Defensive Security Project

by: DeLaun Robinson, Eric Ledesma, Jordan Saldivar, Kyler Dodak

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- As SOC analysts we were tasked with monitoring VSI’s systems and applications.
- We went through previous logs to design reports and got ideas for baselines for those alerts.
- We examined reports based on severity, success/failure, and id signatures. for windows logs and did the same for apache.
- We then built visualizations based off our previously designed reports.
- we then concluded with a general summary and what future mitigations we can implement to help keep the systems functioning.

“Add-On” App
Website Monitoring

Add-On App “Website Monitoring”

- This app is built to monitor websites to detect downtime and performance problems.
- This app has been configured to monitor the health of the VSI company website: https://vsi-corporation.azurewebsites.net

Website Monitoring

- JobeCorp, VSI’s adversary has been known to attack their competitors by defacing their web application. This web app is being used to monitor if the HTML has been modified.
- The Website Monitoring add-on can be used to monitor the severity and health of various logs.
- Various Features:
  - Uptime Calculation
  - Status Monitoring Dashboard
  - Email Outage Alerting
  - Change History Dashboard

Website Monitoring

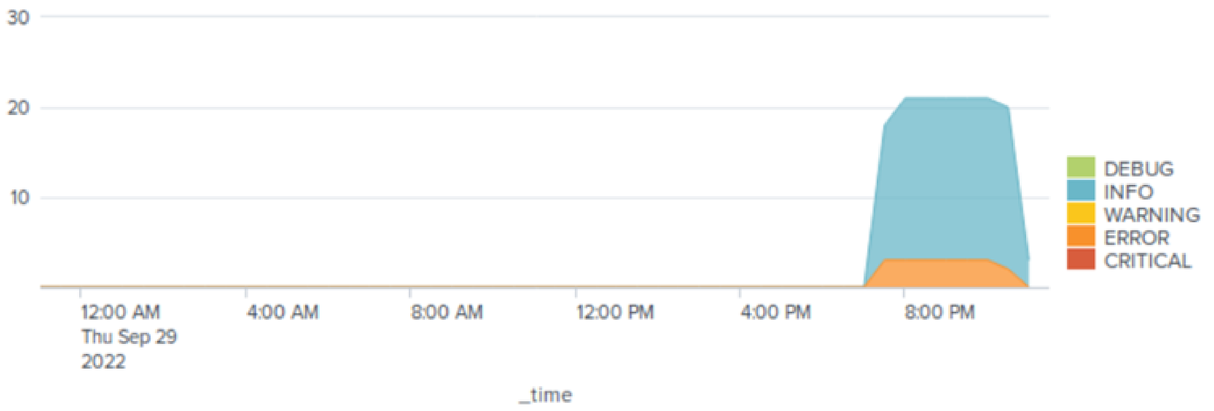
Status Overview

Edit | Export | ...

Last 24 hours | Include only enabl... | Submit | Hide Filters

title	url	response	last_checked	response_time	status	average	range	sparkline_response_time
vsi_corporation_azurewebsites_net_1	https://vsi-corporation.azurewebsites.net	✓ 200	1 minute ago	360 ms	OK	360 ms	360 - 360 ms	

Logs by Severity (over time)

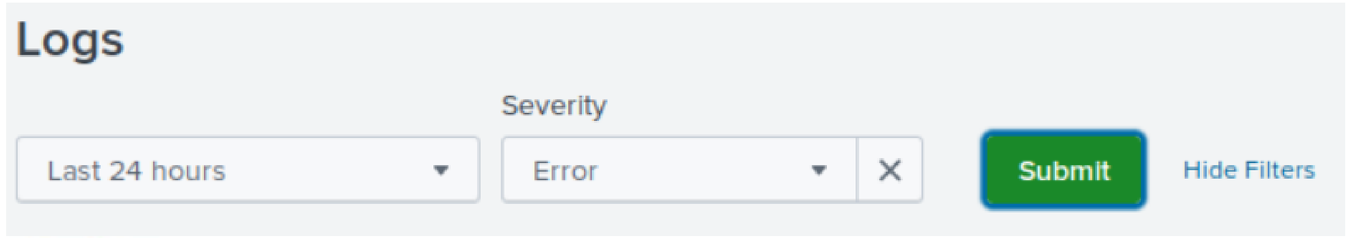


Logs by Severity

severity	sparkline	count
INFO		126
ERROR		20

Website Monitoring

Logs can be filtered by Debug, Info, Warning, Error, or Critical



Latest Logs

time	severity	message
09/29/2022 23:09:24.306	INFO	Removed inactive threads, thread_count=0, removed_thread_count=1
09/29/2022 23:09:19.315	INFO	Performing ping, url="https://vsi-corporation.azurewebsites.net" timeout=30
09/29/2022 23:09:19.300	INFO	Added thread to the queue for stanza=web_ping://vsi_corporation_azurewebsites_net_1, thread_count=1
09/29/2022 22:59:22.927	INFO	Removed inactive threads, thread_count=0, removed_thread_count=1
09/29/2022 22:59:17.933	INFO	Performing ping, url="https://vsi-corporation.azurewebsites.net" timeout=30
09/29/2022 22:59:17.919	INFO	Added thread to the queue for stanza=web_ping://vsi_corporation_azurewebsites_net_1, thread_count=1
09/29/2022 22:52:17.322	INFO	Removed inactive threads, thread_count=0, removed_thread_count=1
09/29/2022 22:52:13.399	INFO	Performing ping, url="https://vsi-corporation.azurewebsites.net/" timeout=30
09/29/2022 22:52:12.318	INFO	Added thread to the queue for stanza=web_ping://vsi_corporation_azurewebsites_net, thread_count=1
09/29/2022 22:49:37.154	INFO	Removed inactive threads, thread_count=0, removed_thread_count=1

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Logs Analyzed

1 Windows Logs

Windows Server Logs that are representative of normal activity for Virtual Space Industries (VSI). The server is supposed to contain intellectual property of VSI's next-generation virtual-reality programs.

