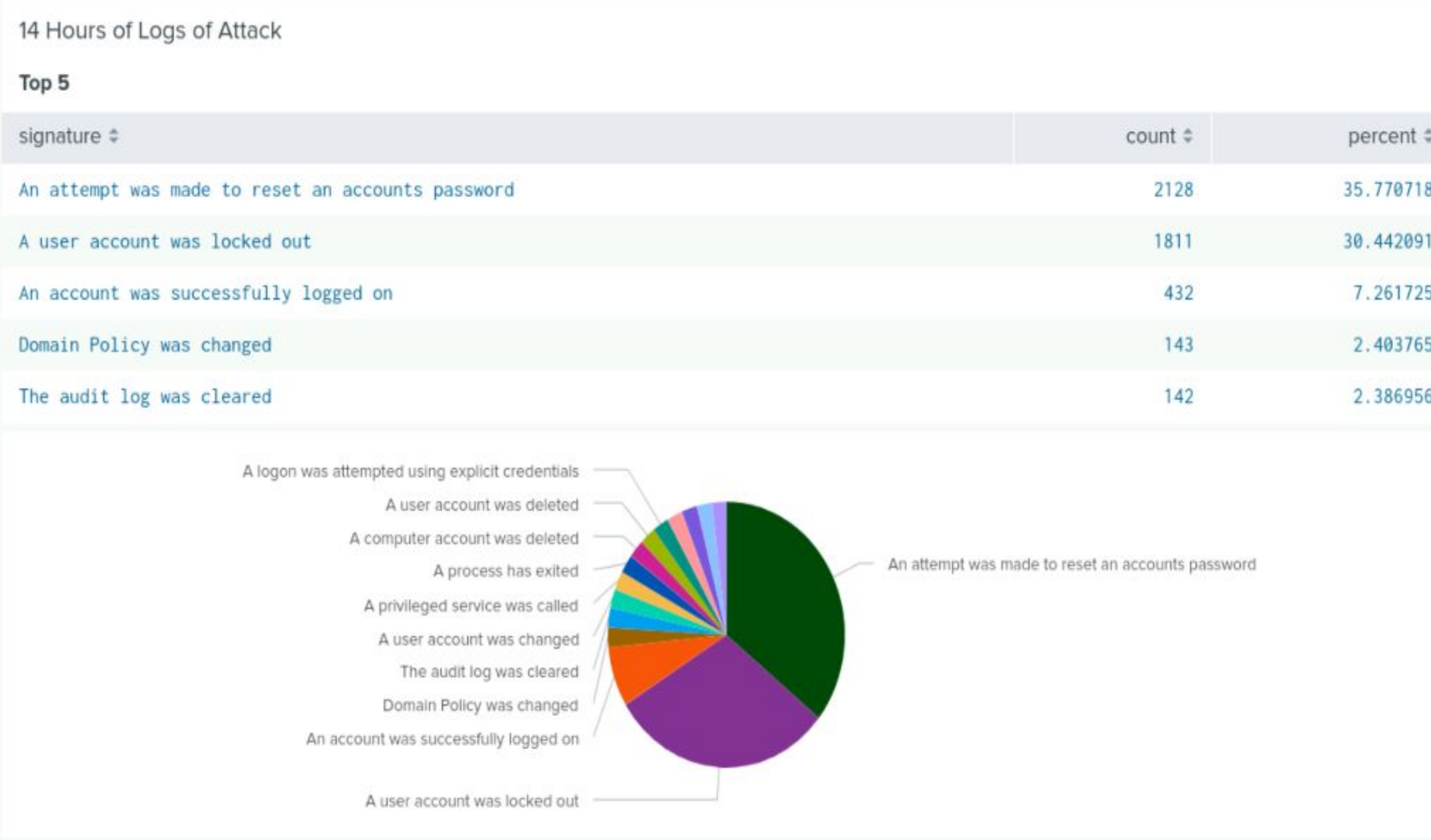


24 Hours of Logs of Regular Activity

Top 5

signature ⇕	count ⇕	percent ⇕
Special privileges assigned to new logon	342	7.178841
A computer account was deleted	340	7.136860
A logon was attempted using explicit credentials	337	7.073887
Domain Policy was changed	329	6.905961
An account was successfully logged on	323	6.780017

An attempt was made to reset an accounts password
A user account was changed
The audit log was cleared
A process has exited
A user account was locked out
System security access was granted to an account
A user account was created
A privileged service was called
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
System security access was removed from an account
A user account was deleted



14 Hours of Logs of Attack

Top 5

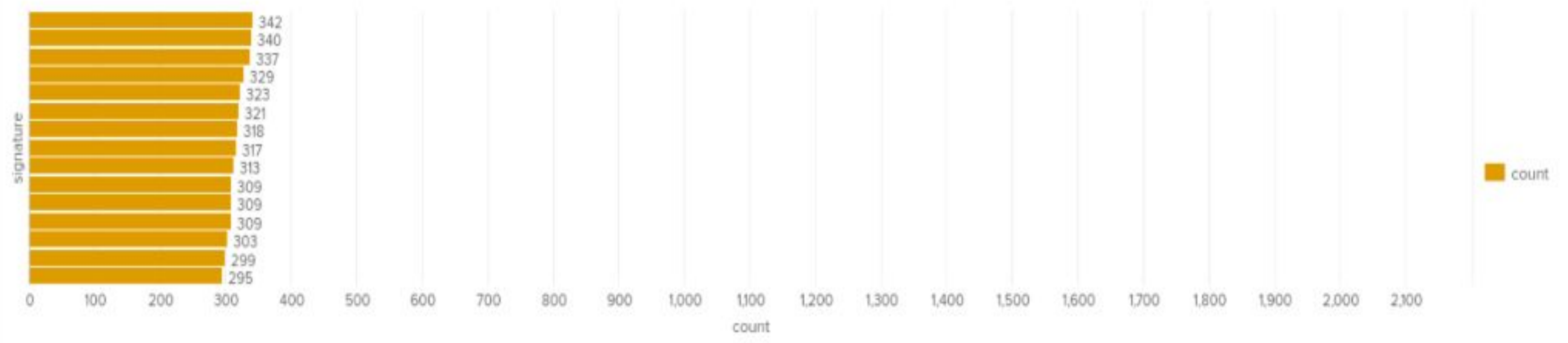
signature ⇕	count ⇕	percent ⇕
An attempt was made to reset an accounts password	2128	35.770718
A user account was locked out	1811	30.442091
An account was successfully logged on	432	7.261725
Domain Policy was changed	143	2.403765
The audit log was cleared	142	2.386956

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

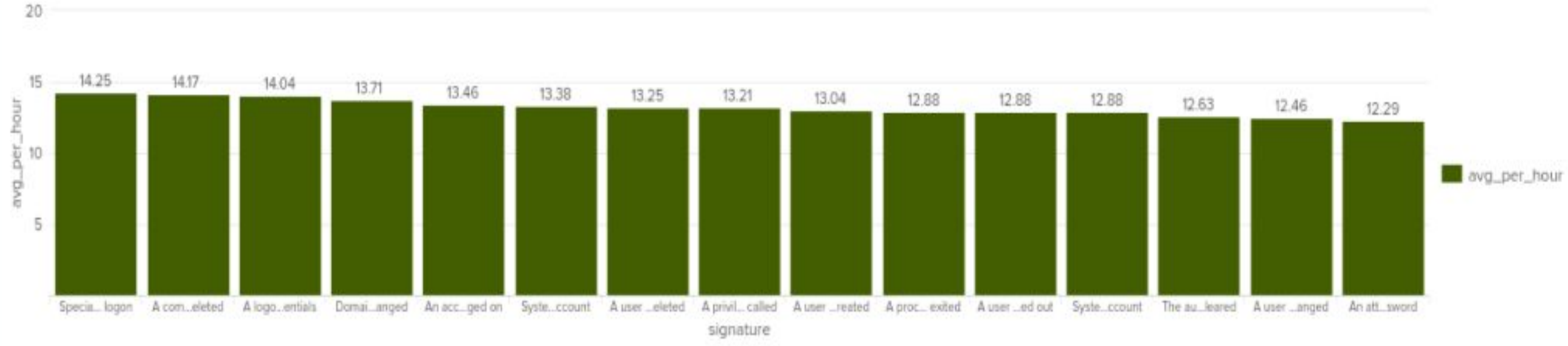
Reports—Windows Security event by Signature Continued

Description	Analysis
The graph on the left shows the counts over the day of all the events by their signature. The graphs on the right show the averages of each event sorted by signature over the duration of each log.	- Activity has gone down for all other signatures. - Possible denial of service where certain events were not able to be accessed. - Possibly an error in the logs where some of the events may be missing.

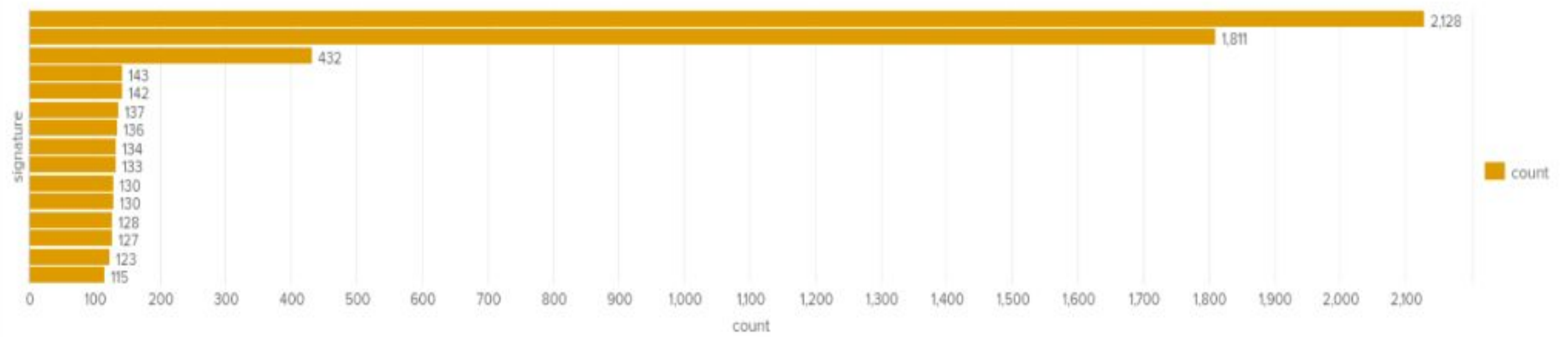
Signature Count Over 24 Hours of Logs of Regular Activity



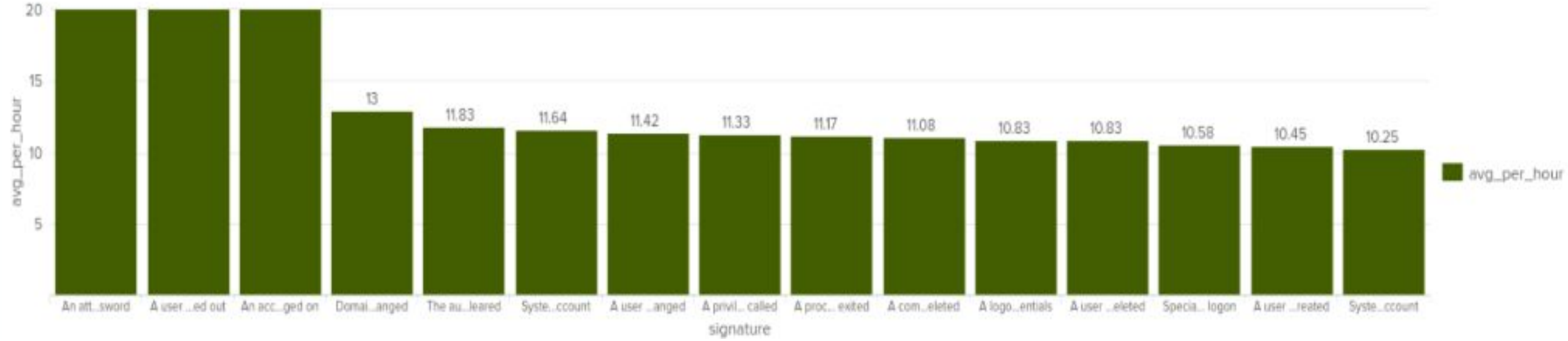
Average Event Count by Hour for the Control Log



Signature Count Over 14 Hours of Logs of Attack

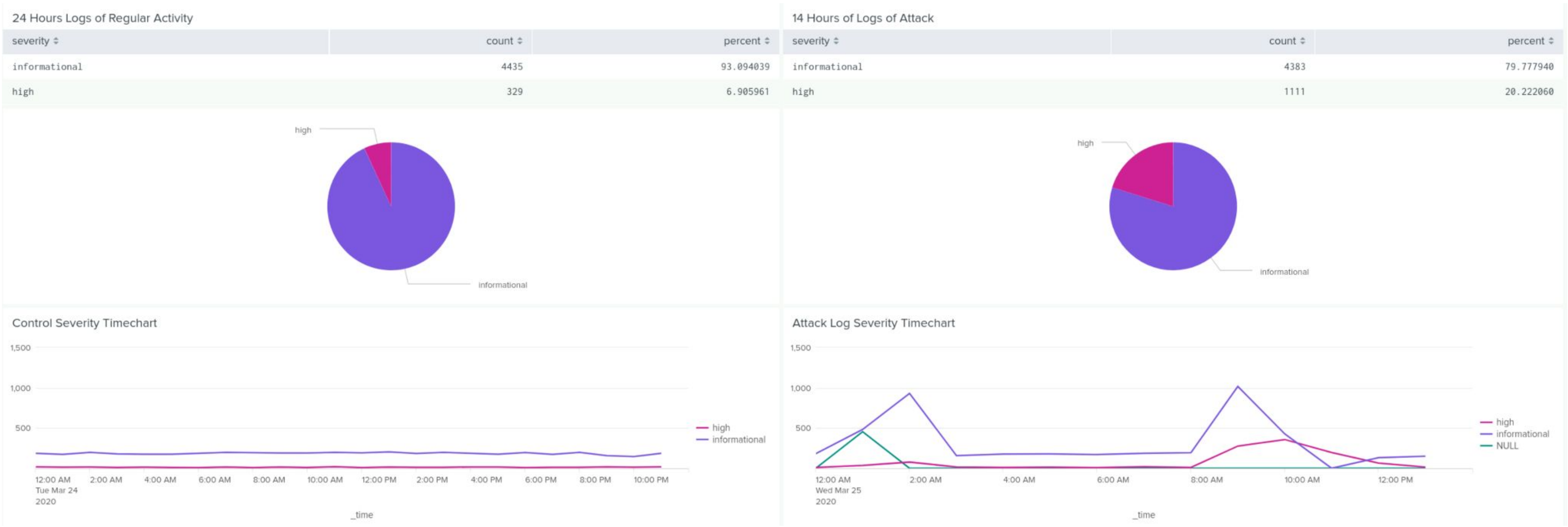


Average Event Count by Hour for the Attack Log



Reports—Windows Security Event Severity Levels

Description	Analysis
This is a visualisation of a report that shows the number of events and their severity levels within a normal day of logs compared to the day the attack occurred.	- The original logs have 93% informational severity and 7% high severity. - The attack logs have 80% informational severity and 20% high severity.



