Defensive Security Project
Group 6

Zakriya Ahmed, Ralphy Ramirez, Tyler Mosely, Edmund Asare, &
Kenneth Pritchett

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

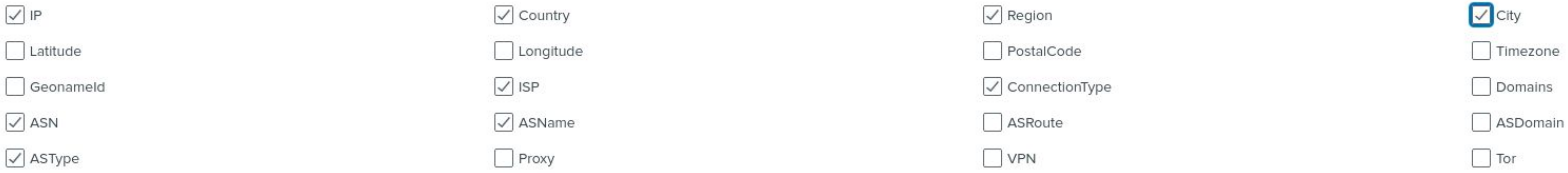
Scenario

- We are playing the role of SOC analysts working for Virtual Space Industries (VSI)
- There are rumors that JobeCorp, a competitor, is planning to launch a cyberattack(s) against VSI
- We are using Splunk to monitor and analyze Windows web server logs as well as apache web server logs, both before and after the attack takes place
- We are tasked with creating reports, alerts, and dashboards displaying various charts that analyze data and indicate which activity is suspicious

[“Add-On” App]

Whois XML IP Geolocation API

This Splunk add-on app allows you to search IPs and get the geographical location of users. There are twenty options for your search that allows you to look for more detailed information on the IP(s) you are looking into.



☑ IP ☑ Country ☑ Region ☑ City

□ Latitude □ Longitude □ PostalCode □ Timezone

□ GeonameId ☑ ISP ☑ ConnectionType □ Domains

☑ ASN ☑ ASName □ ASRoute □ ASDomain

☑ ASType □ Proxy □ VPN □ Tor

Whois XML IP Geolocation API

- JobeCorp, VSI’s adversary, has been known to attack their competitors by using international VPNs and TOR to launch application attacks.

- Using the IP Geolocation Lookup feature of this app would allow admins to look into IPs reaching their company’s websites at high volumes and see if their locations are unusual and if they should be investigated.

- The next slide is a screenshot of a search of the top 5 IPs in the apache_attack_logs.txt file.

- When compared to the apache_logs.txt file (following slide), there are two Ukraine IPs that stand out.

Whois XML IP Geolocation API

After Attack

Edit
Export

IP Geolocation lookup

Enter an IP address (or a comma-separated list).

208.91.156.11, 194.105.145.147, 194.146.132.138, 79.171.127.34, 130.237.218.86

Submit

Select visible fields

☑ IP ☑ Country ☑ Region ☑ City

☐ Latitude ☐ Longitude ☐ PostalCode ☐ Timezone

☐ GeonameId ☑ ISP ☑ ConnectionType ☐ Domains

☑ ASN ☑ ASName ☐ ASRoute ☐ ASDomain

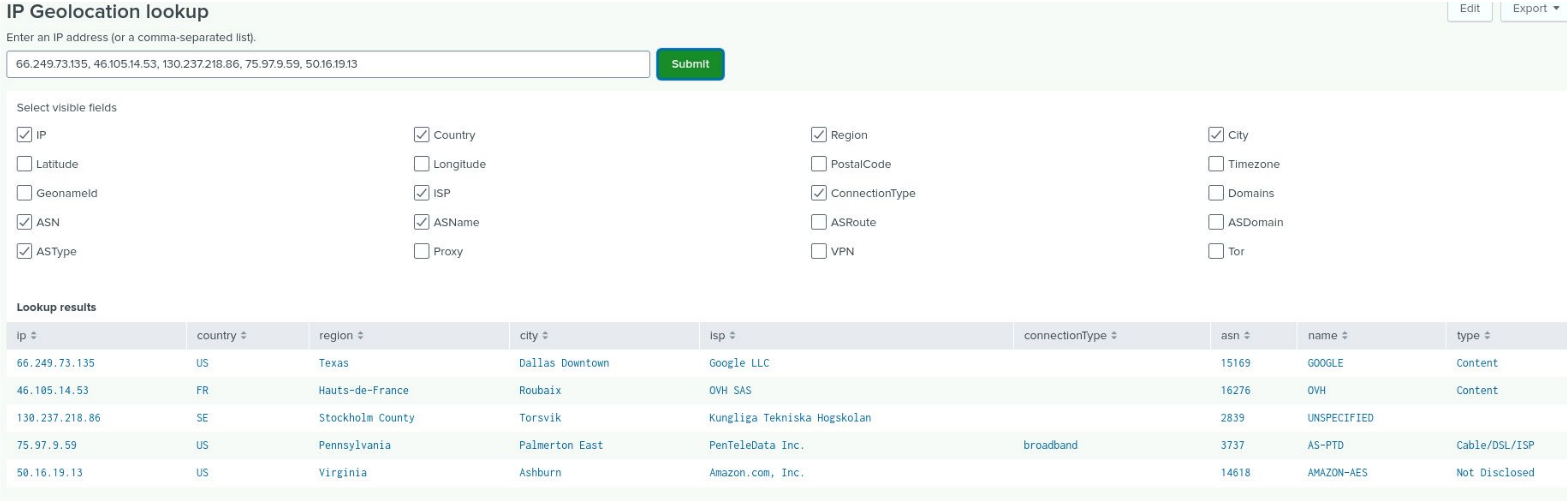
☑ ASType ☐ Proxy ☐ VPN ☐ Tor

Lookup results

ip	country	region	city	isp	connectionType	asn	name	type
208.91.156.11	US	California	Santa Monica	Hulu, LLC		23286	HULU	Content
194.105.145.147	UA	Misto Kyiv	Kyiv	Ciklum LLC		39223	Ciklum	
194.146.132.138	US	New York	New York City	PP "Poisk-Lugansk"		29576	POISK-UA	
79.171.127.34	UA	Kharkivska Oblast	Kharkiv	Maxnet Ltd.		34700	CITYNET-AS	Cable/DSL/ISP
130.237.218.86	SE	Stockholm County	Torsvik	Kungliga Tekniska Hogskolan		2839	UNSPECIFIED	

Whois XML IP Geolocation API

Before Attack



IP Geolocation lookup

Enter an IP address (or a comma-separated list).

66.249.73.135, 46.105.14.53, 130.237.218.86, 75.97.9.59, 50.16.19.13

Select visible fields

☑ IP ☑ Country ☑ Region ☑ City

☐ Latitude ☐ Longitude ☐ PostalCode ☐ Timezone

☐ GeonameId ☑ ISP ☑ ConnectionType ☐ Domains

☑ ASN ☑ ASName ☐ ASRoute ☐ ASDomain

☑ ASType ☐ Proxy ☐ VPN ☐ Tor

Lookup results

ip	country	region	city	isp	connectionType	asn	name	type
66.249.73.135	US	Texas	Dallas Downtown	Google LLC		15169	GOOGLE	Content
46.105.14.53	FR	Hauts-de-France	Roubaix	OVH SAS		16276	OVH	Content
130.237.218.86	SE	Stockholm County	Torsvik	Kungliga Tekniska Hogskolan		2839	UNSPECIFIED	
75.97.9.59	US	Pennsylvania	Palmerton East	PenTeleData Inc.	broadband	3737	AS-PTD	Cable/DSL/ISP
50.16.19.13	US	Virginia	Ashburn	Amazon.com, Inc.		14618	AMAZON-AES	Not Disclosed