2 Apache Logs

Apache Server Logs that are representative of normal activity for Virtual Space Industries (VSI). The server is used for VSI's main public-facing website, vsi-company.com

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signature Report	This report shows the ID number associated with the specific signatures.
Severity Level Report	This report shows the severity levels (informational and high) as well as the count and percentage of each.
Success/Failure Report	This report shows the success and failure of Windows activities.

Images of Reports—Windows

› Signature_Table

Edit ▾ Explore ▾

All time ▾

✓ **15 events** (before 9/27/22 11:36:17.000 PM)

Job ▾ Rows Summary

20 per page ▾

	_time	host	signature	signature_id	source	sourcetype	_raw
1	2020-03-24T23:59:54.000Z	Windows_server_logs	A user account was deleted	4726	windows_server_logs.csv	csv	2020-03-24T23:59:54.000+0000,,"Domain_A Domain_A",,"user_f user_1",,,,,,,,,,,,,,Account Management,,,,,,,ACME-002,,,,,,,,-,4726,A user account was deleted,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A user account was deleted. Subject: Security ID: Domain_A\user_f Account Name ...More
2	2020-03-24T23:59:53.000Z	Windows_server_logs	A user account was created	4720	windows_server_logs.csv	csv	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,,,,,,-,4720,A user account was created,0,,,,,,,\a\g,A:,,,,,,Audit Success,,,,,Security,,,,All,0xBAC3,,,,"SAM Account Name: user_h Display ...More
3	2020-03-24T23:59:31.000Z	Windows_server_logs	A computer account was deleted	4743	windows_server_logs.csv	csv	2020-03-24T23:59:31.000+0000,,"Domain_A Domain_A",,"user_1 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_A\user_1 Acco ...More
4	2020-03-24T23:57:54.000Z	Windows_server_logs	An account was successfully logged on	4624	windows_server_logs.csv	csv	2020-03-24T23:57:54.000+0000,,"Domain_A Domain_A",,"ACME-002 user_e",,,,,,Negotiate,,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An account was successfully
5	2020-03-24T23:57:51.000Z	Windows_server_logs	Special privileges assigned to new logon	4672	windows_server_logs.csv	csv	2020-03-24T23:57:51.000+0000,,Domain_A,,user_c,,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4672,Special privileges assigned to new logon,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x5FC9,,,,,,,,,"Special privileges assigned to new logon. Subject: Security ID: Domain_A\user_c Account Name: user_c ...More
6	2020-03-24T23:56:41.000Z	Windows_server_logs	An attempt was made to reset an accounts password	4724	windows_server_logs.csv	csv	2020-03-24T23:56:41.000+0000,,"Domain_A Domain_A",,"user_a user_d",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,Audit Failure,,,,,Security,,,,,0x6C10,,,,,,,,,"An attempt was made to reset an account's password. Subject ...More
7	2020-03-24T23:56:40.000Z	Windows_server_logs	System security access was granted to an account	4717	windows_server_logs.csv	csv	2020-03-24T23:56:40.000+0000,SeRemoteInteractiveLogonRight,Domain_A,,"ACME-002 Domain_A\user_b",,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4717,System security access was granted to an account,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x3A81,,,,,,,,,"System security access was granted to an account. ...More
8	2020-03-24T23:54:46.000Z	Windows_server_logs	A privileged service was called	4673	windows_server_logs.csv	csv	2020-03-24T23:54:46.000+0000,,Domain_A,,user_f,,,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4673,A privileged service was called,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0xA369,,,,,,,,,"A privileged service was called. Subject: Security ID: Domain_A\user_f Account Name: user_f Account Domain: ...More
9	2020-03-24T23:54:42.000Z	Windows_server_logs	A logon was attempted using explicit credentials	4648	windows_server_logs.csv	csv	2020-03-24T23:54:42.000+0000,,"Domain_A Domain_A",,"ACME-002 jevysworld",,dcab.acmbh.com,,,,,,,,,,,,,,,,,,,ACME-002,,,,,,,,-,4648,A logon was attempted using explicit credentials,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,"{27C4A2F2-13CA-AA25-E903-D31268740239} {00000000-0000-0000-0000-00000000000 ...More
10	2020-03-24T23:54:39.000Z	Windows_server_logs	A user account was locked out	4740	windows_server_logs.csv	csv	2020-03-24T23:54:39.000+0000,,Domain_A,,"user_d user_d",,,,,,,ACME-002,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4740,A user account was locked out,0,,,,,,,,,,,,,,Audit Success,,,,,Security,,,,,0x3EC3,,,,,,,,,"A user account was locked out. Subject:

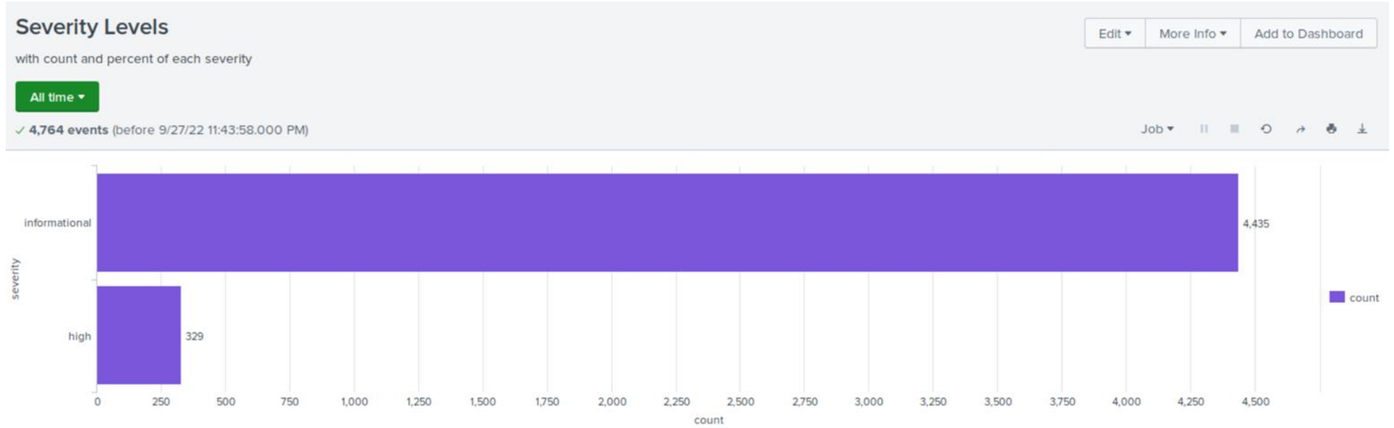
Signature IDs

```
source="windows_server_logs.csv" | dedup signature
```

