VSI Defensive Analysis - Project 3
By: Olivia, TK, Tyler, Dalton, Alex, & Johnny

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- We were to play the role of an SOC analyst at a small company called Virtual Space industries(VSI), which designs virtual-reality programs for businesses
- VSI has heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business
- Acting as SOC analysis, we were takes with using Splunk to monitor against potential attacks on VSI systems and applications

We were tasked with Monitoring these VSI Products:

1. Administrative webpage - which hosts the administrative webpage
2. Apache Web Server - runs many of VSIs's back-end operations

Whois XML IP Geolocation API

Whois XML IP Geolocation API Summary

The Whois XML IP Geolocation API add-on for Splunk adds additional information from IP addresses in scan results and summarizes it in a concise manner. Some of the additional information that can be gathered from IP addresses using Whois includes:

- Detailed IP geographical data, including the ZIP code, city, region, ISO 3166 two-letter country code, and country.
- The precise latitude and longitude coordinates of IP addresses of interest.
- Time zone of the IP address' location in UTC Format.
- Discover which Internet service provider (ISP) a particular IP address is using.
- Find out what kind of network connection the IP address uses, such as cable, DSL, etc.
- Connected domain names associated with the IP address.
- Determine IP addresses' connection types (modem, mobile, broadband, or company).

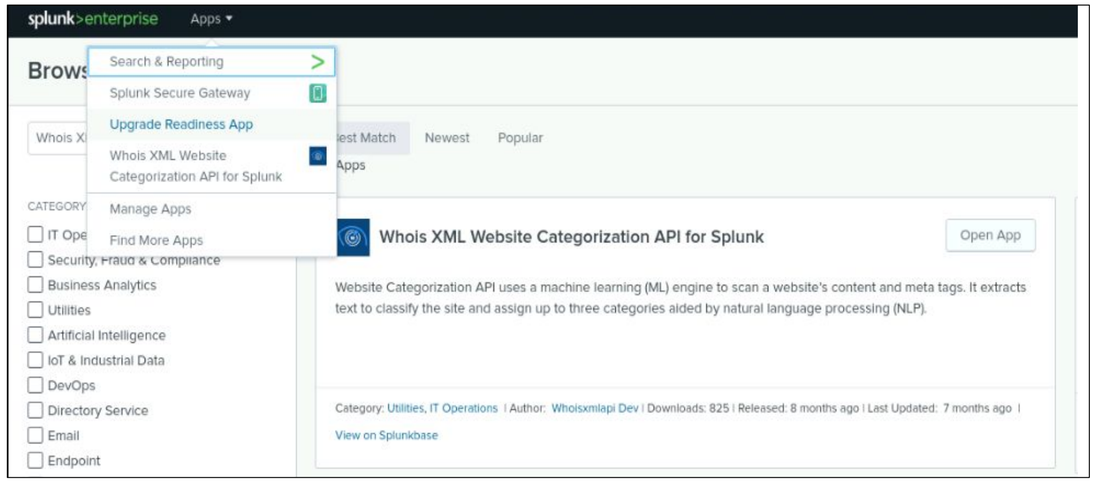
Whois XML IP Geolocation API Use Cases

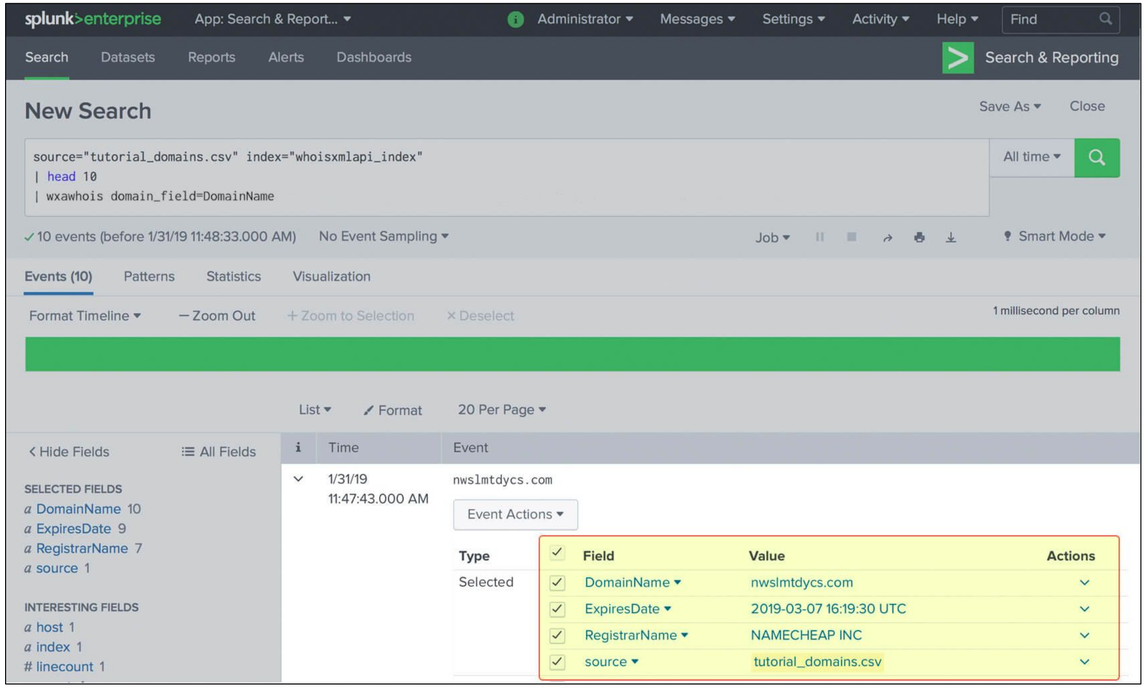
The XML IP Geolocation API would be particularly useful in situations where there is a a lot of international web traffic for an application being logged in Splunk. Being able to easily determine geolocation would be valuable for visualizing patterns of network traffic or origins of a cyber attack. Some other use cases would be:

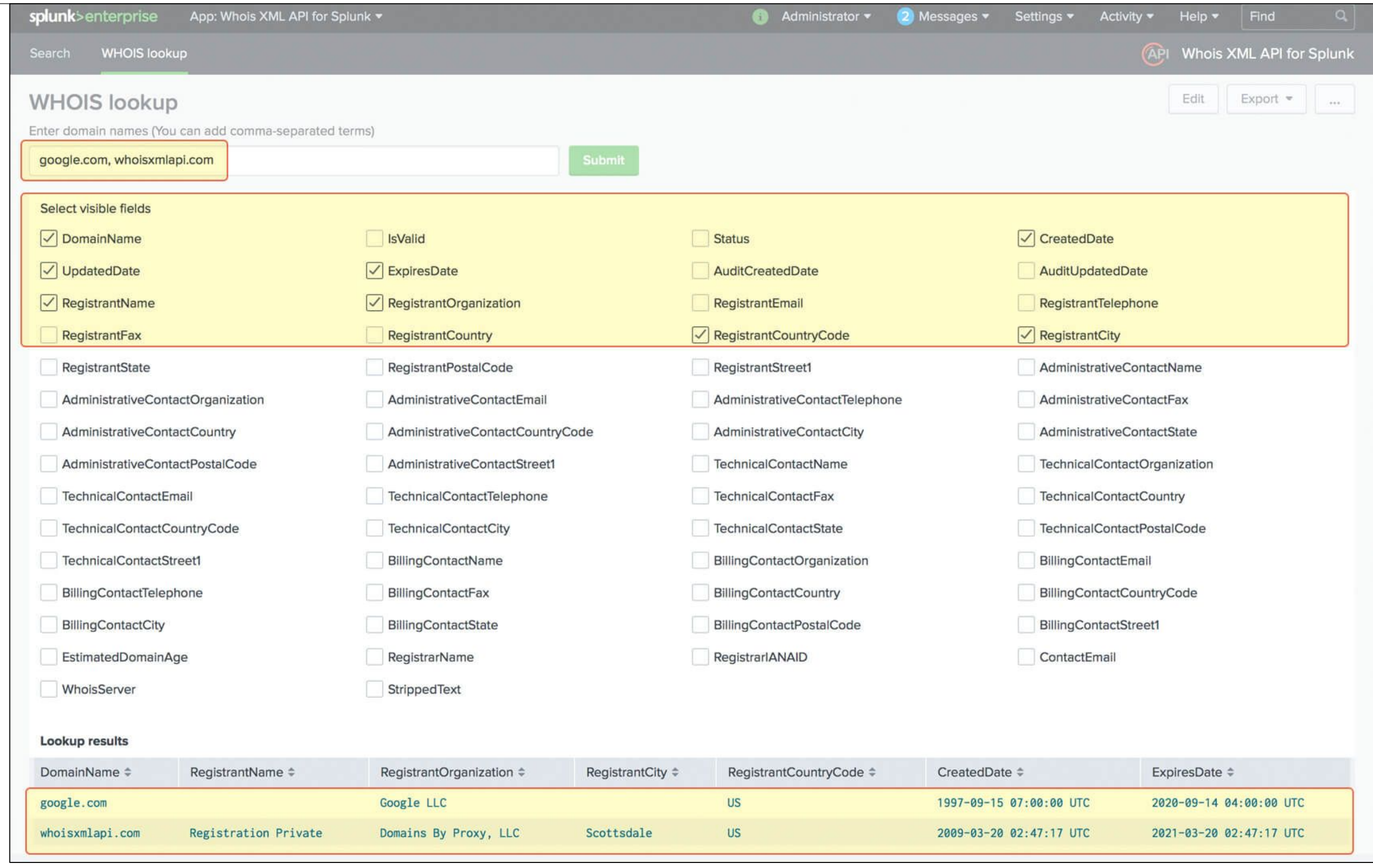
- Keeping track of complex networks where multiple network connection types may be used since Whois XML IP shows connection type.

- Determining the ISP of the users may be useful for legal investigations and as a point of contact for further investigation.

Whois XML IP Geolocation API Images







Logs Analyzed

1 Windows Logs

These contains the intellectual property of VSI's next generation of virtual reality programs.

