Virtual Space Industries Defensive Security Project

by: Rachel Harris & Yesenia Morales

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Our team sought to create a monitoring solution to protect Virtual Space Industries' (VSI) digital assets.

An administrative webpage:

https://vsi-corporation.azurewebsites.net/.

An Apache web server which hosts this webpage.

A Windows operating system which runs many of VSI's back-end operations.

Scenario

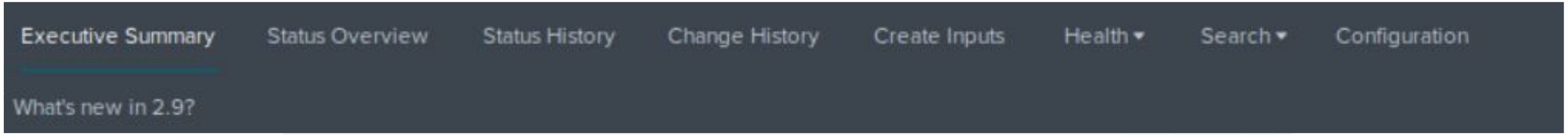
- Our team sought to create a monitoring solution to protect Virtual Space Industries (VSI) digital assets.
  - Monitoring solution consisted of:
    - Windows and Apache log analysis scrutinizing
      - Windows OS: Signature IDs, Account Severity Levels and Success and Failure of Windows Activity
      - Apache Server: HTTP Methods, Referrer Domains and HTTP Response Codes
    - Baseline determination
    - Custom Report, Alert and Dashboard creation for Windows and Apache data
  - Attack Analysis and Interpretation