✓ **15 events** (before 9/27/22 11:36:17.000 PM) No Event Sampling ▾

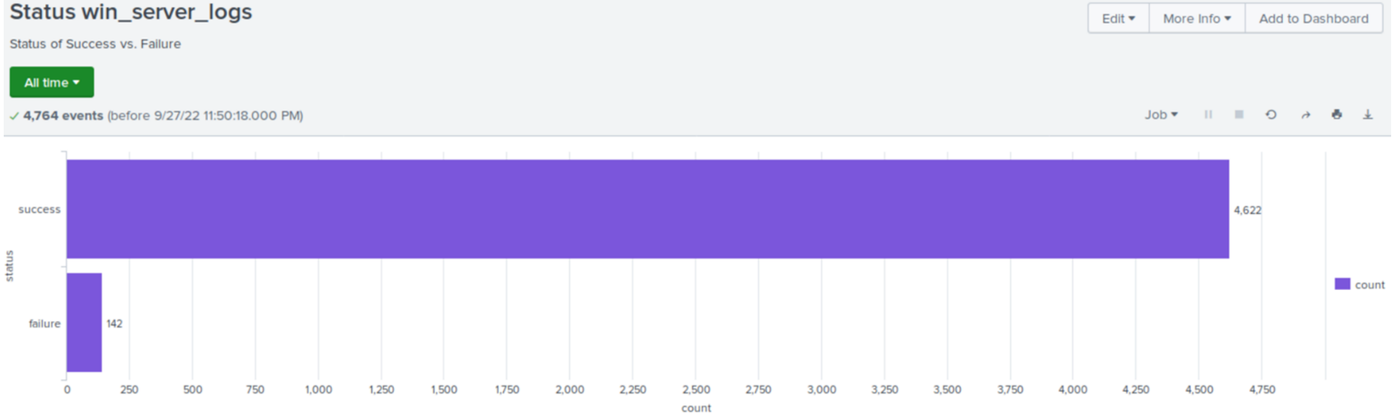
The signature table is showing part a list that organizes signatures with their corresponding ID.

Images of Reports—Windows



2 results 100 per page

severity	count	percent
informational	4435	93.094039
high	329	6.905961



2 results 100 per page

status	count	percent
success	4622	97.019312
failure	142	2.980688

The top graph shows the difference in severity levels currently in use by the windows server. The bottom graph shows the difference in successes and failures in the windows server activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity Alert	An alert to bring attention to a high hourly failure rate	0-10	15

JUSTIFICATION: The baseline was determined based off of the activity of the events on 03/24/20 as they did not exceed 10 on a hour by hour basis. The threshold was determined with a margin of error to be 15, as anything at this point or beyond should be reviewed.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Log-Ins	An alert to notify of a unusually high number of logins within and hour	0-20	30

JUSTIFICATION: The baseline was determined based off of the activity of the events on 03/24/20 as they did not exceed 18 on a hour by hour basis. The threshold was determined with a margin of error to be 30, as anything at this point or beyond should be reviewed.

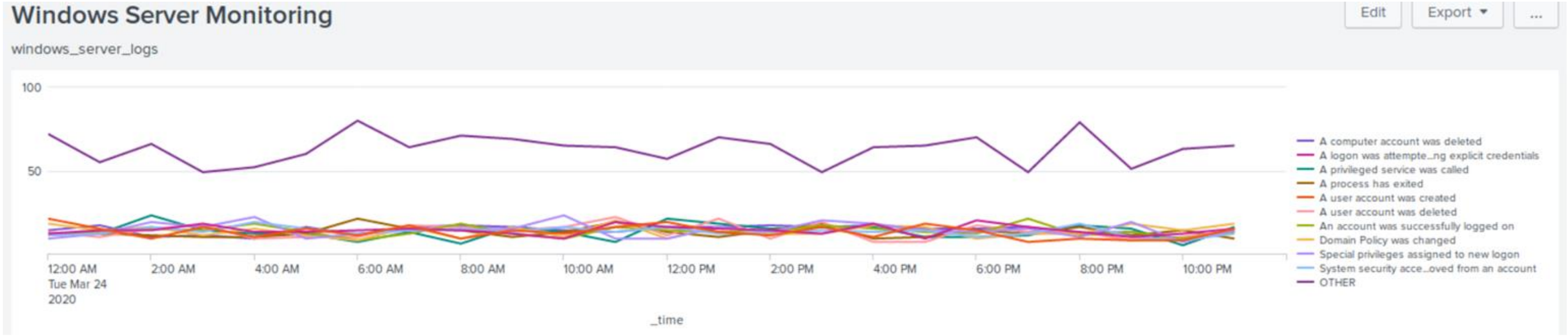
Alerts—Windows

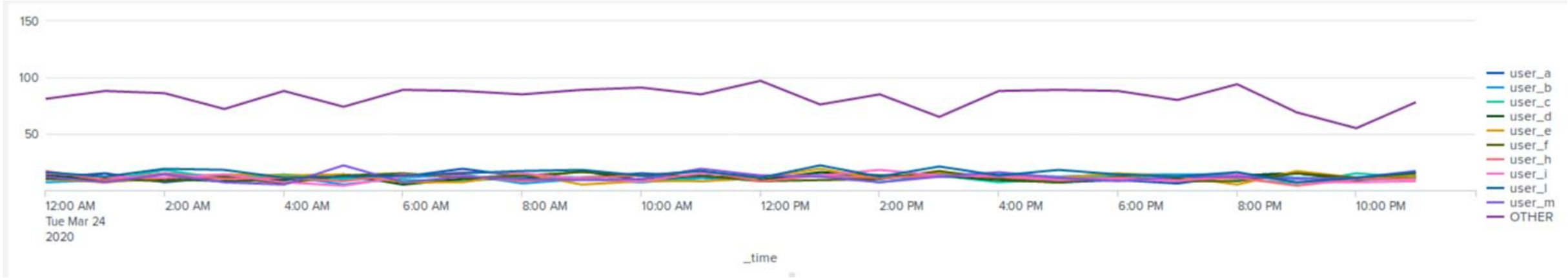
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted	An alert of an unusually high number of user accounts that have been deleted within an hour	0-25	30

JUSTIFICATION: The baseline was determined based off of the activity of the events on 03/24/20 as they did not exceed 22 on a hour by hour basis. The threshold was determined with a margin of error to be 30, as anything at this point or beyond should be reviewed.

