Defensive Security Project

by: Jacob Graber, Keaton Myers, Maia Johnson, Luke Kernan, Collin Lerchie, & Janice Mitchell

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Virtual Space Industries (VSI) warned about potential attacks
- Analysts tasked with using Splunk to monitor for attacks
- Baselined normal activity
- Created reports, alerts, dashboards
- Were victims of a cyberattack
- Received logs covering relevant time period
- Analyzed the logs to determine what was attacked

PCAP Analyzer for Splunk

PCAP Analyzer for Splunk

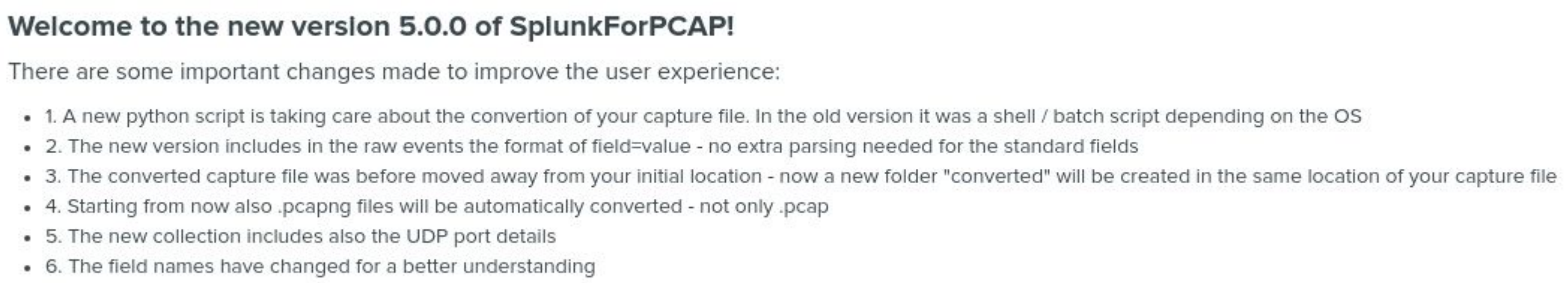
Splunk for PCAP Add-On

- Packet losses
- HTTP method request
- Unsuccessful handshakes
- Helps analyze network performance
- Analyzes network traffic
- Adds layer of IDS

PCAP Analyzer for Splunk

- Will detect cause of error for unsuccessful handshakes
- Will show PCAP data and correlation
- Provide accurate description of:
    - captured packets
    - # of retransmissions
    - % of packet loss

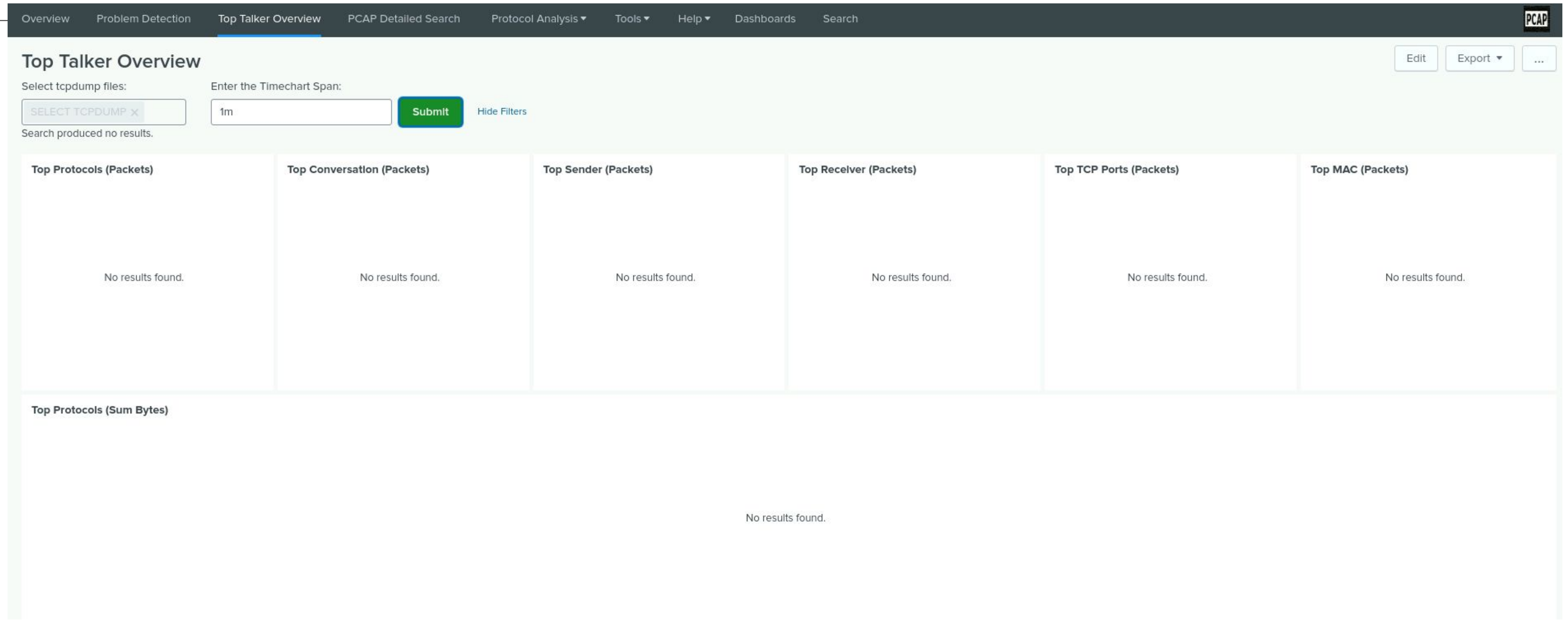
PCAP Analyzer for Splunk



Welcome to the new version 5.0.0 of SplunkForPCAP!

There are some important changes made to improve the user experience:

- 1. A new python script is taking care about the convertion of your capture file. In the old version it was a shell / batch script depending on the OS
- 2. The new version includes in the raw events the format of field=value - no extra parsing needed for the standard fields
- 3. The converted capture file was before moved away from your initial location - now a new folder "converted" will be created in the same location of your capture file
- 4. Starting from now also .pcapng files will be automatically converted - not only .pcap
- 5. The new collection includes also the UDP port details
- 6. The field names have changed for a better understanding



Top Talker Overview

Select tcpdump files: SELECT TCPDUMP ×

Search produced no results.

Enter the Timechart Span: 1m

Top Protocols (Packets): No results found.

Top Conversation (Packets): No results found.

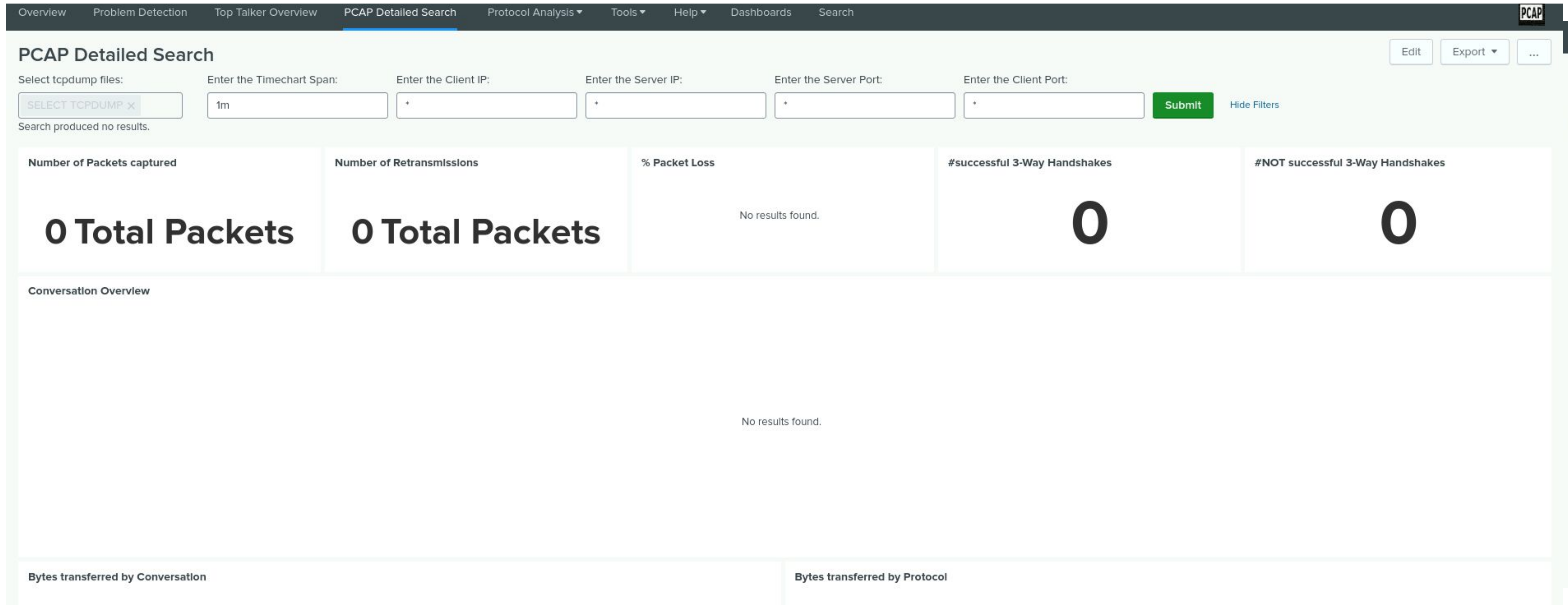
Top Sender (Packets): No results found.

Top Receiver (Packets): No results found.

Top TCP Ports (Packets): No results found.

Top MAC (Packets): No results found.

Top Protocols (Sum Bytes): No results found.



PCAP Detailed Search

Select tcpdump files: SELECT TCPDUMP ×

Search produced no results.

Enter the Timechart Span: 1m

Enter the Client IP: *

Enter the Server IP: *

Enter the Server Port: *

Enter the Client Port: *

Number of Packets captured: 0 Total Packets

Number of Retransmissions: 0 Total Packets

% Packet Loss: No results found.

