

Defensive Security Project

by: Lisa Suzanne, Brenda, Timin, Tom

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Scenario

- VSI SOC Analyst
- We are monitoring Windows and Apache Logs to prevent JobeCorp from disrupting our business
- The products that we have been tasked to monitor
 - Administrative Webpage
 - Apache Web Server
 - Windows OS running VSI backend

Monitoring Environment



WhoisXMLAPI

Whois XML IP Geolocation API

The Whois XML IP Geolocation API is a web service that provides real-time geolocation data for a given IP address. The API can be used to determine the country, city, region, latitude, longitude, and timezone associated with an IP address, as well as the Autonomous System Number (ASN) and Internet Service Provider (ISP) that owns the IP address.

The Whois XML IP Geolocation API is a useful tool for various use cases, such as fraud detection, website localization, and targeted advertising. With its accurate and up-to-date geolocation data, the API can help businesses improve their customer engagement and security measures.



Whois XML IP Geolocation API

Let's imagine VSI wants to expand its customer base by targeting specific regions and countries. Whois XML IP Geolocation API could be incredibly beneficial to the company. By integrating the API into their software, the company could gather detailed information about the location of their potential customers. They could use this information to customize their virtual reality programs to cater to the specific needs of their customers in different regions. For example, they could create programs that highlight cultural differences or emphasize specific products or services that are popular in a particular region.

Furthermore, the API could help the company track the performance of their virtual reality programs in different regions. They could use this information to optimize their programs and make them more effective in specific regions. For example, they could analyze the data to see which regions are showing the most interest in their programs and adjust their marketing strategies accordingly. Overall, by using the Whois XML IP Geolocation API, the small company would be able to make data-driven decisions about how to market their virtual reality programs and which regions to focus on. This could ultimately lead to increased sales and a larger customer base.



Whois XML IP Geolocation API

**Access IP Geolocation Data
Based On Your Business Needs**

WhoisXML API

- IP Geolocation API:** Quickly & easily integrate our data into your applications with API access.
- Bulk IP Geolocation:** Bulk download Geolocation information for up to 100,000 IP addresses that you need at a go, in CSV, JSON or XML format.
- IP Geolocation Database:** Download our entire database in popular CSV and JSON format.



Logs Analyzed

1

Windows Logs

Windows Server logs

- System events
- Security events
- Application events
- Performance events
- Internet Information Services
- Active Directory events
- DNS events

Windows Server Attack Logs

- Audit policy changes
- Account logon events
- Account management events
- Privilege use events
- Object access events:
- Policy change events

2

Apache Logs

Apache Server Logs

- Access logs:
- Error logs:
- Rewrite logs
- SSL logs
- User-agent logs
- Referrer logs

Apache Attack Logs

- IP addresses
- Requested URLs
- HTTP status codes
- User agents
- Timestamps

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signatures and Signature IDs	Table of Signatures and their related Signature IDs
Severity Levels	Severity levels of events and their percentage
Success and Failure of Windows Activities	Pie chart of successful and failed attempts of Windows activity

Images of Reports—Windows

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Signatures and Signature IDs

15 events (before 5/8/23 11:30:12.000 PM)

20 per page

i	Time	Event
>	3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,Domain_A Domain_A",,"user_f user_l",,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_AUser_f Show all 63 lines host = Windows_server_logs signature = A user account was deleted source = windows_server_logs.csv
>	3/24/20 11:59:53.000 PM	2020-03-24T23:59:53.000+0000,,Domain_A Domain_A",2020-03-24 23:59:53 PM,"user_k user_m",,,,server_2/computer_b,,,,,,,,Account Management,,,,,,,,ACME-002,,,aaa,,,,,,,,-,4728,A user account was created,0,,,,,\\a\\g,A,,,,,Audit Success,,,,,Security,,,,,All,0xBAC3,,,,,"SAM Account Name: us er_h Display Name: aaa User Principal Name: ddd8088.local Show all 137 lines host = Windows_server_logs signature = A user account was created source = windows_server_logs.csv
>	3/24/20 11:59:31.000 PM	2020-03-24T23:59:31.000+0000,,Domain_A Domain_A",,"user_l user_e",,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4743,A computer account was deleted,0,,,,,,,,,Audit Success,,,,,Security,,,,,0xAB37,,,,,,,,,"A computer account was deleted. Subject: Security ID: Domain_AUser_l Show all 63 lines host = Windows_server_logs signature = A computer account was deleted source = windows_server_logs.csv
>	3/24/20 11:57:54.000 PM	2020-03-24T23:57:54.000+0000,,Domain_A",,"ACME-002 user_e",,,,Negotiate,,,,,,,,,ACME-002,,,,,,,,No,-,4624,An account was successfully logged on,0,,,,,,,,,Delegation,,0,Audit Success,A966,,,,,Security,,,,,{00000000-0000-0000-0000-000000000000},,"0x70 E4 0x0452",logonProcess1,9,,,,,"An account was successfully logged on. Subject: Show all 159 lines host = Windows_server_logs signature = An account was successfully logged on source = windows_server_logs.csv
>	3/24/20 11:57:51.000 PM	2020-03-24T23:57:51.000+0000,,Domain_A,user_c,,,,,,,,,An account was successfully logged on privileges assigned to new logon,0,,,,,,,,,Audit Success,,,,,Security,,,,,0x5FC9,,,,,,,,,"Special pri

localhost:8000/en-US/app/search/report?s=/servicesNS/admin/search/saved/searches/Signatures%20and%20Signature%2...erver_logs" sourcetype="csv" signature_id="*" signature="*" | dedup signature_id,signature&earliest=0&latest=#