2 Apache Logs

The logs for VSI's main public-facing website - vsi-company.com

Windows Logs

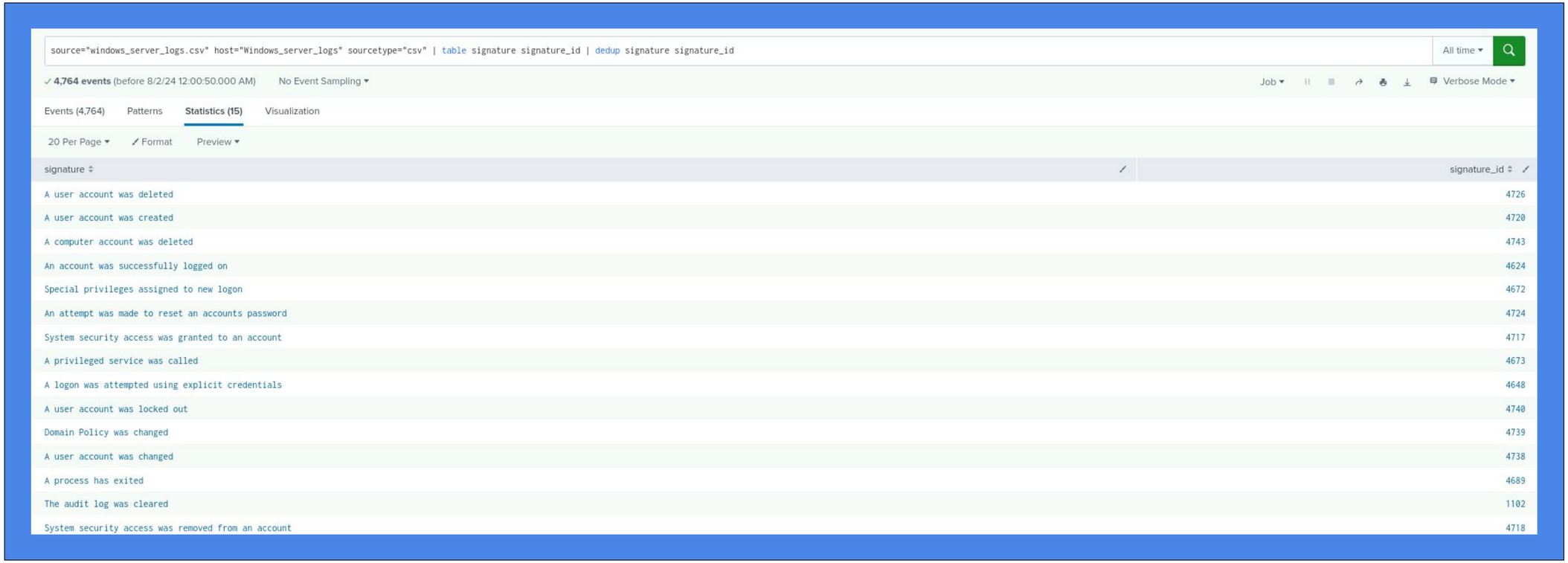
Reports—Windows

Designed the following reports:

Report Name	Report Description
Report 1	Signature and associated signature IDs
Report 2	Severity levels, and percentage of each
Report 3	Success and Failure Report on Windows Server
Report 4	List of active users with the server

Images of Reports—Windows

Report 1 - Signature and IDs



Images of Reports—Windows

Report 2 - Severity Levels

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" | stats count by severity  | eventstats sum(count) as Total | sort - count | eval percentage=round((count/Total)*100,2)
```

All time

✓ 4,764 events (before 8/5/24 11:57:52.000 PM) No Event Sampling

Job Verbose Mode

Events (4,764) Patterns Statistics (2) Visualization

20 Per Page Format Preview

severity	count	Total	percentage
informational	4435	4764	93.09
high	329	4764	6.91

Windows Server Attack Logs Severity Level