24 Hours Logs of Regular Activity

severity ⇕	count ⇕	percent ⇕
informational	4435	93.094039
high	329	6.905961

14 Hours of Logs of Attack

severity ⇕	count ⇕	percent ⇕
informational	4383	79.777940
high	1111	20.222060

Control Severity Timechart

Attack Log Severity Timechart

Reports—Windows Security Activity Status

Description	Analysis
This a report that shows the counts of successful and failed events over the two logs. The graphs below show a timechart of the different statuses over the period of both logs.	There was only a minimal change in the percentages of successful and failed activity. Increased overall traffic over shorter timespan. The time chart shows spikes of each status at different times.

24 Hours of Logs of Regular Activity

status ⇕	count ⇕	percent ⇕
success	4622	97.019312
failure	142	2.980688

14 Hours of Logs of Attack

status ⇕	count ⇕	percent ⇕
success	5856	98.436712
failure	93	1.563288

38hr of traffic by event status being success

1,000
500
count
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
12:00 AM
Wed Mar 25
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
_time
count

38hr of traffic by event status being failure

40
20
count
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
12:00 AM
Wed Mar 25
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
count

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Dashboard Over Initial Logs
Edit
Export
...
Event Count by Signature
Special privi... new logon 342
A computer ...as deleted 340
A logon wa... credentials 337
Domain Pol...as changed 329
An account ...y logged on 323
System sec... an account 321
A user acco...as deleted 318
A privileged ... was called 317
A user acco...as created 313
System sec... an account 309
A user acco...s locked out 309
A process has exited 309
The audit log was cleared 303
A user acco...as changed 299
An attempt ...ts password 295
signature
count
0 50 100 150 200 250 300 350
count
Number of Unique Users
unique_users
50 45 40 35 30 25
12:00 AM Tue Mar 24 2020
6:00 AM
12:00 PM
6:00 PM
_time
Different Activity By Signature
An attempt was made ...n accounts password
A user account was changed
The audit log was cleared
A process has exited
A user account was locked out
System security acce... granted to an account
A user account was created
A privileged service was called
Special privileges assigned to new logon
A computer account was deleted
A logon was attempte...ng explicit credentials
Domain Policy was changed
An account was successfully logged on
System security acce...oved from an account
A user account was deleted
Activity by User
40 30 20 10
user_a
user_b
user_c
user_d
user_e
user_f
user_h
user_i
user_l
user_m
OTHER
12:00 AM Tue Mar 24 2020
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
_time
1m ago
Signature Line Charts
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
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts pass...
Domain Policy was changed
Special privileges assigned to new logon
50
12:00 AM Tue Mar 24 2020
8:00 AM
4:00 PM
Single Point Average of Events by Signature
A computer account was deleted 14.167
A logon was attempted using explicit credentials 14.042
A privileged service was called 13.208
A process has exited 12.875
A user account was changed 12.458
A user account was created 13.042
A user account was deleted 13.25
A user account was locked out 12.875
An account was successfully logged on 13.458
An attempt was made to reset an accounts pass... 12.292
Domain Policy was changed 13.708
Special privileges assigned to new logon 14.25
0 10 20 30 40

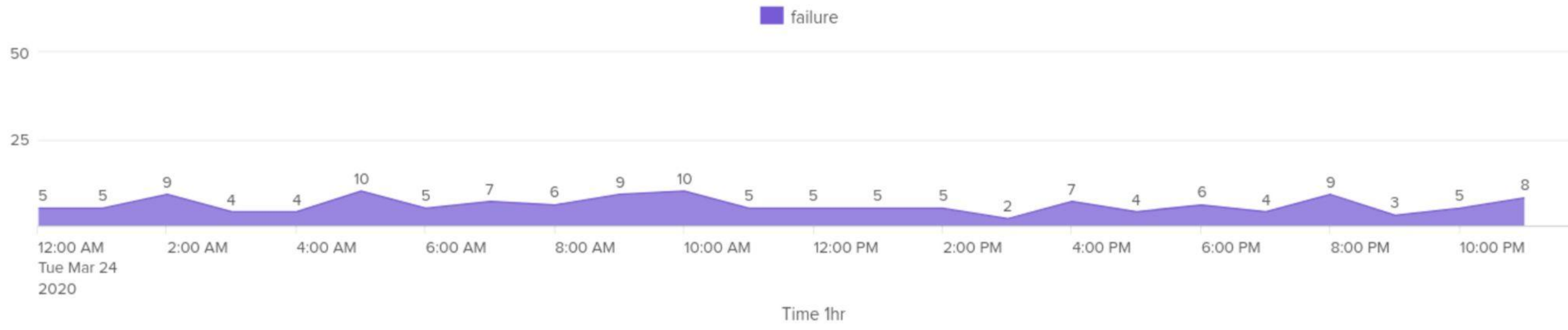
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Dashboard Over Attack Logs
Edit
Export
...
Event Count by Signature
An attempt ...ts password 2,128
A user acco...s locked out 1,811
An account ...y logged on 432
Domain Poi...as changed 143
The audit log was cleared 142
A user acco...as changed 137
A privileged ... was called 136
A process has exited 134
A computer ...as deleted 133
A user acco...as deleted 130
A logon wa... credentials 130
System sec... an account 128
Special privi... new logon 127
System sec... an account 123
A user acco...as created 115
signature
0
500
1,000
1,500
2,000
count
count
Number of Unique Users
50
40
30
20
10
unique_users
12:00 AM Wed Mar 25 2020
4:00 AM
8:00 AM
12:00 PM
_time
unique_users
Different Activity By Signature
Special privileges assigned to new logon
System security acce...oved from an account
A logon was attempte...ng explicit credentials
A user account was deleted
A computer account was deleted
A process has exited
A privileged service was called
A user account was changed
The audit log was cleared
Domain Policy was changed
An account was successfully logged on
A user account was locked out
An attempt was made ...n accounts password
Activity by User
40
30
20
10
12:00 AM Wed Mar 25 2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
_time
user_a
user_b
user_c
user_e
user_f
user_i
user_j
user_k
user_l
user_m
OTHER
Signature Line Charts
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
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts pass...
Domain Policy was changed
Special privileges assigned to new logon
50
12:00 AM Wed Mar 25 2020
4:00 AM
8:00 AM
Single Point Average of Events by Signature
A computer account was deleted 11.083
A logon was attempted using explicit credentials 10.833
A privileged service was called 11.333
A process has exited 11.167
A user account was changed 11.417
A user account was created 10.454
A user account was deleted 10.833
A user account was locked out 150.917
An account was successfully logged on 30.857
An attempt was made to reset an accounts pass... 163.692
Domain Policy was changed 13
Special privileges assigned to new logon 10.583
0
10
20
30
40

Windows Alerts

Status: “Failed windows Activity”

Failed Windows Activity 24 hrs

Note: No irregular Activity

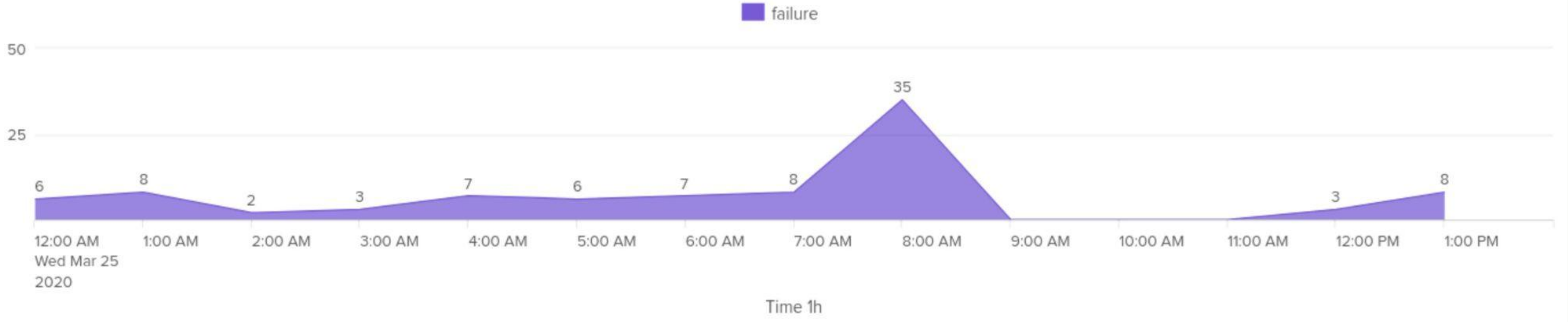


Baseline:

Baseline of 10 failed events per hr as 7 - 10 occurs several times.

Failed Windows Activity over 14 hrs

Note: A Noticeable drop in activity from 9 - 11am



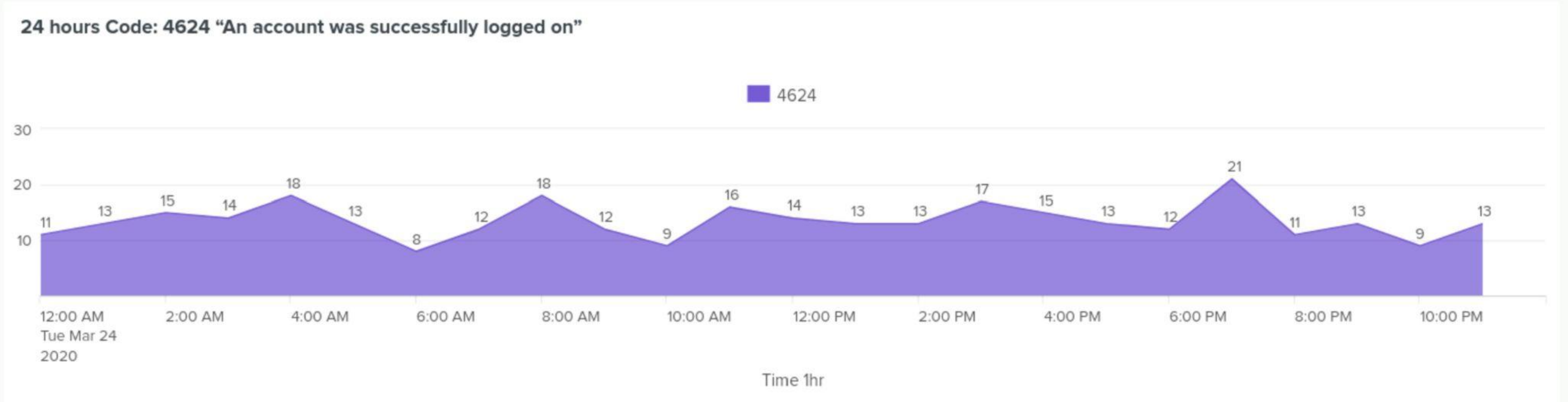
Alert Created:

Alert created to send an email failed Windows activity reaches 12 per hour

Code: 4624 "An account was successfully logged on"

Code:4624 over 24 hrs

Note: No Irregular Activity

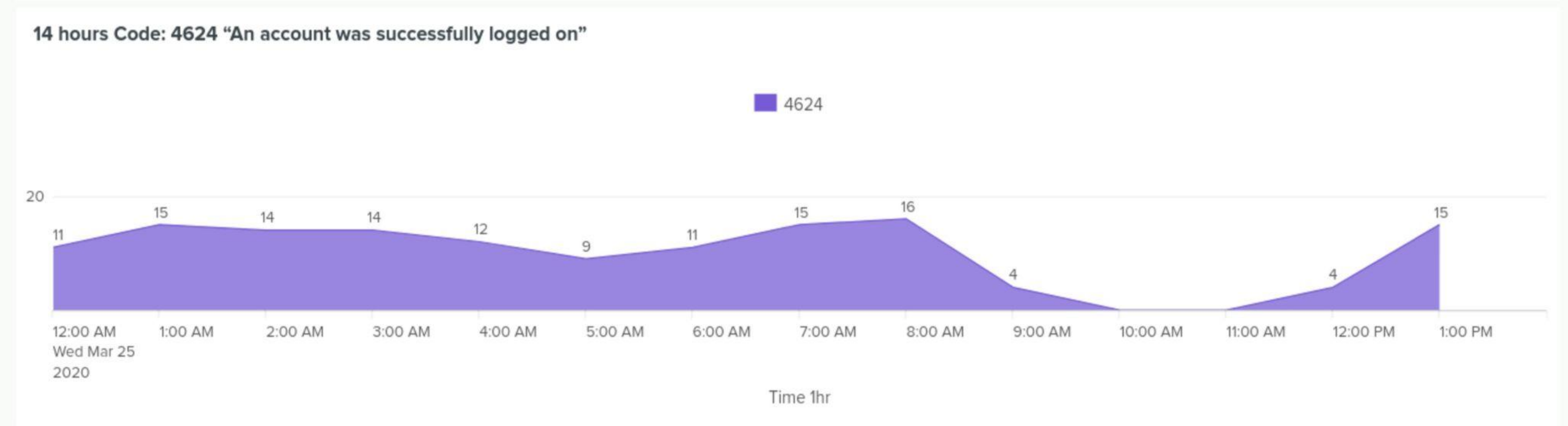


Baseline:

Baseline of 21 successful logged on as 18 and 21 occurred

Code:4624 over 14 hrs

Note: At 8am the attack logs show a major decrease in successful logins to zero



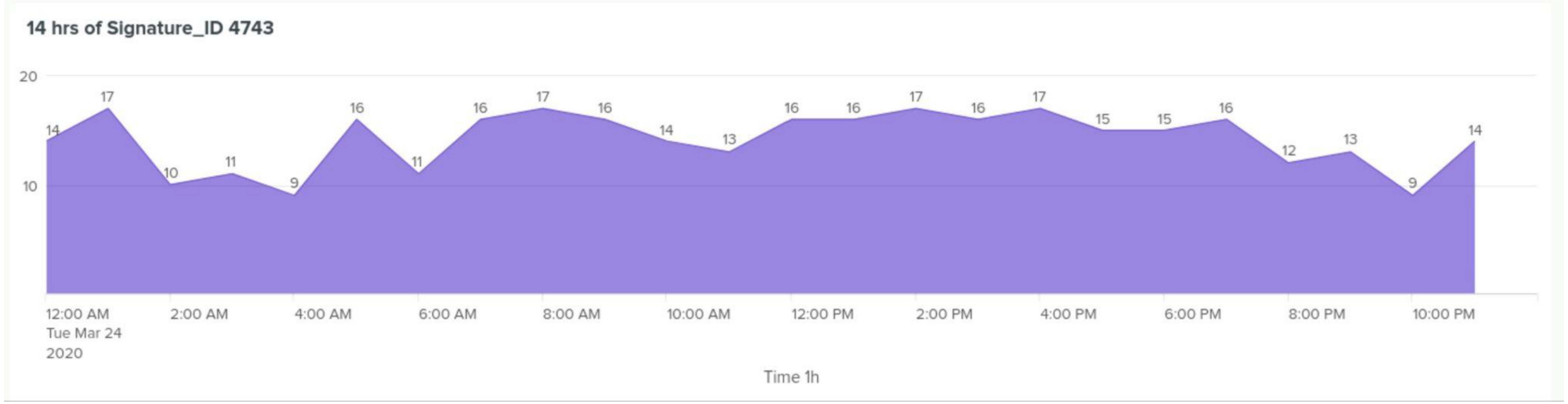
Alert Created:

Alert created a to send and email if the hourly Successful logins reaches 25

Code: 4743 ***“***A computer account was deleted”

A computer account was deleted 24 hrs

`Note: No irregular Activity`

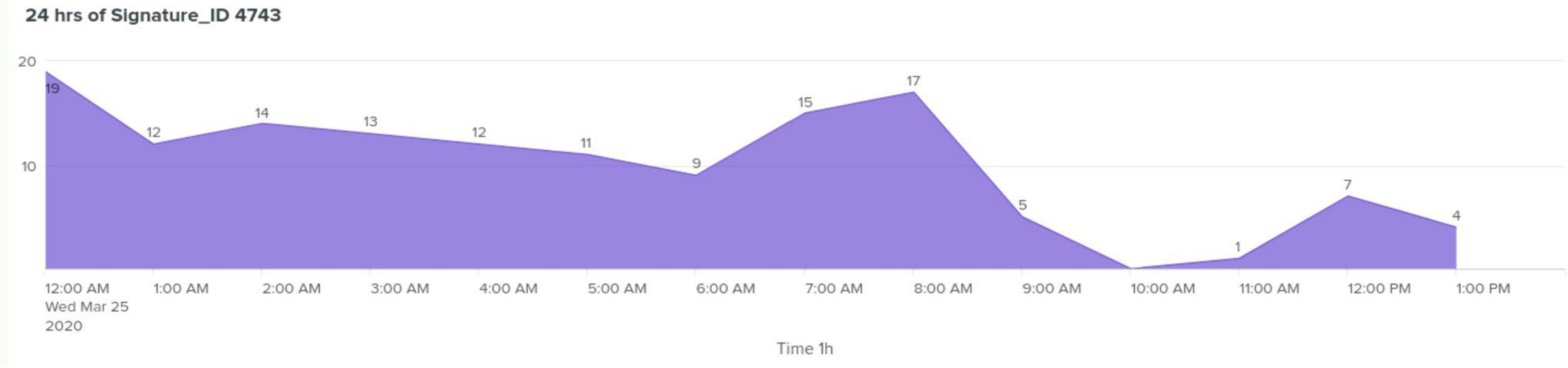


Baseline:

`Baseline of 17 Deleted accounts per hr as 9 to 17 which occurs several times.`

A computer account was deleted 14 hrs

`Note: A Noticeable drop in activity from 9 - 11am`



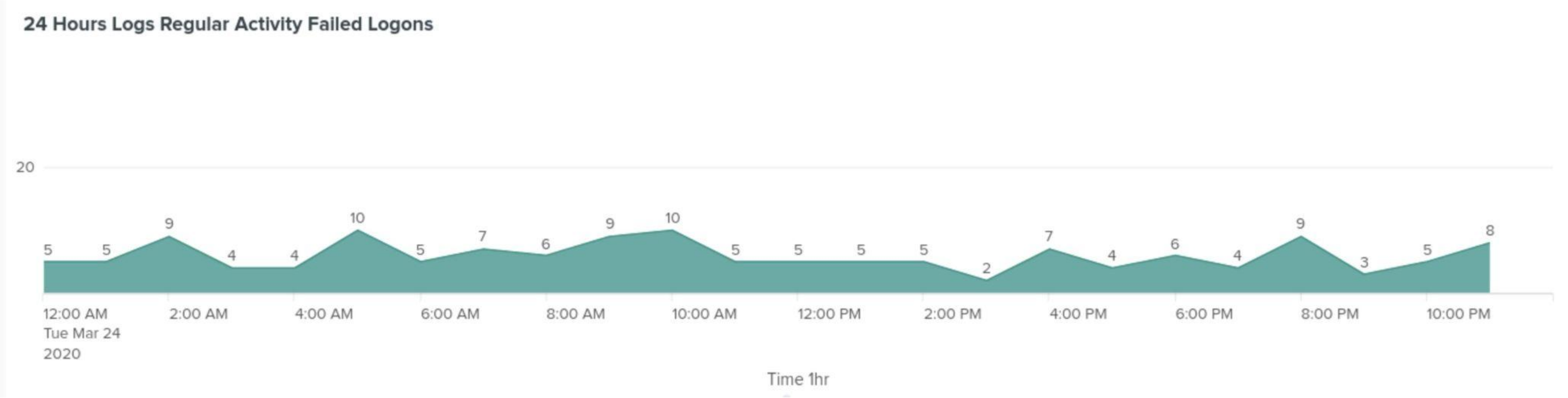
Alert Created:

`Alert created to send an email if the Deleted accounts per hr reaches 20`

Remediation:Failed Logon

Failed logons in 24 hrs

Note: No irregular Activity

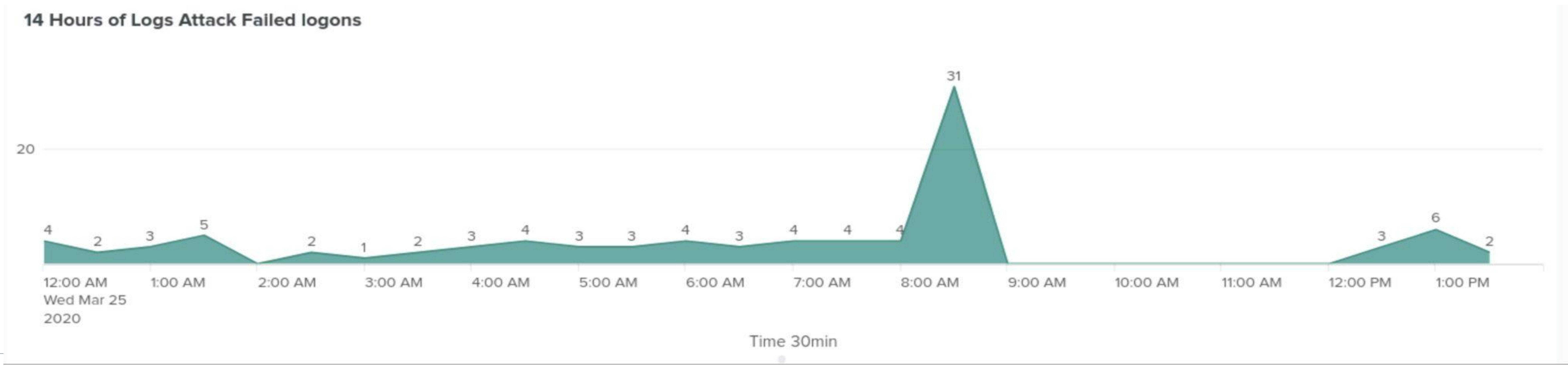


Baseline:

Baseline of 11 Failed logons as 9 10 occurred several times.

Failed logons in 14 hrs

Note: At 8am the attack logs show a major increase in failed logins



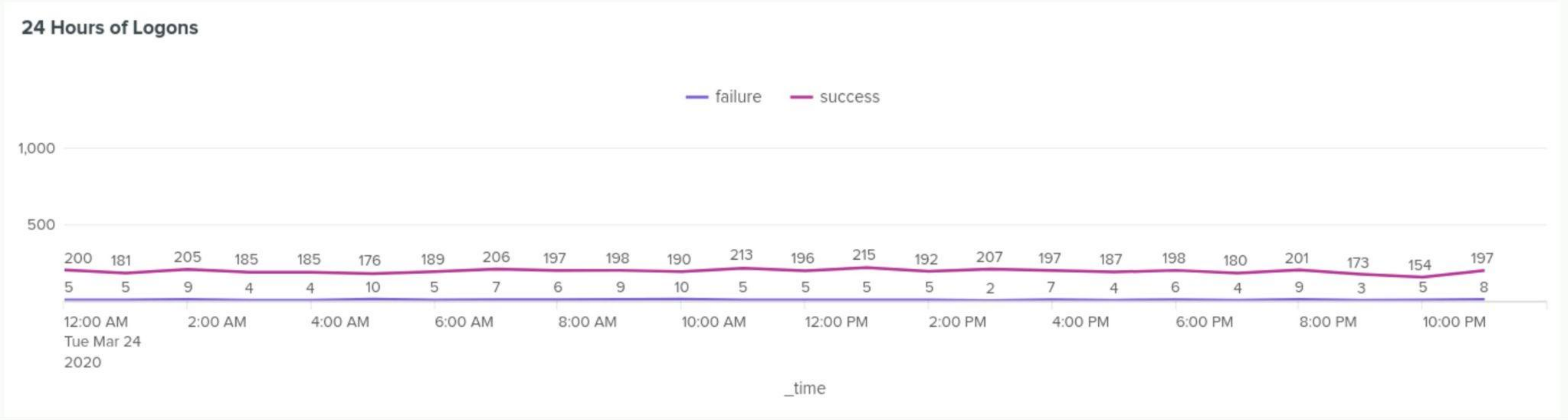
Alert Created:

Alert created to send an email if the hourly Failed logons reaches 12

Remediation: Alert logon attempts

Login Attempts 24 hrs

Note: No Irregular Activity

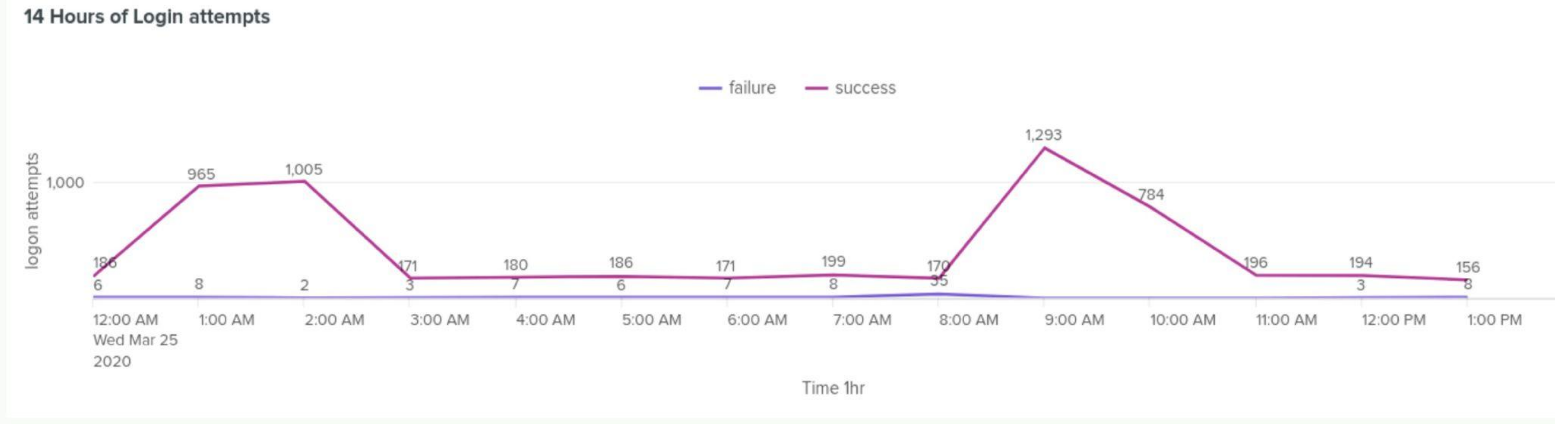


Login Attempts 14 hrs

Note: A spike of 35 failed attempts was recorded just before attack starts, also no failed during attack

Alert Created:

Alert created to send an email when logon attempts reach 300 per hr

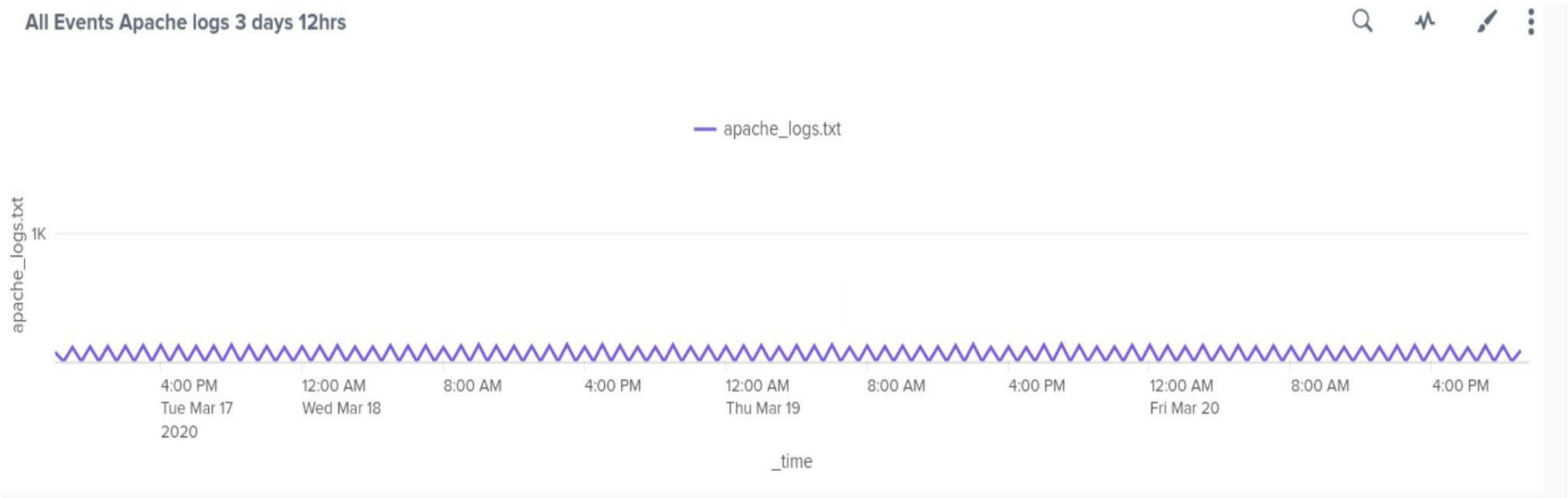


Apache Logs

Apache logs

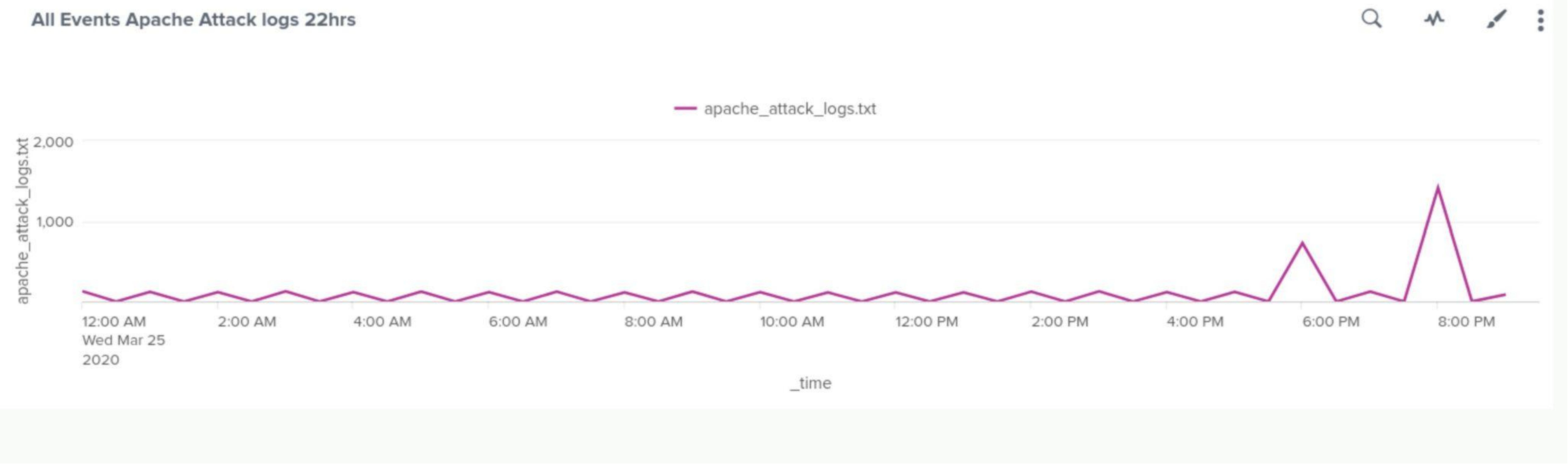
Apache_logs.txt

- **Duration:** 3 days 12hrs
- **Date:** 17 - 20 Mar 2020
- **Events:** 10,000

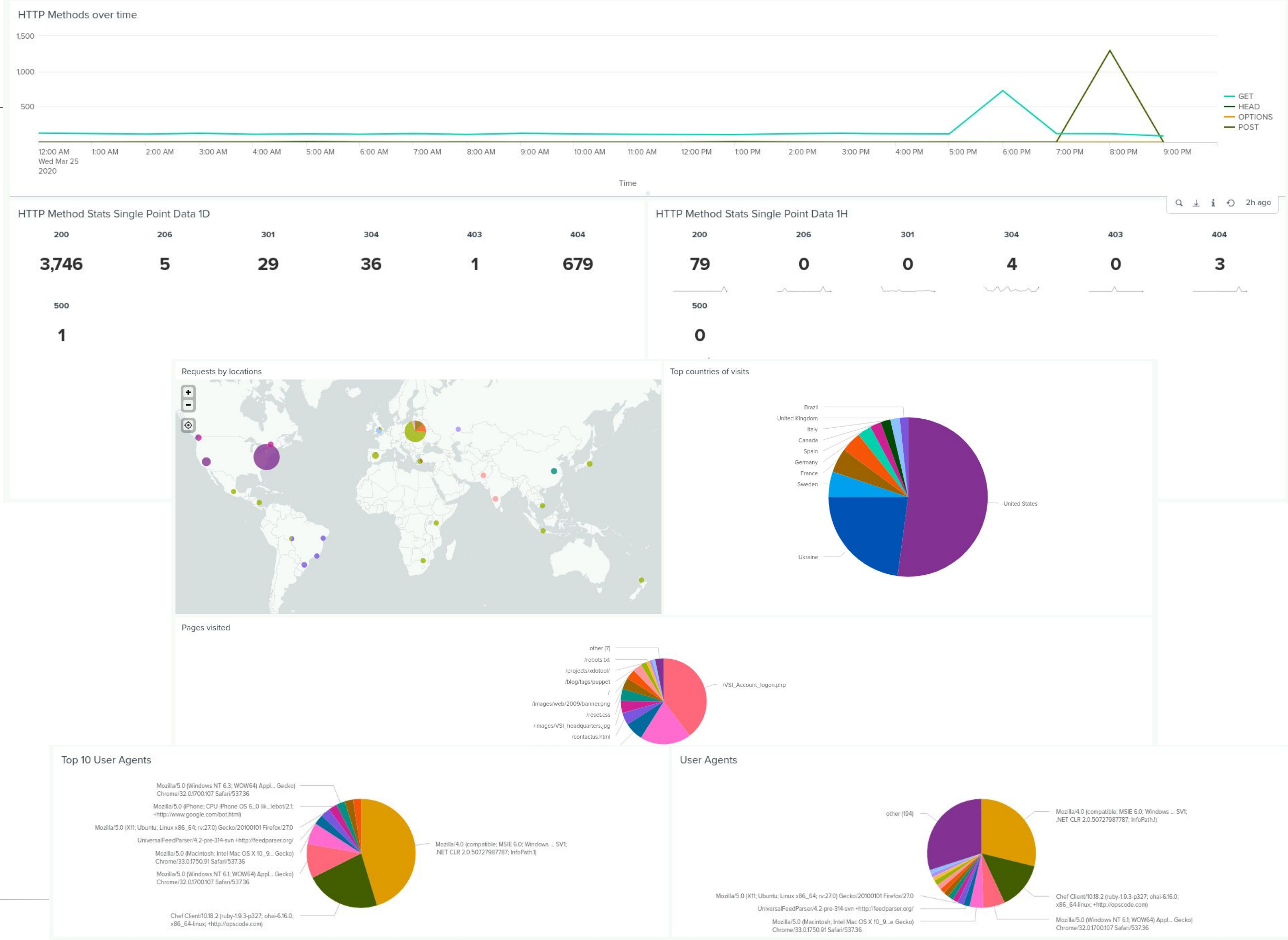


Apache_attack_logs.txt

- **Duration:** 22 hrs
- **Date:** 25 Mar 2020
- **Events:** 4497



Dashboard


HTTP Methods over time
1,500
1,000
500
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
2:00 PM
3:00 PM
4:00 PM
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
Time
GET
HEAD
OPTIONS
POST
2h ago
Requests by locations
+
-
Top countries of visits
Brazil
United Kingdom
Italy
Canada
Spain
Germany
France
Sweden
United States
Ukraine
Pages visited
other (7)
/robots.txt
/projects/xdotool/
/blog/tags/puppet
/
/images/web/2009/banner.png
/reset.css
/images/VSI_headquarters.jpg
/contactus.html
/VSI_Account_logon.php
Top 10 User Agents
Mozilla/5.0 (Windows NT 6.3; WOW64) Appl... Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 lik...lebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9... Gecko) Chrome/33.0.1750.91 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) Appl... Gecko) Chrome/32.0.1700.107 Safari/537.36
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)
Mozilla/4.0 (compatible; MSIE 6.0; Windows ... SV1; .NET CLR 2.0.50727987787; InfoPath.1)
User Agents
other (194)
Mozilla/4.0 (compatible; MSIE 6.0; Windows ... SV1; .NET CLR 2.0.50727987787; InfoPath.1)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9...e Gecko) Chrome/33.0.1750.91 Safari/537.36
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)
Mozilla/5.0 (Windows NT 6.1; WOW64) Appl... Gecko) Chrome/32.0.1700.107 Safari/537.36

HTTP Method Stats Single Point Data 1D

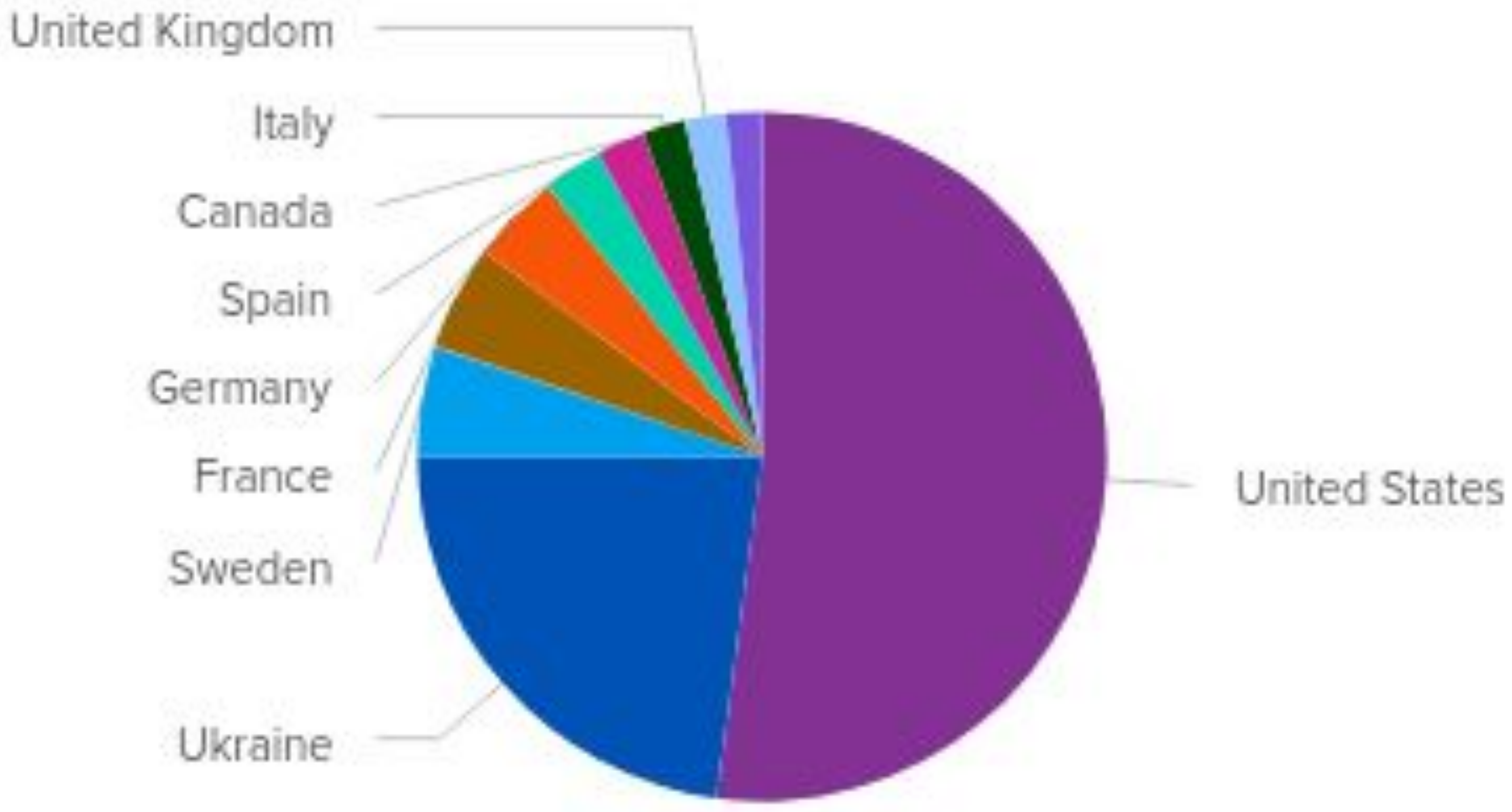
200	206	301	304	403	404	500
3,746	5	29	36	1	679	1