Logs Analyzed

1 Windows Logs

- These server logs contain information pertaining to VSI's new virtual reality technology
- Logs contain Windows server activity events including severity level events, success vs. failure rates, signature IDs, and user activity events

2 Apache Logs

- These server logs contain information pertaining to VSI's public website, vsi-company.com
- Logs contain URI stats, user activity on the website, user logon events & account manipulation, HTTP response methods & codes, as well as geostatistics

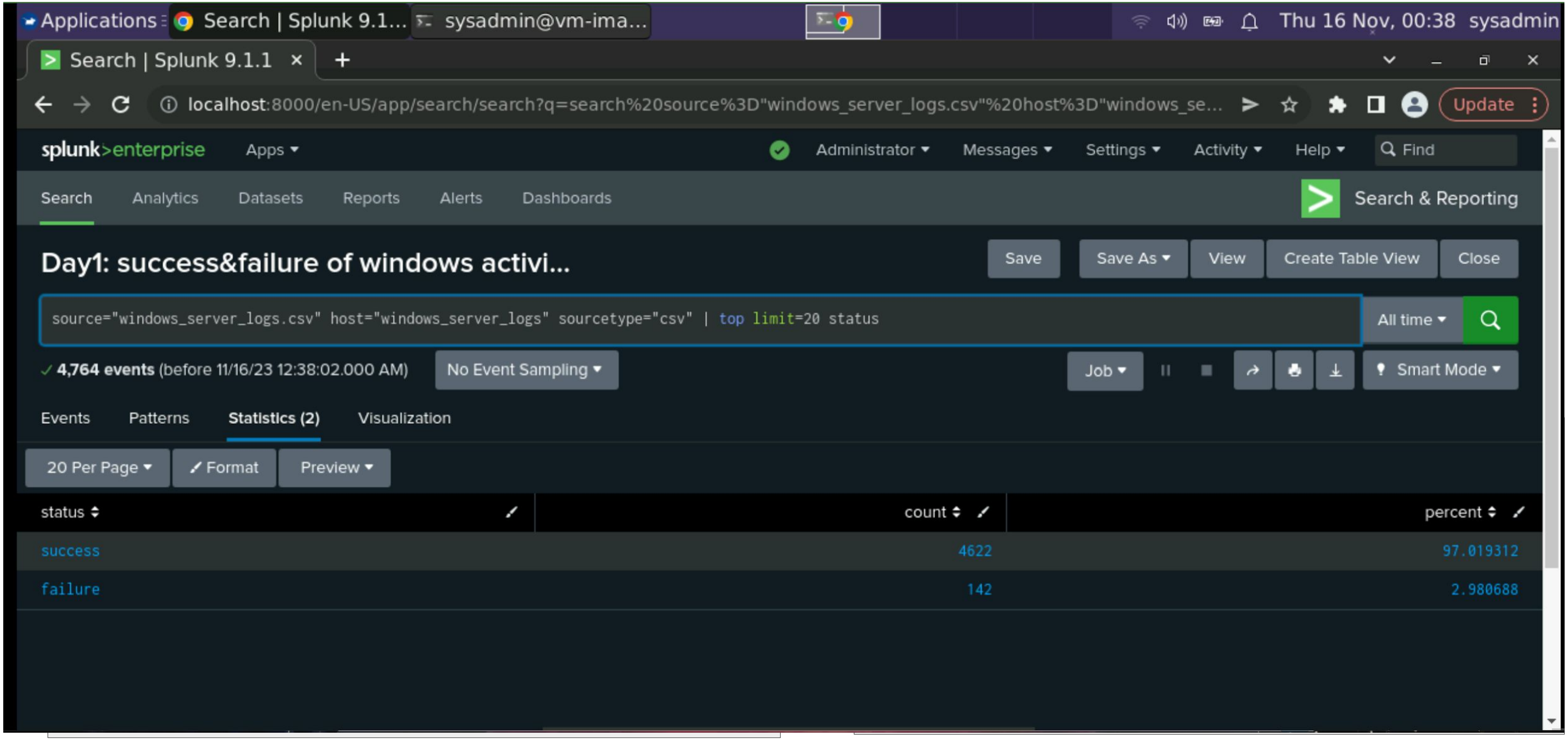
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Severity Levels	Documents the number of events that are considered of either informational severity or high severity
Signature & Signature IDs	Documents the signatures (account actions in plaintext) that have occurred and the frequency
Success & Failure	Documents the number of failed vs. successful events & requests that have occurred

Images of Reports—Windows: Success & Failure



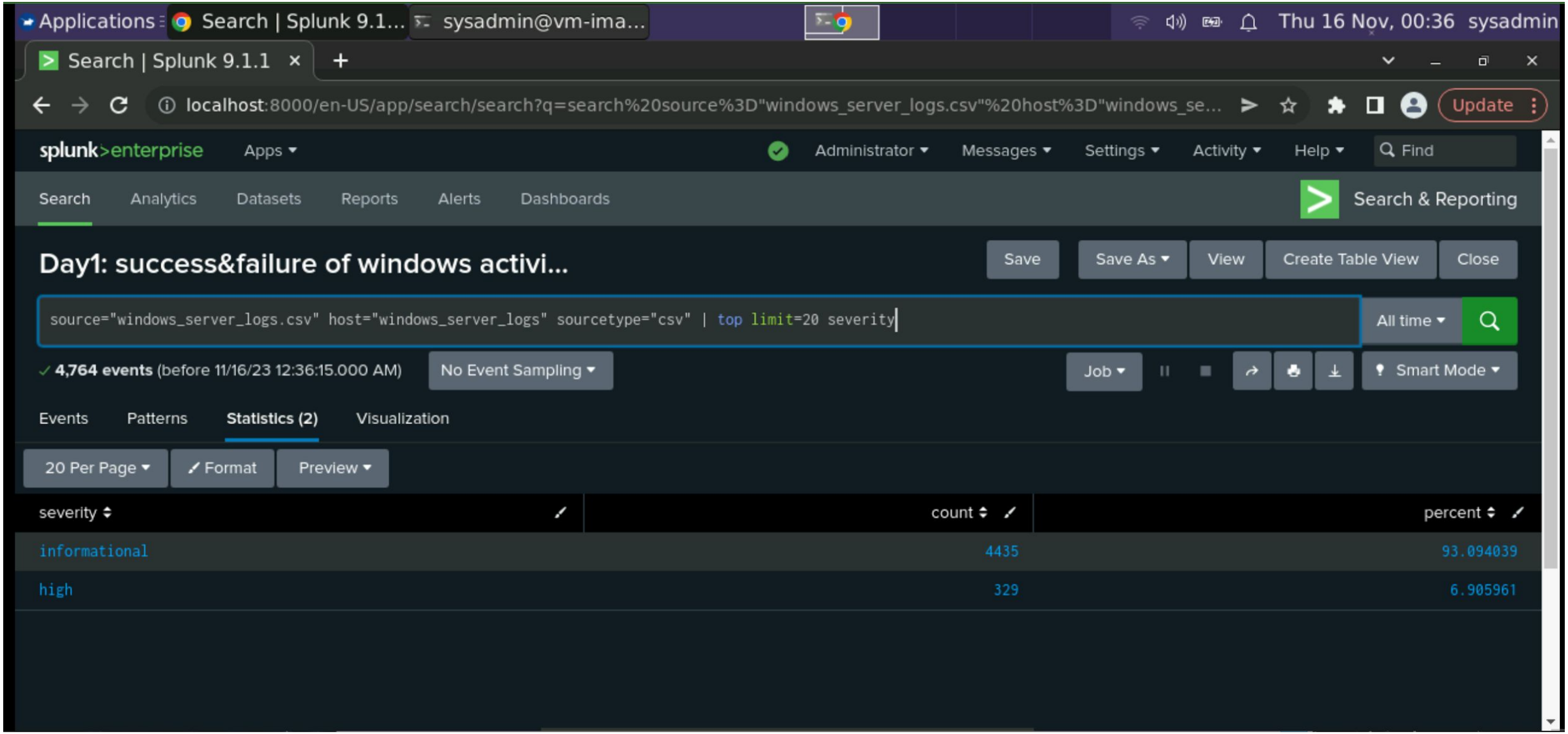
Day1: success&failure of windows activi...