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

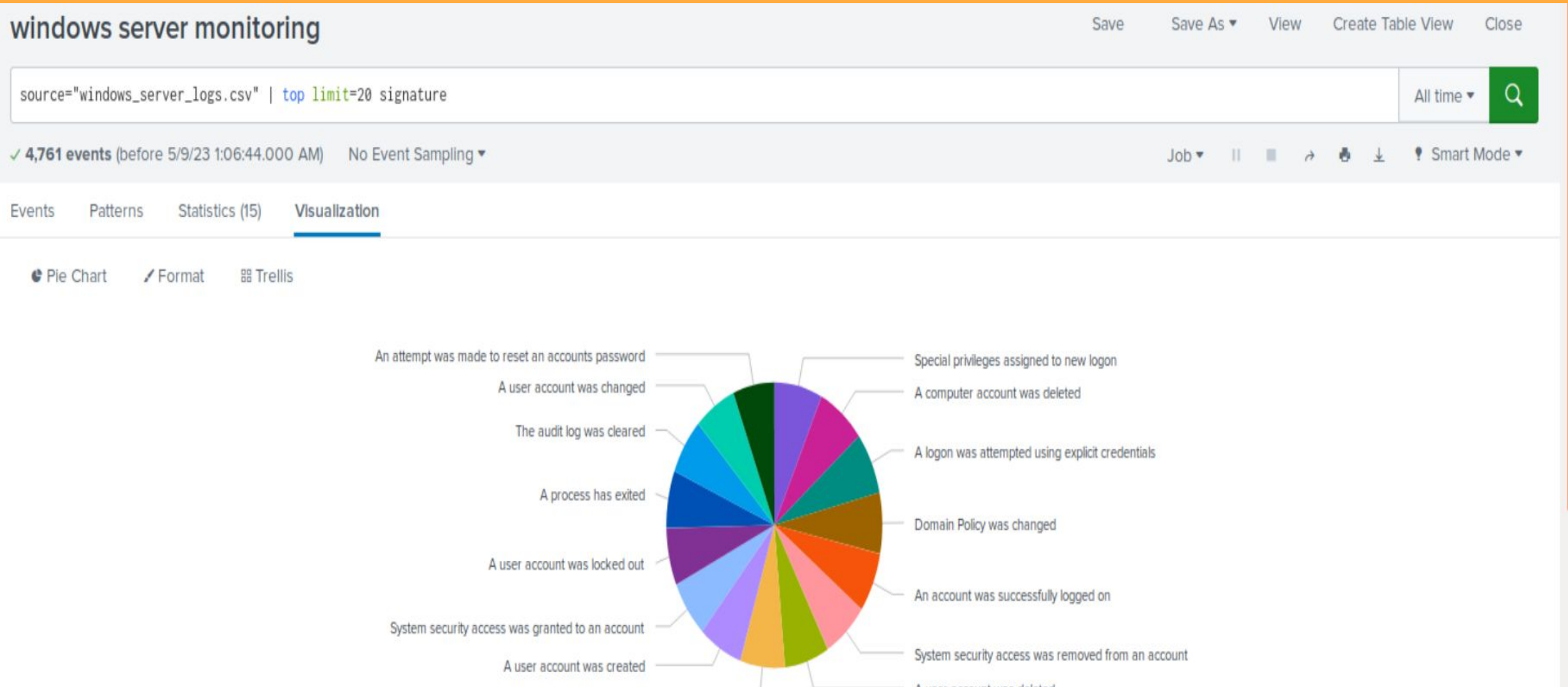
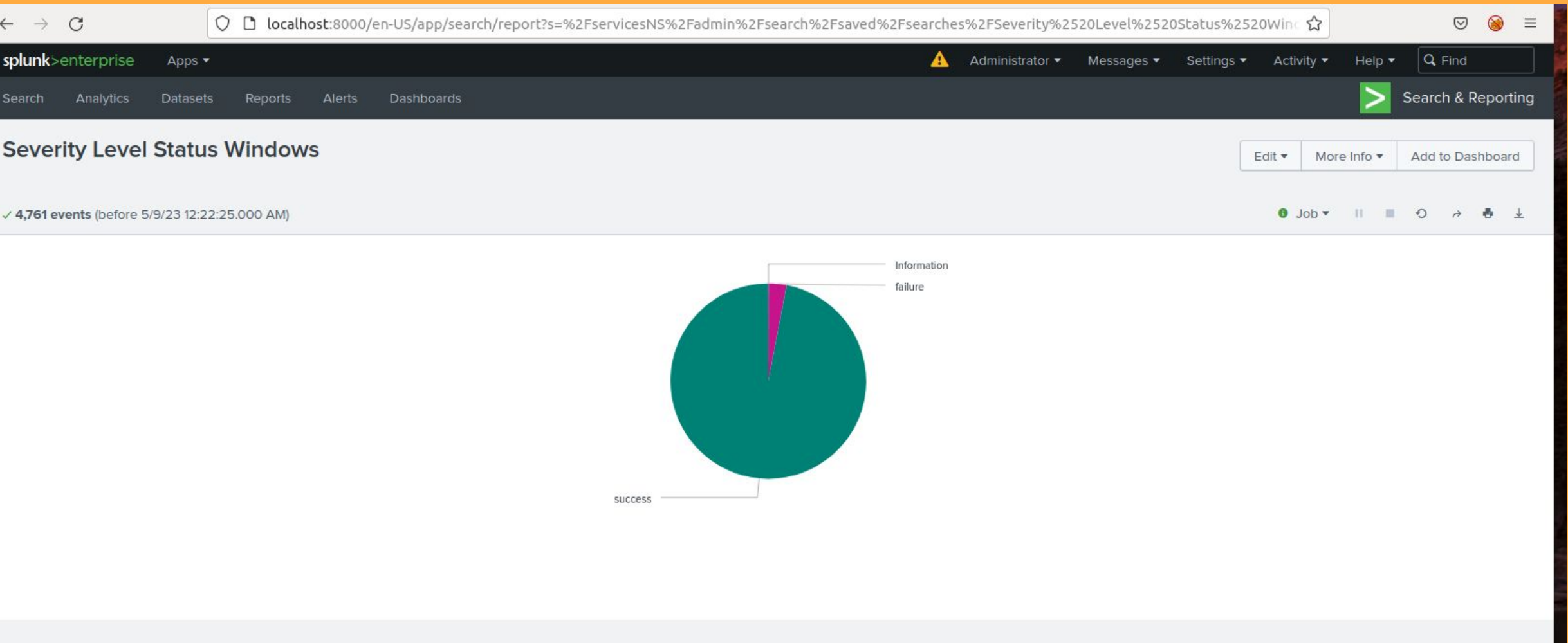
Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Severity Levels Windows

4,761 events (before 5/9/23 12:03:34.000 AM)

results 20 per page

Severity	count
Informational	4429
High	329



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Login Windows Attempts	Failed Login Windows Activity within 1 hour	5	8

JUSTIFICATION: The average failed attempts per hour is about 5, and the majority of instances where that number exceeds 8 happened outside of business hours.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
USER ACCOUNT DELETED	An alert for accounts deleted being	7	12

JUSTIFICATION: The average accounts deleted per hour is about 7, and the maximum at any given point is around 12.