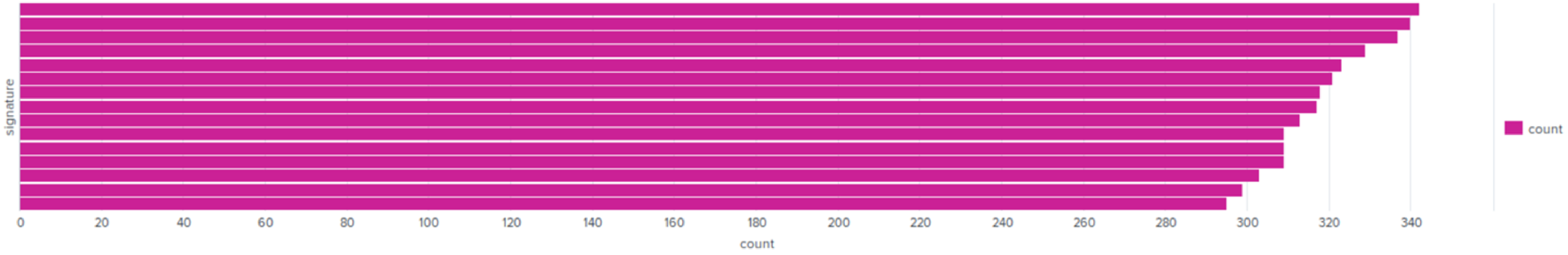
Dashboards—Windows

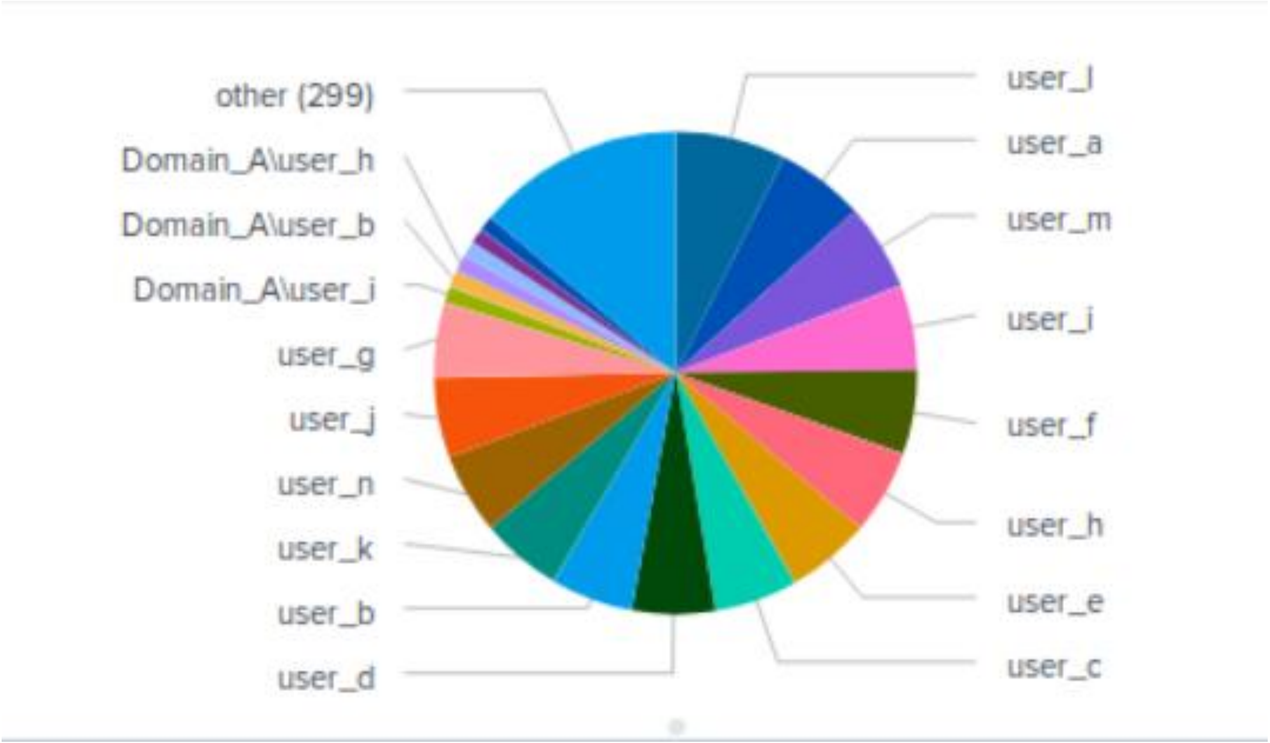




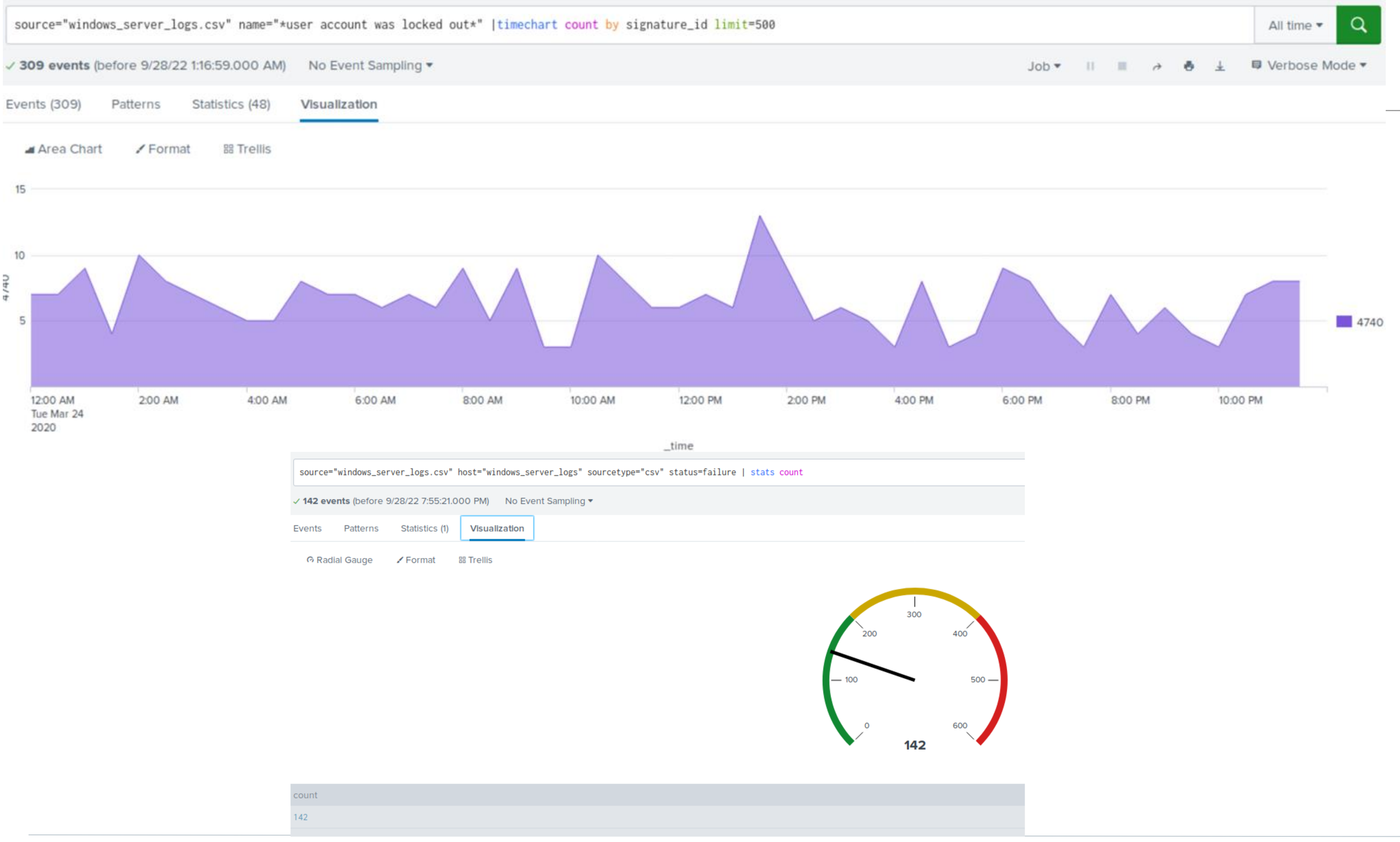
Top: Line Chart displaying the different "signature" field values over time. **Bottom**: Line Chart that displays the different "user" field values over time.

Dashboards—Windows





Two separate charts illustrating the count of different users.