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

✓ 4,764 events (before 11/16/23 12:38:02.000 AM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

Images of Reports—Windows: Severity Levels



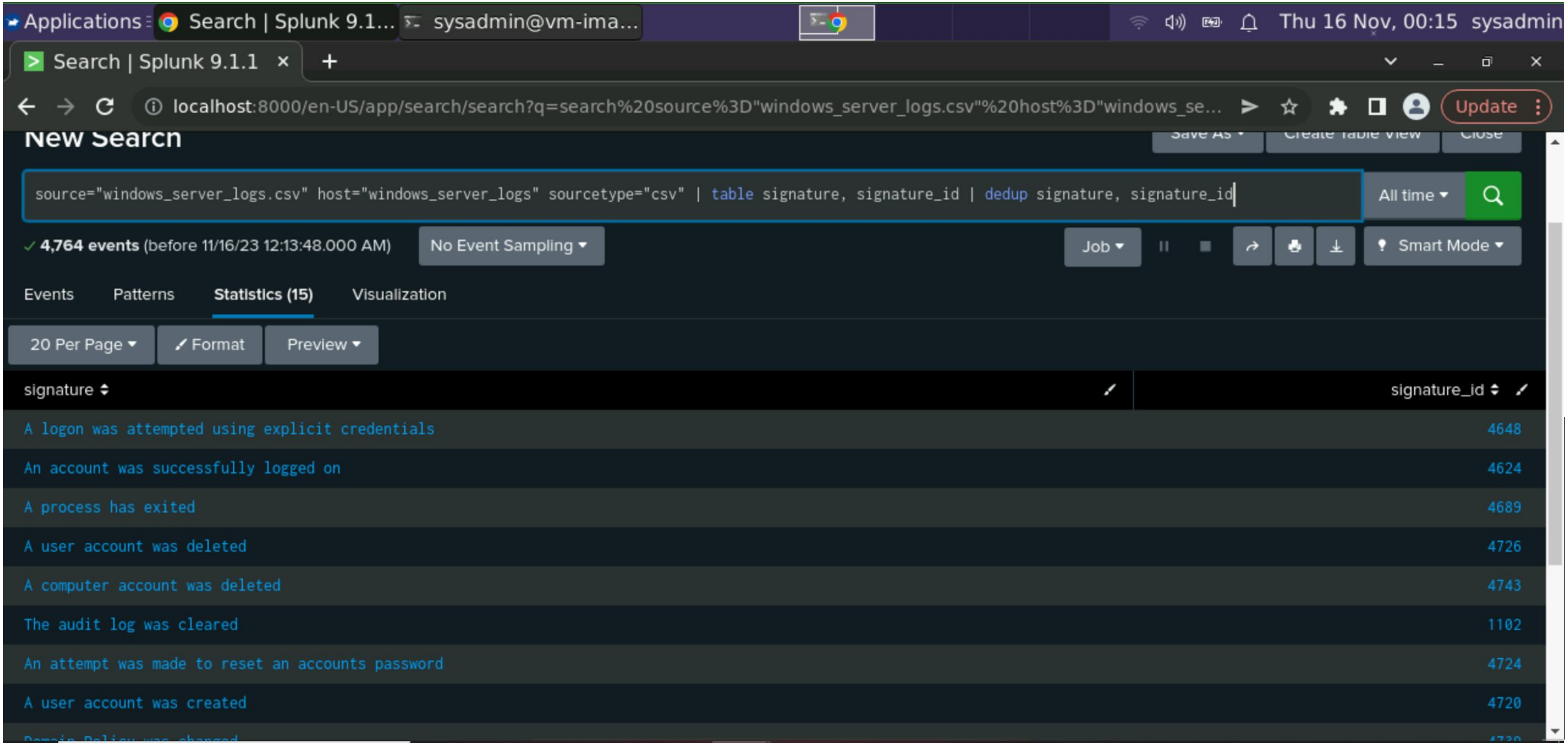
Day1: success&failure of windows activi...

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

✓ **4,764 events** (before 11/16/23 12:36:15.000 AM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Images of Reports—Windows: Signature & Signature ID



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

✓ **4,764 events** (before 11/16/23 12:13:48.000 AM)

signature	signature_id
A logon was attempted using explicit credentials	4648
An account was successfully logged on	4624
A process has exited	4689
A user account was deleted	4726
A computer account was deleted	4743
The audit log was cleared	1102
An attempt was made to reset an accounts password	4724
A user account was created	4720
Domain Policy was changed	4739

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Failed Windows Activity	Keeps track of the hourly level of failed Windows activity	8	15

JUSTIFICATION: Hourly count was values 5-10, so around 8 would make sense for a baseline. Anything over 15 could be deemed suspicious as it is not seen going over 10 per hour.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of Signature ID 4624	Keeps track of hourly count of signature ‘An account was successfully logged on ‘	13-17	25

JUSTIFICATION: Hourly counts that occurred most were values 13-17 so that was chosen for the baseline. Threshold of 25 was determined because there was only one hour where the hourly count was over 20.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of Signature ID 4726	Keeps track of hourly count of signature ‘A user account was deleted’	13-17	25

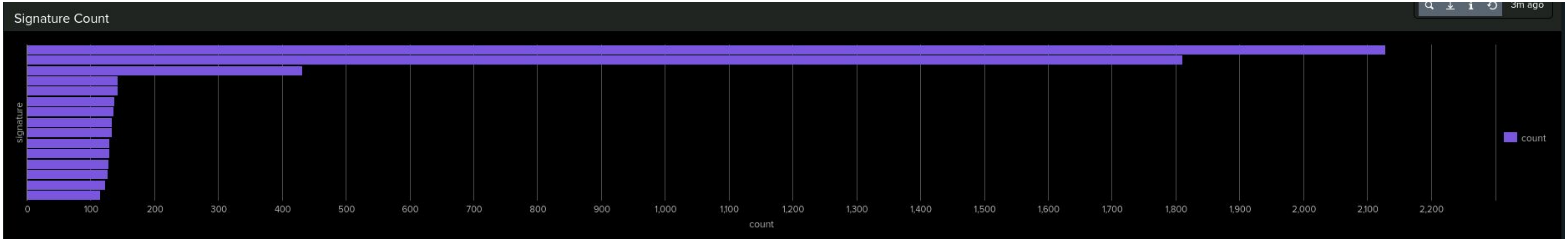
JUSTIFICATION: Hourly count was similar to Signature ID 4624, so same baseline and threshold used.