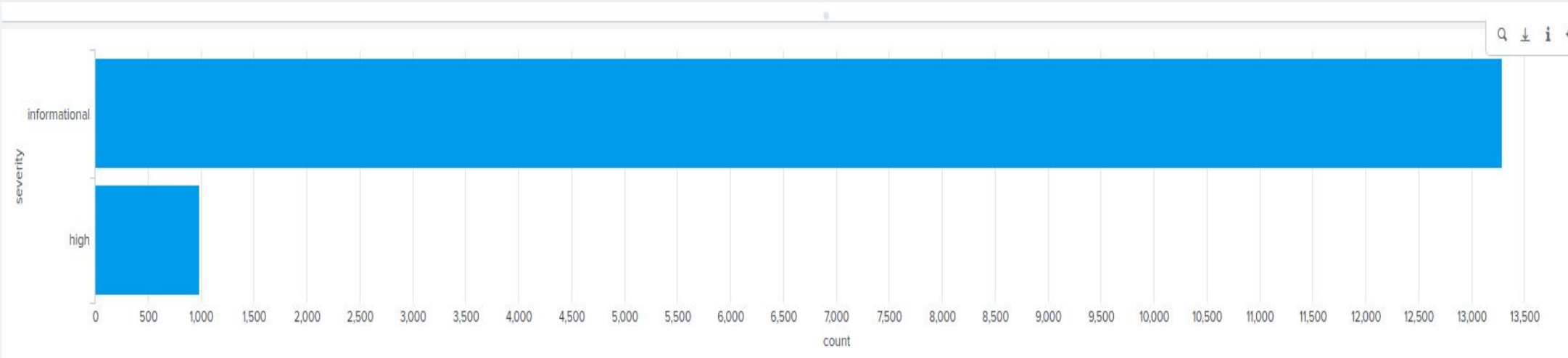
Alerts—Windows

Designed the following alerts:

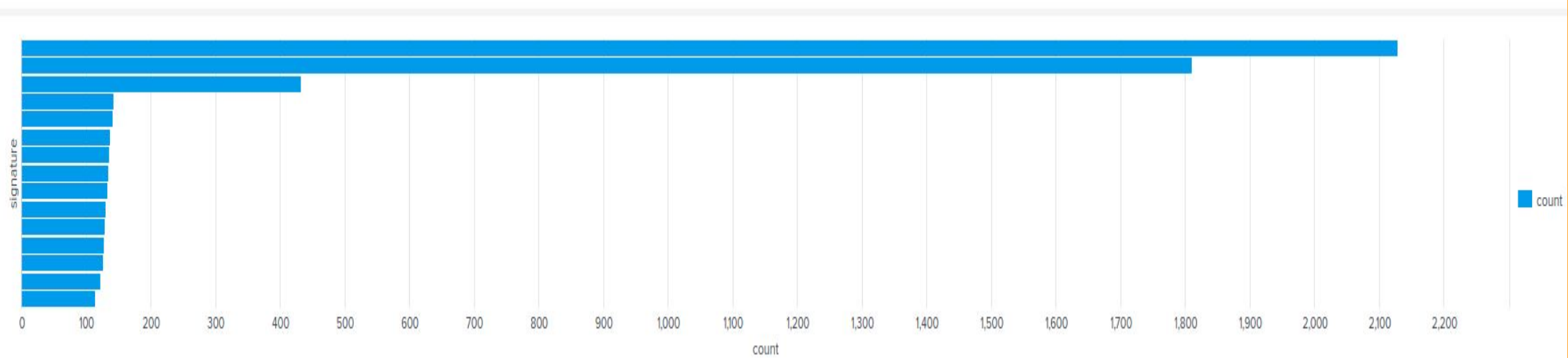
Alert Name	Alert Description	Alert Baseline	Alert Threshold
An account was successfully logged on	a baseline and threshold for the hourly count of accounts logged on	7	15

JUSTIFICATION:The average amount of accounts logged on per hour is about 7, and the maximum at any given point is around 15.

Dashboards—Windows



Attack Logs												
_time ↕	A computer account was deleted ↕	A privileged service was called ↕	A process has exited ↕	A user account was changed ↕	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 password ↕	Domain Policy was changed ↕	The audit log was cleared ↕	OTHER ↕	NULL ↕
2020-03-24 19:00	19	14	8	10	14	16	11	10	10	12	68	0
2020-03-24 20:00	12	20	13	7	7	805	15	11	16	16	51	0
2020-03-24 21:00	9	3	16	9	5	896	14	3	17	8	27	0
2020-03-24 22:00	13	13	12	16	9	10	14	6	16	14	51	0
2020-03-24 23:00	12	18	8	11	14	12	12	11	10	16	63	0
2020-03-25 00:00	11	14	12	16	17	19	9	8	14	10	62	0
2020-03-25 01:00	9	14	12	17	13	3	11	14	8	13	64	0
2020-03-25 02:00	15	8	15	17	11	11	15	16	20	7	70	1
2020-03-25 03:00	17	13	23	11	11	16	16	12	11	16	59	0
2020-03-25 04:00	5	2	1	3	3	1	4	1258	0	4	12	0
2020-03-25 05:00	0	0	0	0	0	0	23	761	0	0	0	0
2020-03-25 06:00	0	0	0	0	0	0	196	0	0	0	0	0
2020-03-25 07:00	7	9	7	11	13	6	77	6	6	9	46	0
2020-03-25 08:00	4	8	7	9	13	16	15	12	15	17	48	0



Apache Logs

Reports—Apache

Designed the following reports:

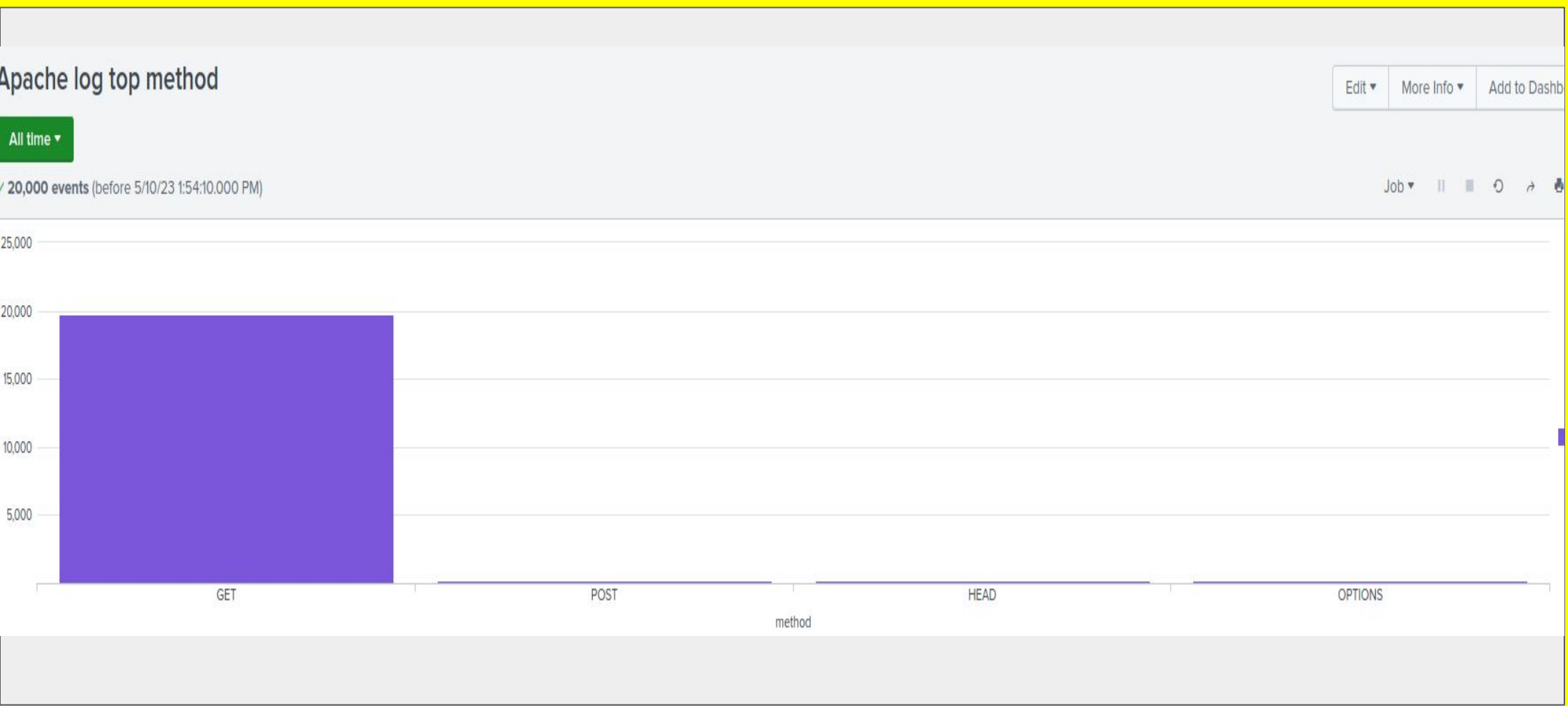
Report Name	Report Description
HTTP Methods	Table of all HTTP Methods
Top 10 Referrer Domains	Table of the top 10 Referrer Domains that refer to VSI's website
HTTP Response Code Counts	Table showing the count of each HTTP response code

Images of Reports—Apache

HTTP Methods		
All time		
10,000 events (before 5/9/23 2:06:22.000 AM)		
20 per page		
#	Time	Event
>	3/20/20 9:05:59.000 PM	5.18.83.53 - - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/7C?N:0+A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:59.000 PM	66.249.73.135 - - [20/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:58.000 PM	63.140.98.80 - - [20/Mar/2020:21:05:58 +0000] "GET /images/YSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:57.000 PM	38.99.236.50 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:57.000 PM	63.140.98.80 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/css/reset.css HTTP/1.1" 200 1382 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:56.000 PM	180.76.6.56 - - [20/Mar/2020:21:05:56 +0000] "GET /robots.txt HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:55.000 PM	38.99.236.50 - - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/images/xkcd-perlswing-many.png HTTP/1.1" 200 180207 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:55.000 PM	38.99.236.50 - - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/js/reveal.js HTTP/1.1" 200 29108 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:55.000 PM	38.99.236.50 - - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/css/print.css HTTP/1.1" 200 3995 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200
>	3/20/20 9:05:54.000 PM	38.99.236.50 - - [20/Mar/2020:21:05:54 +0000] "GET /presentations/logstash-puppetconf-2012/css/main.css HTTP/1.1" 200 26498 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = Apache_Logs source = apache_logs.txt status = 200

Top 10 URI		
All time		
10,000 events (before 5/9/23 2:12:24.000 AM)		
10 results 20 per page		
uri #	count #	percent #
/YSI_Company_Homepage.html	887	8.670000
/contactus.html	546	5.460000
/reset.css	538	5.380000
/images/YSI_headquarters.jpg	533	5.330000
/images/web/2009/banner.png	516	5.160000
/blog/tags/puppet?flav=rss20	488	4.880000
/projects/xdotool/	224	2.240000
/?flav=rss20	217	2.170000
/	197	1.970000
/robots.txt	180	1.800000

HTTPS Methods Count	
All time	
10,000 events (before 5/9/23 2:15:33.000 AM)	
4 results 20 per page	
method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106



Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Threshold of high HTTP Posts	Alert if hourly count of the HTTP Post method exceeds the threshold.	3	5

JUSTIFICATION: Most events were consistent around 3. Setting threshold to 5 will capture all events out of “normal” range.