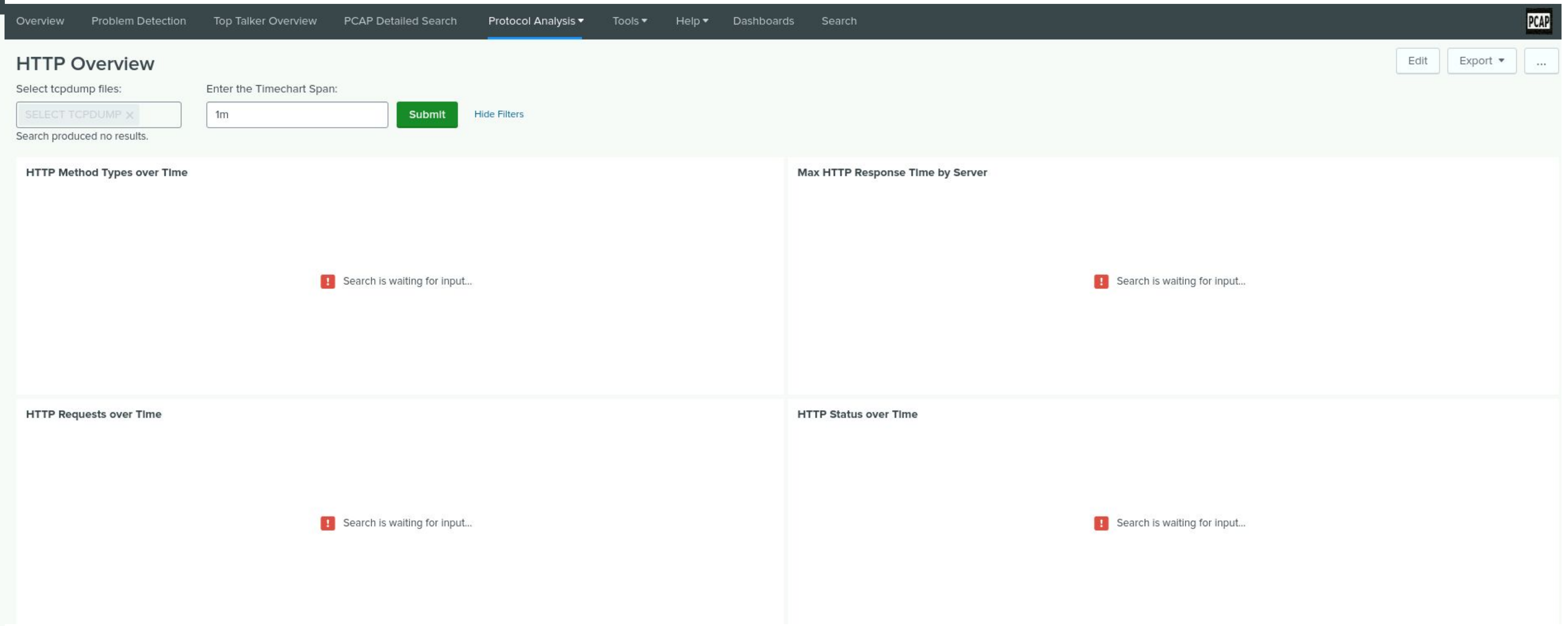
#successful 3-Way Handshakes: 0

#NOT successful 3-Way Handshakes: 0

Conversation Overview: No results found.

Bytes transferred by Conversation

Bytes transferred by Protocol



HTTP Overview

Select tcpdump files: SELECT TCPDUMP ×

Search produced no results.

Enter the Timechart Span: 1m

HTTP Method Types over Time: ! Search is waiting for input...

Max HTTP Response Time by Server: ! Search is waiting for input...

HTTP Requests over Time: ! Search is waiting for input...

HTTP Status over Time: ! Search is waiting for input...

Logs Analyzed

1 Windows Logs

These server logs showed security events from Windows event logs that occurred during normal business operations

2 Apache Logs

These server logs are from the server for VSI’s public-facing website and shows the different types of HTTP activity during normal business operations

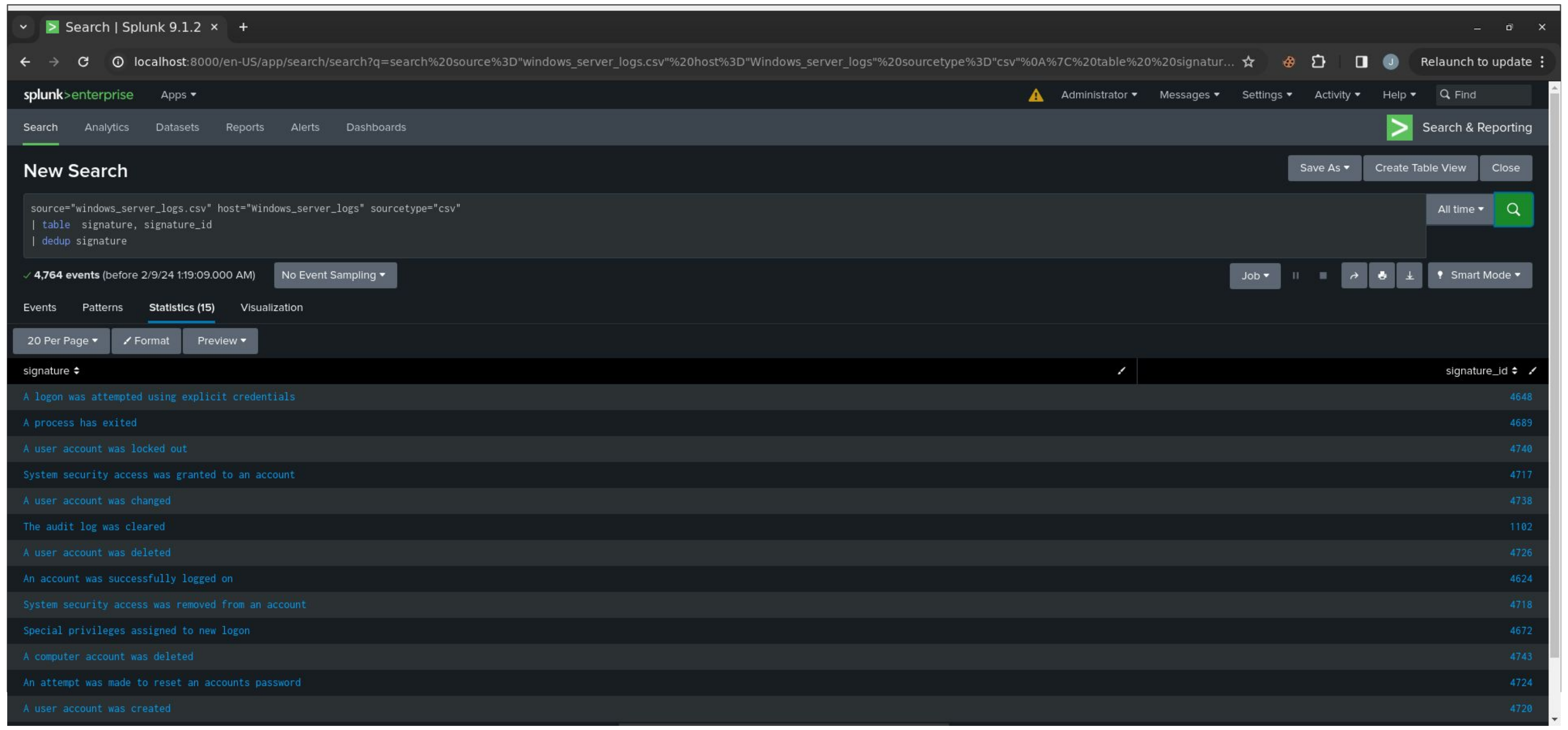
Windows Logs

Reports—Windows

Designed the following reports:

Report Name	**Report Description**
Signatures and Associated IDs	Shows a table of all signatures and their corresponding ID number for Windows activity
Severity Levels	Shows the count and percentage of the severity levels associated with activity attempts in the Windows baseline log
Attempt Status	Shows the count and percentage of successful and failed activity attempt in the Windows baseline log

Images of Reports—Windows

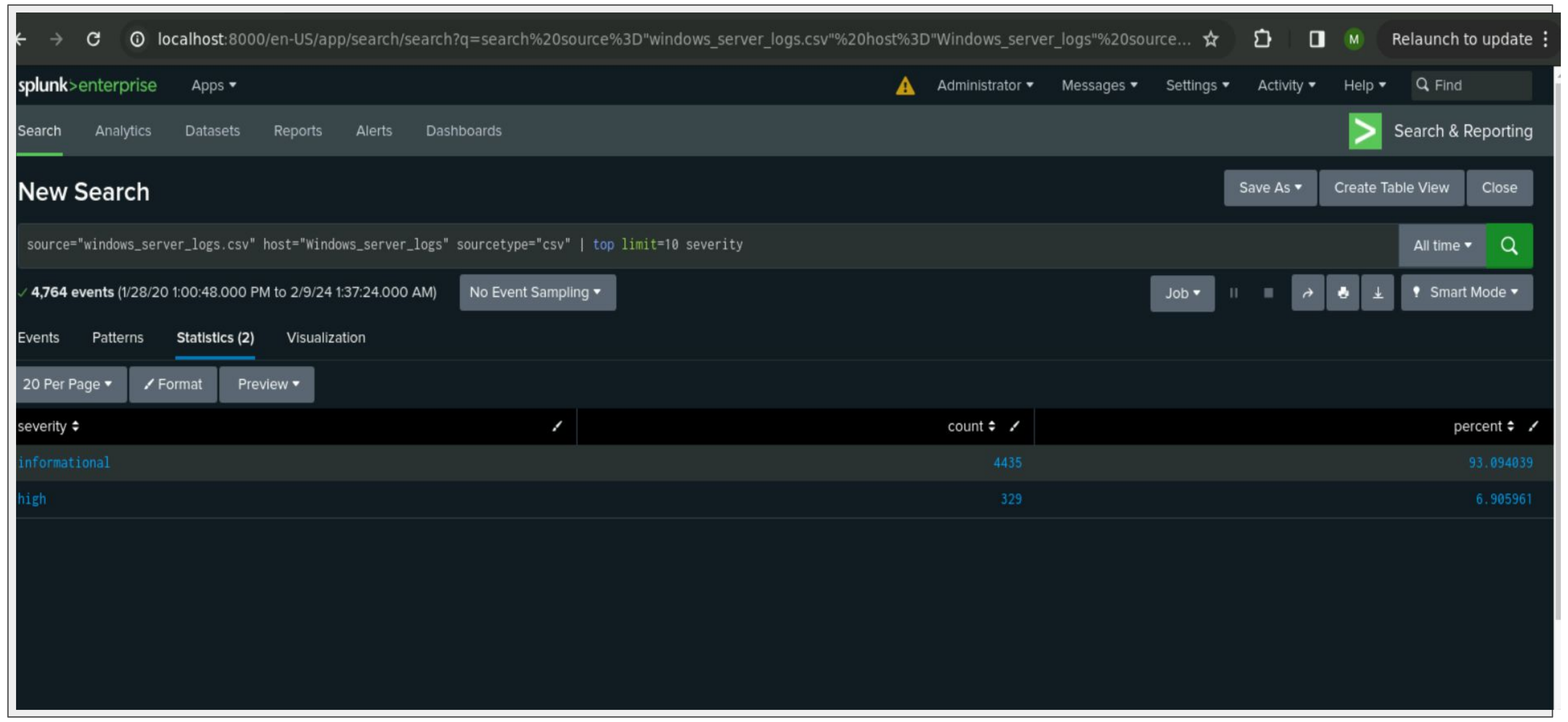


New Search

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

✓ 4,764 events (before 2/9/24 1:19:09.000 AM)