```
source="windows_server_attack_logs.csv" | stats count by severity  | eventstats sum(count) as Total | sort - count | eval percentage=round((count/Total)*100,2)
```

✓ 5,949 events (before 8/5/24 11:59:03.000 PM) No Event Sampling

Job

Events (5,949) Patterns Statistics (2) Visualization

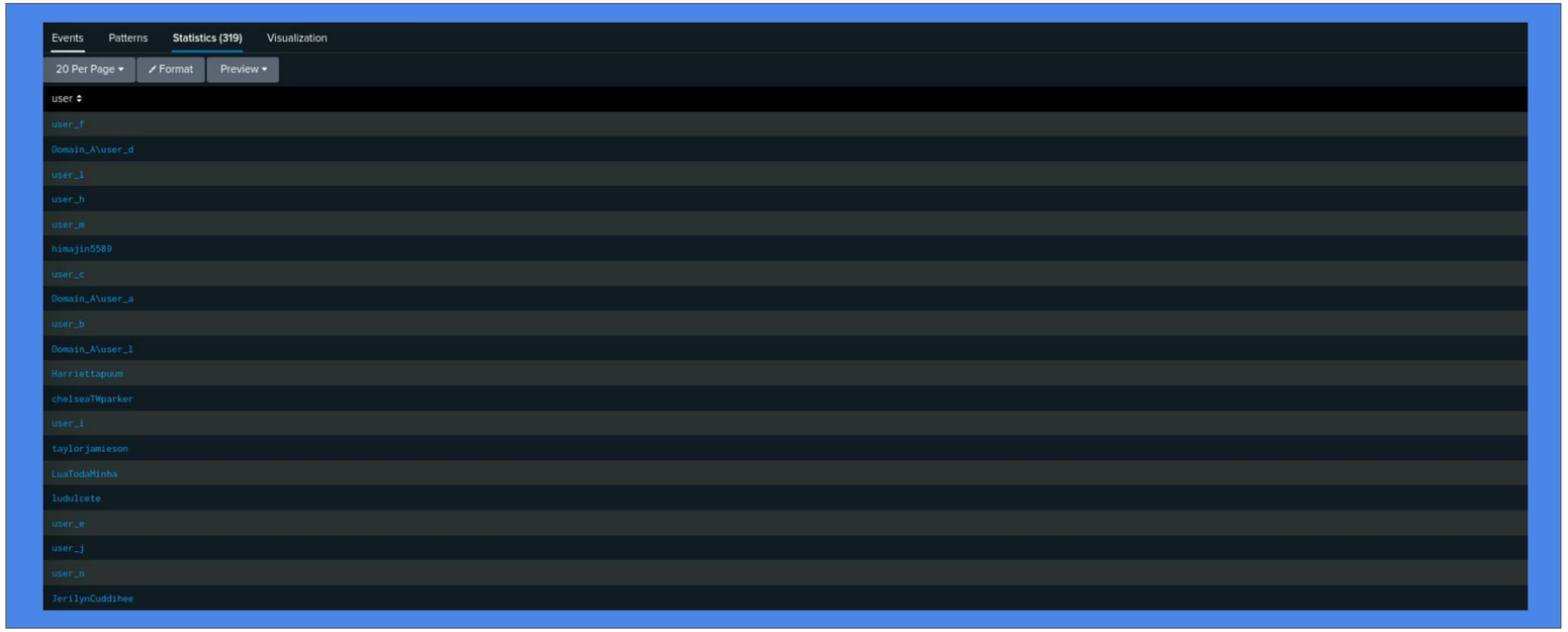
20 Per Page Format Preview

severity	count	Total
informational	4383	5494
high	1111	5494

Images of Reports–-Windows

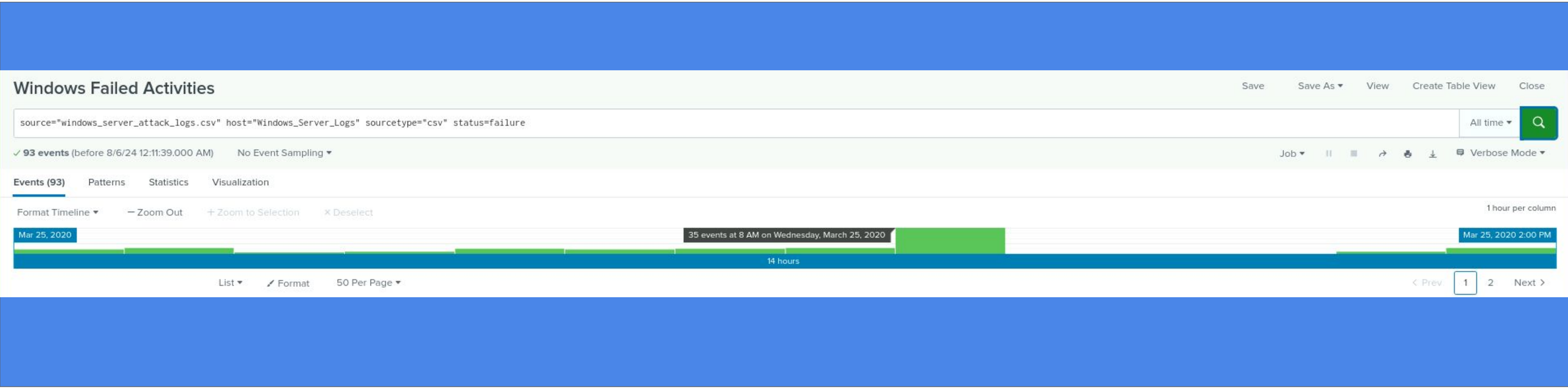
Report 3 - Success and Falures

Report 4 - Active Users



Images of Reports—Windows

Failed Activity Report



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert 1	Failed Windows activities	6	Number of Results is > 20 in 1 hour

JUSTIFICATION: Found the average of 6 and decided on the Threshold of 20 in one hour.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert 2	An account was successfully logged on	11	Number of Results is > 25 in 1 hour

JUSTIFICATION: Found average of 11 for baseline. And decided to alert when exceeding 25 in one hour.

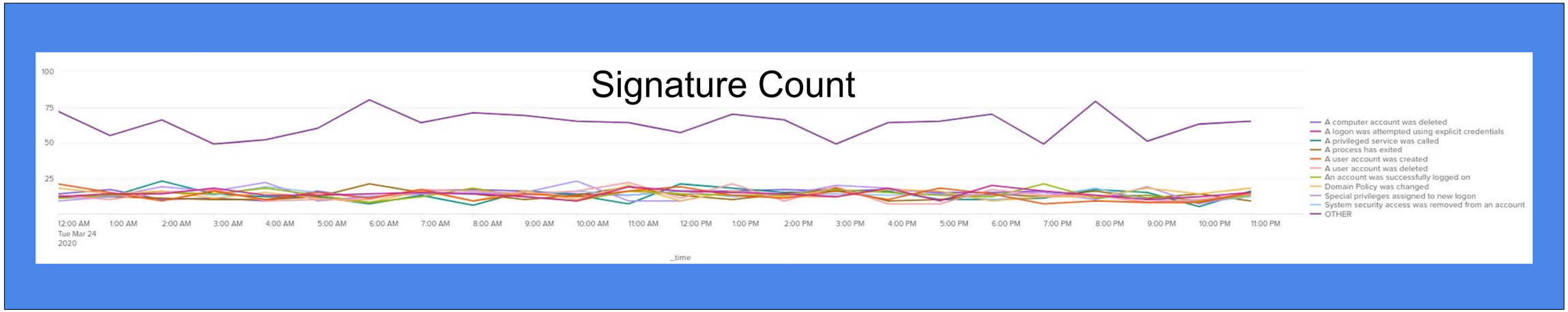
Alerts—Windows

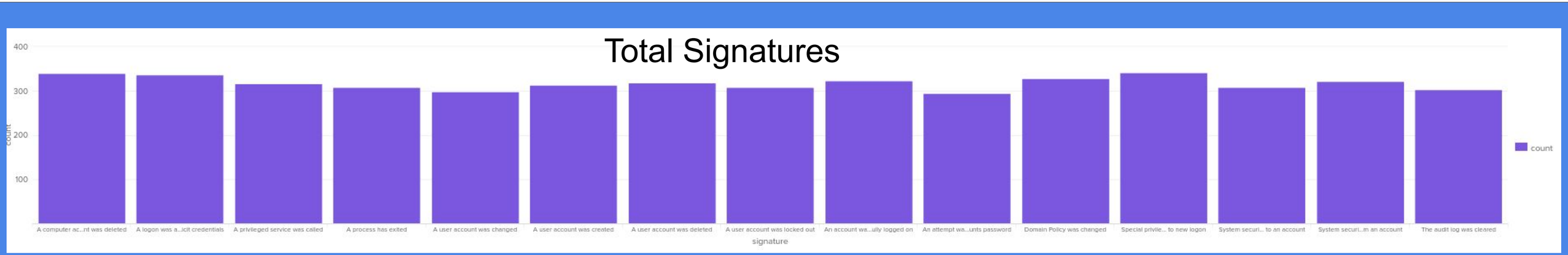
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert 3	A user account was deleted	20	Number of Results is > 35 in 1 hour

JUSTIFICATION: Found the baseline of 20 and decided on a Threshold to alert when exceeding 35 Alerts in one hour.

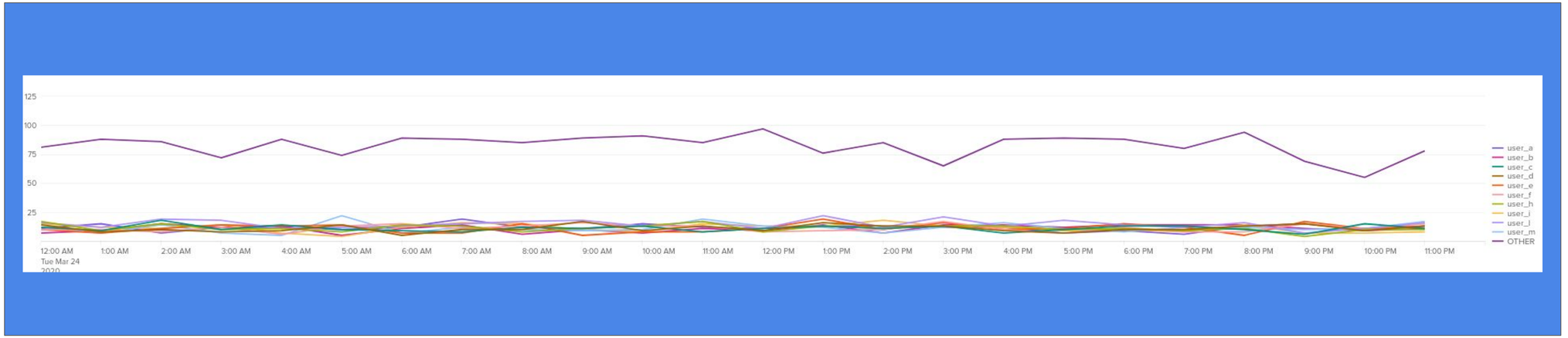
Dashboards—Windows



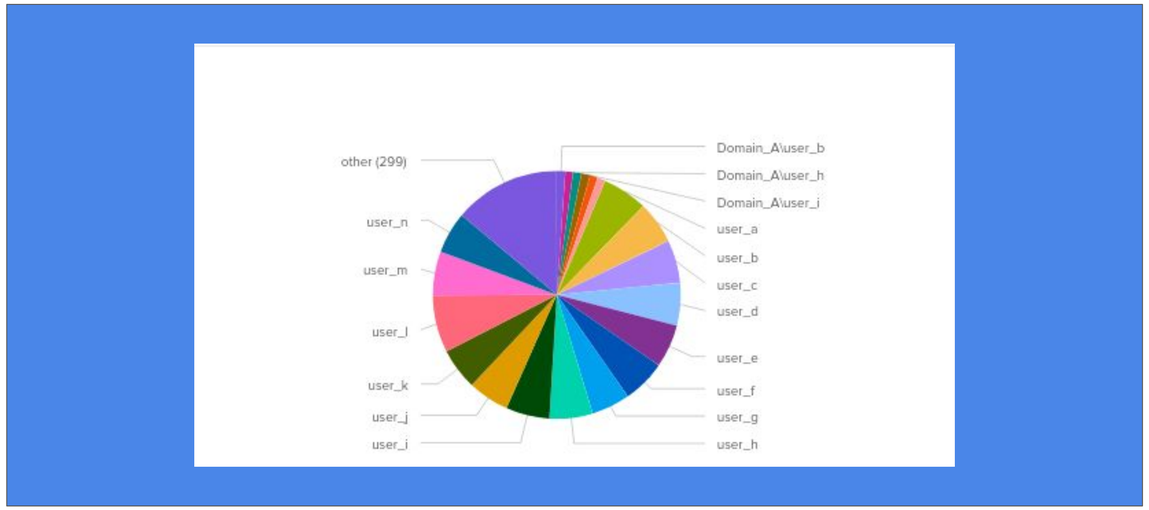


Dashboards—Windows

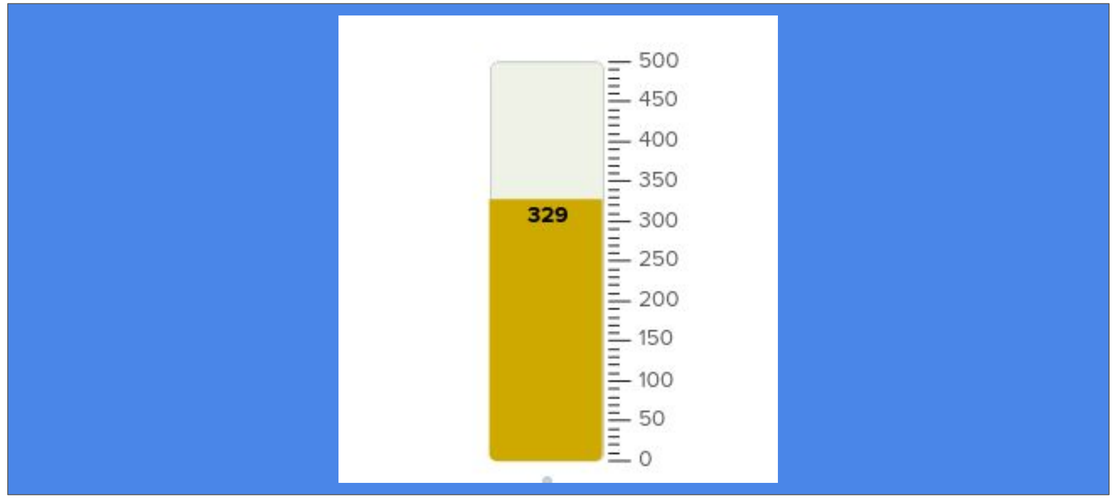
Line Chart of Different Users



User Count



Severity Count Baseline - High



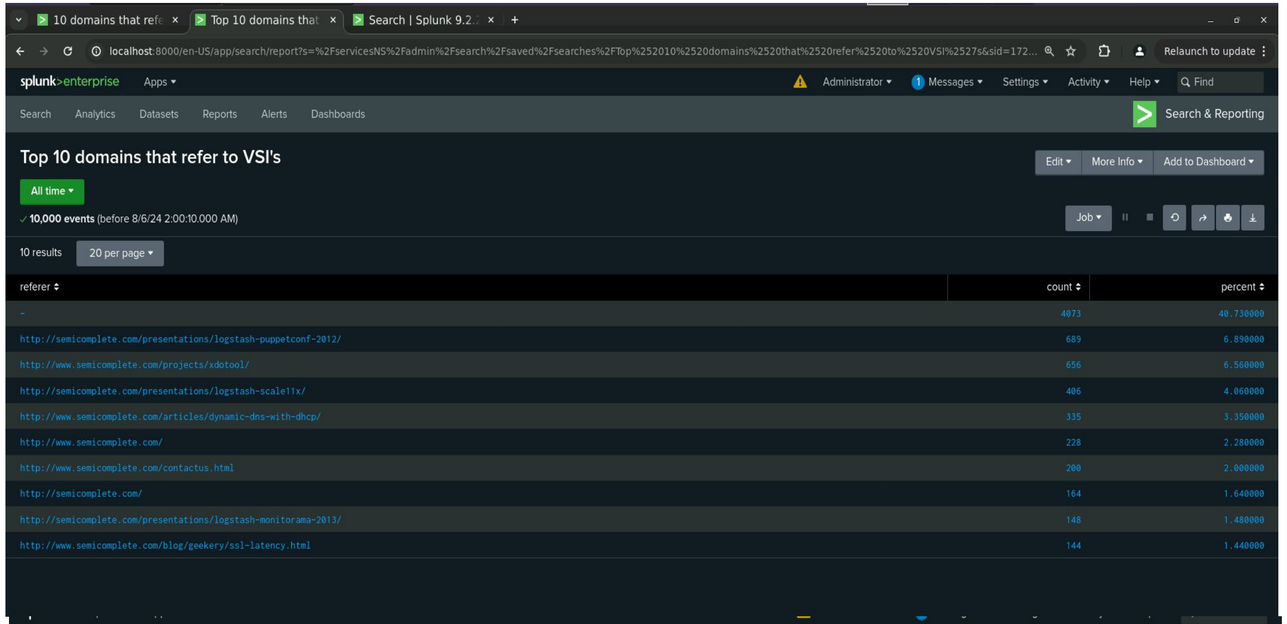
Apache Logs

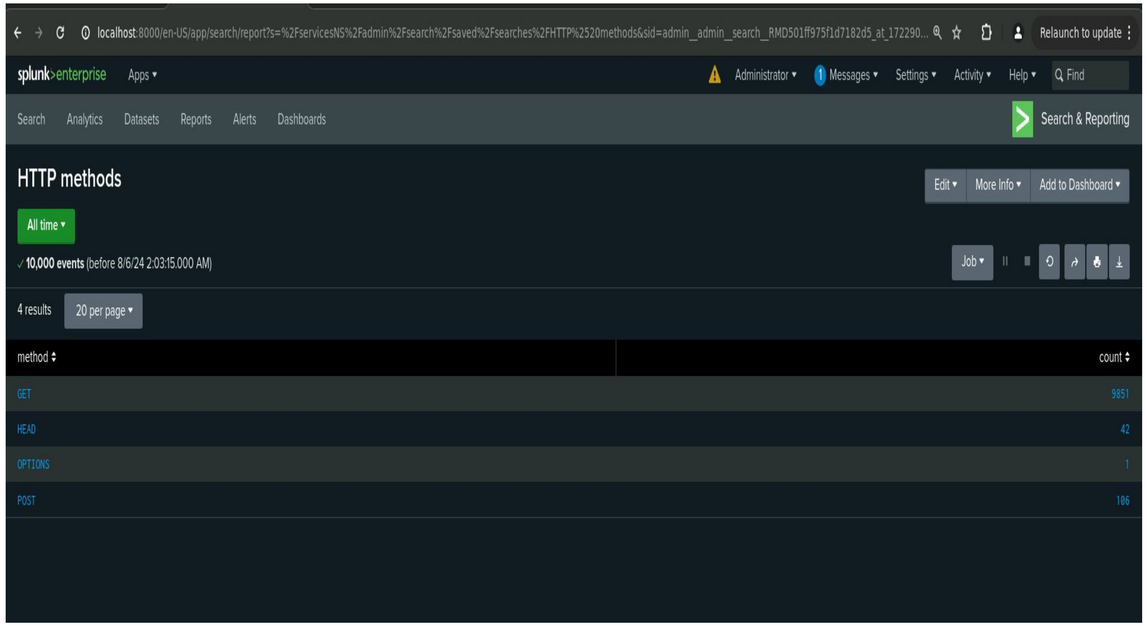
Reports—Apache

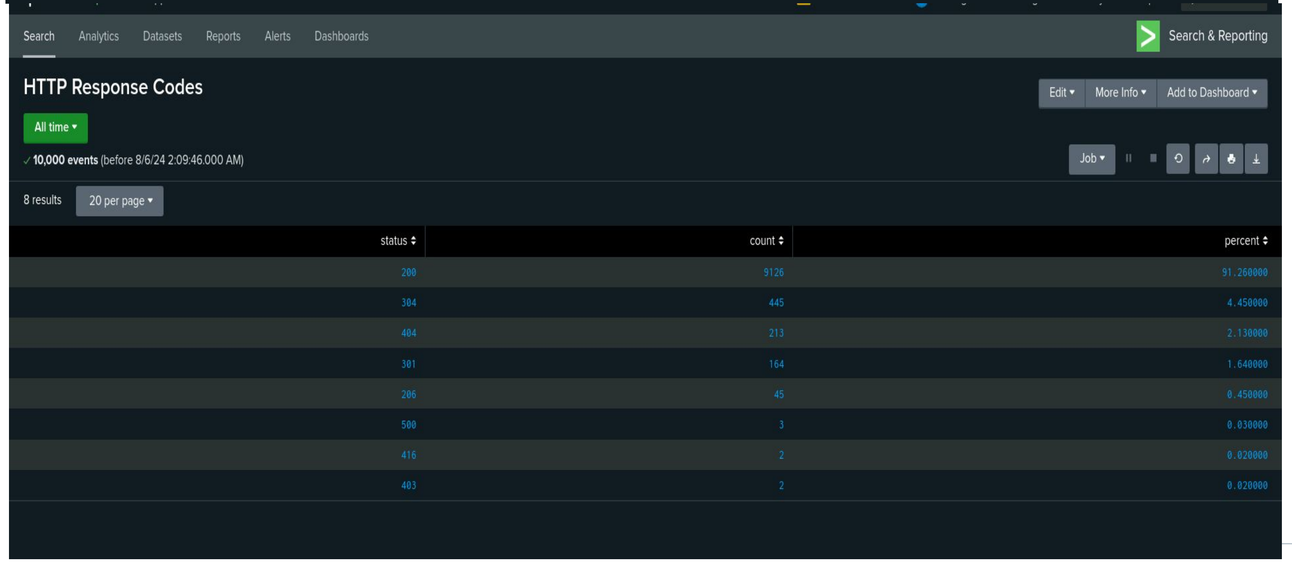
Designed the following reports:

Report Name	Report Description
HTTP Methods	**A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.)**
Top 10 domain that refer to VSI's	A report that display the top 10 domains that refer to VSI
HTTP Response codes	A report that displays the count of HTTP response codes that will provide insight in suspicious levels of HTTP response codes