Top: Chart displaying count over time of user account locked out. Bottom: Radial gauge displaying count of failures in report.

Apache Logs

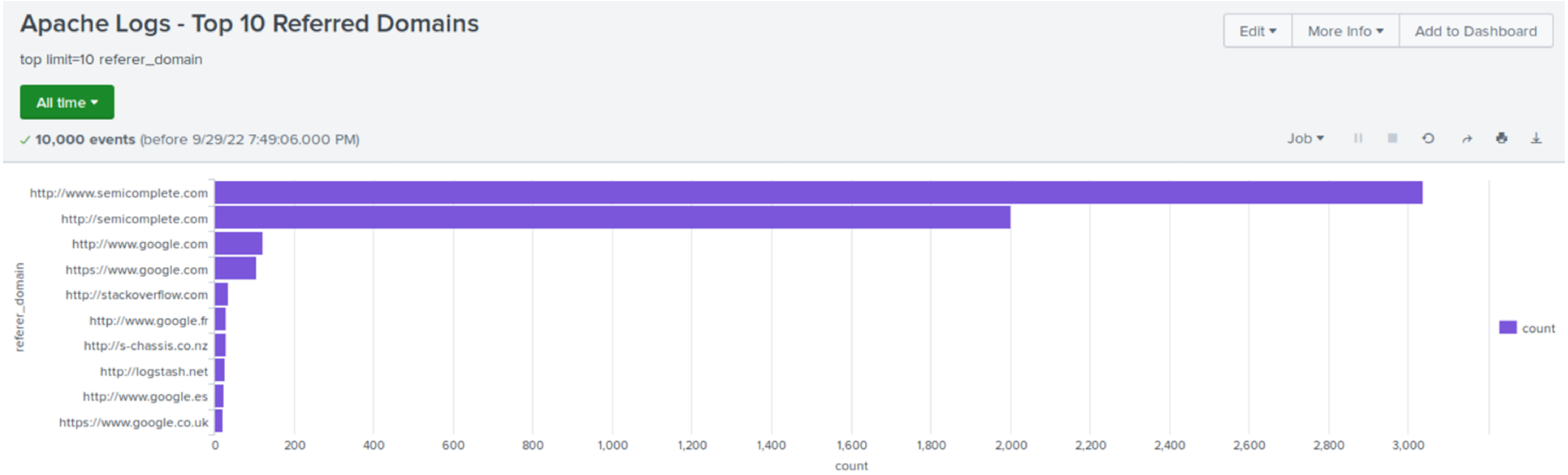
Reports—Apache

We designed the following reports:

Report Name	Report Description
HTTP Methods	This report shows the different HTTP methods used.
Response Codes	This report shows the count of each HTTP response codes.
Top 10 Referred Domains	This report shows the top 10 domains that refer to VSI’s website.