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

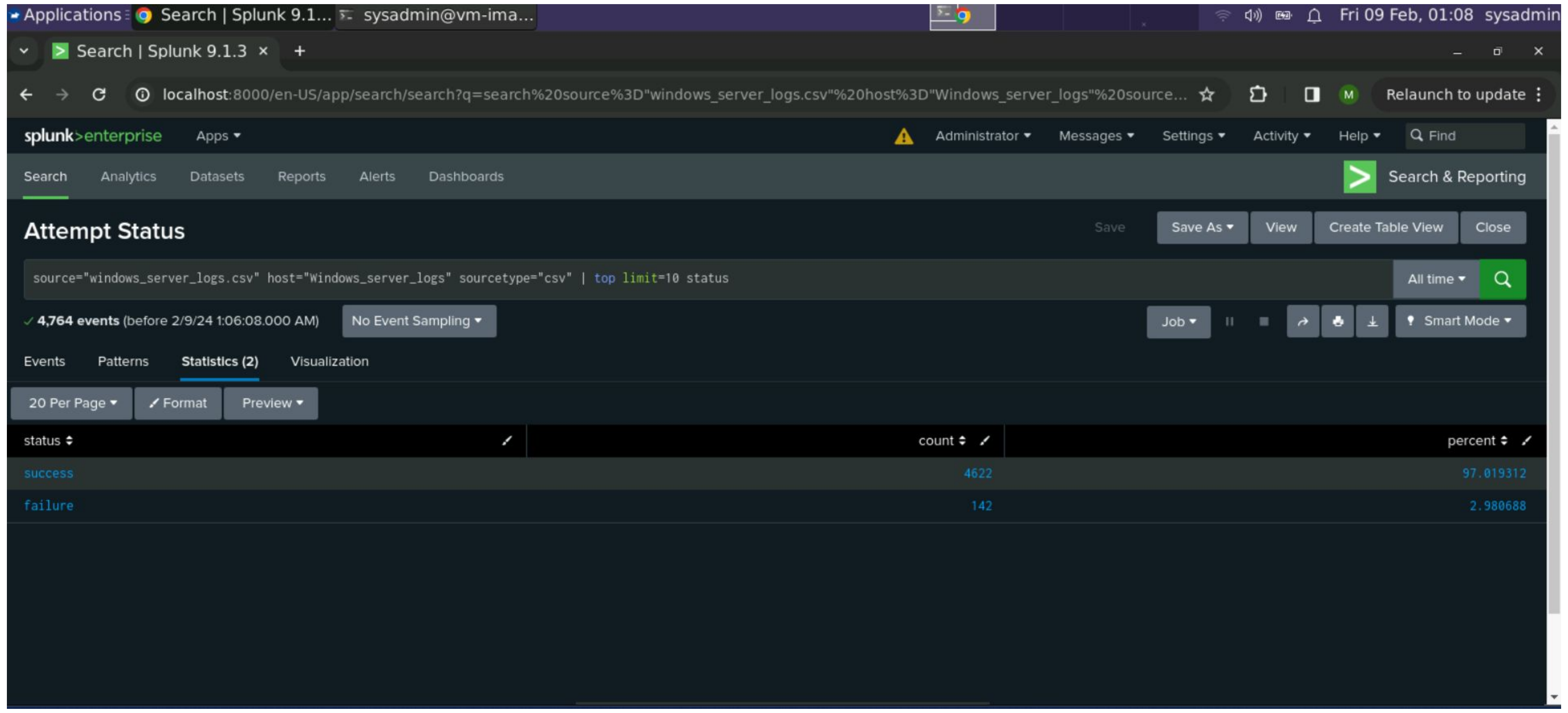


New Search

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | top limit=10 severity
```

✓ 4,764 events (1/28/20 1:00:48.000 PM to 2/9/24 1:37:24.000 AM)

severity	count	percent
informational	4435	93.094039
high	329	6.905961



Attempt Status

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | top limit=10 status
```

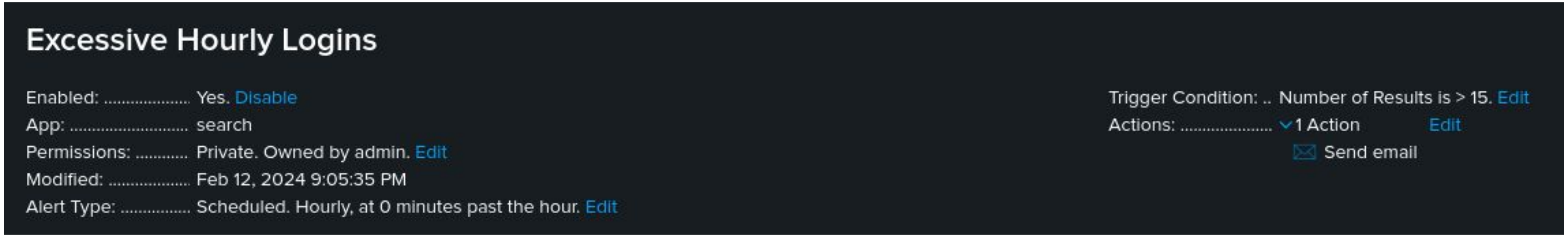
✓ 4,764 events (before 2/9/24 1:06:08.000 AM)

status	count	percent
success	4622	97.019312
failure	142	2.980688

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Hourly Logins	In a given hour, if the number of logins exceeds x, an email alert will generate.	323 successful logins over 24 hours	>25



Excessive Hourly Logins

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 12, 2024 9:05:35 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

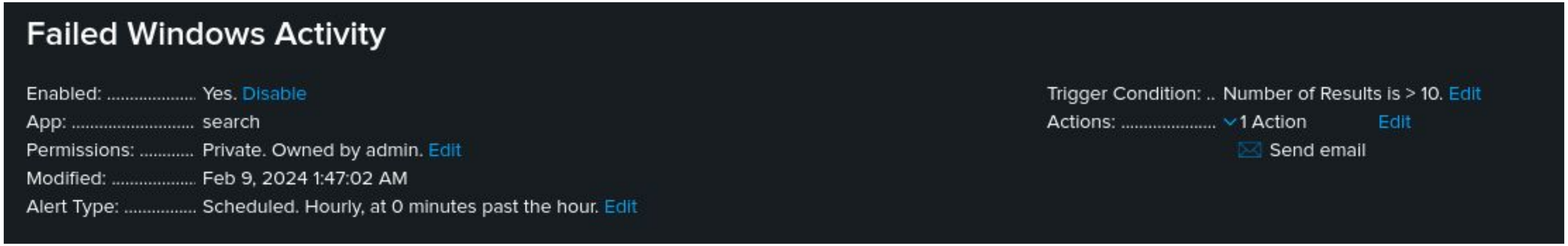
Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

JUSTIFICATION: The typical data included a range of 8-21 in any given hour, with the average being 13.5 per hour. In order to prevent too many false positives, the threshold is set for failures in excess of 25 per hour to generate the alert and email.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	In a given hour, if the number of failures exceeds 10, an email alert will generate.	142 Failures over 24 hours	>10



Failed Windows Activity

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 9, 2024 1:47:02 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

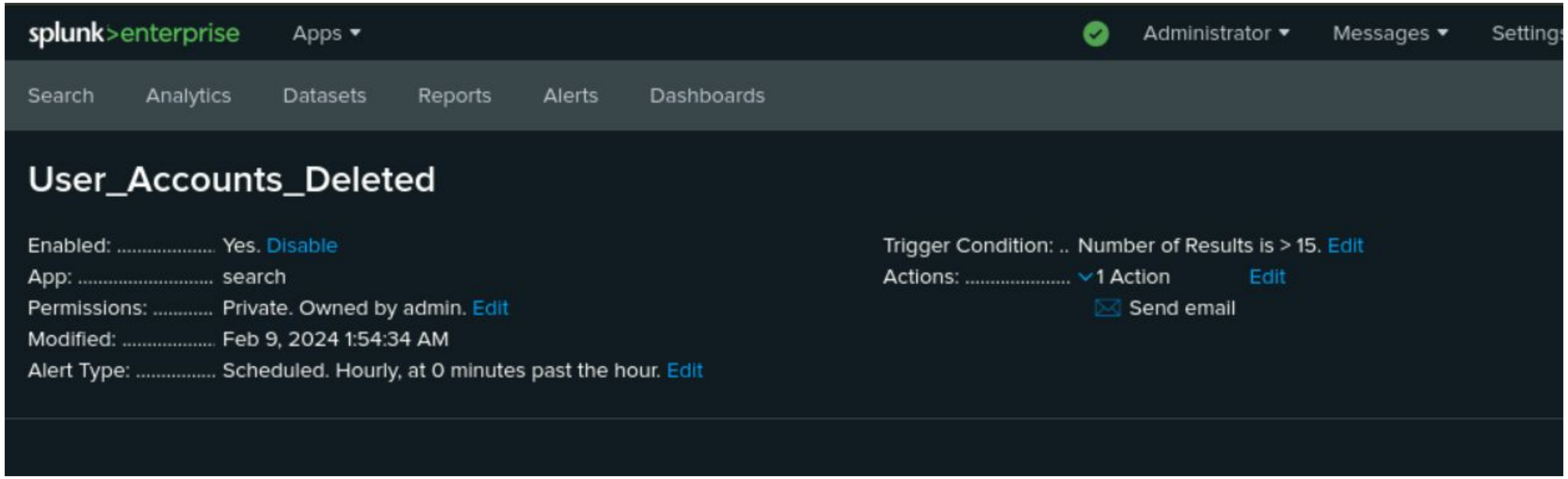
Trigger Condition: .. Number of Results is > 10. Edit
Actions: .... 1 Action Edit
Send email

JUSTIFICATION: The typical data included a range of 2-10 in any given hour, with the average being 5.9 per hour. In order to prevent too many false positives, the threshold is set for failures in excess of 10 per hour to generate the alert and email.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User_Accounts_Deleted	Alert triggers once the threshold of user accounts has been deleted	10 per hour	15 per hour