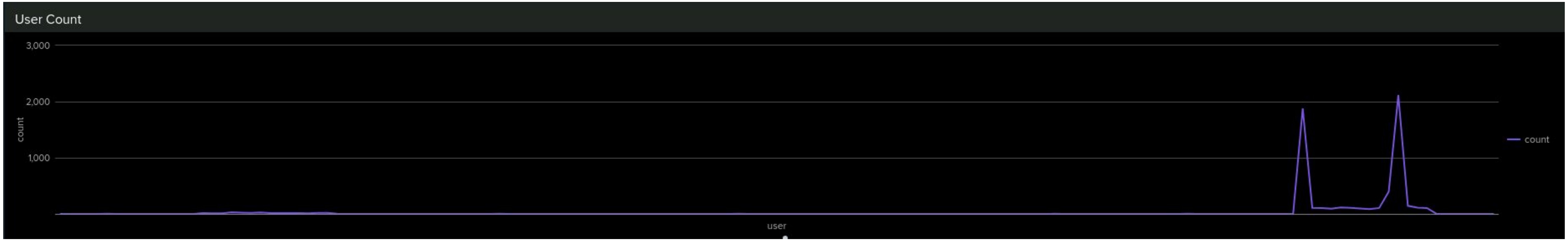
Dashboards—Windows

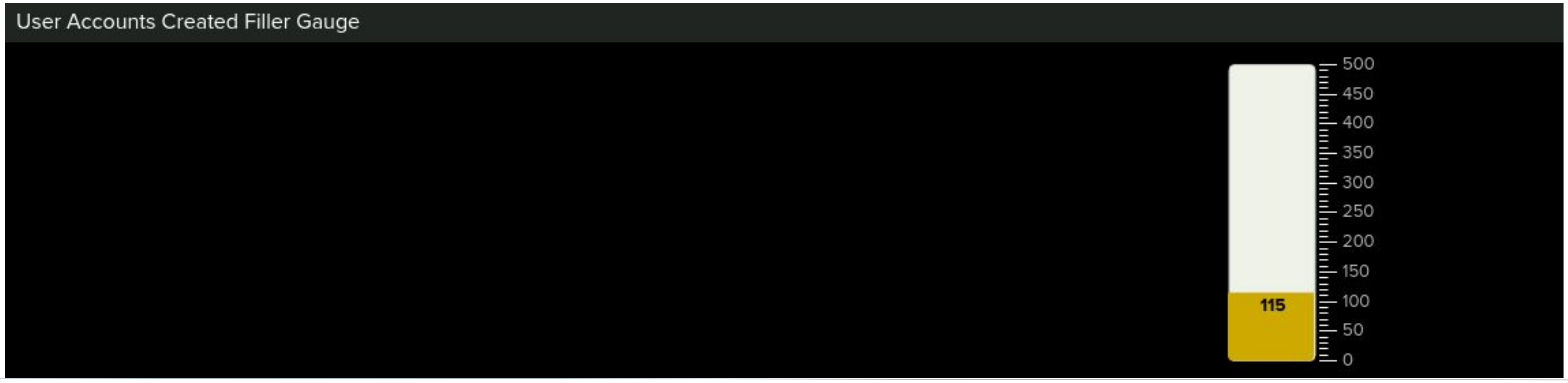
Signature Time Chart
Signature Time Chart
1,500
1,000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER

2m ago
User Time Chart
User Time Chart
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
_time
user_a
user_b
user_c
user_e
user_f
user_i
user_j
user_k
user_l
user_m
OTHER

Dashboards—Windows







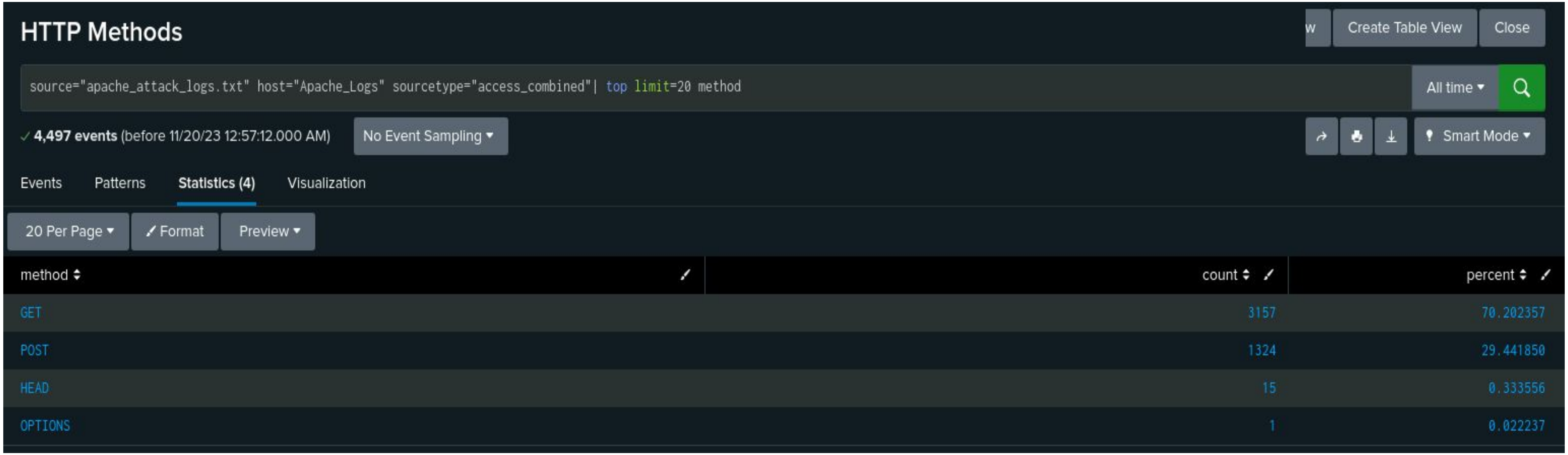
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Shows the number of requests of each of the different HTTP methods being requested against VSI’s web server.
Top 10 Domains	Shows the top 10 domains that refer to VSI’s website
HTTP Response Code Count	Shows the count of each HTTP responses

Images of Reports—Apache

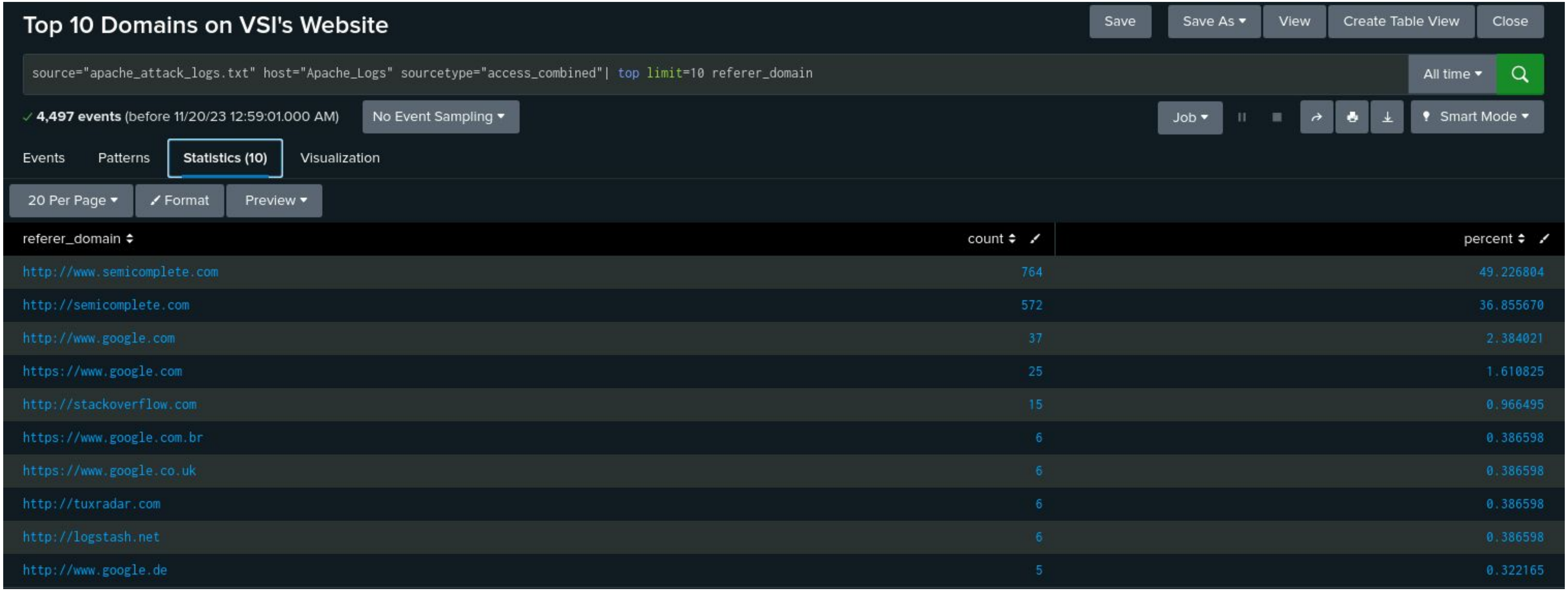


```
source="apache_attack_logs.txt" host="Apache_Logs" sourcetype="access_combined"| top limit=20 method
```