Images of Reports—Apache

Images of Reports—Apache



Images of Reports—Apache

Apache Logs - Response Codes

200-500 response code count

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **10,000 events** (before 9/30/22 12:29:24.000 AM)

Job ▾

8 results 100 per page ▾

status	Count of 1664472632.1979
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Threshold: Hourly Activity Outside the USA	The threshold for activity from any country outside of the USA has been reached.	—	—

JUSTIFICATION: We were not able to set up this alert.

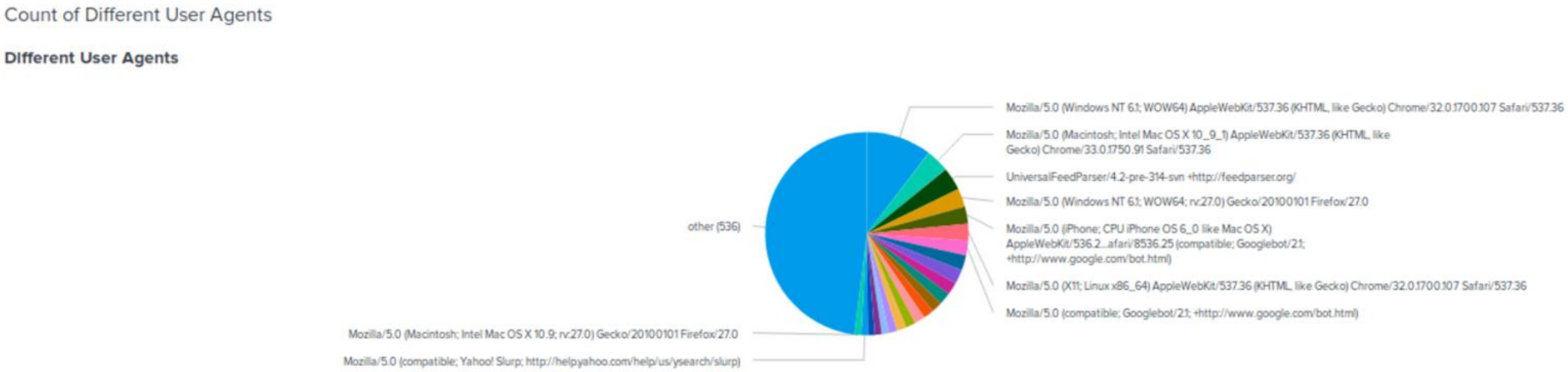
Alerts—Apache

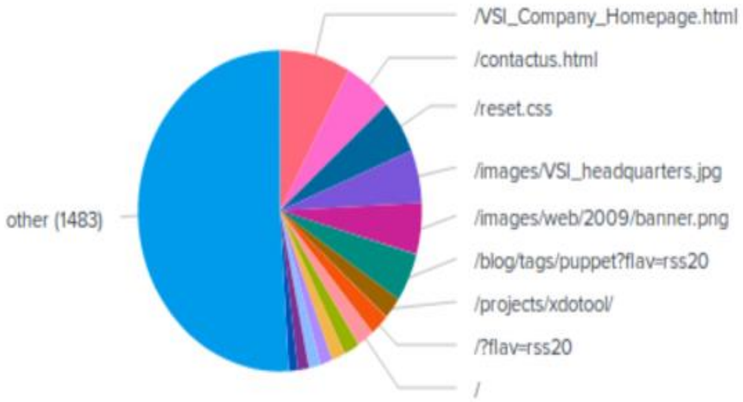
Designed the following alerts:

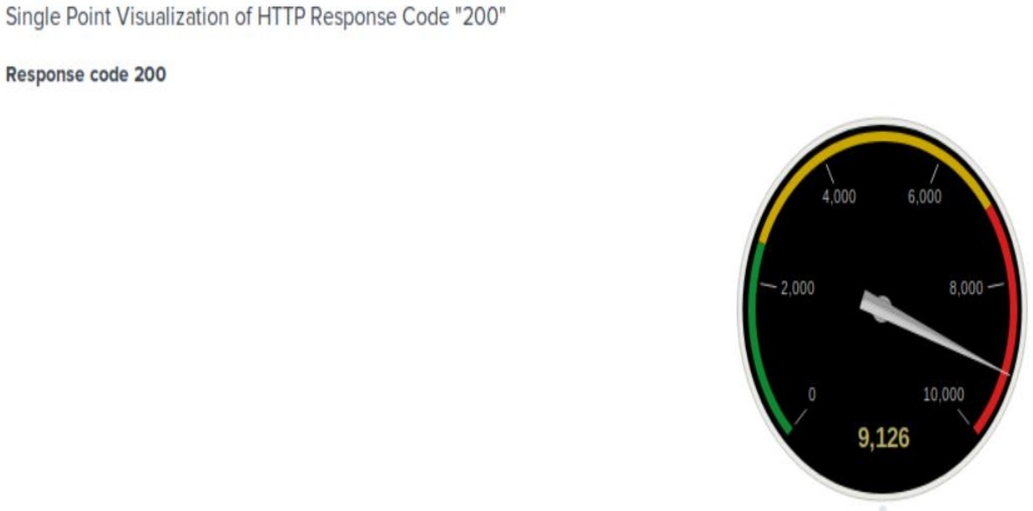
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Threshold: Hourly Count of HTTP POST method	The threshold for HTTP POST methods has been reached.	0-14	25

JUSTIFICATION: Analysing the data at per hour, a median of the HTTP POST method comes out to around 14. According to current records, the maximum number HTTP POST has reached is 23.