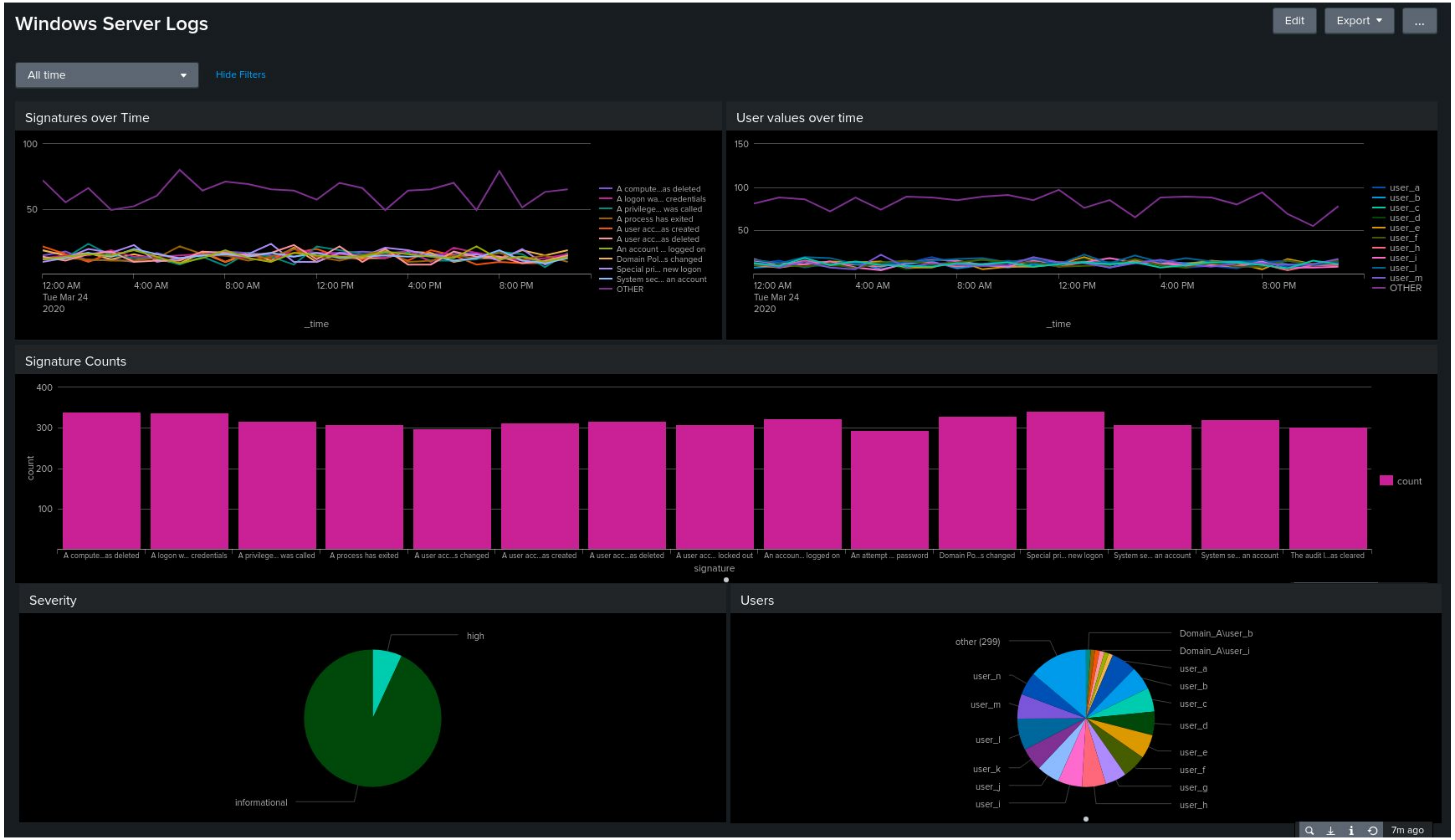
User_Accounts_Deleted

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 9, 2024 1:54:34 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

Justification- The average account deletion per hour sat around 10 while only on occasion topping 15.

Dashboards—Windows



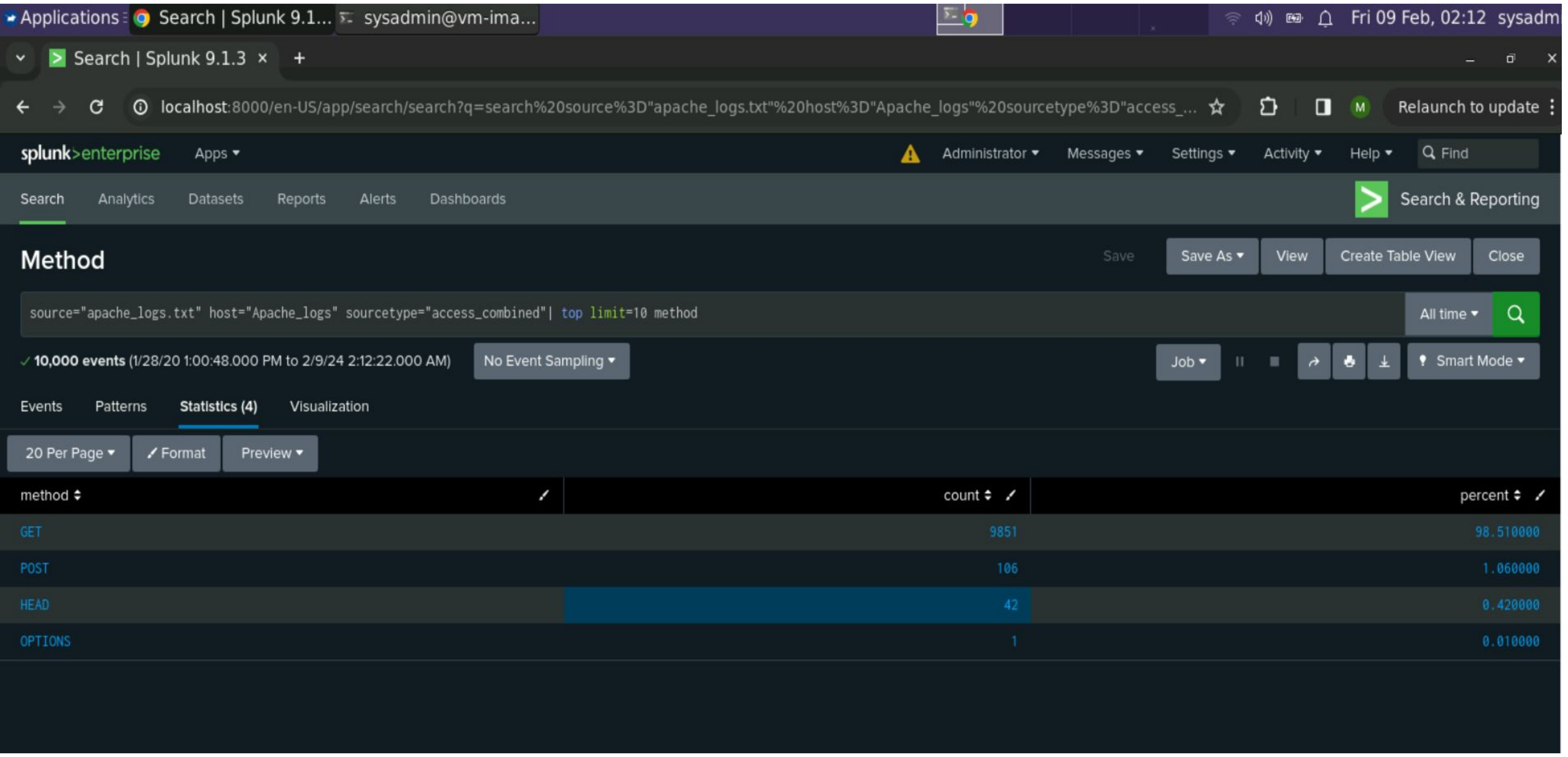
Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Method	Lists the HTTP methods used in requests
Referrer Domains	Shows the top 10 domains that refer to VSI’s website
HTTP Response Codes	Shows a list of all the HTTP response codes with their count and percentage