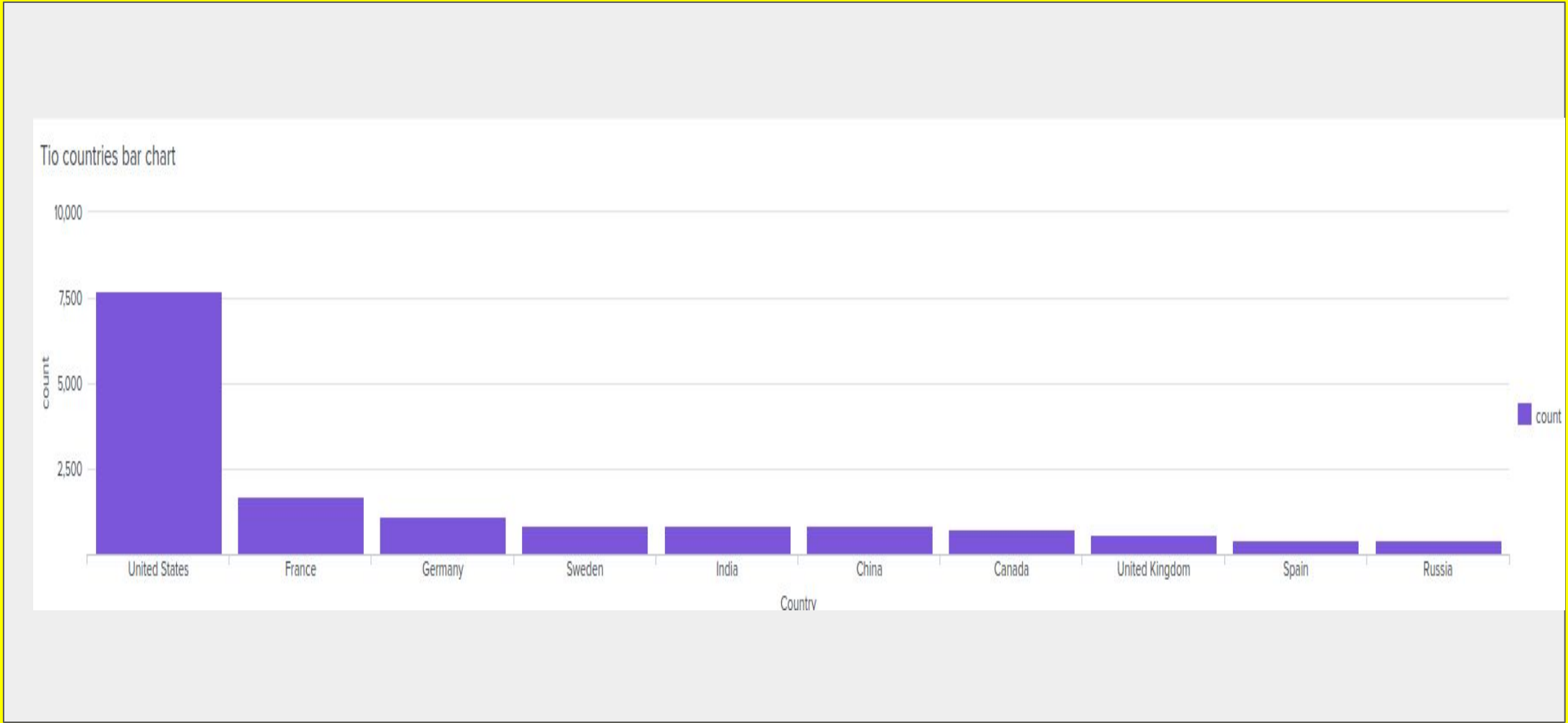
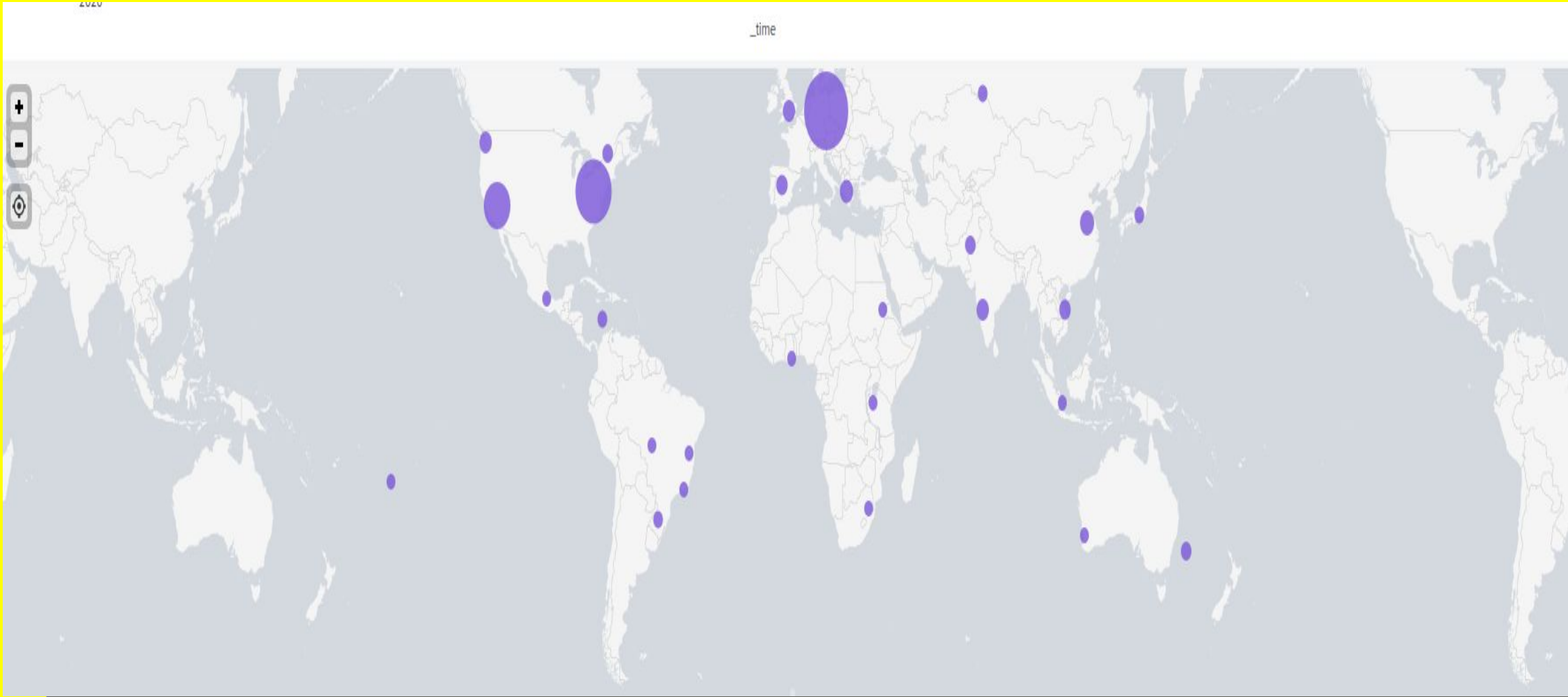
Alerts—Apache

Designed the following alerts:

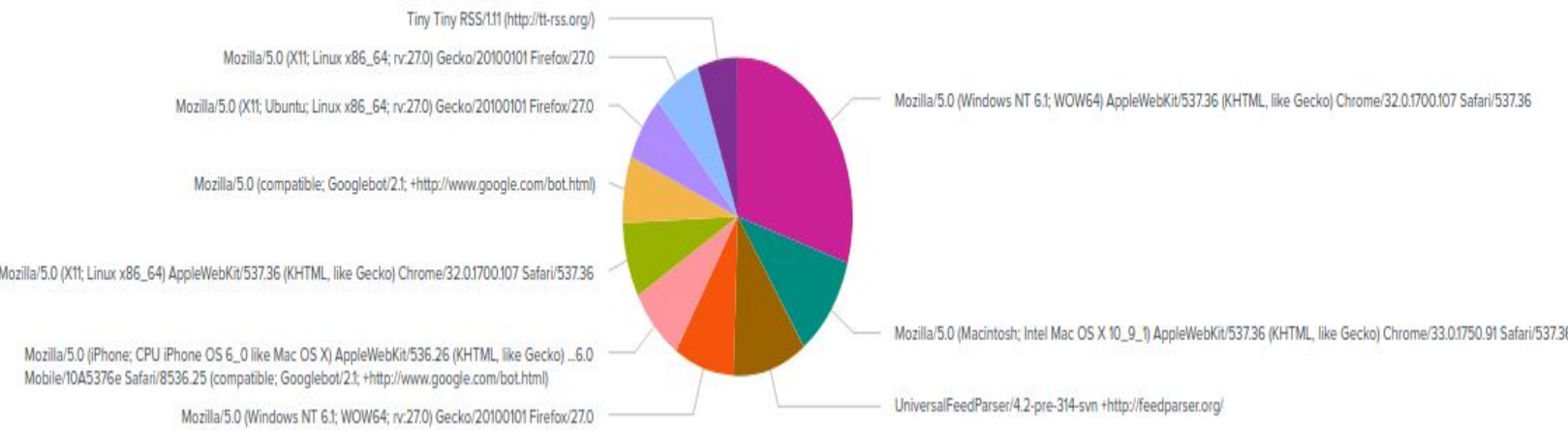
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly activity from Country outside US	Set alert to capture influx of traffic outside of US hourly	90	180

JUSTIFICATION: Events in normal range seem to be between 90 and 170. If we capture anything over 180, we will capture suspicious activity.