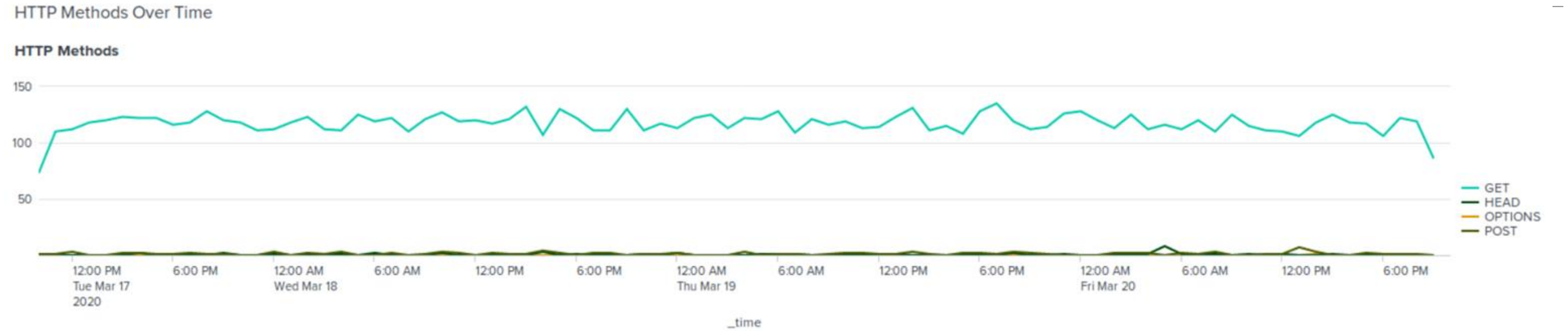
Dashboards—Apache







Dashboards—Apache



Top: Line Graph displaying different HTTP Methods Over time. **Bottom:** Geographical Map showing Location based on "clientip" field.

Attack Analysis

Attack Summary—Windows

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

- The reports from analyzing the attack logs seemed to be too much of high level overviews to see anything obviously wrong. Without looking into anything further, it would be easy to overlook as the failure rate total was lower during the attack than a normal day. However, there was a noticeable increase in “high” severity changes.

Attack Summary—Windows

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

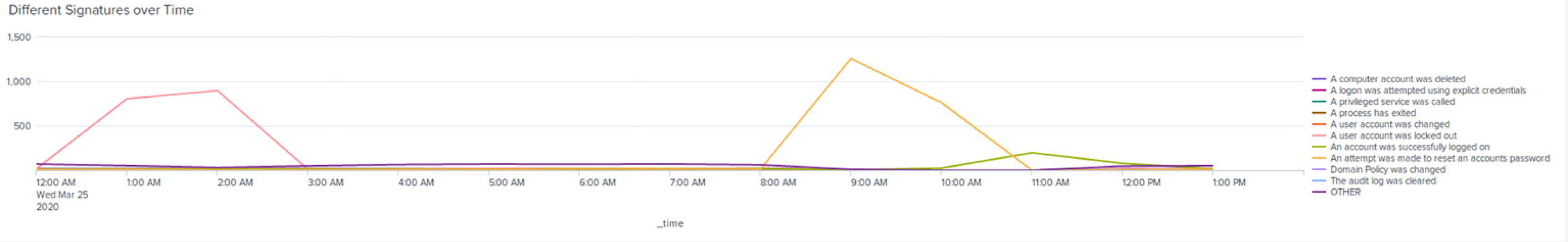
- Looking at the windows alerts, it was beginning to be easier to see more glaring issues that occurred on the specified dates. Users a and k seemed to be the culprits and the thresholds for the alerts we had in place would have been sufficient. Alert emails would have been sent out to the proper people.

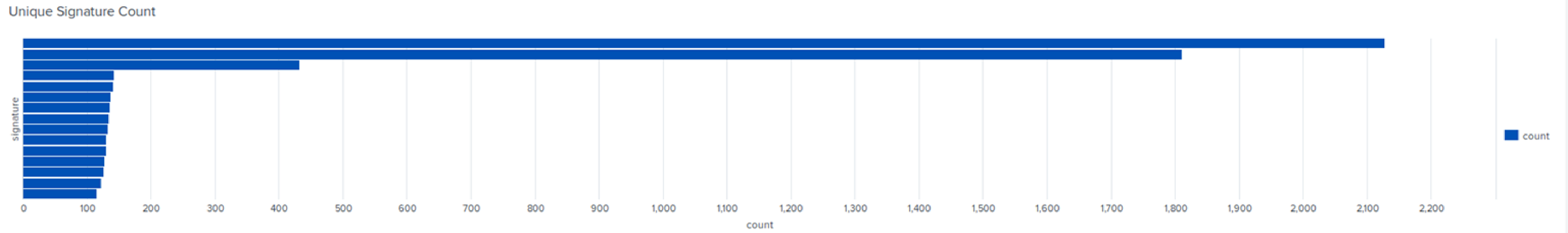
Attack Summary—Windows

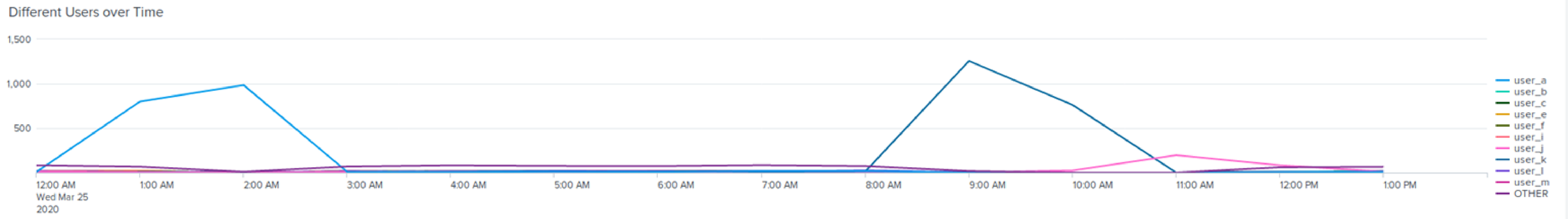
Summarize your findings from your dashboards when analyzing the attack logs.

- After analyzing the dashboards, it was much more obvious to see that users a and k we’re most likely working in tandem to brute force attack logins and then a few hours later change the passwords. The screenshots on the next slide provide evidence to this theory. The dashboard definitely makes it easier to see the event as a whole.

Screenshots of Attack Logs







Attack Summary—Apache

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

- Again, the reports are a bit too broad to pick up on an obvious attack information, however, we did find that there were way more HTTP POST methods.