Images of Reports—Apache

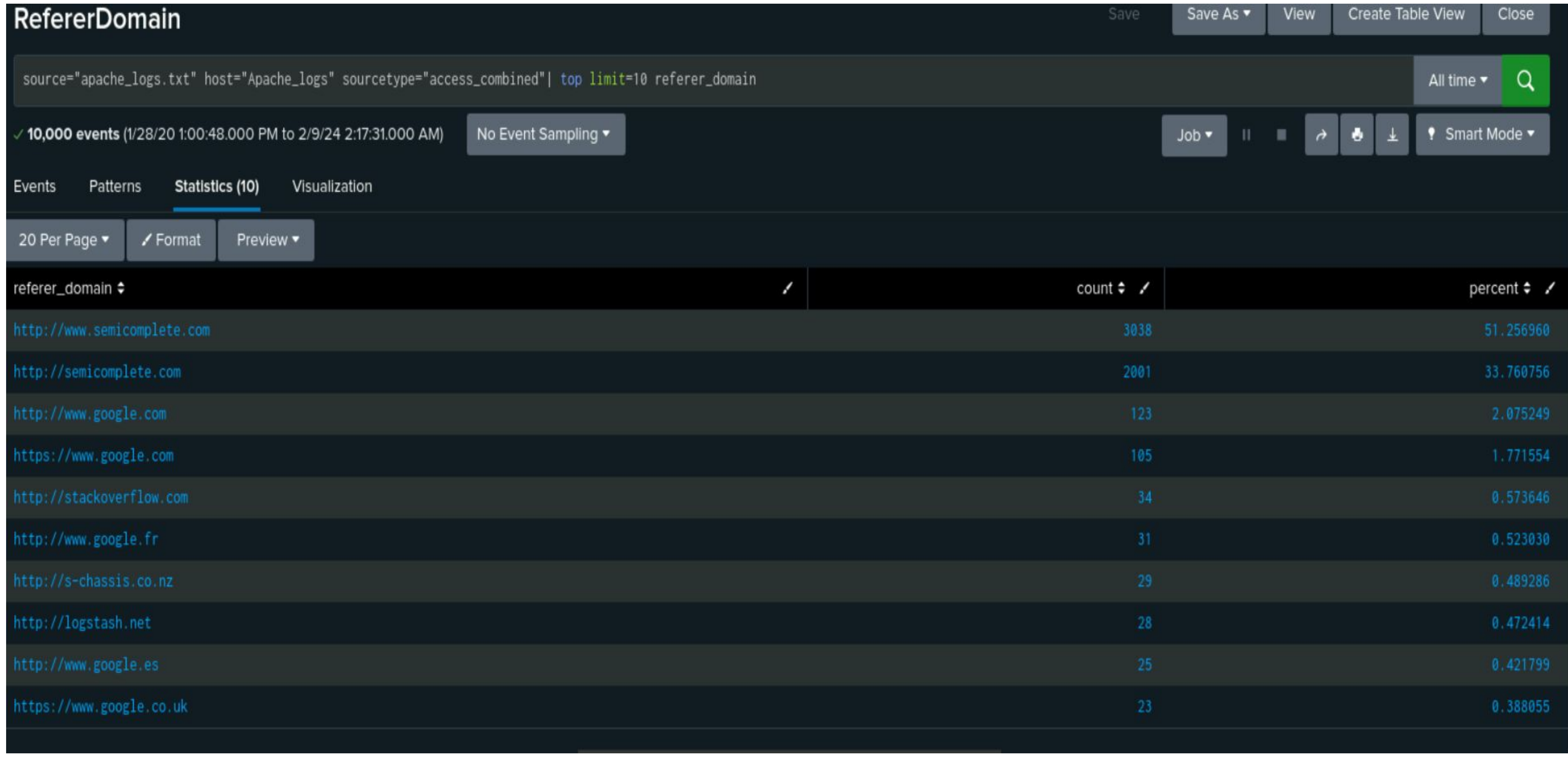


Method

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 method
```

✓ **10,000 events** (1/28/20 1:00:48.000 PM to 2/9/24 2:12:22.000 AM)

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

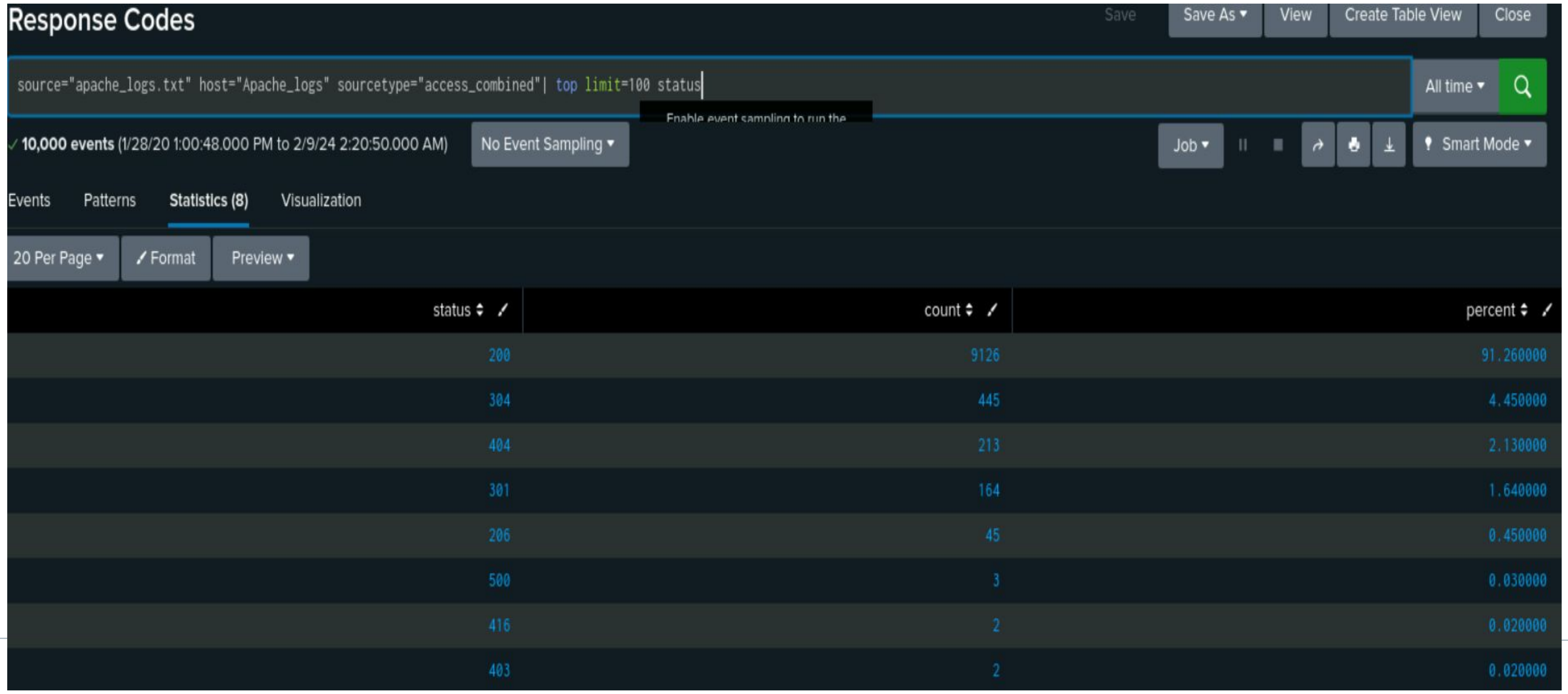


RefererDomain

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ **10,000 events** (1/28/20 1:00:48.000 PM to 2/9/24 2:17:31.000 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



Response Codes

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=100 status
```

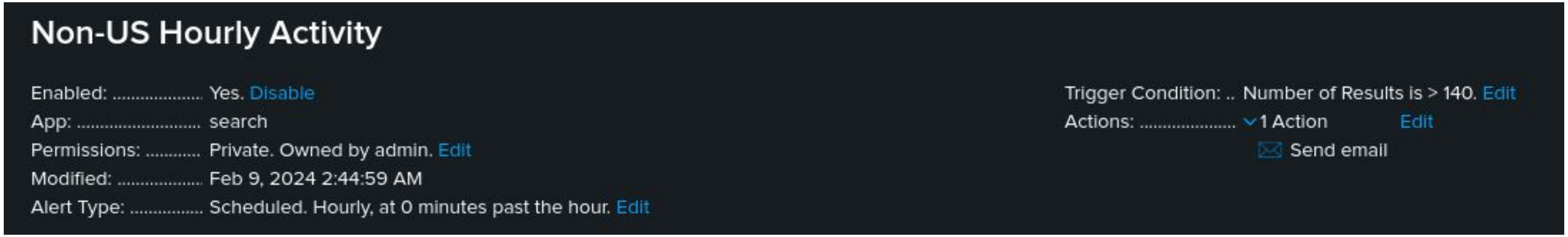
✓ **10,000 events** (1/28/20 1:00:48.000 PM to 2/9/24 2:20:50.000 AM)

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
403	2	0.020000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Hourly Activity	Triggers alert when Non-US activity exceeds the threshold.	10,000 over 3.5 days	>140



Non-US Hourly Activity

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 9, 2024 2:44:59 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

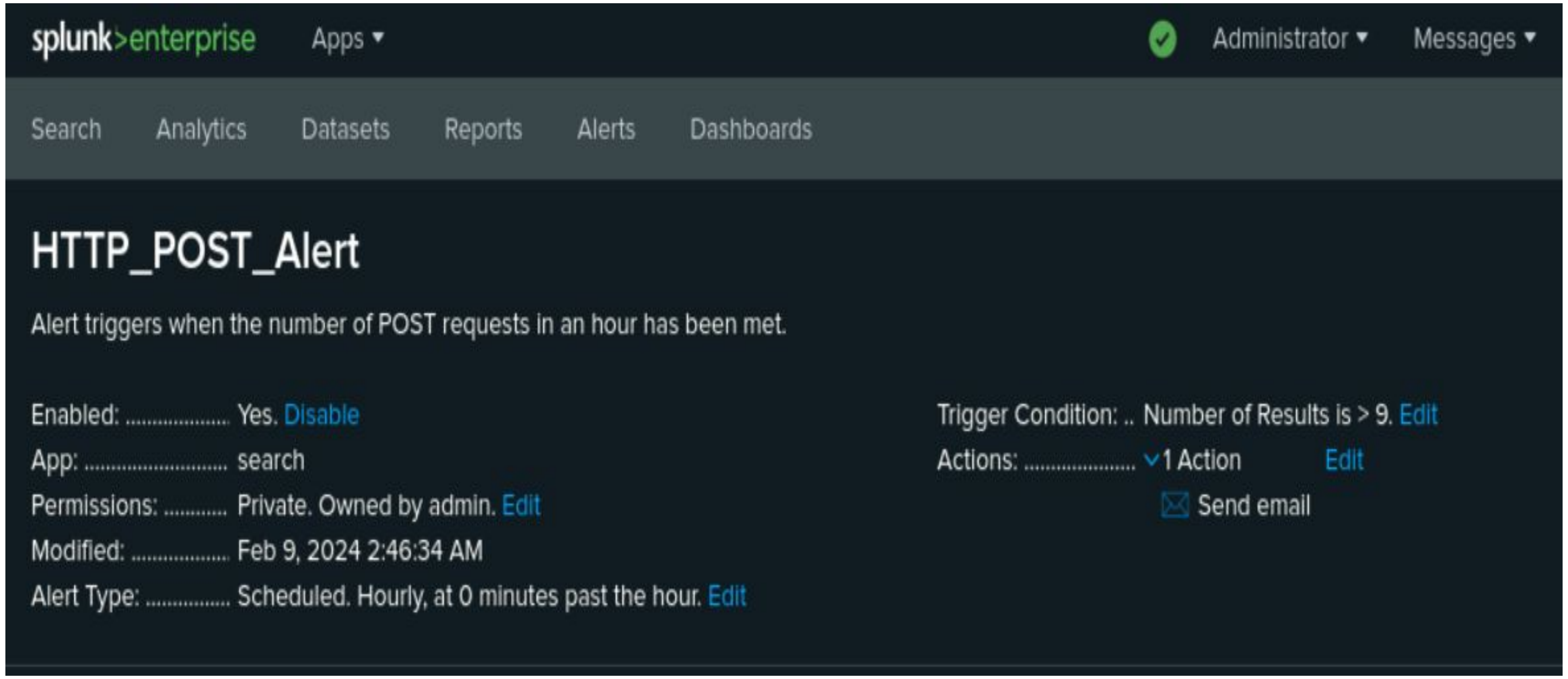
Trigger Condition: .. Number of Results is > 140. Edit
Actions: .... 1 Action Edit
Send email

JUSTIFICATION: The typical data included a range of 74-136 in any given hour, with the average being 122 per hour. In order to prevent too many false positives, the threshold is set for failures in excess of 140 per hour to generate the alert and email.

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP_POST_Alert	Triggers alert when the threshold of HTTP POST request is hit.	3 POST requests per hour	Over 9 POST requests per hour



HTTP_POST_Alert

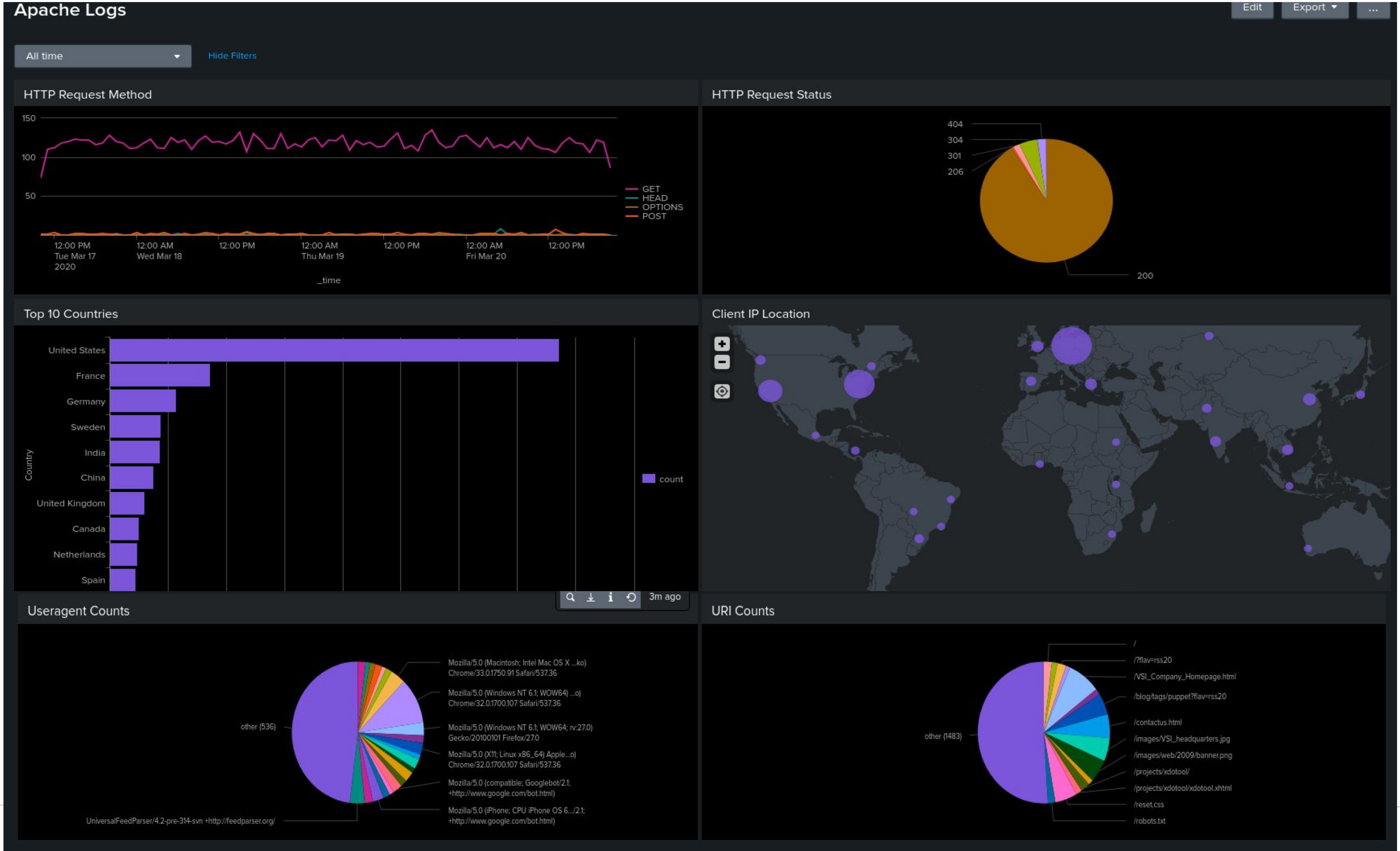
Alert triggers when the number of POST requests in an hour has been met.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Feb 9, 2024 2:46:34 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 9. Edit
Actions: .... 1 Action Edit
Send email

JUSTIFICATION: 9 POST requests per hour would signify a tripling in the average request's, this would require further investigation as a false positive would be unlikely.