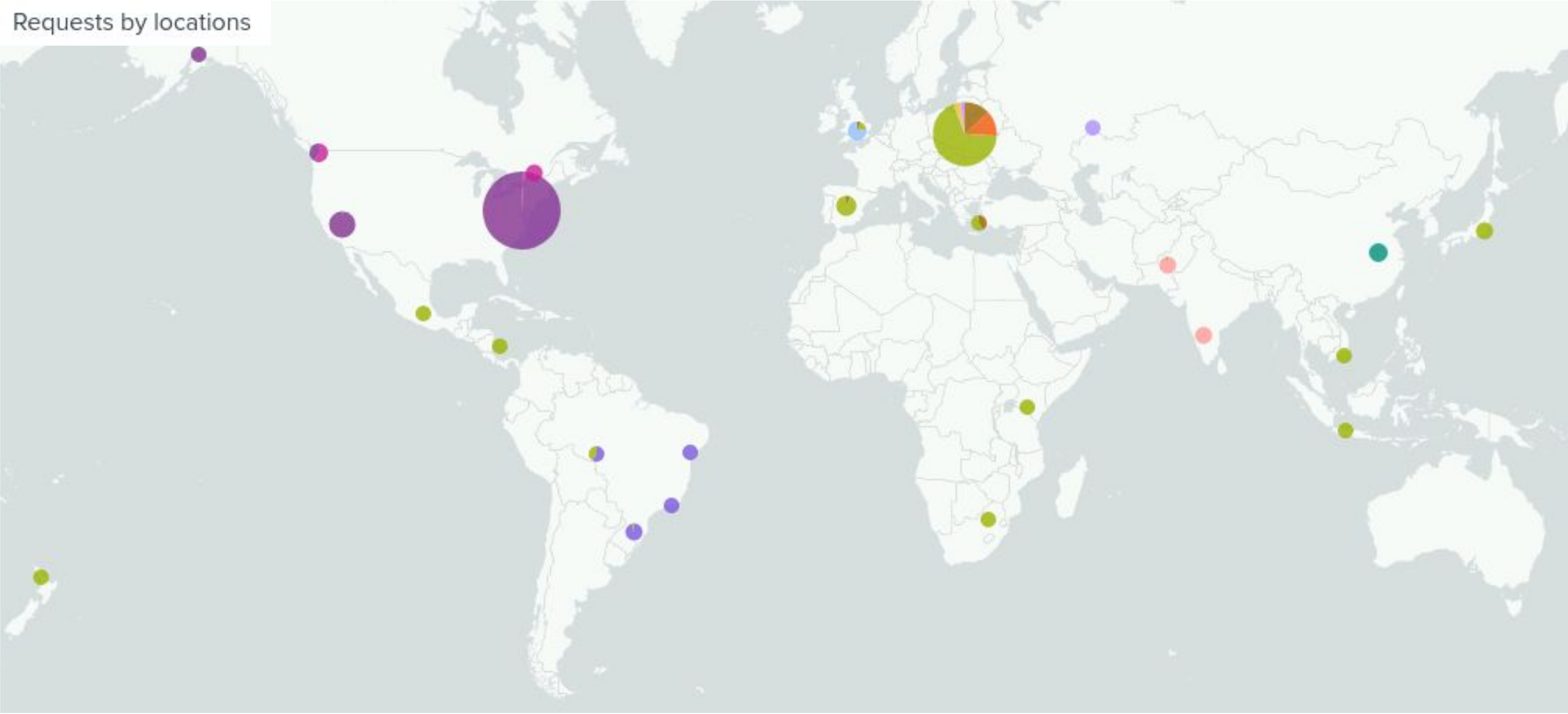
HTTP Method Stats Single Point Data 1H

200	206	301	304	403	404	500
79	0	0	4	0	3	0

Dashboard—Requests by locations

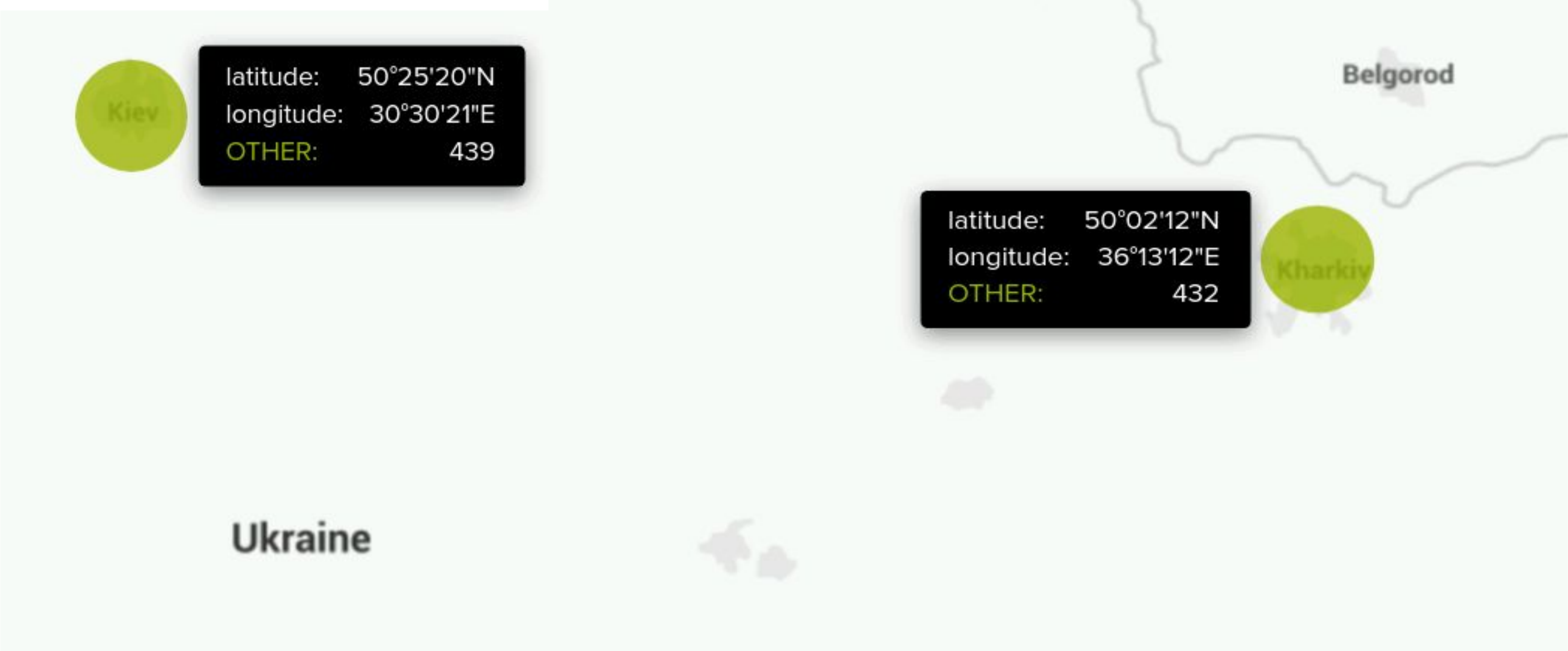
Analysis Apache_attack_logs.txt
High level of activity in Ukraine, specifically Kiev and Kharkiv





Dashboard—Requests by locations

Analysis Apache_attack_logs.txt
Kiev reaches a peak of 439 and Kharkiv 432



latitude:	50°25'20"N
longitude:	30°30'21"E
OTHER:	439

latitude:	50°02'12"N
longitude:	36°13'12"E
OTHER:	432

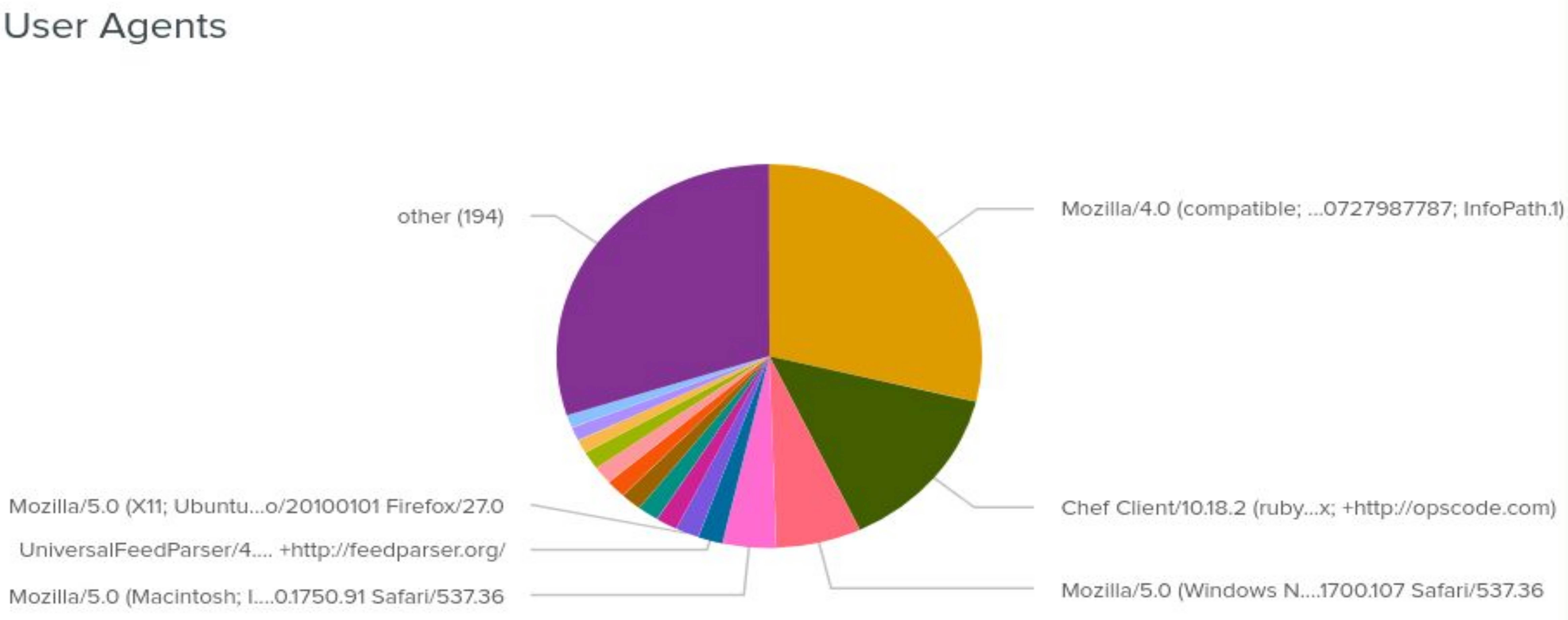
Dashboard—User Agents

Description
Allows us to identify users browsers, operating systems and device type when making requests to web servers

Top 10 User Agents
Mozilla/5.0 (Windows NT 6.3; WOW64) Appl... Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 lik...lebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9... Gecko) Chrome/33.0.1750.91 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) Appl... Gecko) Chrome/32.0.1700.107 Safari/537.36
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)
Mozilla/4.0 (compatible; MSIE 6.0; Windows ... SV1; .NET CLR 2.0.50727987787; InfoPath.1)
User Agents
other (194)
Mozilla/4.0 (compatible; MSIE 6.0; Windows ... SV1; .NET CLR 2.0.50727987787; InfoPath.1)
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9...e Gecko) Chrome/33.0.1750.91 Safari/537.36
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)
Mozilla/5.0 (Windows NT 6.1; WOW64) Appl... Gecko) Chrome/32.0.1700.107 Safari/537.36

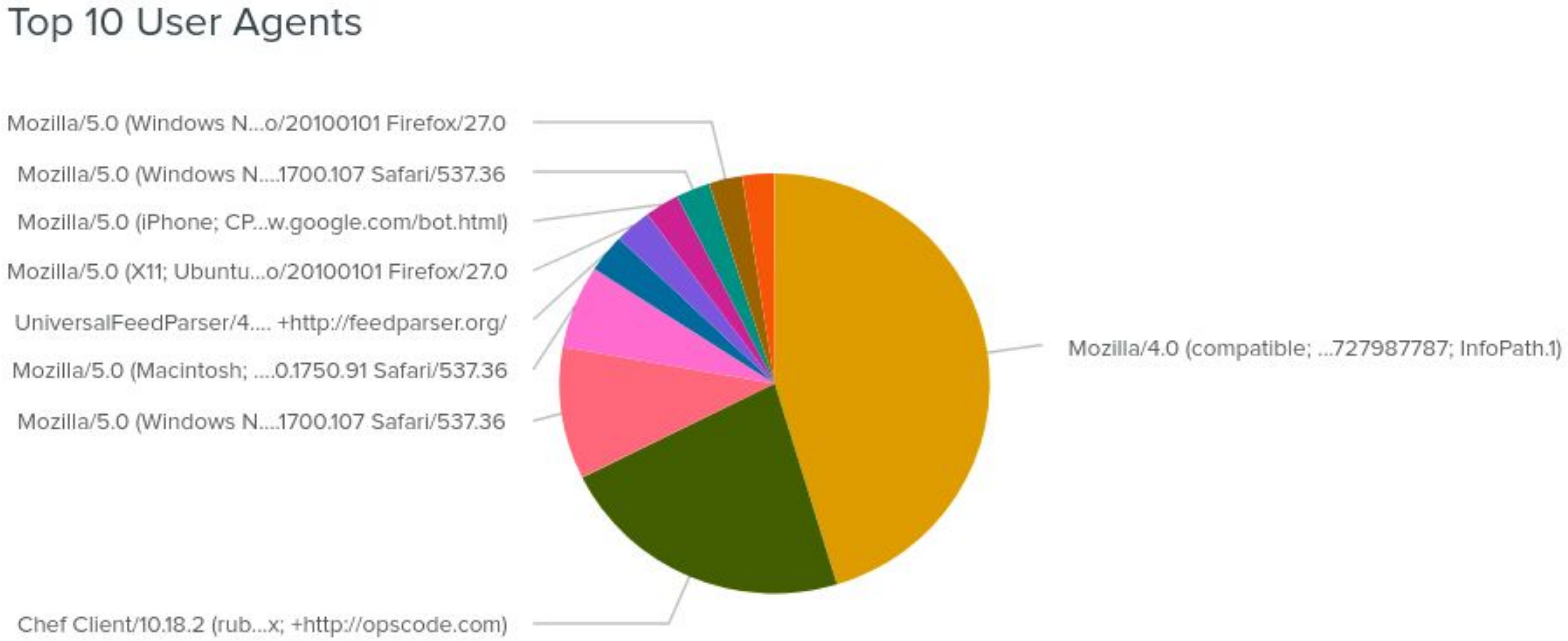
Dashboard—User Agents

Description
Allows us to identify users browsers, operating systems and device type when making requests to web servers



Dashboard—User Agents

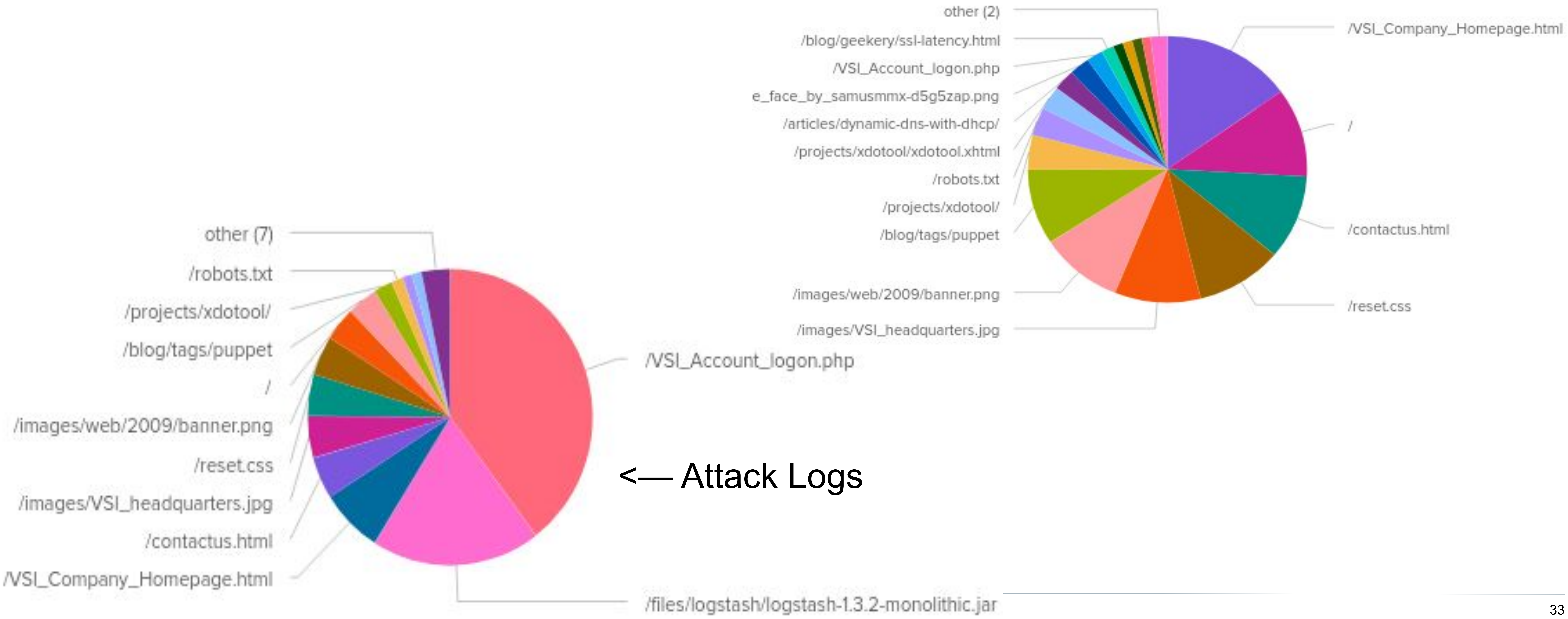
Description
Allows us to identify users browsers, operating systems and device type when making requests to web servers