Images of Reports—Apache







Report Image

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
International Activity	An alert that triggers from hourly activities from countries other than the united states.	80	100

JUSTIFICATION: Most activity range from 1 - 94 events per hour before it reaches 100. With only 10 events over 100 events per hour.

Search used: source=’apache_logs.txt” | iplocation clientip | where Country!=”United States”

Alerts—Apache

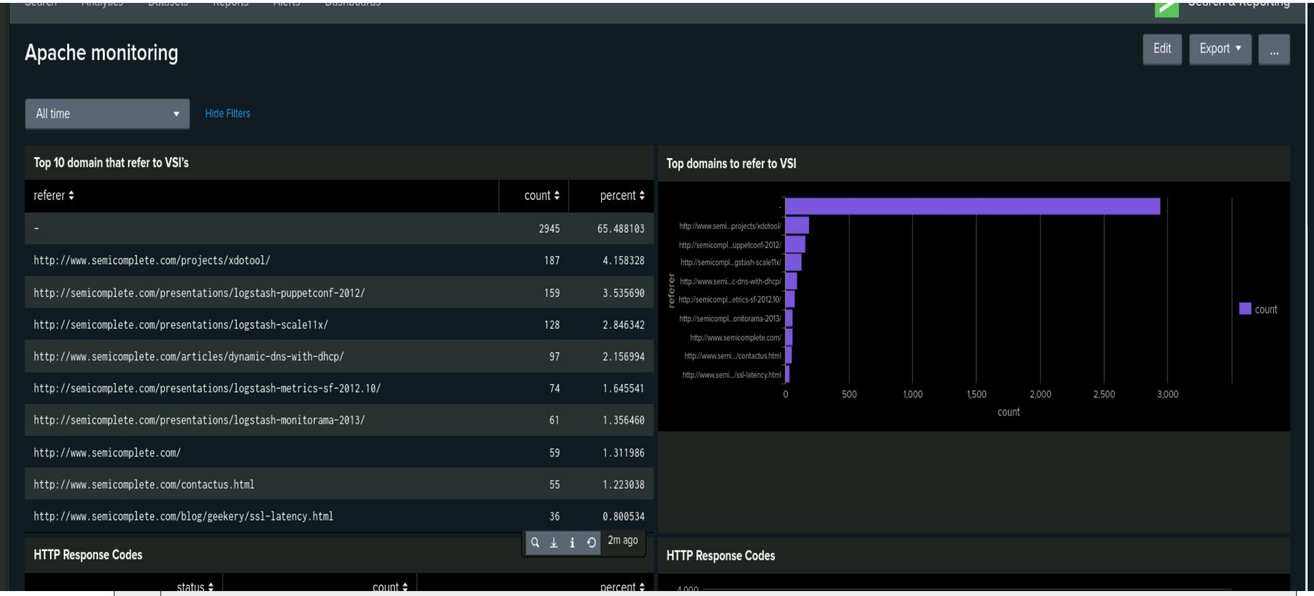
Designed the following alerts:

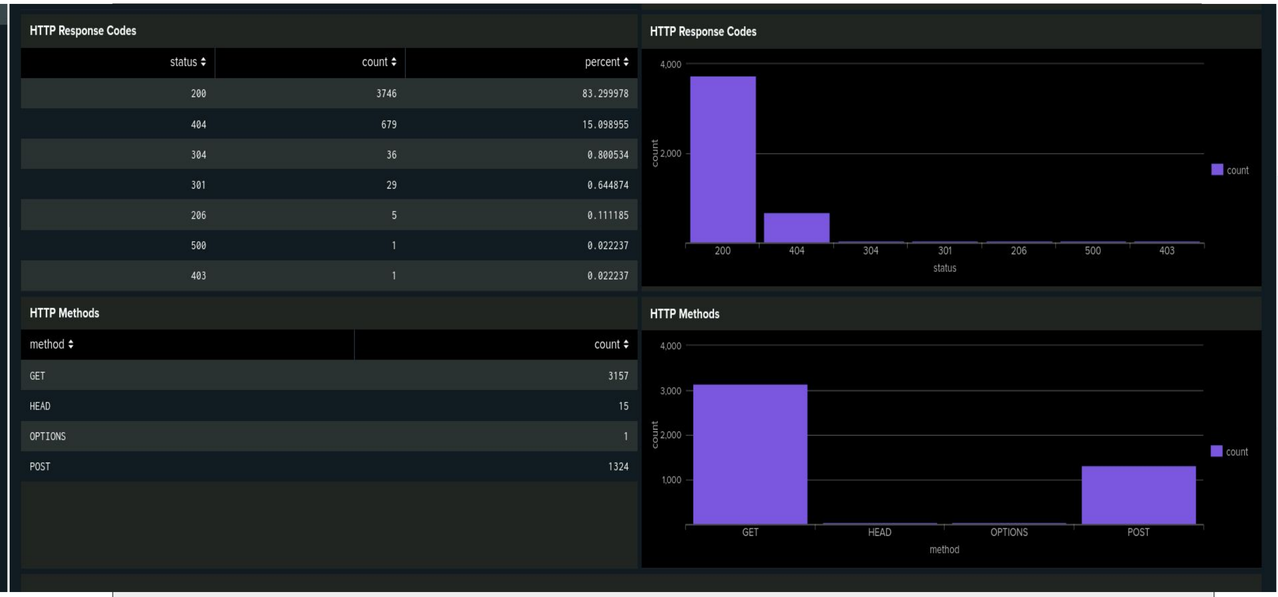
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post	The alert will trigger at 5 or more Post methods. This will help with identifying suspicious activity	2	5

JUSTIFICATION: a majority of event in the apache_logs.txt file indicate 2-3 HTTP Post responses per hour. Setting the threshold at 5 will trigger one event on Friday, March 20th at 1pm.

Search used: source=”apache_logs.txt” method=POST

Dashboards—Apache





Place image here

Place image here

Attack Analysis

Attack Summary—Windows

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

- High severity level events increased significantly.
- Failed Windows events saw a significant change in frequency, while also experiencing a major spike.

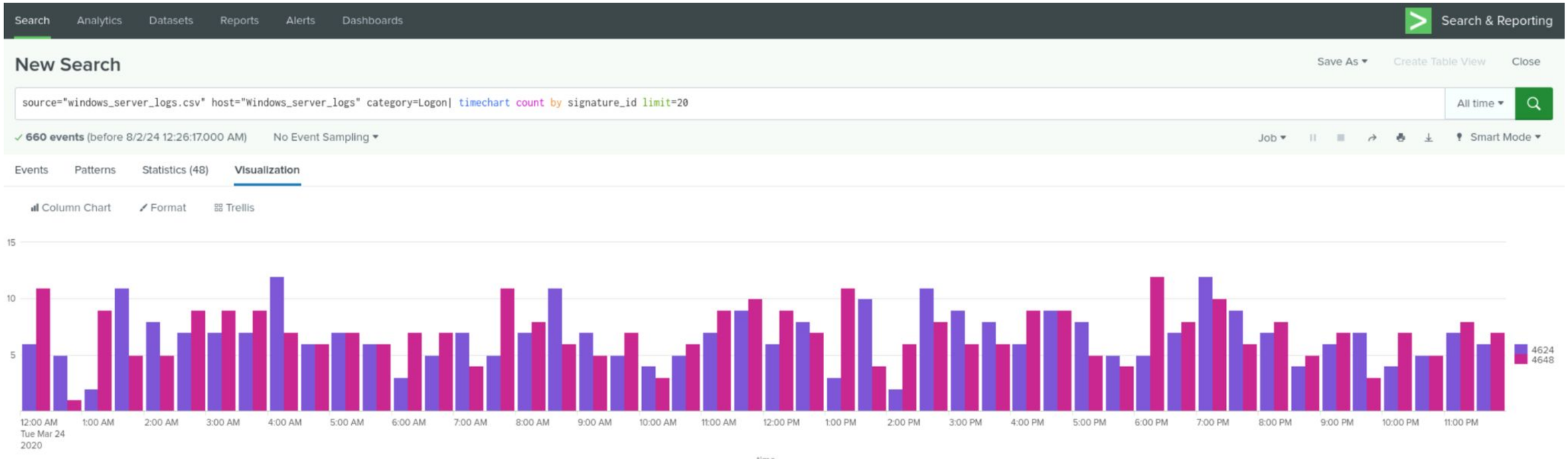
Attack Summary—Windows

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

- We created the following thresholds for each alert:
  - “An account was successfully logged on” - Threshold: **>25 in one hour**
  - “SOC Alert for Failed Activities” - Threshold: **>20 in one hour**
  - “A user account was deleted” - Threshold: **>25 in one hour**

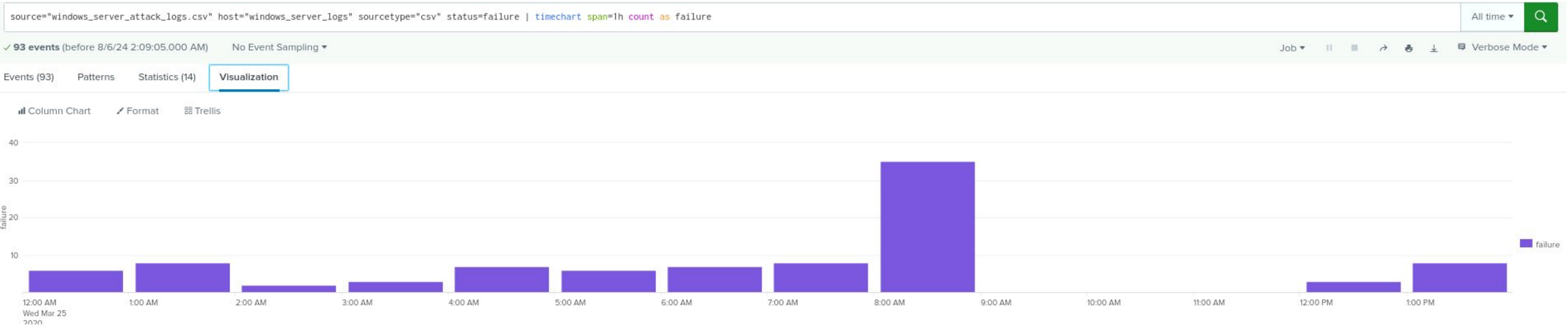
Attack Summary—Windows

- “An account was successfully logged on” - Threshold: **>25 in one hour**



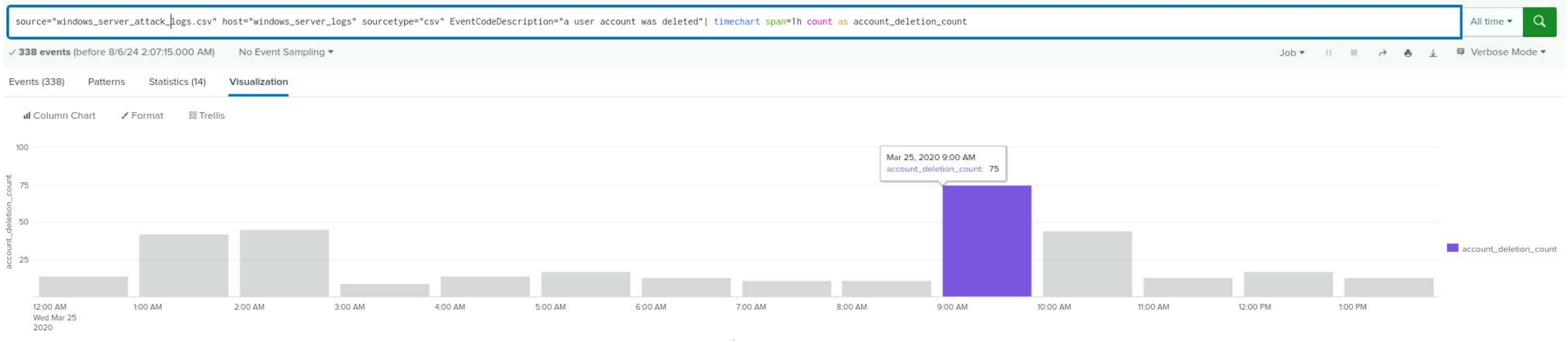
Attack Summary—Windows

- “SOC Alert for Failed Activities” - Threshold: **>20 in one hour**



Attack Summary—Windows

- “A user account was deleted” - Threshold: **>25 in one hour**

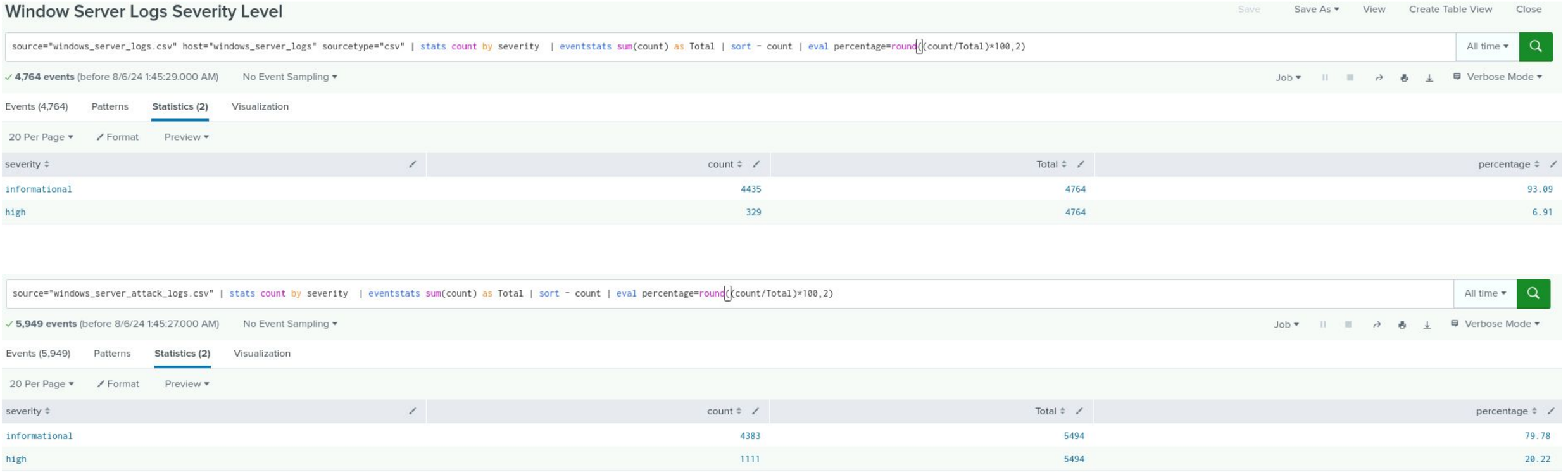


Attack Summary—Windows

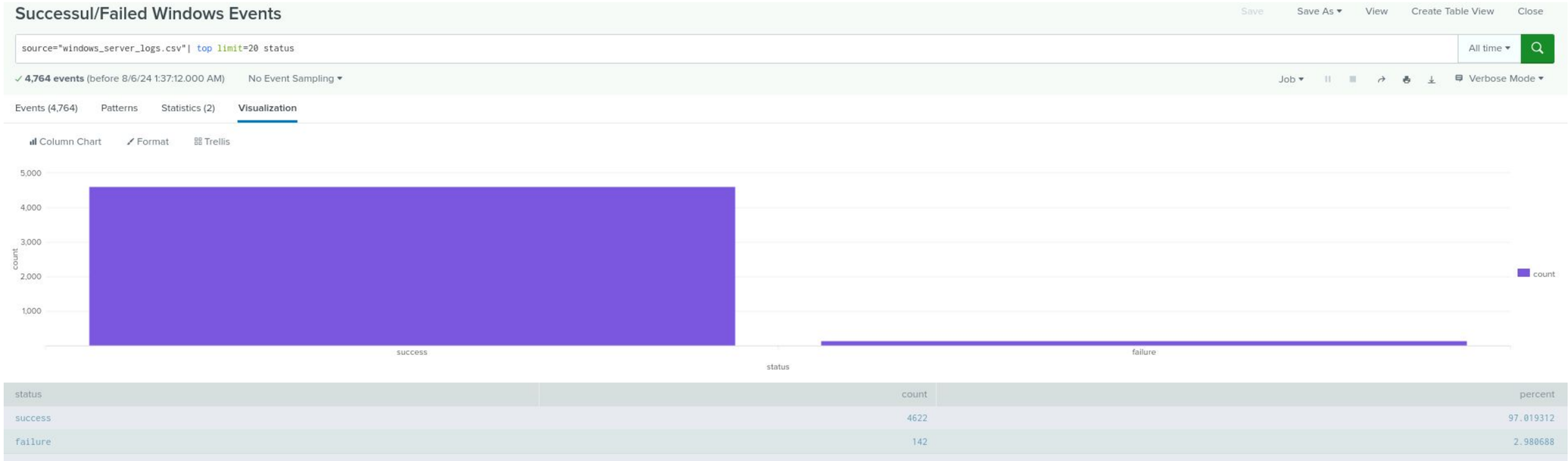