Dashboards—Apache



Top 10 User agents



status code 200 "Success" single point visualization



Attack Analysis-Windows

Attack Summary—Windows

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

1. Report analysis for “failure” activity has no significant changes
 - a. Windows logs show 2.98% failure and Windows attack logs 1.56%
2. Time Charts indicate suspicious activity was high for “Reset Passwords” and “User account lockouts”.
 - a. Highest lock out peaked from 7-10PM on March 24
 - i. 896 incidents
 - b. Highest attempts to reset password peaked from 3-6 AM on March 25
 - i. 1258 highest

Attack Summary—Windows

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

- Alert set for “4726” -User Deleted threshold set for events greater than 10
 - Not a significant change-Threshold set correctly.
 - There was a slight uptick in deleted accounts On March 24 7-10PM Tuesday March 25th and another slight increase 2-3AM Wednesday March 25th.
- Alert set for An Account was successfully logged on. Peak was 196 Events
 - Set at threshold of 15.
 - Threshold set correctly as we would have received notification. Perhaps increasing it to reduce alert fatigue would be best action.

Attack Summary—Windows

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

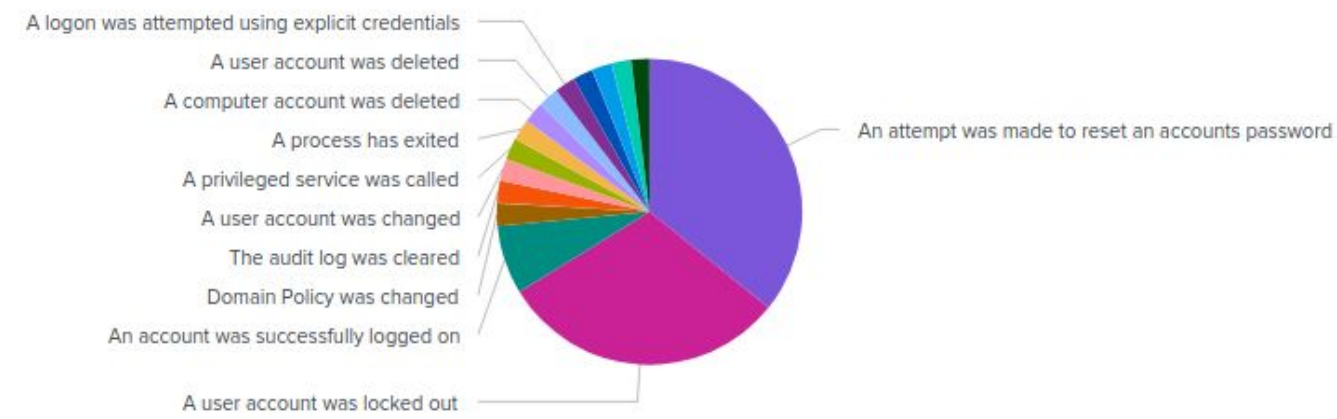
- There was suspicious activity noted in our signatures
 - “An Attempt was made to reset an account password”
 - 1258 highest volume
 - Attempts were at peak from 3-6am March 25th
 - “A user account was locked out”
 - 896 highest volume
 - Attempts were at peak from 7-10PM March 24th

Attack Summary—Windows

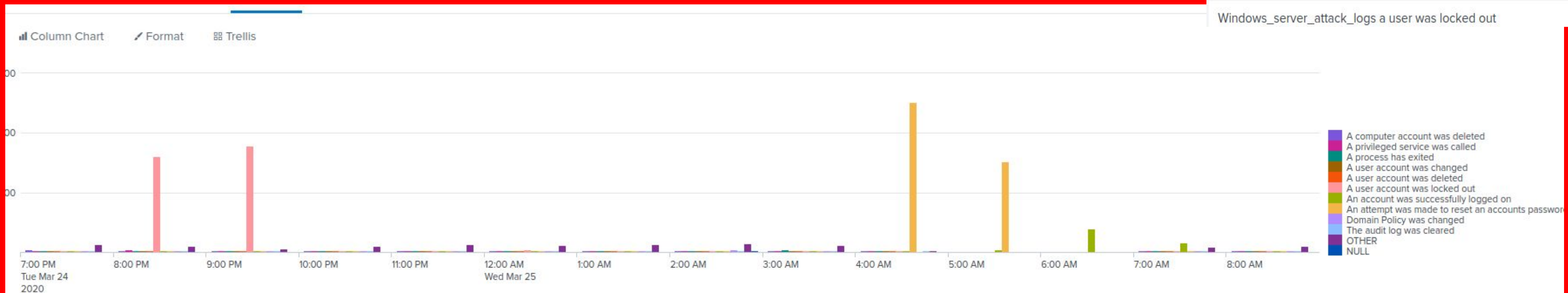
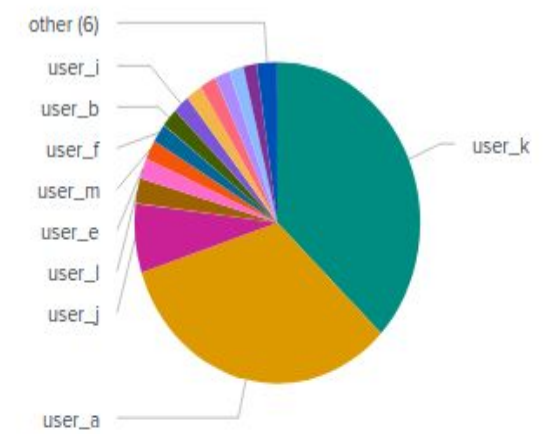
Summarize your findings from your dashboards when analyzing the attack logs.