✓ **4,497 events** (before 11/20/23 12:57:12.000 AM)

method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

Images of Reports—Apache



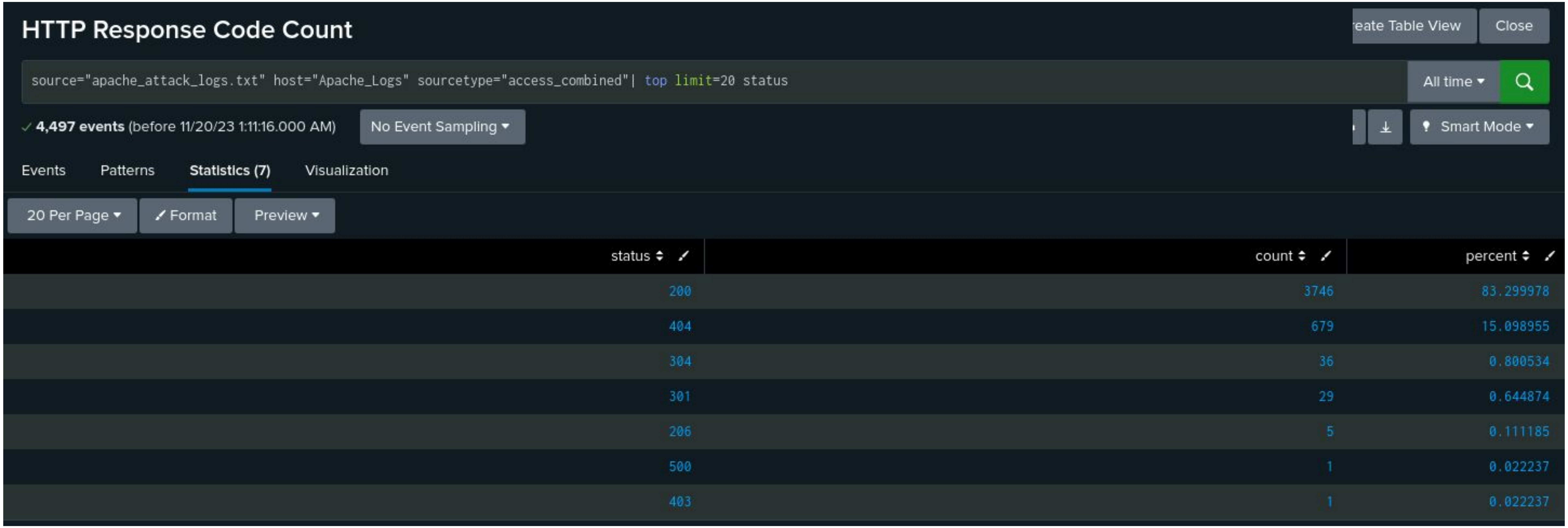
Top 10 Domains on VSI's Website

```
source="apache_attack_logs.txt" host="Apache_Logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ **4,497 events** (before 11/20/23 12:59:01.000 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

Images of Reports—Apache



HTTP Response Code Count