Summarize your findings from your dashboards when analyzing the attack logs.

- A large number of requests to **reset user passwords** occurred.
- A large amount of users became **locked out**.
- **User_a** and u**ser_k** showed significant spikes in activity during the attack.

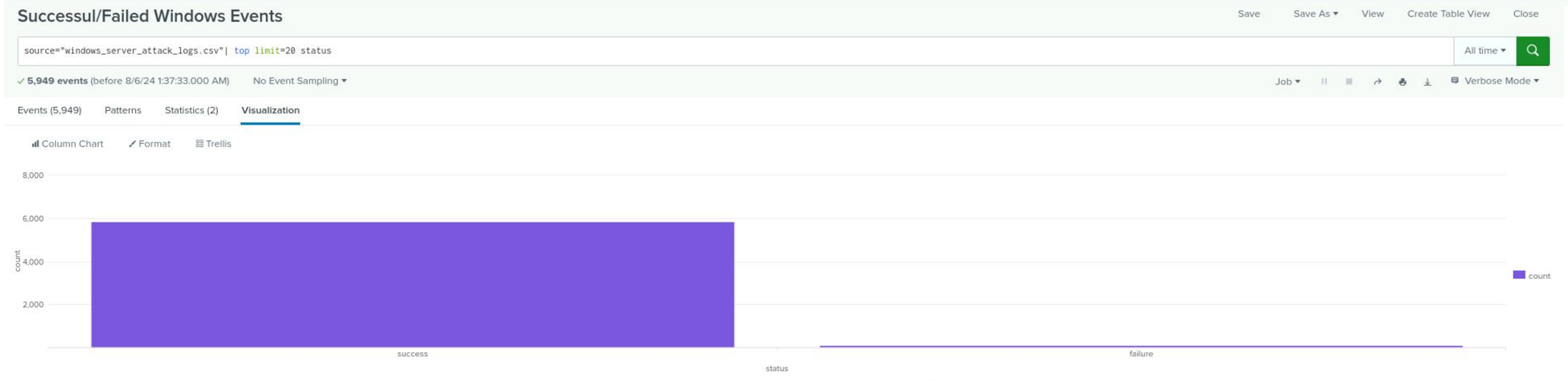
Screenshots of Attack Logs



Screenshots of Attack Logs

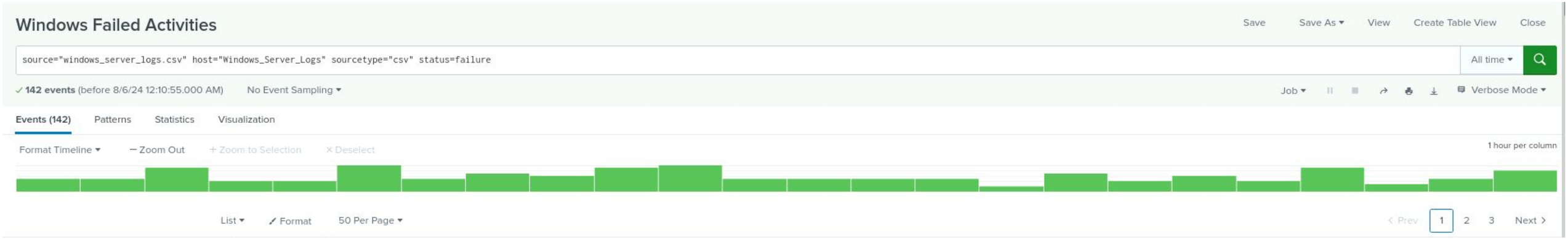


status	count	percent
success	4622	97.019312
failure	142	2.980688



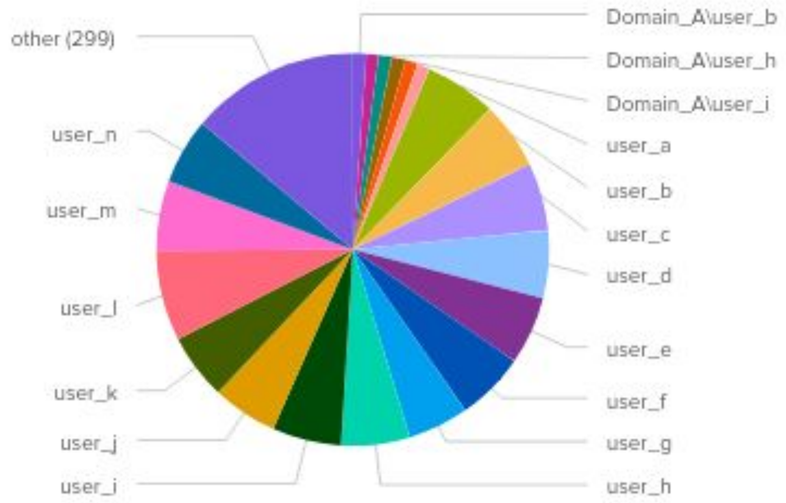
status	count	percent
success	5856	98.436712
failure	93	1.563288

Screenshots of Attack Logs

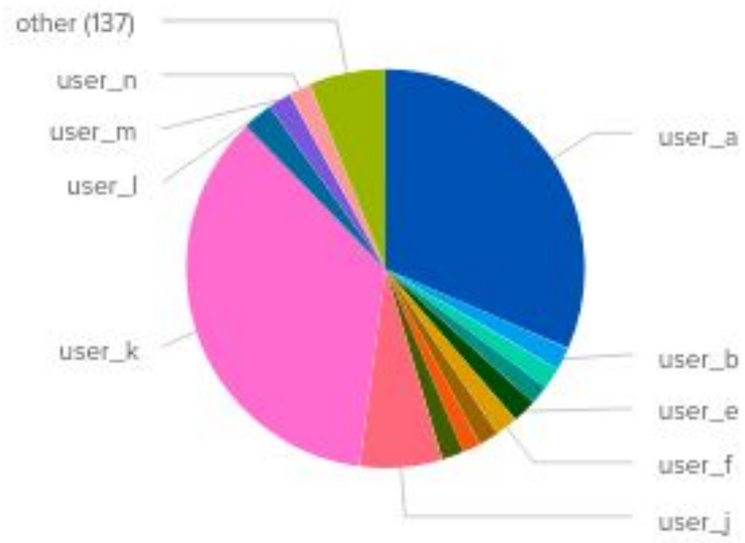


Screenshots of Attack Logs

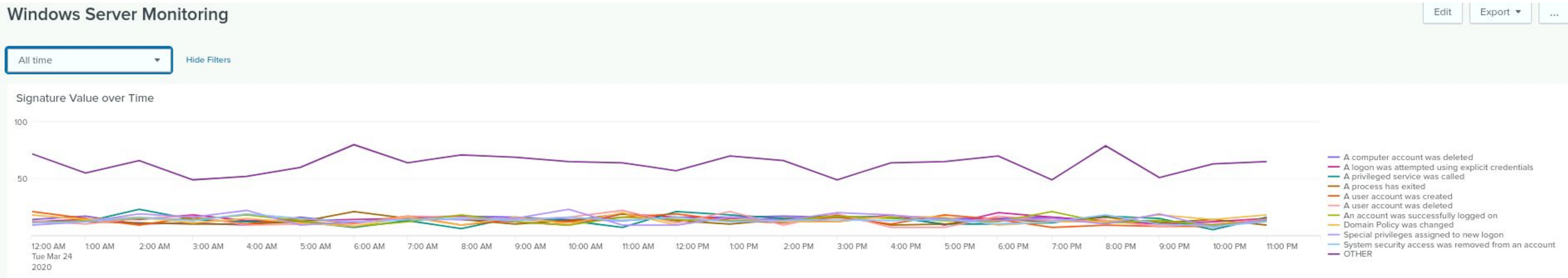
Standard User Activity

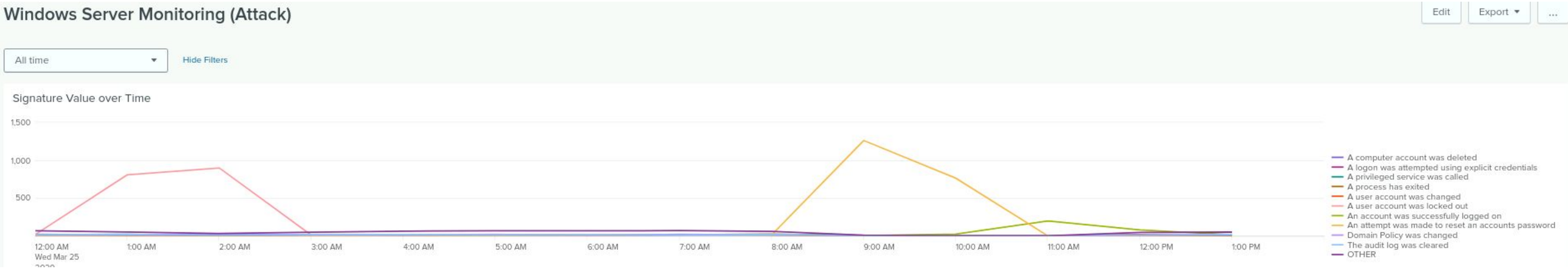


User Activity during Attack



Screenshots of Attack Logs

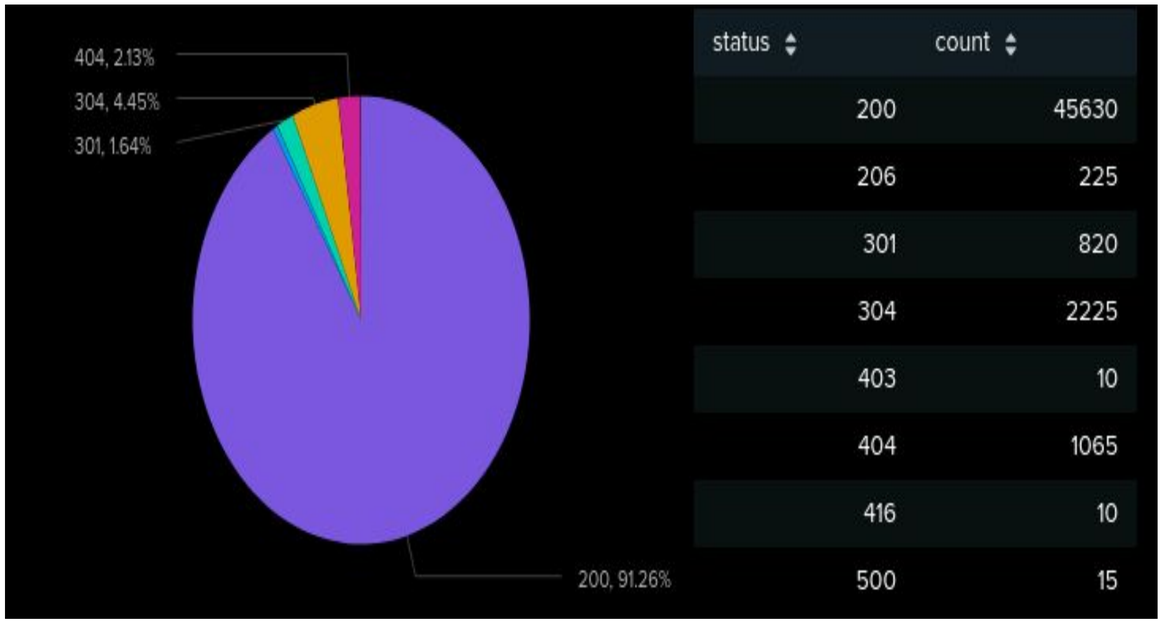




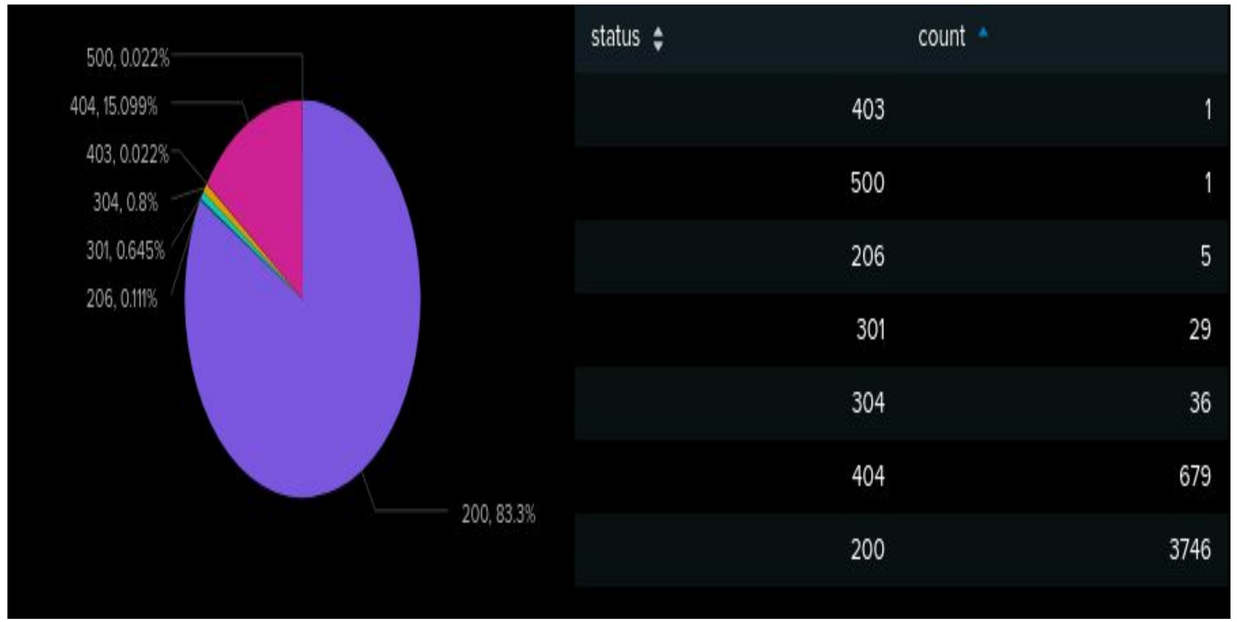
Attack Summary—Apache

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

- There was a significant increase in POST and HTTP methods
- Report for HTTP Response Codes Report showed that ‘404’ went from 2% to 15%



status	count
200	45630
206	225
301	820
304	2225
403	10
404	1065
416	10
500	15



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

Attack Summary—Apache

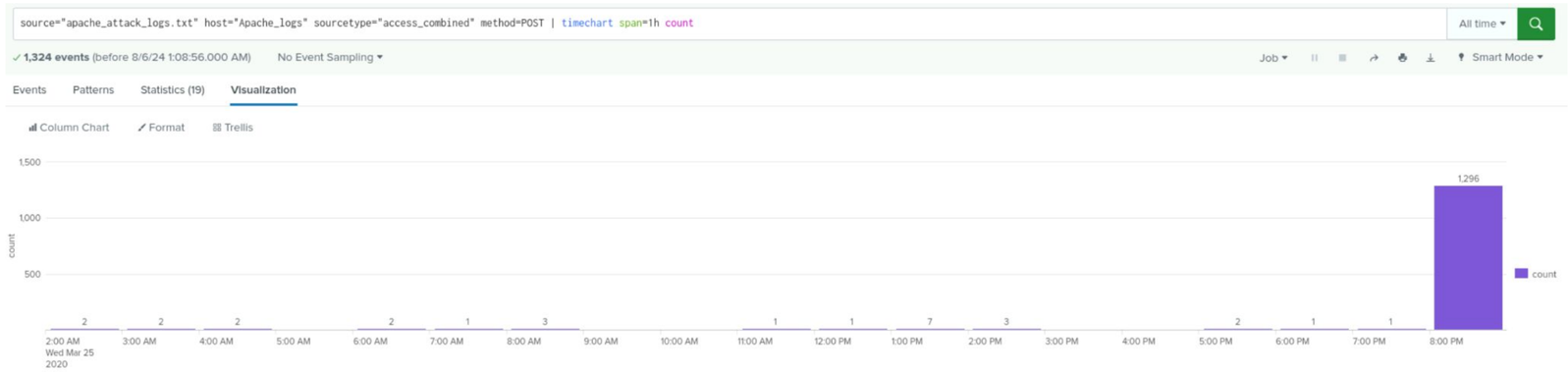
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- reset.css is seen being used excessively by one user in particular. reset.css is used to remove inconsistencies between browsers
- reset.css is used every single time this user accesses the homepage, contacts, and photos of the company building.
- CSS has an extreme lack of security and can be used to both upload malware, and wipe away potential fingerprints.

Attack Summary—Apache

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

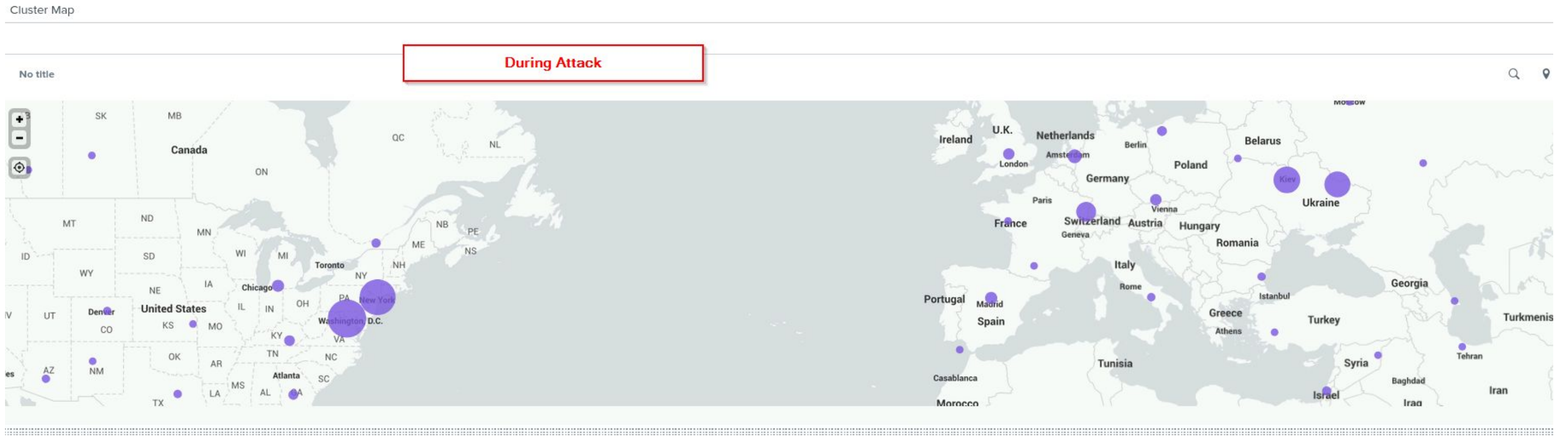
- Our Time Chart of HTTP methods revealed suspicious volumes of POST and GET methods atypical of standard HTTP request traffic
  - POST Methods were used, but there was also an atypical spike in GET requests just before the POST cluster
  - The attacks started at 5:00 PM and ended at 9:00 PM on Wed, March 25th