Dashboard—URI Data

Analysis

/VSI_Account_logon.php page requests peak at 1,323, covering 39.7%



<— Attack Logs

Dashboard—HTTP Methods over time

Analysis
Spike in GET requests at 6 PM followed by spike in POST 2 hours later

HTTP Methods over time
300
200
100
12:00 PM
Tue Mar 17
2020
6:00 PM
12:00 AM
Wed Mar 18
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Thu Mar 19
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Fri Mar 20
6:00 AM
12:00 PM
6:00 PM
Time
GET
HEAD
OPTIONS
POST

HTTP Methods over time
1,500
1,000
500
12:00 AM
Wed Mar 25
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
Time
GET
HEAD
OPTIONS
POST

Dashboard—HTTP Methods over time Single Point Data

Apache Attack Log Analysis

HTTP Method Stats Single Point Data 1H

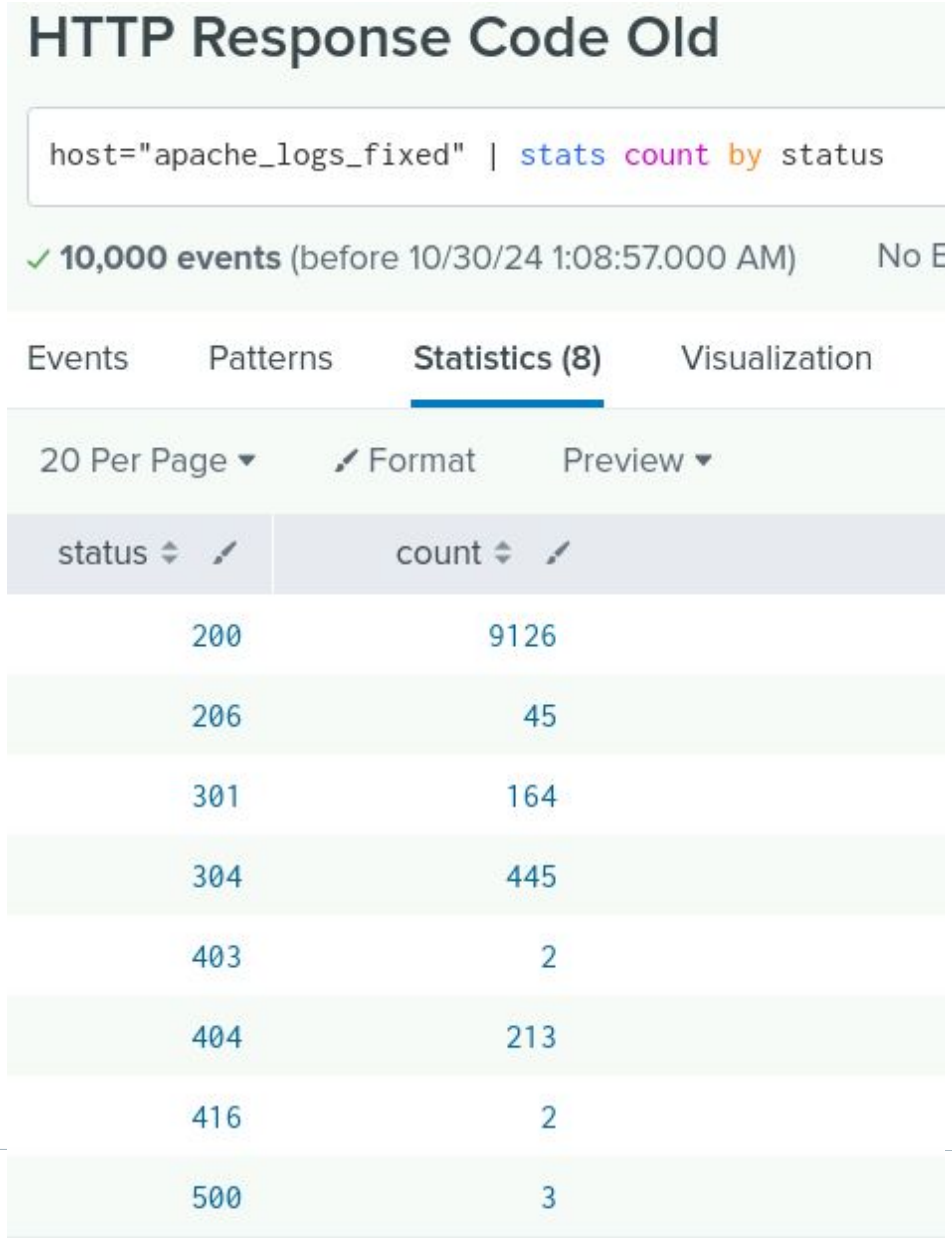
200	206	301	304	403	404	500
79	0	0	4	0	3	0

HTTP Method Stats Single Point Data 1D

200	206	301	304	403	404	500
3,746	5	29	36	1	679	1

Reports—HTTP Response Code

Description	Analysis
Counts the number of HTTP responses.	A large increase in the incidence of “404”

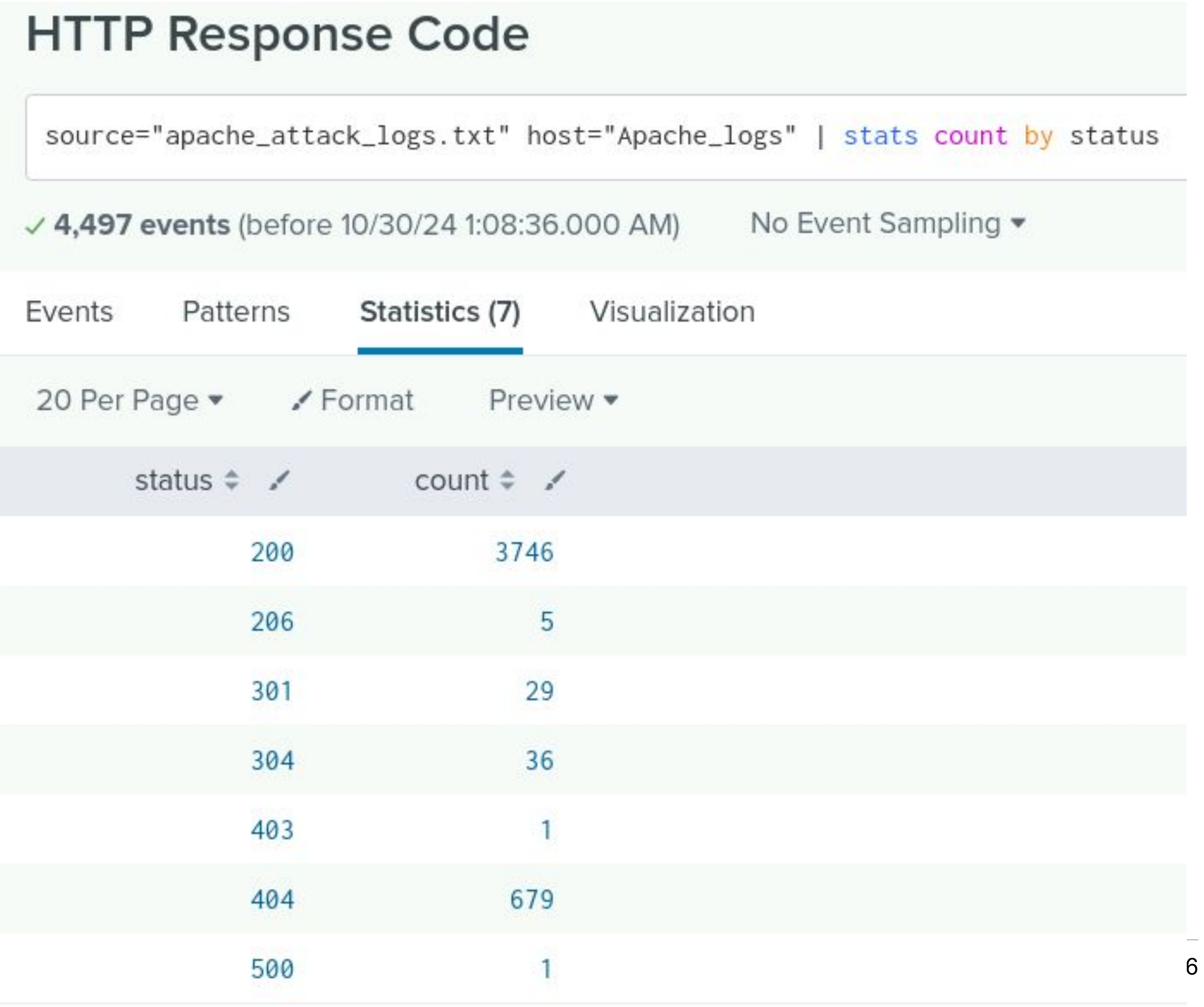


HTTP Response Code Old

```
host="apache_logs_fixed" | stats count by status
```

✓ 10,000 events (before 10/30/24 1:08:57.000 AM) No E

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



HTTP Response Code

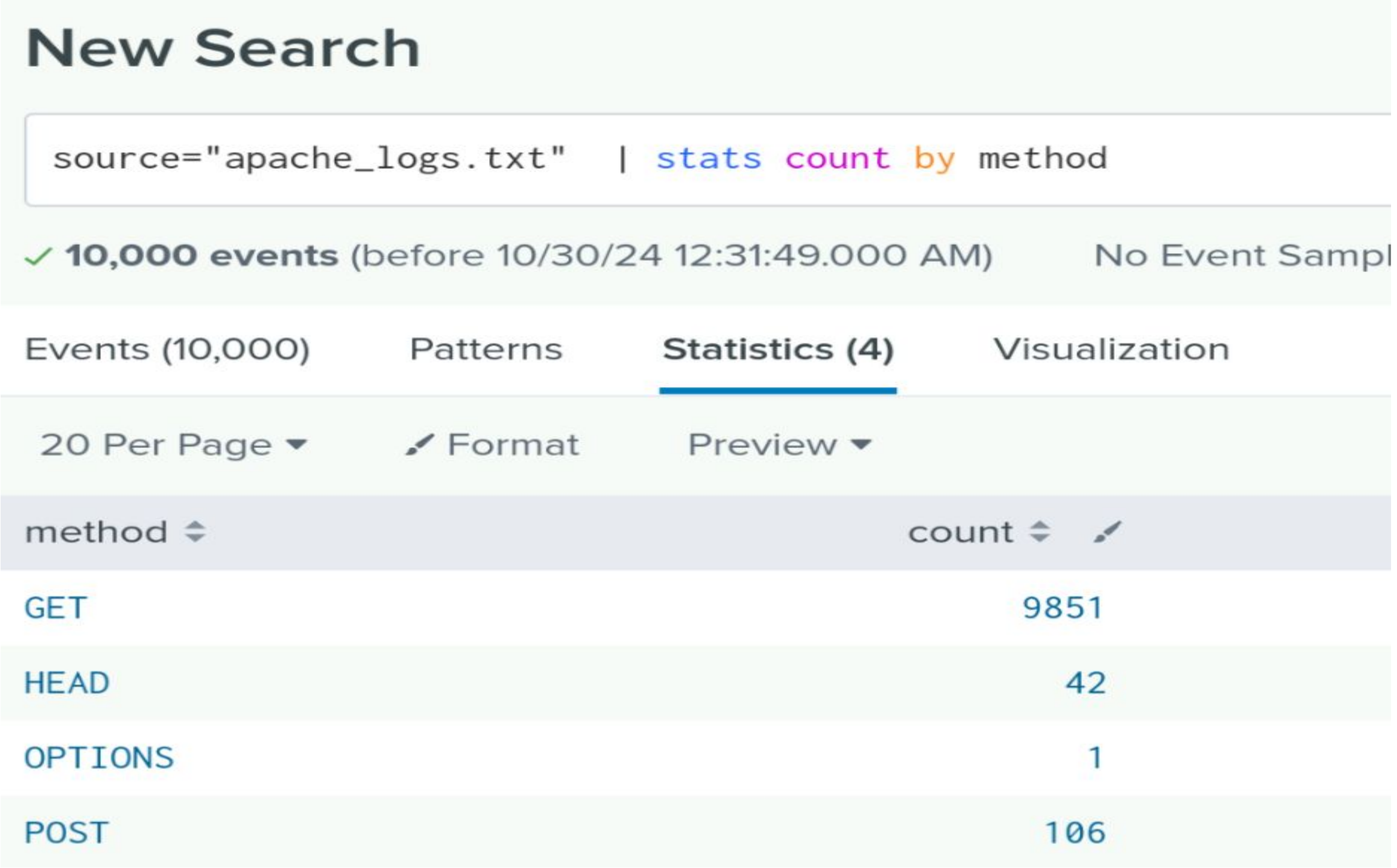
```
source="apache_attack_logs.txt" host="Apache_logs" | stats count by status
```

✓ 4,497 events (before 10/30/24 1:08:36.000 AM) No Event Sampling ▾

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

Reports—HTTP Method Stats

Description	Analysis
Counts the number of HTTP method requests.	POST requests increasing by over 1000, from around 1% of requests to over 29% of requests.