```
source="apache_attack_logs.txt" host="Apache_Logs" sourcetype="access_combined"| top limit=20 status
```

✓ **4,497 events** (before 11/20/23 1:11:16.000 AM)

status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity of Foreign IPs	Keeps track of hourly activity from non-US IPs	125	200

JUSTIFICATION: The hourly count of activity was around 115-135 so 125 was determined as the baseline. There was no hour where the activity count was over 150 so we chose 200 as the threshold.

Alerts—Apache

Designed the following alerts:

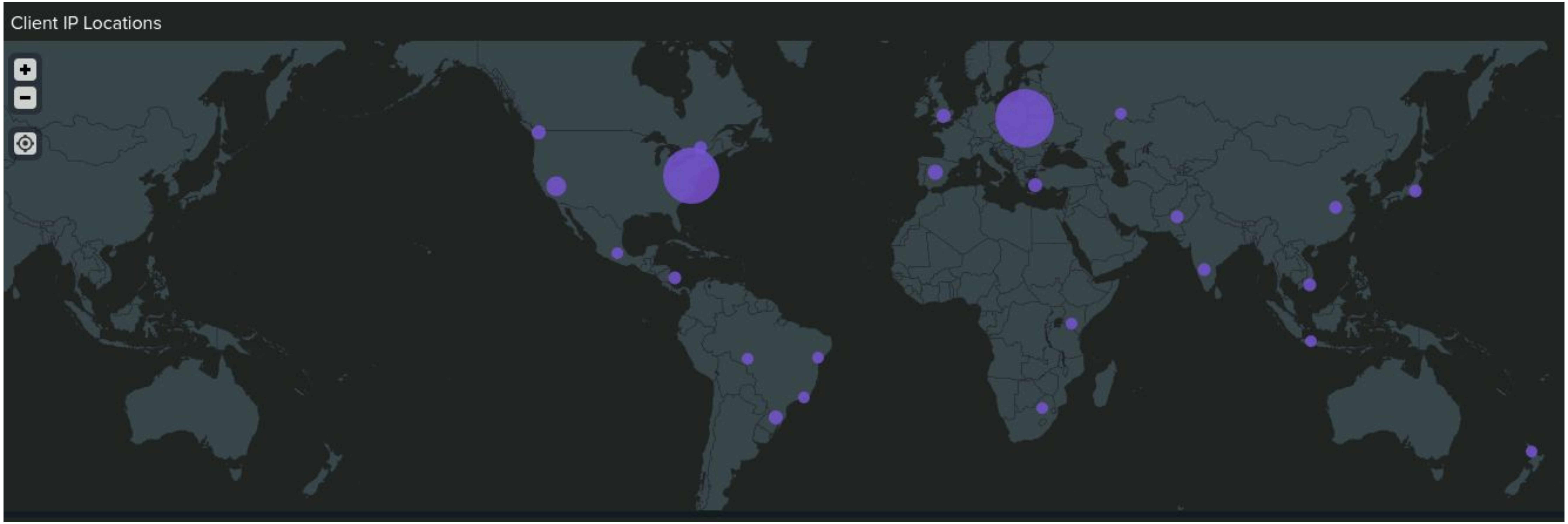
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of HTTP POST	Keeps track of hourly POST requests	4	10

JUSTIFICATION: Hourly POST requests were around 0-7 so 4 was determined as the baseline. The hourly count never exceeded 7 so 10 was chosen as the threshold.

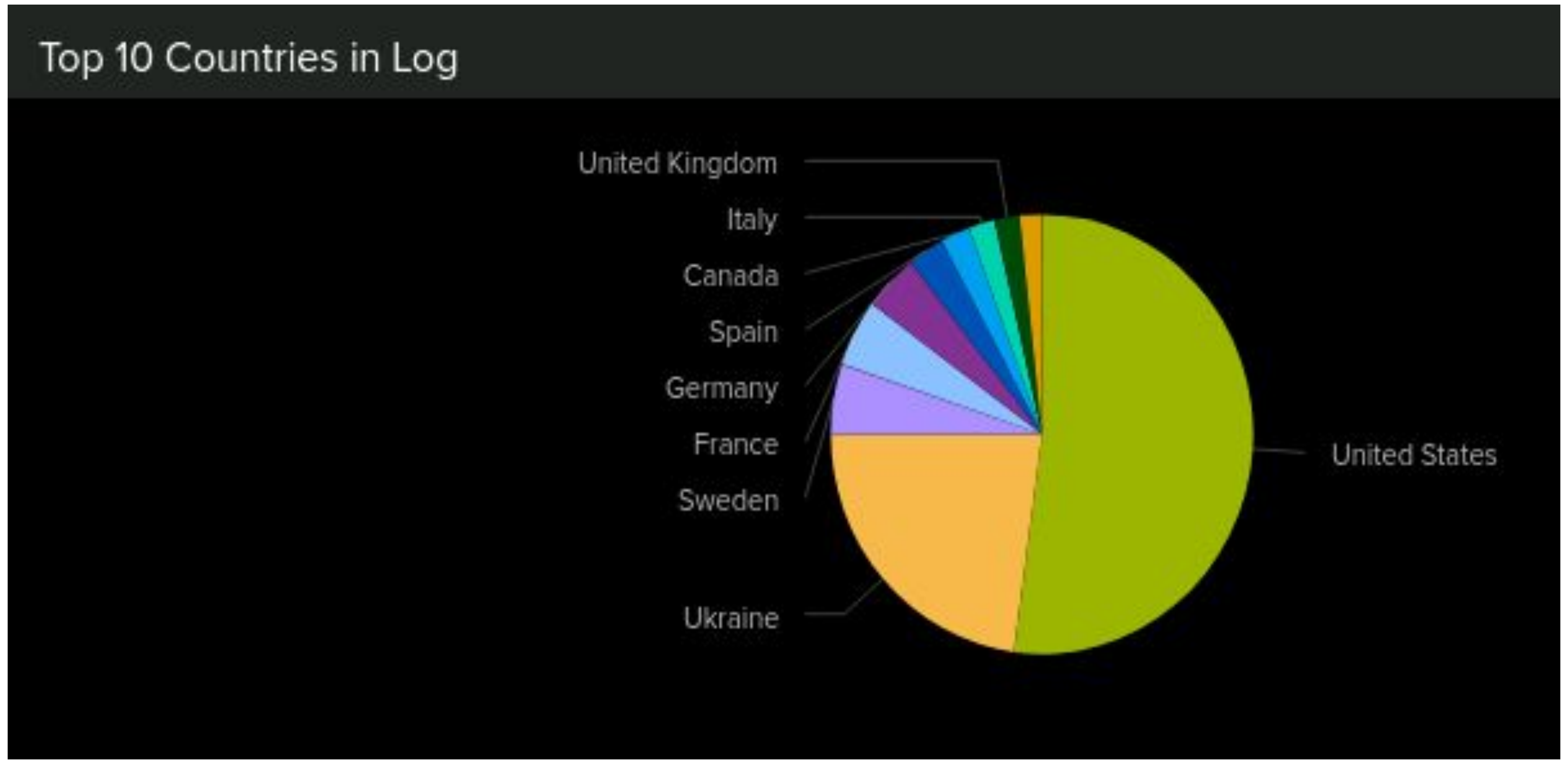
Dashboards—Apache

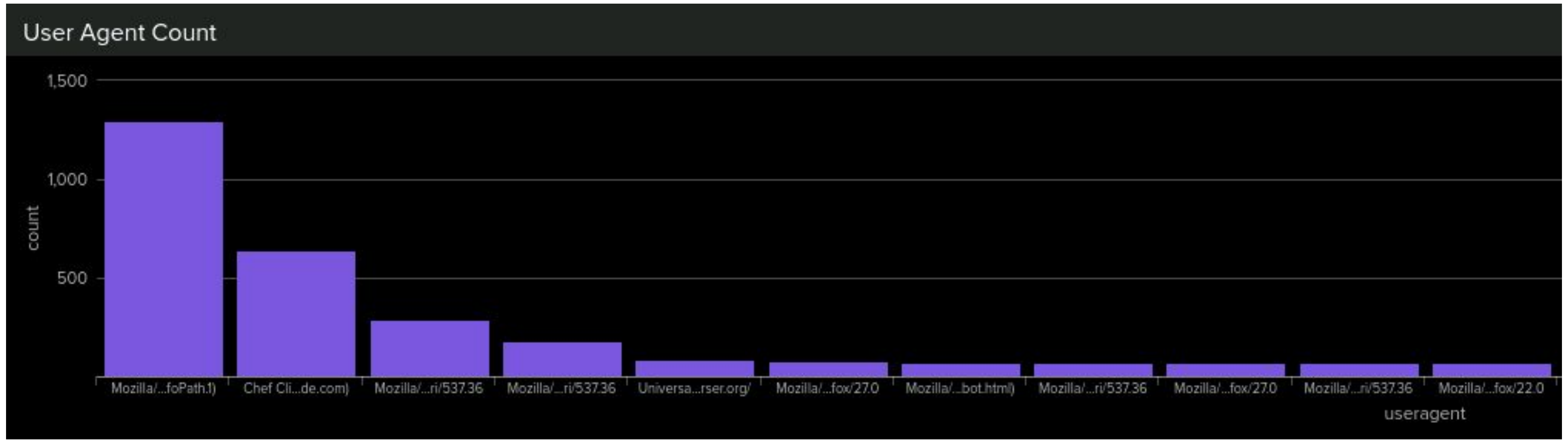
HTTP Method Line Chart

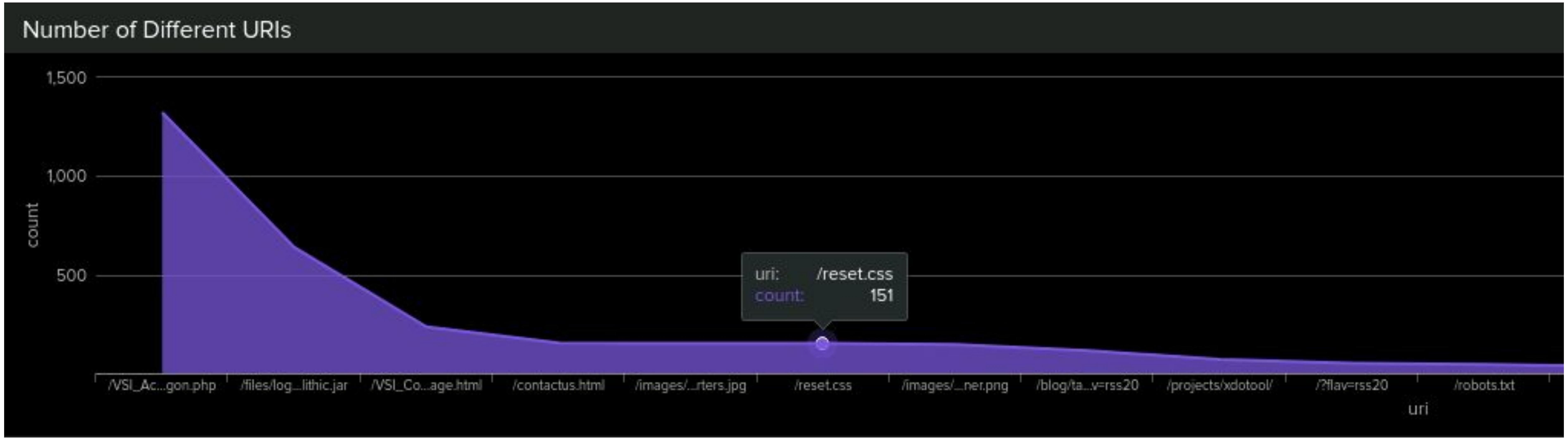
1,500
1,000
500
12:00 AM Wed Mar 25 2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
2:00 PM
3:00 PM
4:00 PM
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
_time
GET
HEAD
OPTIONS
POST


Client IP Locations

Dashboards—Apache







Attack Analysis

Attack Summary—Windows

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

- Report Analysis for Severity: Note an increase of almost 700 events for high severity, from 329 to 1111 events. This could be seen as suspicious.