    - Peak count of POST were 1296 at 8PM



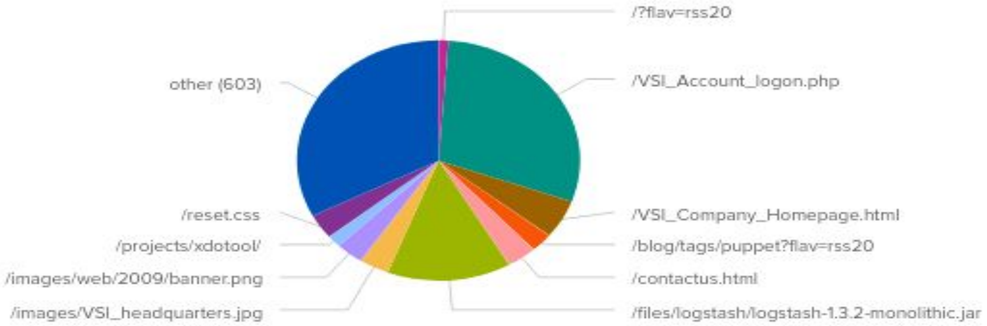
Attack Summary—Apache

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

- On Wednesday, March 25 at 8 PM - there was a suspicious volume of HTTP POST traffic incoming from Ukraine - **937 attacks**
  - In particular, the cities of Kiev and Kharkiv, have an unusually large amount of traffic for the region which is not seen during normal operations
    - Kiev - 439, Kharkiv - 432
  - An influx of the HTTP POST traffic coming in from Ukraine was sending many attempts to the login page
  - When looking up the HTTP response codes, we noticed an influx of 404 codes



Attack Summary—Apache



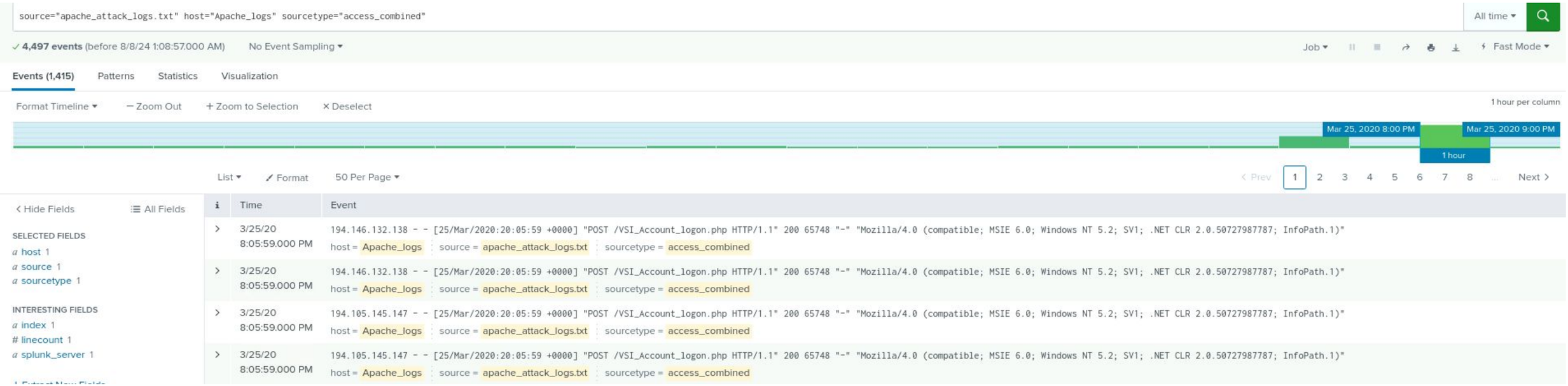
Dashboard Analysis for URI Data

- There was a large uptick in visits to the two following URIs:
  - → /VSI_Account_logon.php
  - → /files/logstash/logstash-1.3.2-monolithic.jar

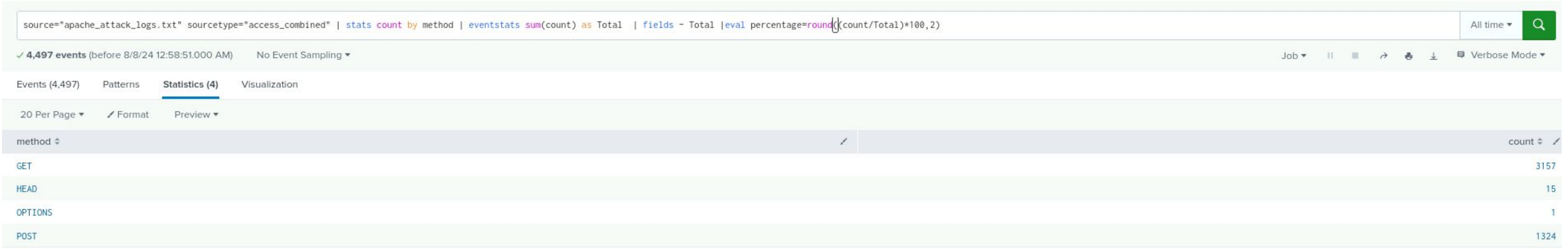
- The logon.php screen activity could indicate a brute force attack is being attempted in a login field or another kind of attack related to .php. The .jar URI could indicate a vulnerable .jar file, which are known to be exploitable and are often considered insecure file types

- Based on the URI chart, it appears that VSI_Account_logon.php was the main focal point

Screenshots of Attack Logs



Screenshots of Attack Logs



Interesting notes

(likely irrelevant information, but interesting all the while)

Within the pre-attack apache logs, there is a 1088 GET requests for a file by the name of "ahhh___rage_face_by_samusmmx-d5g5zap.png”

Another interesting file in the pre-attack apache logs, there are an excessive amount of Requests for a file called "Result:+%E8%F1%EF%EE%EB%FC%E7%EE%E2%E0%ED+%ED%E8%EA%ED%E5%E9%EC+%22newkoversjup%22;+ReCaptcha+%E4%E5%F8%E8%F4%F0%EE%E2%E0%ED%E0;+%28JS%29;+%E7%E0%F0%E5%E3%E8%F1%F2%F0%E8%F0%EE%E2%E0%EB%E8%F1%FC;+%ED%E5+%ED%E0%F8%EB%EE%F1%FC+%F4%EE%F0%EC%FB+%E4%EB%FF+%EE%F2%EF%F0%E0%E2%EA%E8;+Result:+%EE%F8%E8%E1%EA%E0:+%22i+never+really+liked+c%27s+assert%28%29+feature.+if+an+assertion+is+violated,+it%27lltell+you+what+assertion+failed+but+completely+lacks+any+context:%22;+%ED%E5+%ED%E0%F8%EB%EE%F1%FC+%F4%EE%F0%EC%FB+%E4%EB%FF+%EE%F2%EF%F0%E0%E2%EA%E8;" Which seems to contain a rant about assertion feature (cleaned up excessive plus signs, all remaining represent line breaks)