- Two users show suspicious activity
 - User A Peak time was March 24th 7PM-10PM
 - 984 incidents
 - User K Peak time was March 25th 3AM-6AM
 - 1256 incidents

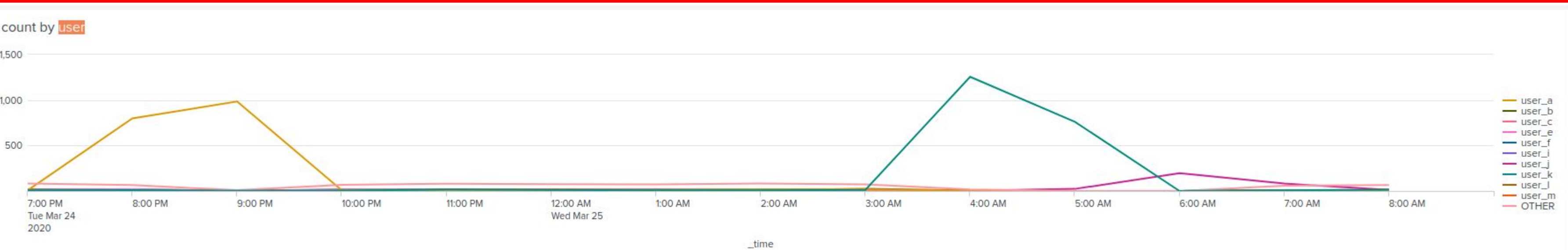
Screenshots of Attack Logs



top 20 users



Windows_server_attack_logs a user was locked out



Attack Logs												
_time %	A computer account was deleted %	A privileged service was called %	A process has exited %	A user account was changed %	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 password %	Domain Policy was changed %	The audit log was deleted %	OTHER %	NULL %
2020-03-24 19:00	19	14	8	10	14	16	11	18	10	12	68	0
2020-03-24 20:00	12	20	13	7	7	805	15	11	16	16	51	0
2020-03-24 21:00	9	3	16	9	5	856	14	3	17	8	27	0
2020-03-24 22:00	13	13	12	16	9	108	14	6	16	14	51	0
2020-03-24 23:00	12	18	8	11	14	12	12	11	10	16	63	0
2020-03-25 00:00	11	14	12	16	17	19	9	8	14	10	62	0
2020-03-25 01:00	9	14	12	17	13	3	11	14	8	13	64	0
2020-03-25 02:00	15	8	15	17	11	11	15	16	20	7	70	1
2020-03-25 03:00	17	13	23	11	11	16	16	12	11	16	59	0
2020-03-25 04:00	5	2	1	3	3	1	4	1258	0	4	12	0
2020-03-25 05:00	0	0	0	0	0	0	23	761	0	0	0	0
2020-03-25 06:00	0	0	0	0	0	0	196	0	0	0	0	0
2020-03-25 07:00	7	9	7	11	13	6	77	6	6	9	46	0
2020-03-25 08:00	4	8	7	9	13	16	15	12	15	17	48	0

Attack Analysis-Apache

Attack Summary—Apache

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

- For the report analysis of methods we found that there was a spike in GET from 6am to 7am with 729 and POST from 8pm to 9pm with 1,296
- For the report analysis for referrer domain we found that both `www.semicomplete.com` and `semicomplete.com` were the top two hits with counts of 764 and 572
- for the report analysis for HTTP response codes we found that a jump in status code 200 to 3,746 and in status code 404 to 679