- Report Analysis for Failed Activities: A decrease of about 50 failed activities and an increase of about 1200 successful logins. The drastic increase of successful logins could be seen as suspicious.

Attack Summary—Windows

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

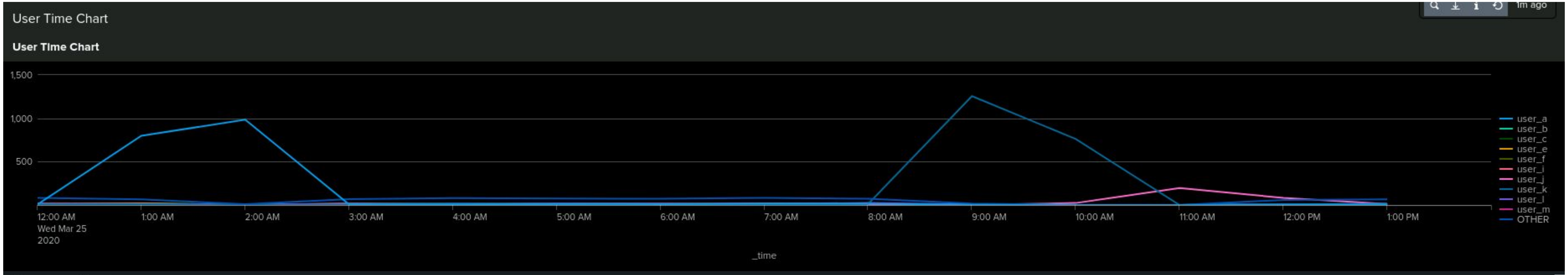
- Alert Analysis for Failed Windows Activity: 8AM shows a count of 35 failed activity events. Our threshold of 15 would have detected this activity.
- Alert Analysis for Successful Logins: 2AM shows 20 logins, 11 of them being from user_a alone. Our threshold of 25 hourly logins would not have alerted this activity.
- Alert Analysis for Deleted Accounts: The hourly count for deleted accounts was lower than a normal day and was not deemed as suspicious.

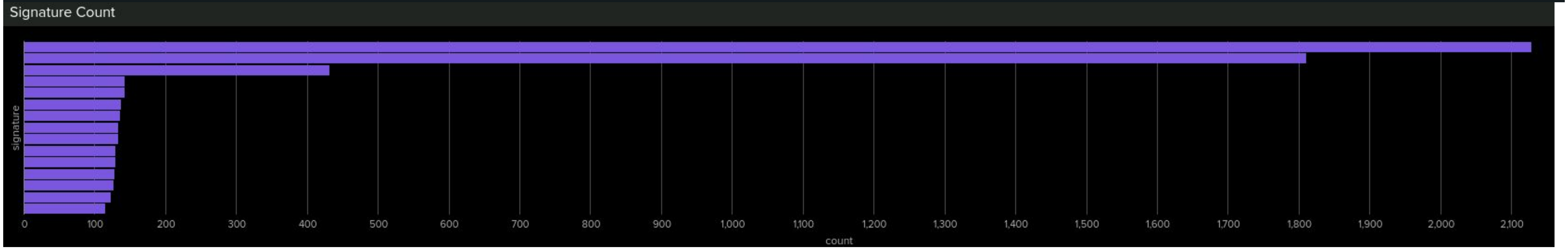
Attack Summary—Windows

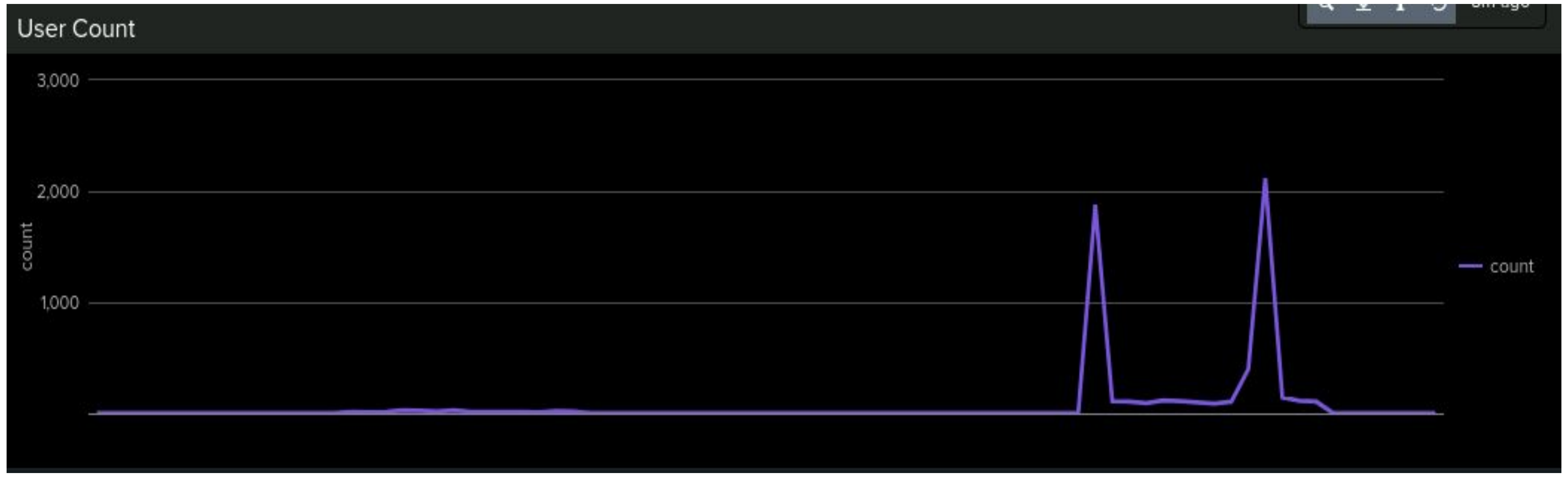
Summarize your findings from your dashboards when analyzing the attack logs.

- Dashboard Analysis for Time Chart of Signatures: There was an increase in ‘A user account was locked out’ from 12AM-3AM with a peak of 896 at 2AM and an increase in ‘An attempt was made to reset an accounts password’ from 8AM-11AM with a peak of 1,258 at 9AM
- Dashboard Analysis for Users: Users a and k have increased activity. User_a’s activity lasted from 12AM-3AM with a peak of 984 at 2AM. User_k’s activity lasted from 8AM-11AM with a peak of 1,256 at 9AM.

Screenshots of Attack Logs







Attack Summary—Apache

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

- Report Analysis for Methods: There was a dramatic increase in the number of POST requests. It went from 106 to 1324. This is suspicious activity.