Interesting notes

Likely more relevant and all the more interesting

After the attacks, there is a noticeable surge in web crawler and bot presence. web crawlers in and of themselves are harmless but are extremely good at clogging up HTTP request logs, especially when large in numbers. What makes this so interesting is that most come from some browser and are branded as such, but some others have little to no clear origin at all.

useragent ▲	count
-	66
Baiduspider-image+(+http://www.baidu.com/search/spider.htm)	3
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)	1914
Dalvik/1.6.0 (Linux; U; Android 4.1.2; C2105 Build/15.0.A.2.17)	3
Dalvik/1.6.0 (Linux; U; Android 4.2.2; A114 Build/JDQ39)	3
Dalvik/1.6.0 (Linux; U; Android 4.2.2; Symphony W68 Build/JDQ39)	3
Digg Feed Fetcher 1.0 (Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_1) AppleWebKit/534.48.3 (KHTML, like Gecko) Version/5.1 Safari/534.48.3)	18
ELinks (0.4.3; NetBSD 3.0.2_PATCH sparc64; 141x19)	3
FeedBurner/1.0 (http://www.FeedBurner.com)	72
Feedbin - 1 subscribers	36
Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 1 subscribers; feed-id=11390274670024026467)	6
Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 1 subscribers; feed-id=8003088278240648013)	6
Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 16 subscribers; feed-id=3388821348893992437)	21
Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 22 subscribers; feed-id=8321906634162087507)	21
Feedfetcher-Google; (+http://www.google.com/feedfetcher.html; 3 subscribers; feed-id=14171215010336145331)	18
Feedly/1.0 (+http://www.feedly.com/fetcher.html; like FeedFetcher-Google)	9
Googlebot-Image/1.0	15
LAVA.KKT35+.FARSIGHTED60D_CN_11B_HW (MAUI/KKT35_S116_20130820;BDATE/2013/08/20 14:41;LCD/240320;CHIP/MT6260;KEY/Normal;TOUCH/0;CAMERA/1;SENSOR/0;DEV/FARSIGHTED60D_CN_11B_HW;WAP Browser/MAUI (HTTPS)) LAVA_KKT35_S116_20130820 Release/2013.08.20 WAP Browser/MAUI (HTTPS) Profile/ Q03C1-2.40 en-US	45