Dashboards—Apache

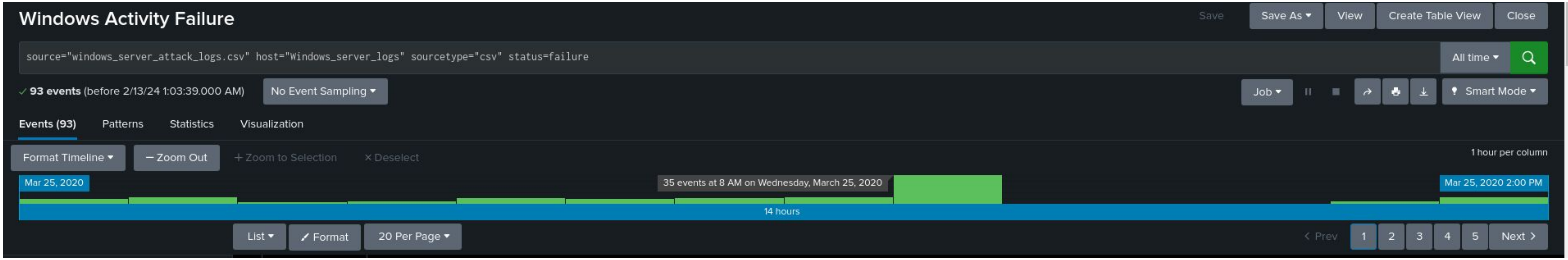

Apache Logs
Edit
Export ▾
...
All time ▾
Hide Filters
HTTP Request Method
150
100
50
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 PM
12:00 AM Thu Mar 19
12:00 PM
12:00 AM Fri Mar 20
12:00 PM
_time
GET
HEAD
OPTIONS
POST
HTTP Request Status
404
304
301
206
200
Top 10 Countries
Country
United States
France
Germany
Sweden
India
China
United Kingdom
Canada
Netherlands
Spain
count
3m ago
Client IP Location
Useragent Counts
other (536)
Mozilla/5.0 (Macintosh; Intel Mac OS X ...ko) Chrome/33.0.1750.91 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) ...o) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
Mozilla/5.0 (X11; Linux x86_64) Apple...o) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mozilla/5.0 (iPhone; CPU iPhone OS 6.../2.1; +http://www.google.com/bot.html)
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
URI Counts
other (1483)
/
/?flav=rss20
/VSI_Company_Homepage.html
/blog/tags/puppet?flav=rss20
/contactus.html
/images/VSI_headquarters.jpg
/images/web/2009/banner.png
/projects/xdotool/
/projects/xdotool/xdotool.xhtml
/reset.css
/robots.txt

Attack Analysis

Attack Summary—Windows

Report findings when analyzing the attack logs:

- On Wednesday, March 25, 2020 at 9 AM there was a large volume of Windows activity failure.



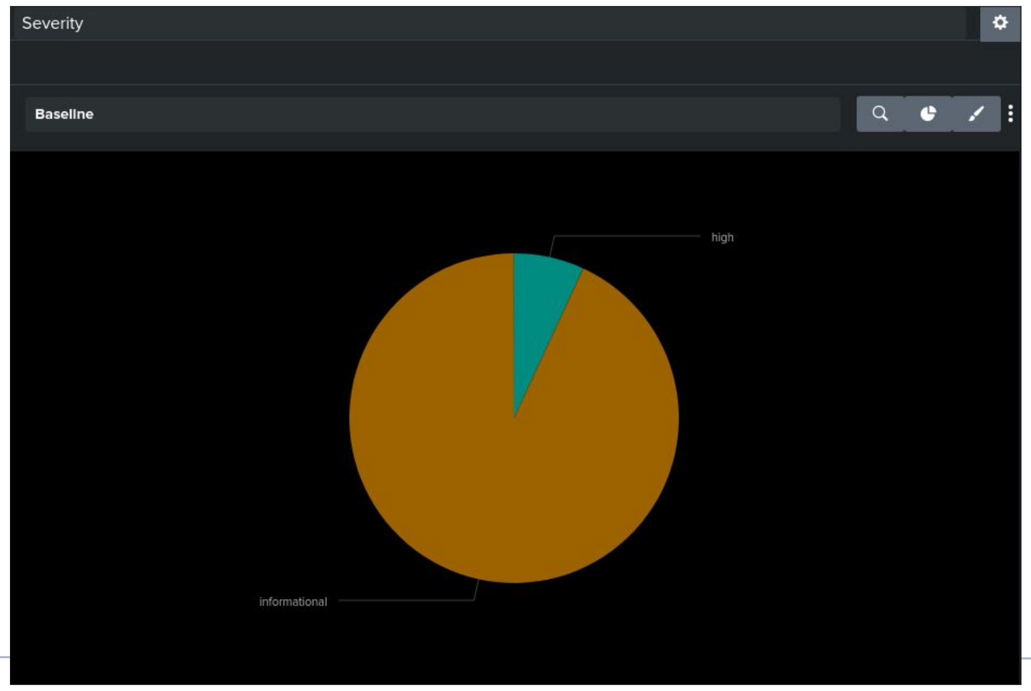
Windows Activity Failure

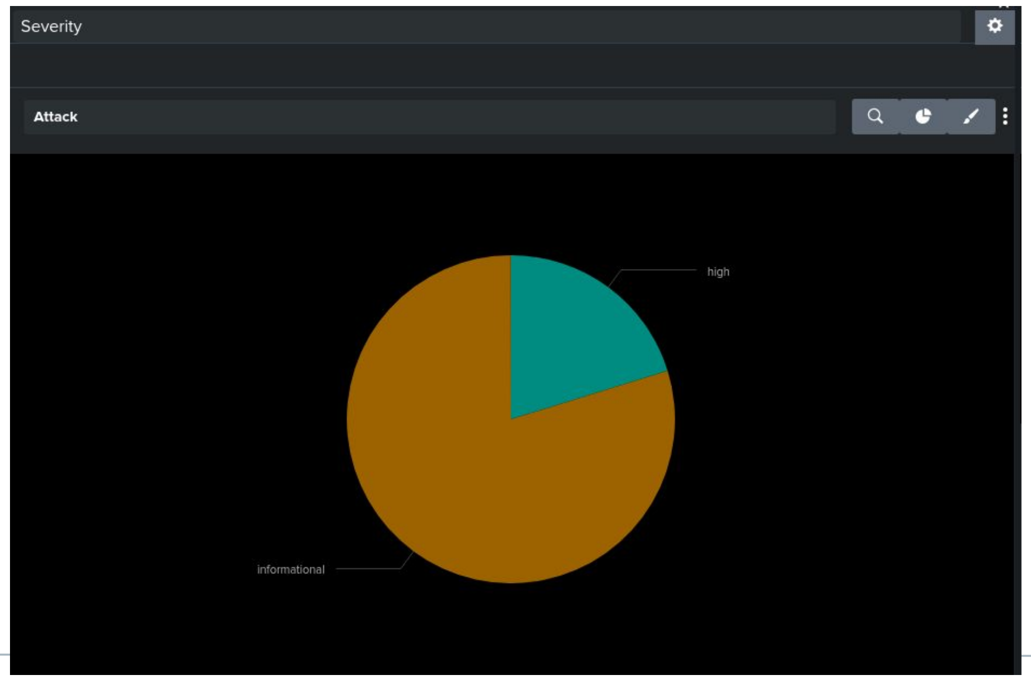
```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" status=failure
```

✓ 93 events (before 2/13/24 1:03:39.000 AM)

35 events at 8 AM on Wednesday, March 25, 2020

- Severity anomalies (high versus informational)
    - Variance suggests suspicious volume of high severity.

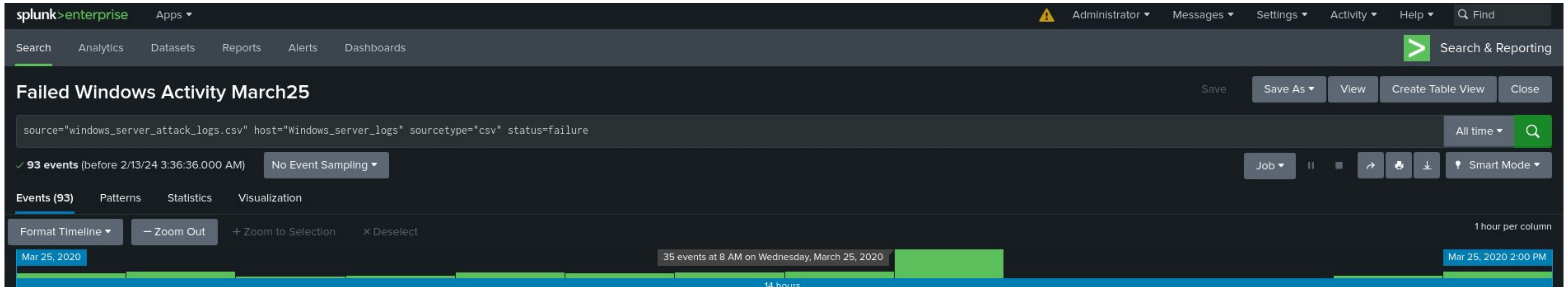




Attack Summary—Windows

Alert findings when analyzing the attack logs:

- Suspicious increase in activity failures



Failed Windows Activity March25

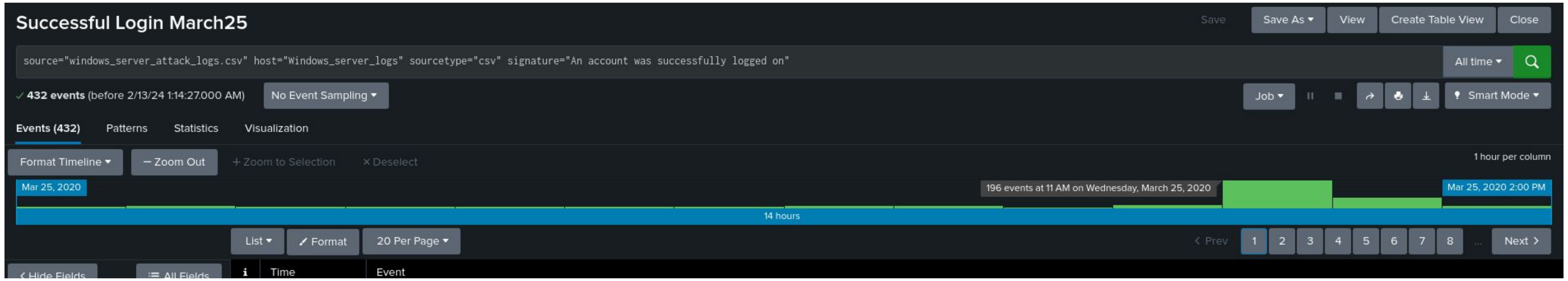
```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" status=failure
```

✓ **93 events** (before 2/13/24 3:36:36.000 AM)

Events (93)