Attack Summary—Apache

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

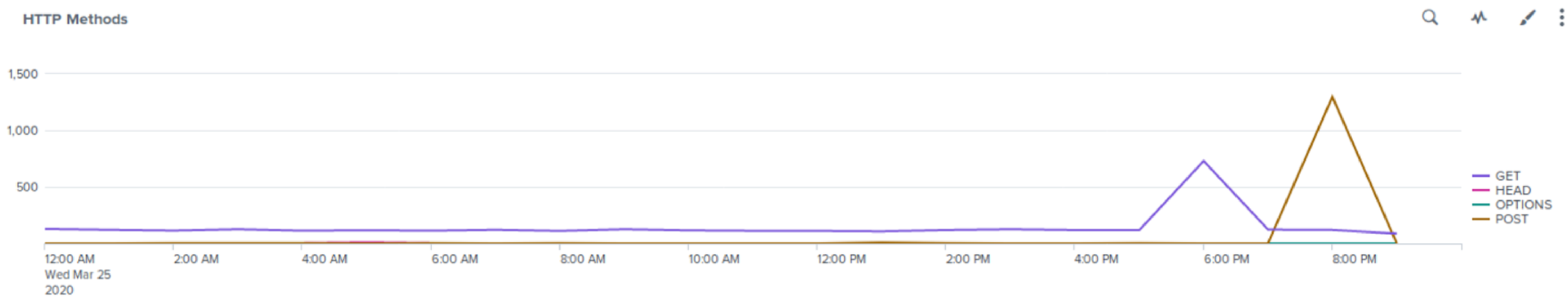
- The alert for Hourly Activity Outside the USA we did not get to work correctly, so unfortunately, we don’t have thresholds or baselines for that.
- Our baseline and threshold were properly set for the HTTP POST method.

Attack Summary—Apache

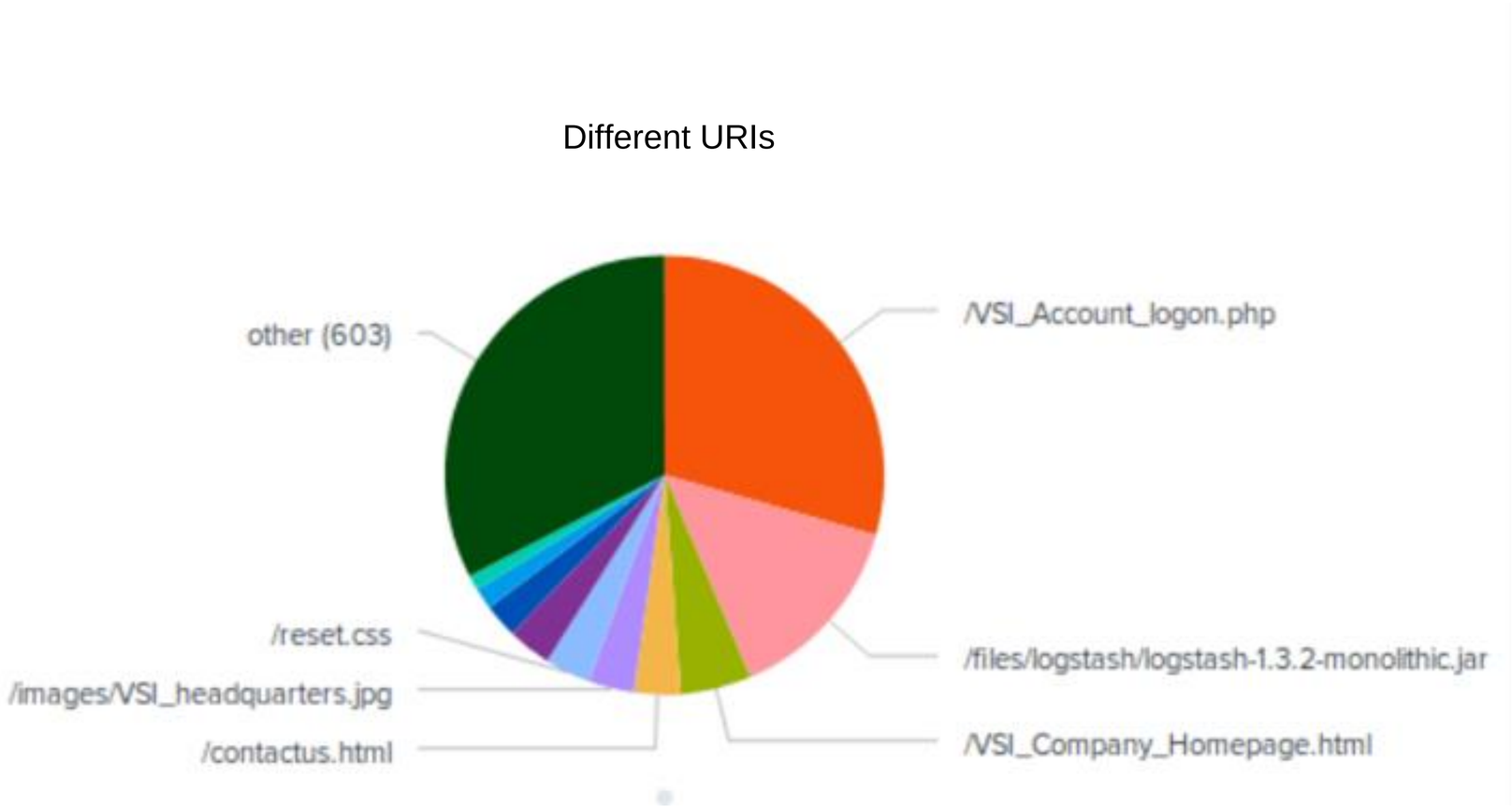
Summarize your findings from your dashboards when analyzing the attack logs.

- The HTTP POST method spikes significantly in one hour - 8PM.
- The Geomap indicates the attack was from Ukraine.
- Looking at the Different URI chart, it clearly indicates the attack is brute force. The /VSI_Account_logon.php page has an unusual large spike in activity.

Screenshots of Attack Logs



Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?

  Brute Force attacks were attempted from outside of the USA, most likely from Ukraine.

- To protect VSI from future attacks, what future mitigations would you recommend?

  We would recommend a Web Application Firewall to automatically block or drop incoming suspicious activities - including brute force attacks. A WAF can also be configured to filter out traffic from outside of the USA.