LiveJournal.com (webmaster@livejournal.com; for http://www.livejournal.com/users/cshpsionic/; 8 readers)	6
LiveJournal.com (webmaster@livejournal.com; for http://www.livejournal.com/users/semicomplete_rs/; 1 readers)	9

useragent ▾	count ▲
python-requests/1.2.0 CPython/2.7.4 Linux/3.8.0-33-generic	3
portscout/0.8.1	9
msnbot-media/1.1 (+http://search.msn.com/msnbot.htm)	6
magpie-crawler/1.1 (U; Linux amd64; en-GB; +http://www.brandwatch.net)	3
fetch libfetch/2.0	3
facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)	9
distilator/0.1 (http://people.freebsd.org/~ehaupt/distilator/)	6
curl/7.22.0 (i686-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23 librtmp/2.3	3
binlar_2.6.3 test@mgmt.mic	3
binlar_2.6.3 (test@mgmt.mic)	3
Xenu Link Sleuth/1.3.8	6
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	252
Twitterbot/1.0	18
Tiny Tiny RSS/1.11 (http://tt-rss.org/)	147
SimplePie/1.3.1 (Feed Parser; http://simplepie.org; Allow like Gecko) Build/20140115031959	3
Safari/9537.73.11 CFNetwork/673.0.3 Darwin/13.0.0 (x86_64) (MacBookPro8%2C1)	81
SAMSUNG-SGH-E250/1.0 Profile/MIDP-2.0 Configuration/CLDC-1.1 UP.Browser/6.2.3.3.c.1.101 (GUI) MMP/2.0 (compatible; Googlebot-Mobile/2.1; +http://www.google.com/bot.html)	15
Ruby	6
Robosourcer/1.0	3
Opera/9.80 (X11; Linux x86_64) Presto/2.12.388 Version/12.16	6

Summary and Future Mitigations

Project 3 Summary

- **What were your overall findings from the attack that took place?**
  - Our overall finding found that VSI had multiple attacks on March 25, on their Windows and Apache servers. Brute Force attacks came from different countries from around the world.

- **To protect VSI from future attacks, what future mitigations would you recommend?**
  - **Two-Factor/Multi-Factor Authentication** - implementing 2FA/MFA will add extra layer of security, making it significantly harder for attackers to gain unauthorized access even if they obtain user passwords.

  - **Account Lock Policy:** Configure account lockout mechanisms to lock users out after a certain number of failed login attempts. This will help to prevent brute-force attacks by limiting the number of attempts an attacker can make.