Attack Summary—Apache

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

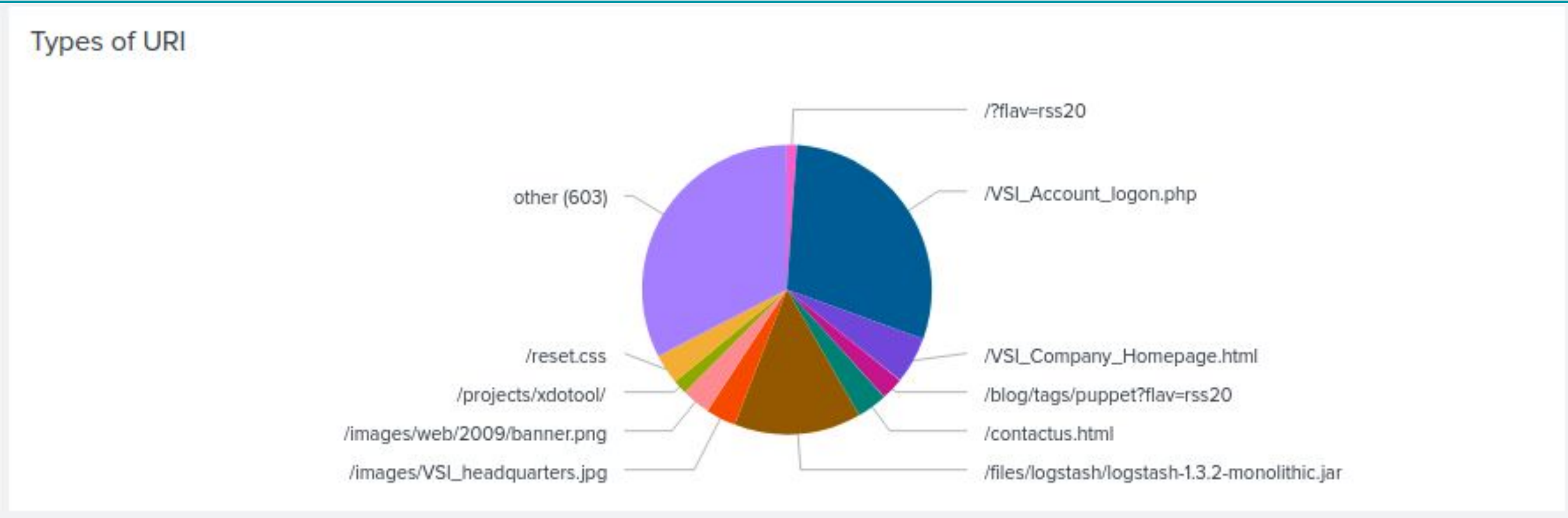
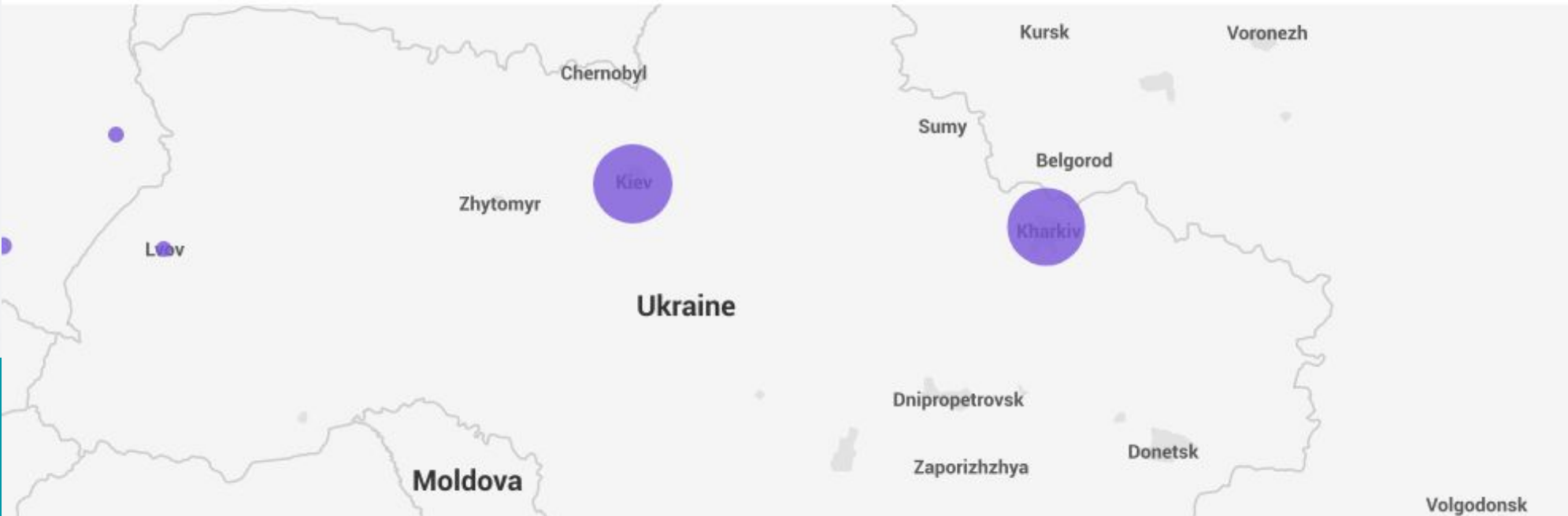
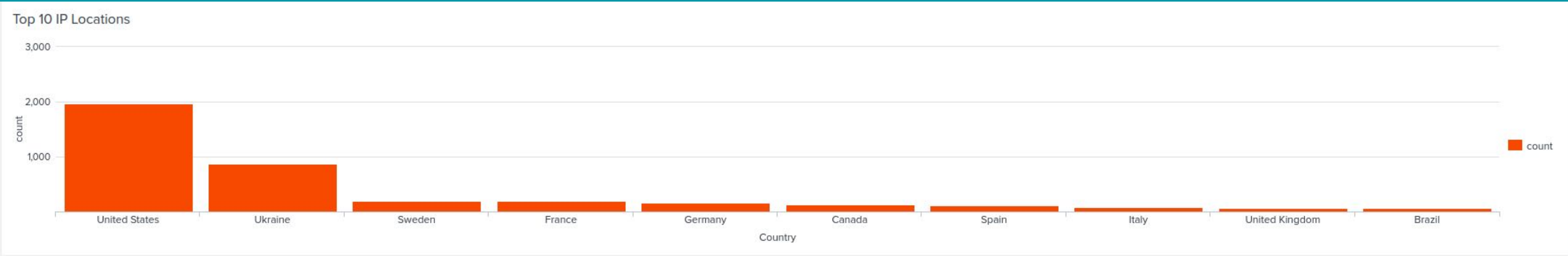
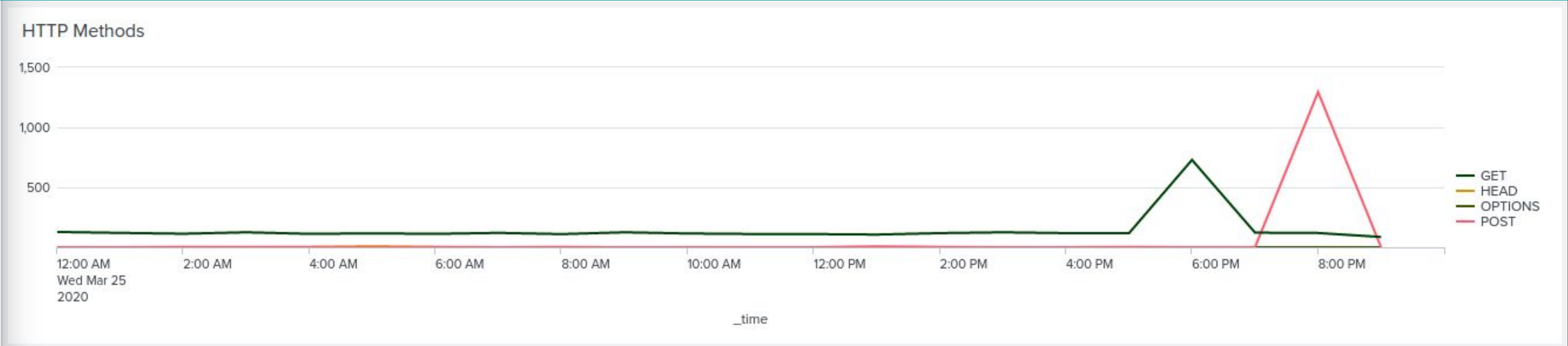
- Alert set for Hourly activity outside of the US, baseline: 90, threshold: 180
 - Yes, our threshold would have been set off by the attack and not by any other hour
- Alert set for HTTP Post activity, baseline: 2, threshold: 5
 - Our threshold would have been set off, but it would have also set off an alert at 1pm on March 25th. We could raised our threshold to about 10 to avoid false positives.

Attack Summary—Apache

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

- Time Chart of HTTP Methods: There was a spike in GETs at 6pm to 729 and a spike in POSTs at 8pm to 1,296
- Cluster Map of Logins: There was a spike of logins from Ukraine, Kiev and Kharkiv, to 877
- Top URI Pie Chart: The VSI_Account_logon.php page was the most used with a count of 1323, leading to believe that some kind of attack occurred on this page. Brute Force, Password Guessing, Command Injection, Local File Inclusion, XSS, SQL Injections, amongst others are all possibilities of the attack.

Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary & Mitigation

- Majority of attacks seem to be coming in from Ukraine.
- To protect VSI from future attacks - Additional security measure proposal:
 - To limit successful brute force attacks, implement increases security around credentials
 - Limit login attempts to 5
 - Increase password complexity with characters, numbers, letters.
 - Implement MFA and/or Captcha
 - Implement firewall rules
 - Block all traffic coming in from various countries
 - To limit XSS, File Inclusion, SQL Injections, and Command Injection
 - Input Validation
 - Output Encoding
 - Store Files in Database
 - Parameterized Queries
 - Server Side Validation