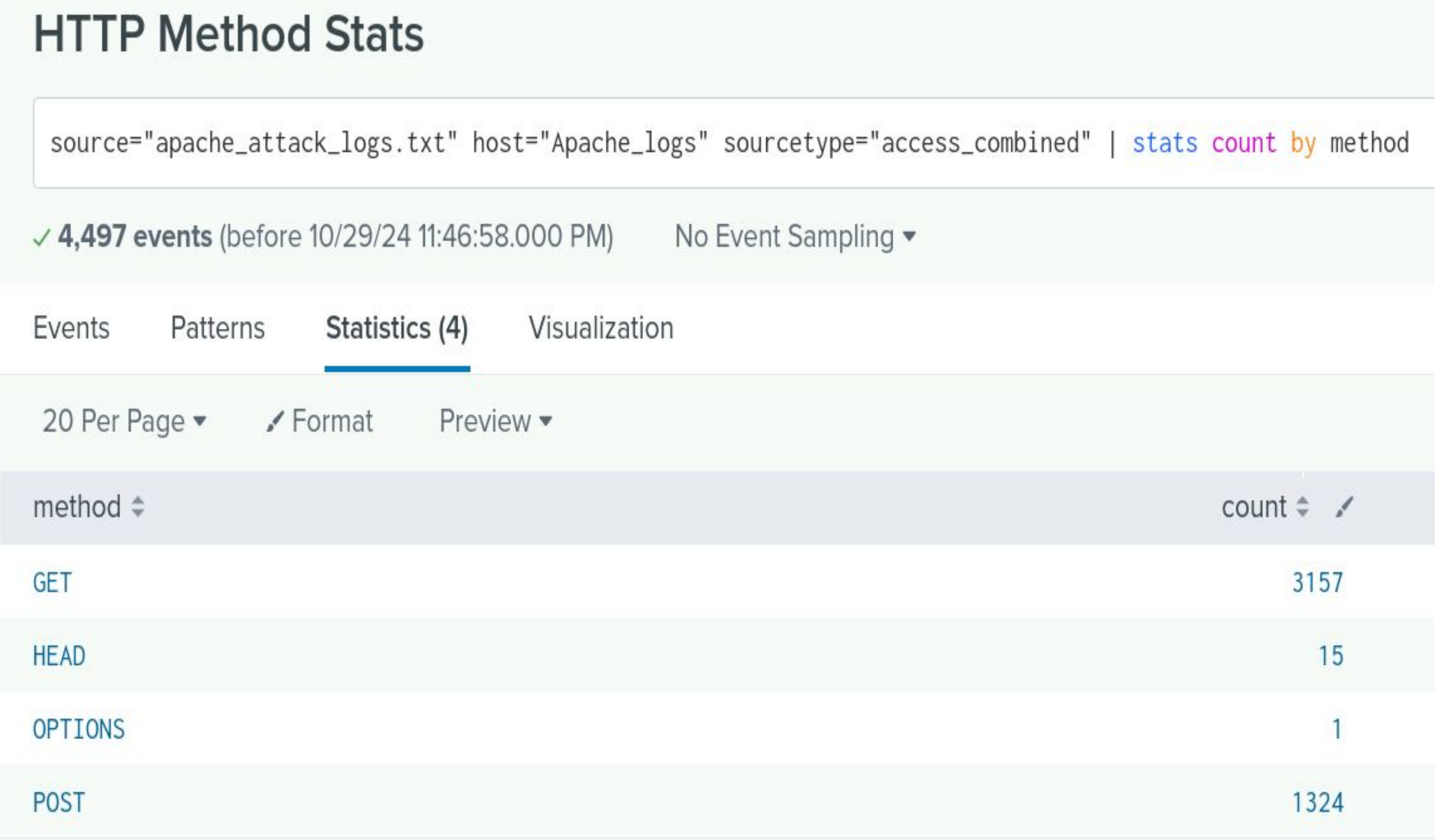


New Search

```
source="apache_logs.txt"  | stats count by method
```

✓ 10,000 events (before 10/30/24 12:31:49.000 AM) No Event Sampl

method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106



HTTP Method Stats

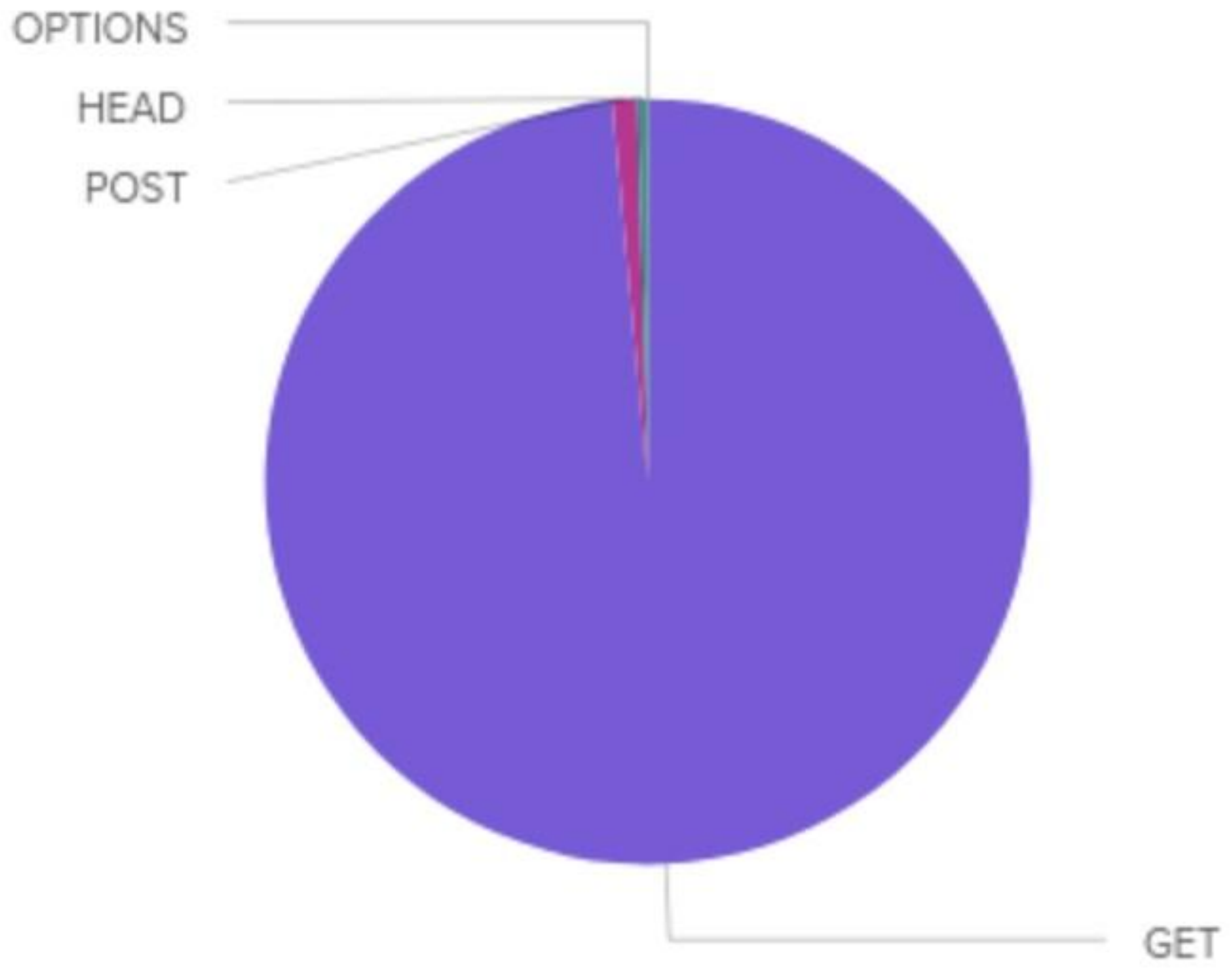
```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" | stats count by method
```

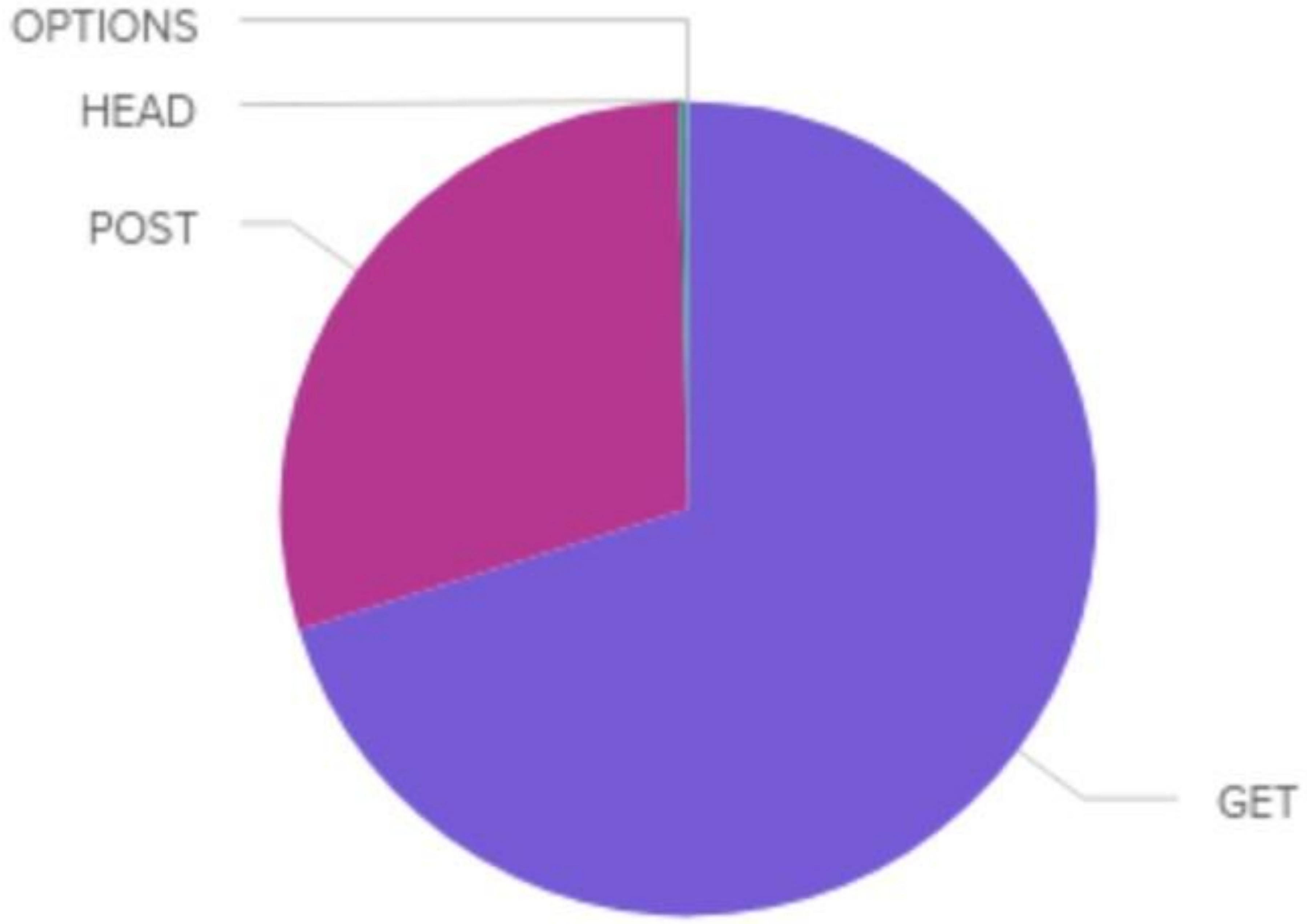
✓ 4,497 events (before 10/29/24 11:46:58.000 PM) No Event Sampling ▾

method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

Reports—HTTP Method Stats

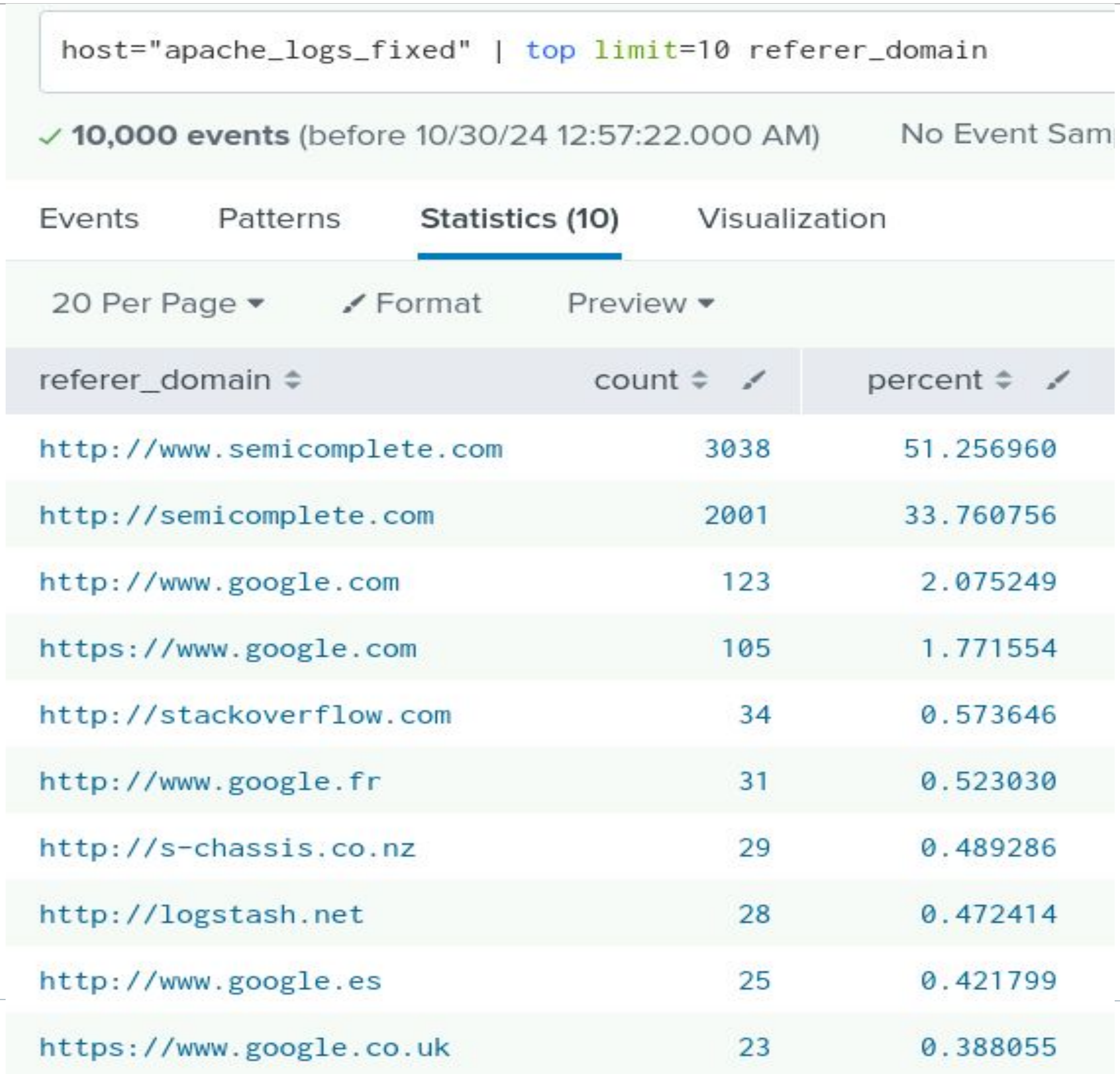
Description	Analysis
Counts the number of HTTP method requests.	POST requests increasing by over 1000, from around 1% of requests to over 29% of requests.