- Report Analysis for Referrer Domains: There does not seem to be suspicious changes in referrer domains.
- Report Analysis for HTTP Response Codes: Error 404 codes increased by about 400 events.

Attack Summary—Apache

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

- Alert Analysis for International Activity: There was a suspicious volume of international activity from Ukraine. The country went from being outside of the top ten countries to being the one with the most activity following the US.
- Alert Analysis for HTTP POST Activity: There were 1,296 events at 8AM, this was deemed suspicious as the normal hourly count of POST requests is significantly lower.

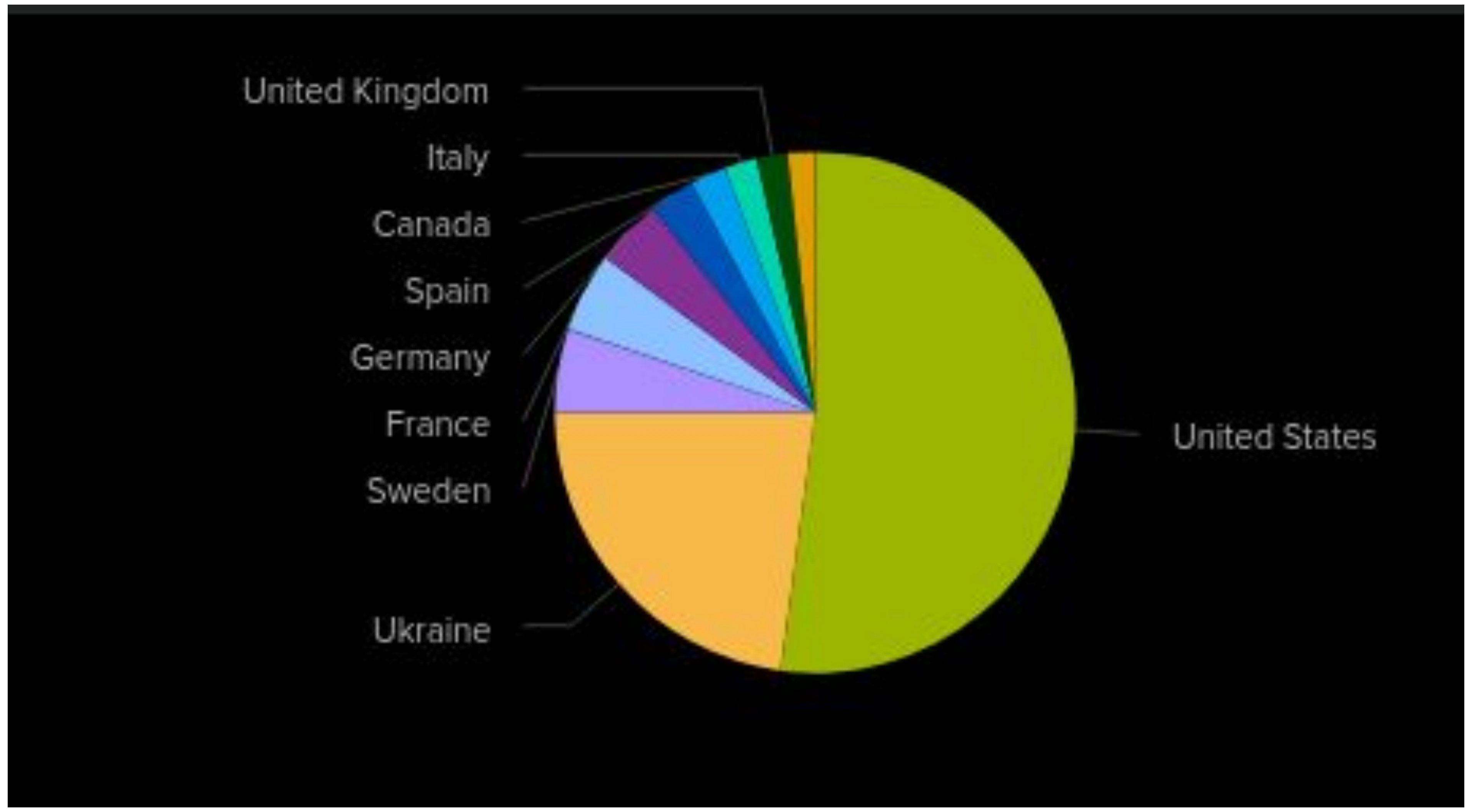
Attack Summary—Apache

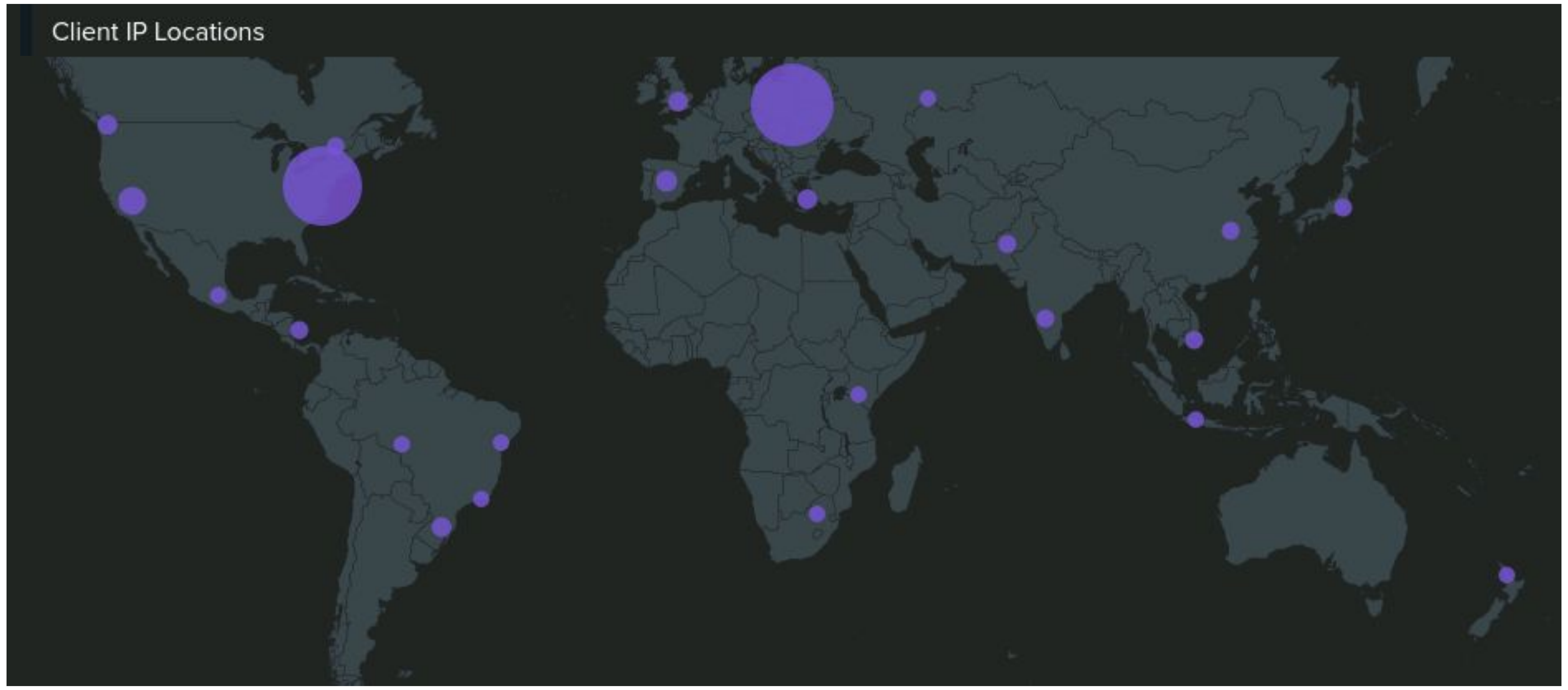
Summarize your findings from your dashboards when analyzing the attack logs:

- Dashboard Analysis for Cluster Map: Suspiciously high volume of activity is seen in Ukraine. Specifically the cities of Kiev and Kharkiv, with counts of 439 and 432 respectively.
- Dashboard Analysis for URI Data: The URI hit the most was /VSI_Account_logon.php

Screenshots of Attack Logs

HTTP Method Line Chart
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





Summary and Future Mitigations

- Implement a WAF to securely monitor traffic and report malicious activity
- Review the public information that is accessible online and revise/remove any sensitive data
- Block traffic originating from foreign IP addresses

Thank You!