35 events at 8 AM on Wednesday, March 25, 2020

- Suspicious increase in successful logins
  - User_j



Successful Login March25

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv" signature="An account was successfully logged on"
```

✓ **432 events** (before 2/13/24 1:14:27.000 AM)

Events (432)

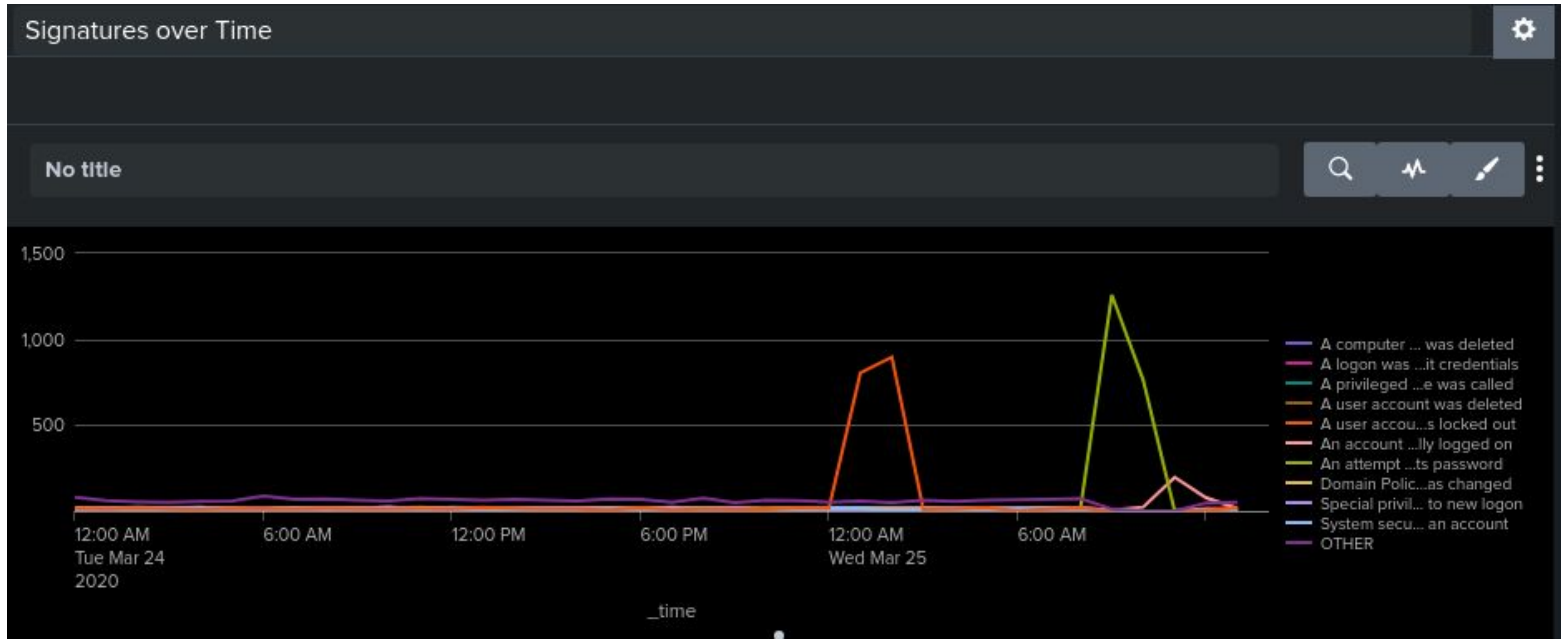
196 events at 11 AM on Wednesday, March 25, 2020

- No concerning activity for deleted accounts

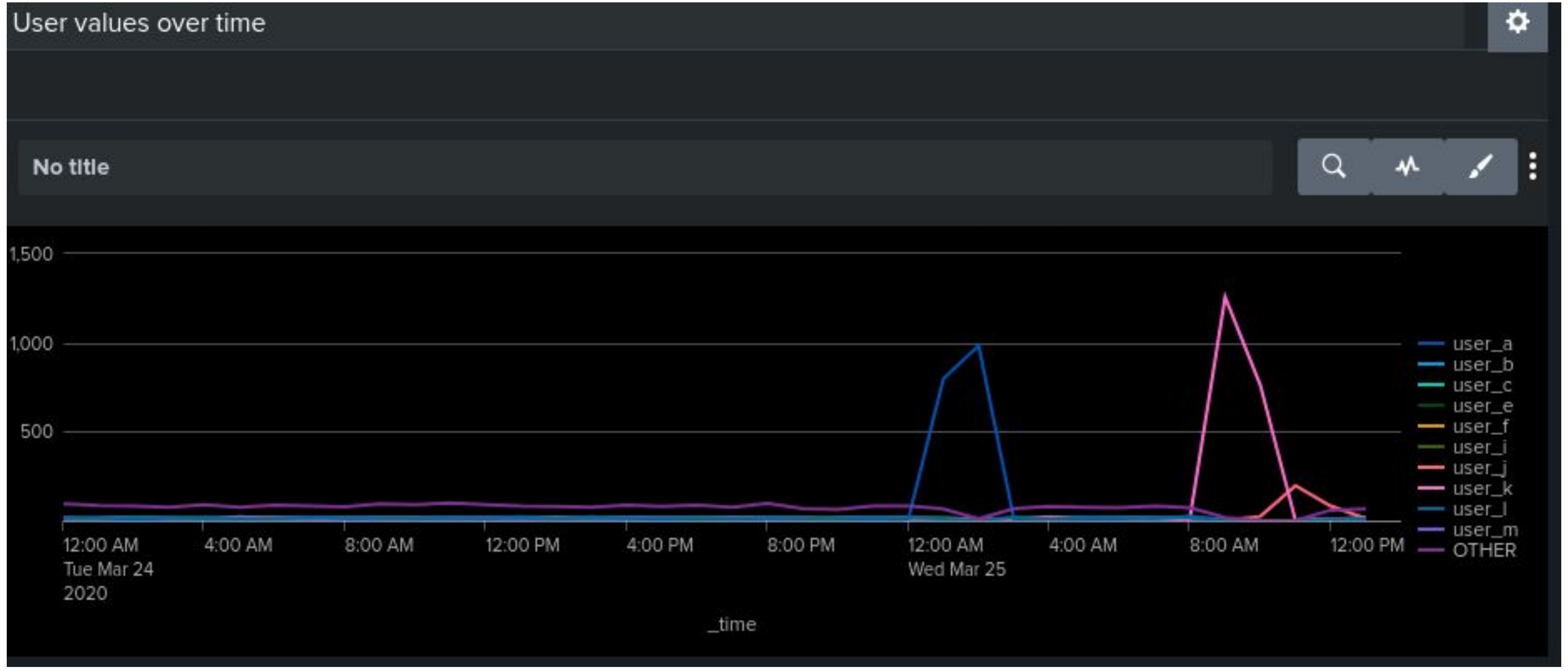
Attack Summary—Windows

Dashboard findings when analyzing the attack logs:

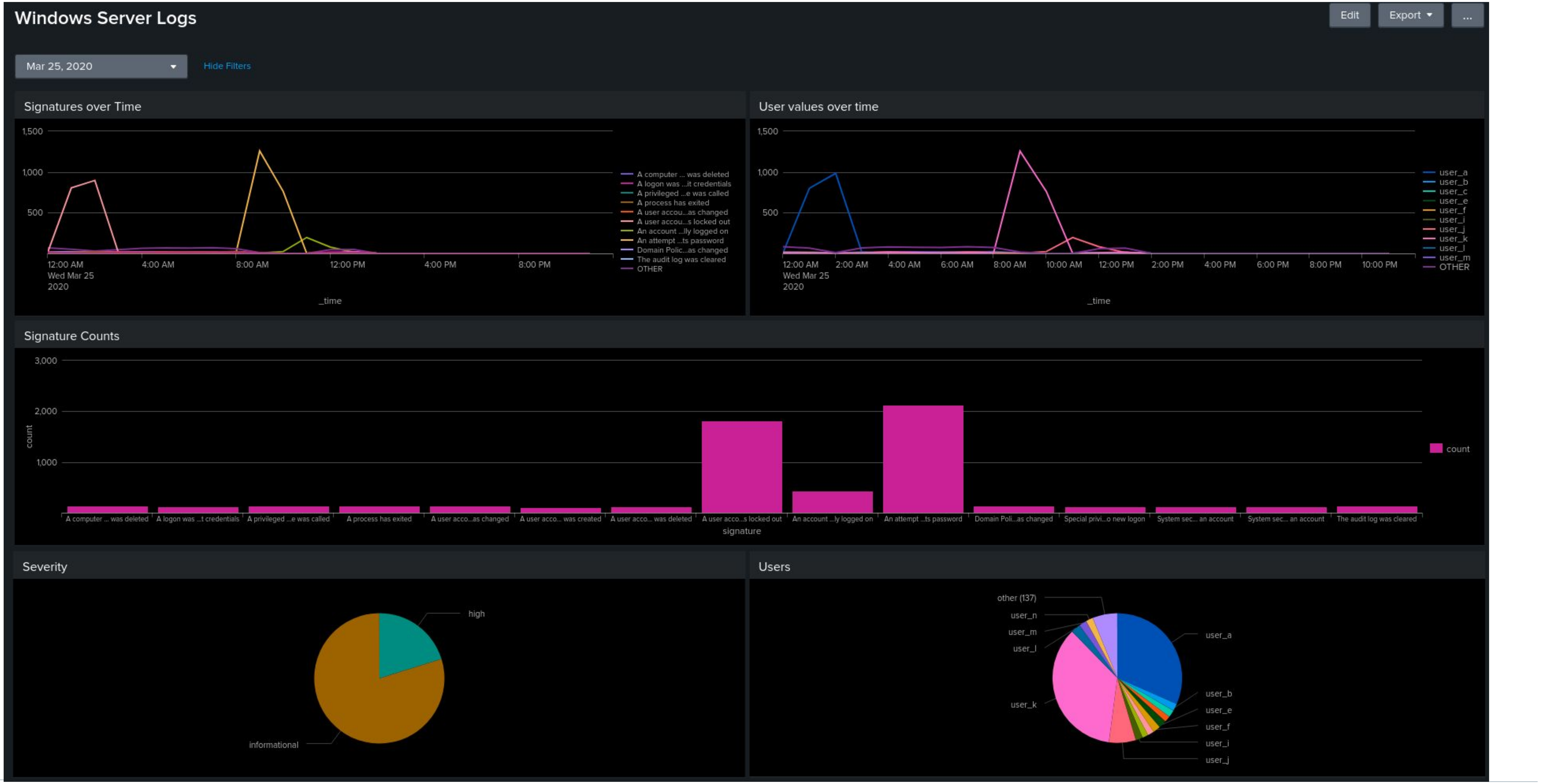
- Excessive signature counts
  - Account lockouts
  - Password reset requests



- Excessive activity by specific users for the same time periods.
  - User a
  - User k



Windows Dashboard for Date of Attack



Windows Server Logs

Mar 25, 2020

Signatures over Time

User values over time

Signature Counts

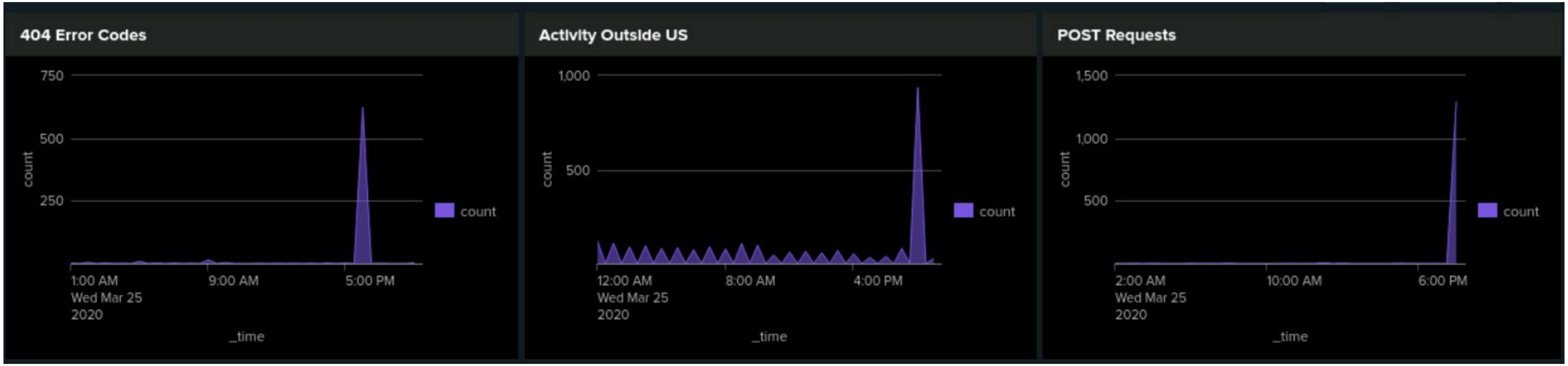
Severity

Users

Attack Summary—Apache

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

- A significant increase in POST request methods occurred during 8PM
- Traffic increase originating from countries other than the US coincided with the increase in POST requests
- Spike in 404 status error codes was also identified to have occurred during the same time range



Attack Summary—Apache

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

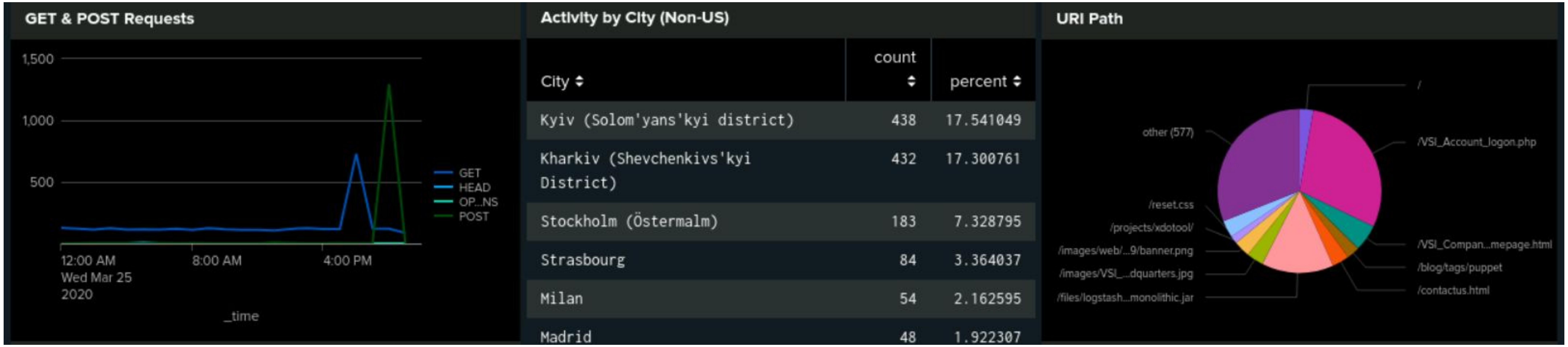
- The increase in POST request occurring during 8PM would surpass the threshold of more than 9 request within an hour causing our alert to trigger.
- The increase of traffic originating from outside of the US would also surpass the set threshold of 140 events within an hour causing the alert to trigger while also avoiding false positives.

Attack Summary—Apache

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

- Significant increase in GET & POST requests
- Activity originating from outside the US increasing

  -Kiev and Kharkiv were the top two results making up 34% of activity
- Suspicious volume of of the /VSI_Account_logon.php URI Path

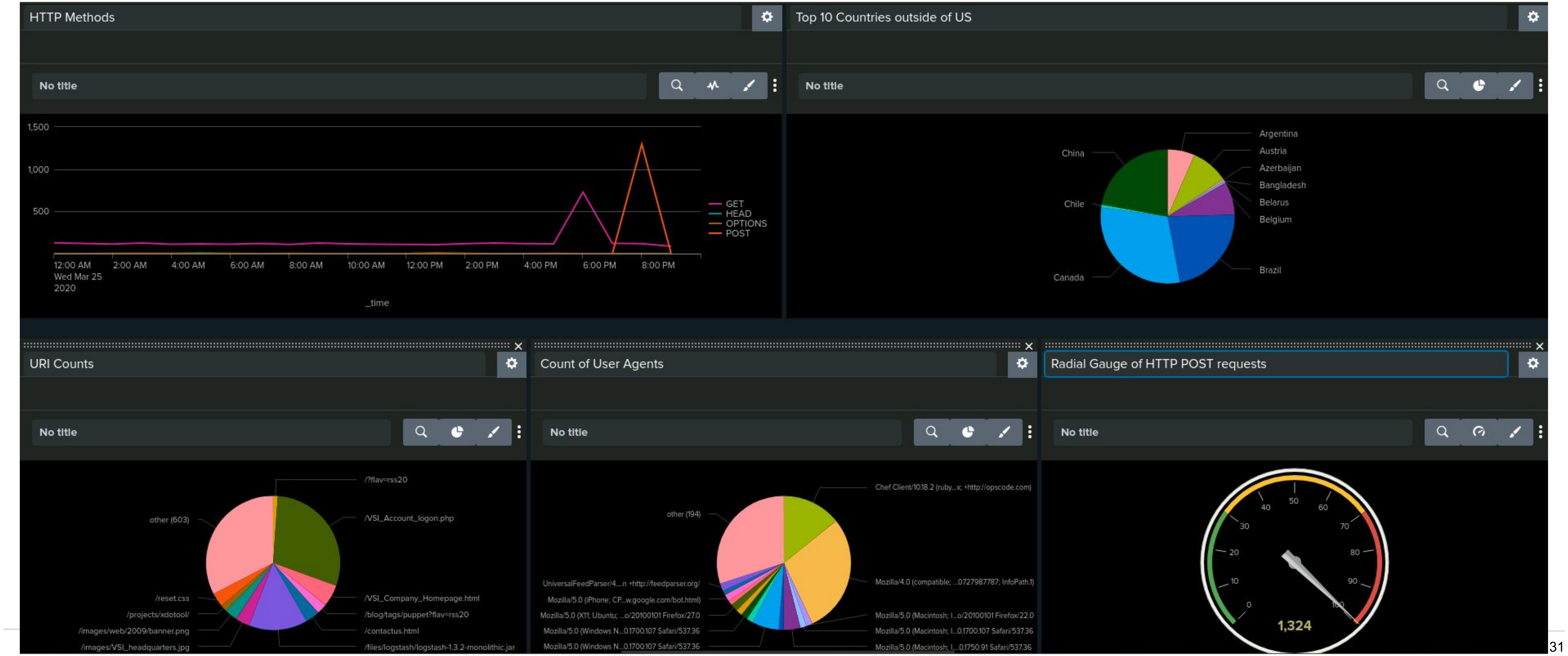


Activity by City (Non-US)

City ⬍	count ⬍	percent ⬍
Kyiv (Solom'yans'kyi district)	438	17.541049
Kharkiv (Shevchenkivs'kyi District)	432	17.300761
Stockholm (Östermalm)	183	7.328795
Strasbourg	84	3.364037
Milan	54	2.162595
Madrid	48	1.922307

Screenshots of Attack Logs

Dashboard analysis for Apache attack logs


HTTP Methods
No title
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
Top 10 Countries outside of US
No title
Argentina
Austria
Azerbaijan
Bangladesh
Belarus
Belgium
Brazil
China
Chile
Canada
URI Counts
No title
/?flav=rss20
/VSI_Account_logon.php
other (603)
/reset.css
/projects/xdotool/
/images/web/2009/banner.png
/images/VSI_headquarters.jpg
/VSI_Company_Homepage.html
/blog/tags/puppet?flav=rss20
/contactus.html
/files/logstash/logstash-1.3.2-monolithic.jar
Count of User Agents
No title
Chef Client/10.18.2 (ruby...x; +http://opscode.com)
other (194)
UniversalFeedParser/4....n +http://feedparser.org/
Mozilla/5.0 (iPhone; CP...w.google.com/bot.html)
Mozilla/5.0 (X11; Ubuntu; ...o/20100101 Firefox/27.0
Mozilla/5.0 (Windows N...0.1700.107 Safari/537.36
Mozilla/5.0 (Windows N...0.1700.107 Safari/537.36
Mozilla/4.0 (compatible; ...0727987787; InfoPath.1)
Mozilla/5.0 (Macintosh; I...o/20100101 Firefox/22.0
Mozilla/5.0 (Macintosh; I...0.1700.107 Safari/537.36
Mozilla/5.0 (Macintosh; I....0.1750.91 Safari/537.36
Radial Gauge of HTTP POST requests
No title
0
10
20
30
40
50
60
70
80
90
100
1,324

Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
  - VSI experiences multiple attacks March 25th
  - Brute force attacks
  - Ukraine IP addresses
- To protect VSI from future attacks, what future mitigations would you recommend?
  - Lockout Policies
  - Multi-factor authentication
  - Firewalls restricting IP addresses from certain locations