Reports—Top 10 Domains

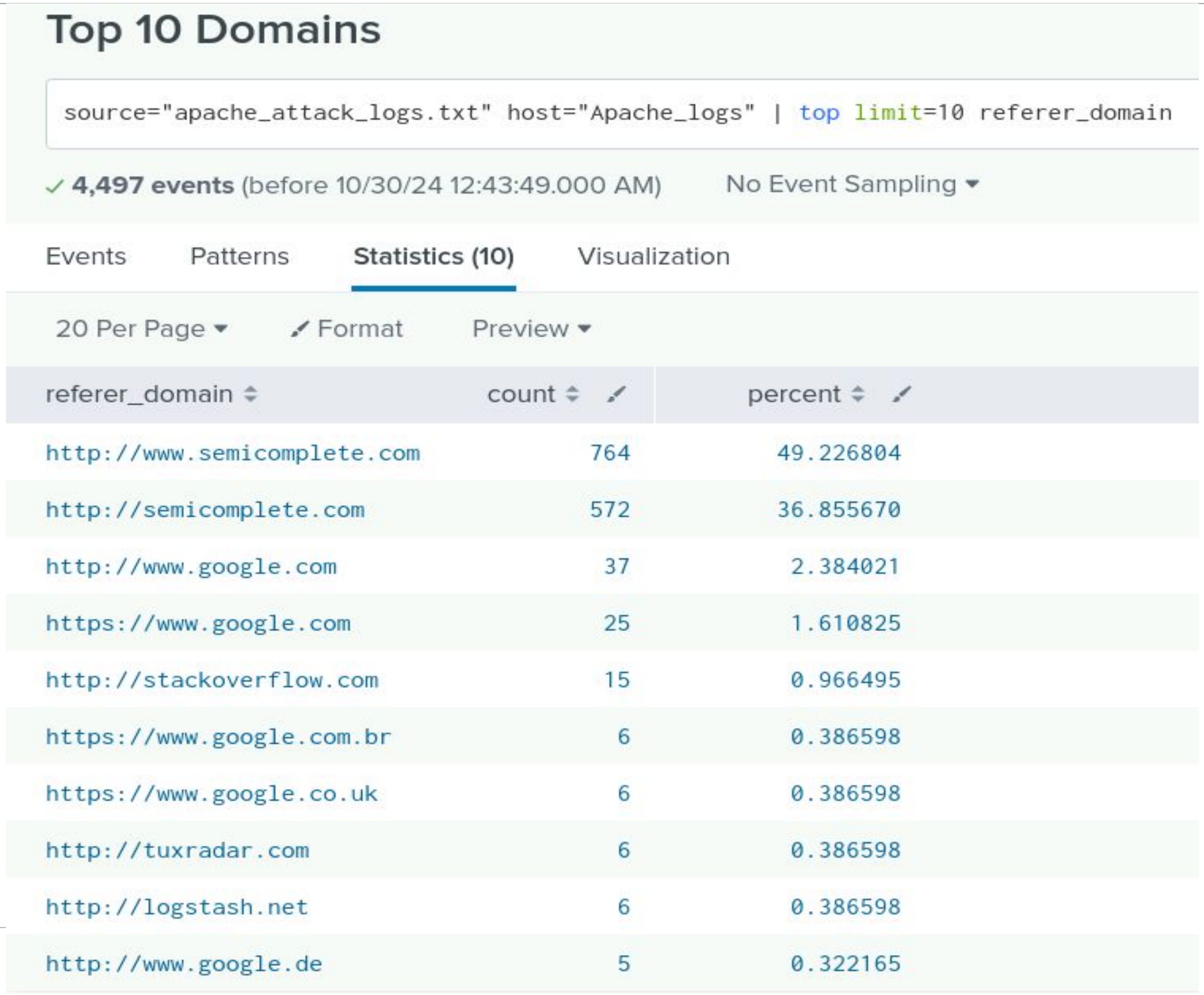
Description	Analysis
Shows a list of the top 10 domains.	No suspicious change was detected.



```
host="apache_logs_fixed" | top limit=10 referer_domain
```

✓ **10,000 events** (before 10/30/24 12:57:22.000 AM)

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



Top 10 Domains

```
source="apache_attack_logs.txt" host="Apache_logs" | top limit=10 referer_domain
```

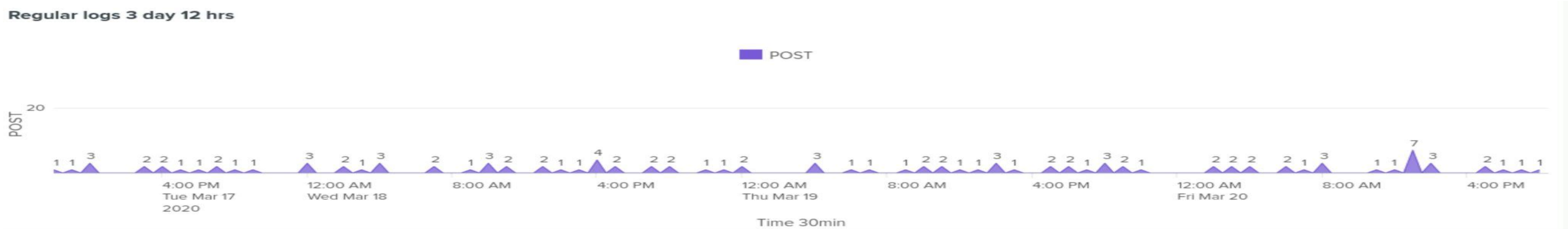
✓ **4,497 events** (before 10/30/24 12:43:49.000 AM)

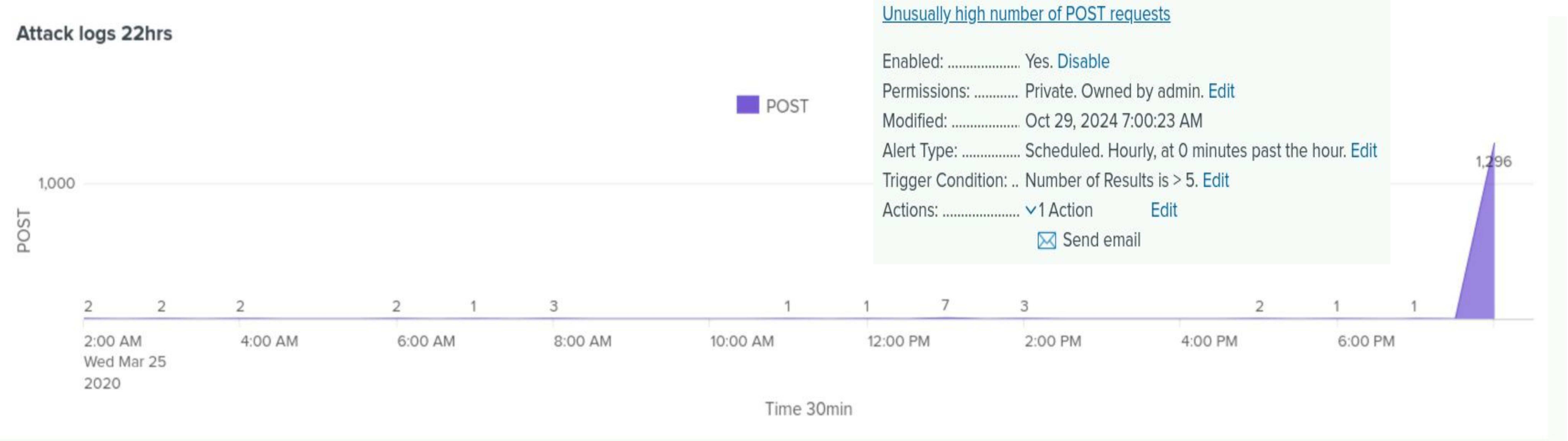
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Apache Alerts

Alerts—Unusually high number of POST requests

Description	Alert Baseline	Alert Threshold	Analysis
Counts the number of HTTP POST activity.	4	6	1,296 events at 8:00 PM





Unusually high number of POST requests

Enabled: .... Yes. Disable

Permissions: .... Private. Owned by admin. Edit

Modified: .... Oct 29, 2024 7:00:23 AM

Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

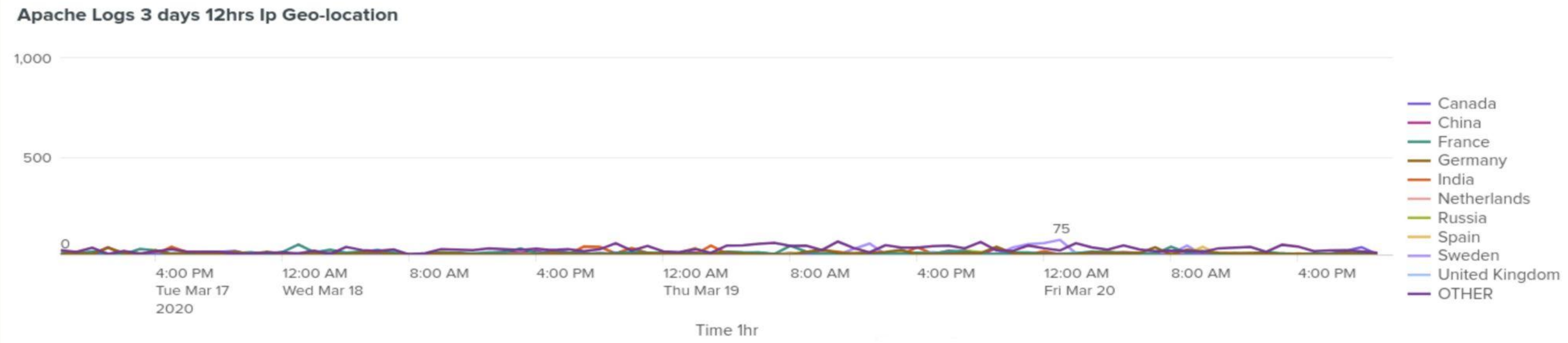
Trigger Condition: .. Number of Results is > 5. Edit

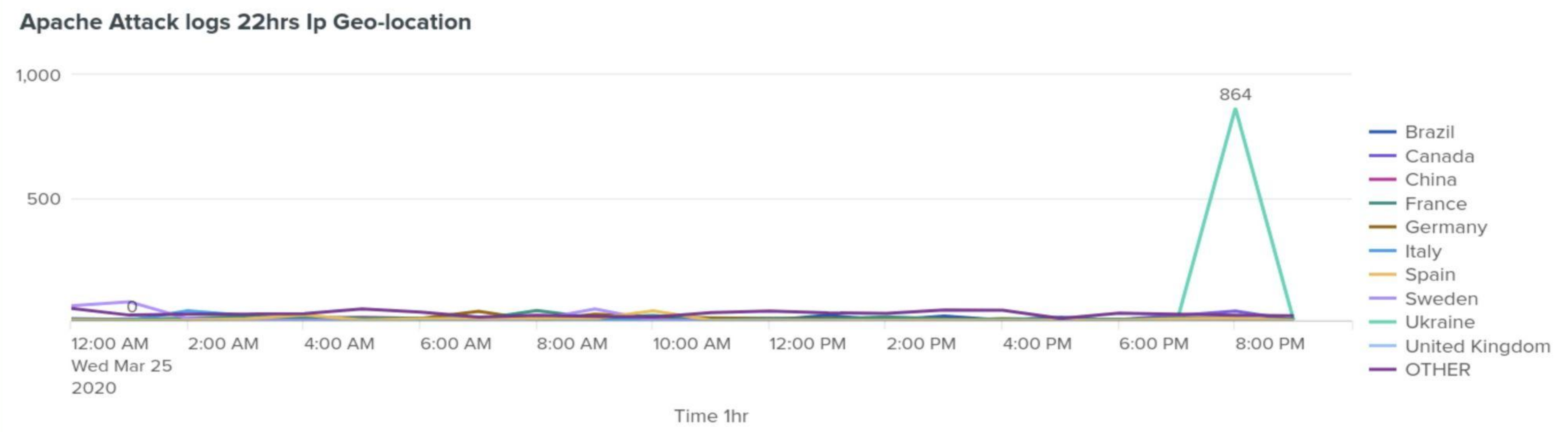
Actions: .... ∨1 Action Edit

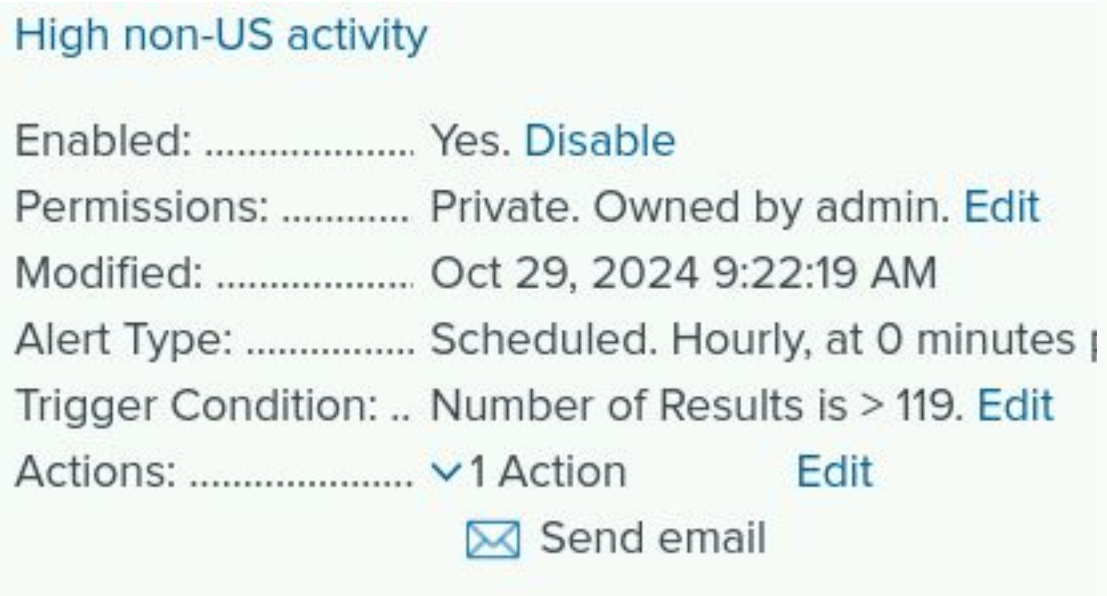
✉ Send email

Alerts—High non-US activity

Description	Alert Baseline	Alert Threshold	Analysis
Sends an email alert when there is a high number of traffic outside of the US	80	120	864 events at 8 PM







High non-US activity

Enabled: .... Yes. Disable

Permissions: .... Private. Owned by admin. Edit

Modified: .... Oct 29, 2024 9:22:19 AM

Alert Type: .... Scheduled. Hourly, at 0 minutes p

Trigger Condition: .. Number of Results is > 119. Edit

Actions: .... ∨1 Action Edit

✉ Send email

Summary and Future Mitigations

Project 3 Summary - Findings

- **Overall Findings:**
  - Windows logs
    - Potentially failed attack at 2am.
    - Apparent successful attack at 8am.
    - Attacks appear to have changed a number of passwords once gaining access.
  - Apache logs
    - Possible that attacker is attempting brute force login attempts.
    - Unusually high amount of requests to the account logon page.
    - Possible the spike in GET requests relate to an attacker scraping the website for reconnaissance.
    - Spike in POST requests (likely used to submit the login form), the attacker could be trying many usernames/passwords in an attempt to find valid credentials.
    - High non-US activity at the same time as POST requests.

Project 3 Summary - Mitigations

- **Future Mitigations:**
  - Adjust alerts as mentioned.
  - Brute force protection on website - Rate limits, MFA, strong password requirements.
  - As web server is admin page, consider if needs to be accessible from web.
  - Anomaly-Based IPS to limit unusual Windows activity (e.g. huge amount of password resets).
  - Geo-Blocking - Consider blocking or challenging access from regions where legitimate traffic is unlikely.
  - Web Application Firewall (WAF) - Use a WAF to detect and block suspicious requests that could indicate reconnaissance or scraping.