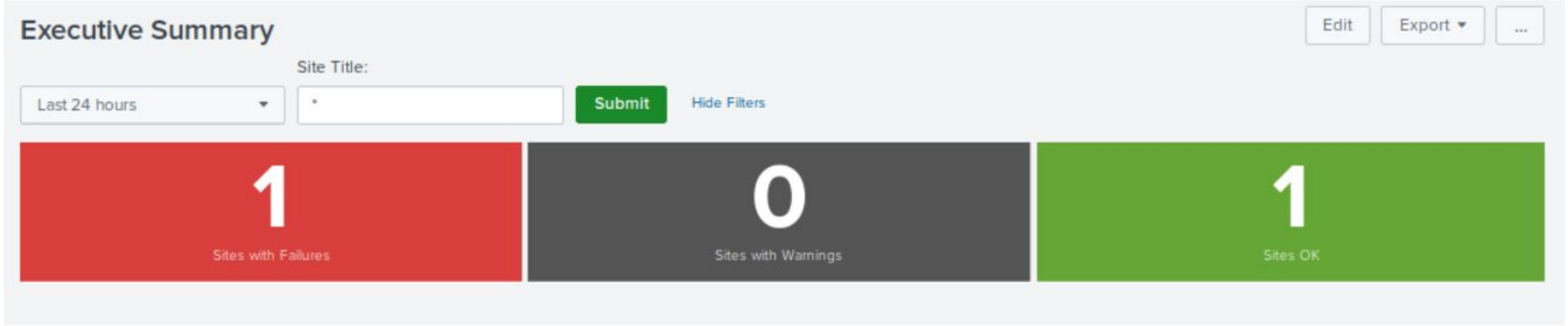
Website Monitoring Add-on

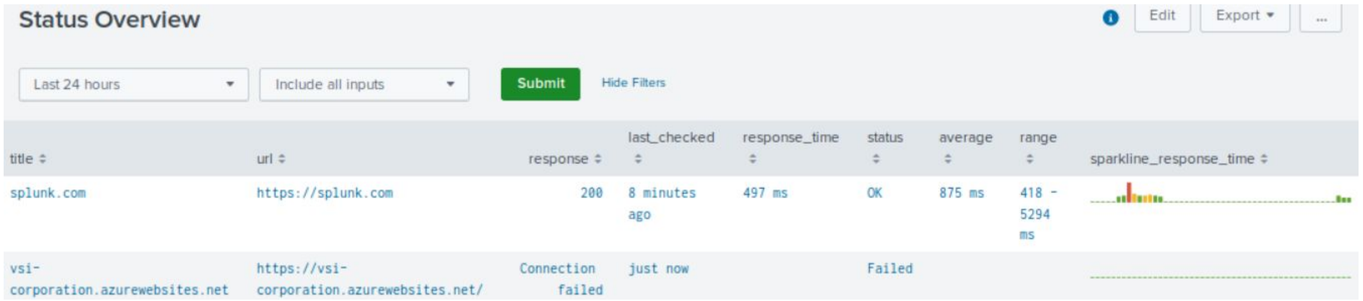
Website Monitoring

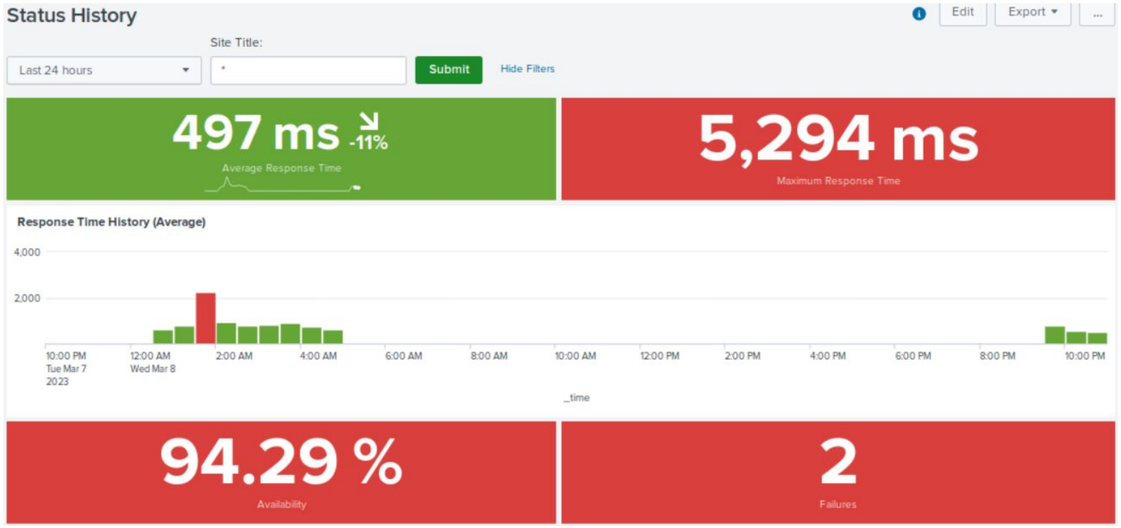
- Detects downtime and performance problems.
- Modular input that can be setup easily (in 5 minutes or less)
- Was developed by a developer named Luke Murphey
- Status Monitoring Dashboard: provides the response time for your monitored websites and provides a historical analysis of the site's responsiveness
- Change History Dashboard: provides information regarding when the monitored pages changed

Website Monitoring

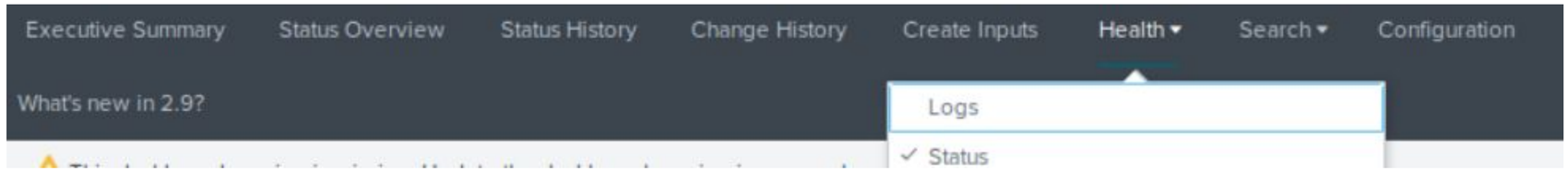








Website Monitoring



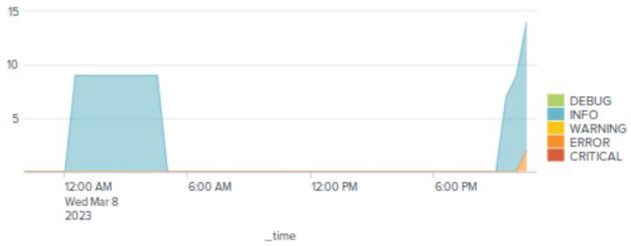
Logs

Edit Export ...

Severity

Last 24 hours | Informational (or above) | Submit | Hide Filters

Logs by Severity (over time)



Logs by Severity

severity	sparkline	count
INFO		109
ERROR		2

Latest Logs

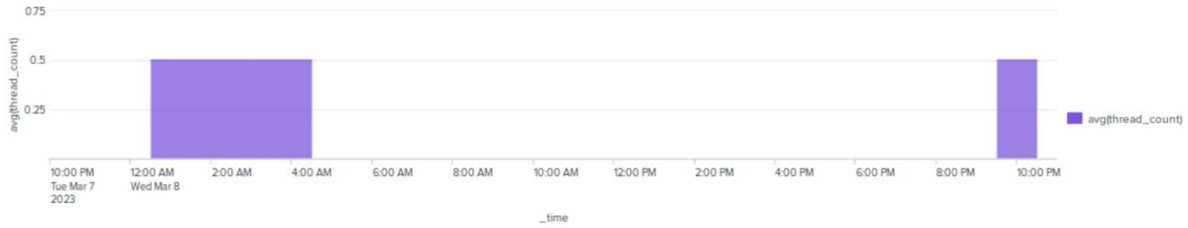
time	severity	message
03/08/2023 22:46:44.015	INFO	Removed inactive threads, thread_count=0, removed_thread_count=1
03/08/2023 22:46:40.000	INFO	Performing ping, url="https://splunk.com" timeout=30
03/08/2023 22:46:39.009	INFO	Added thread to the queue for stanza=web_ping://splunk_com, thread_count=1
03/08/2023 22:44:48.687	INFO	Removed inactive threads, thread_count=0, removed_thread_count=1
03/08/2023 22:44:44.622	ERROR	A connection exception was thrown when executing a web request against url=https://vsi-corporation.azurewebsites.net/, this can happen if the domain name, IP address is invalid or if network connectivity is down or blocked by a firewall; see help_url=http://lukemurphey.net

Status

Edit Export ...

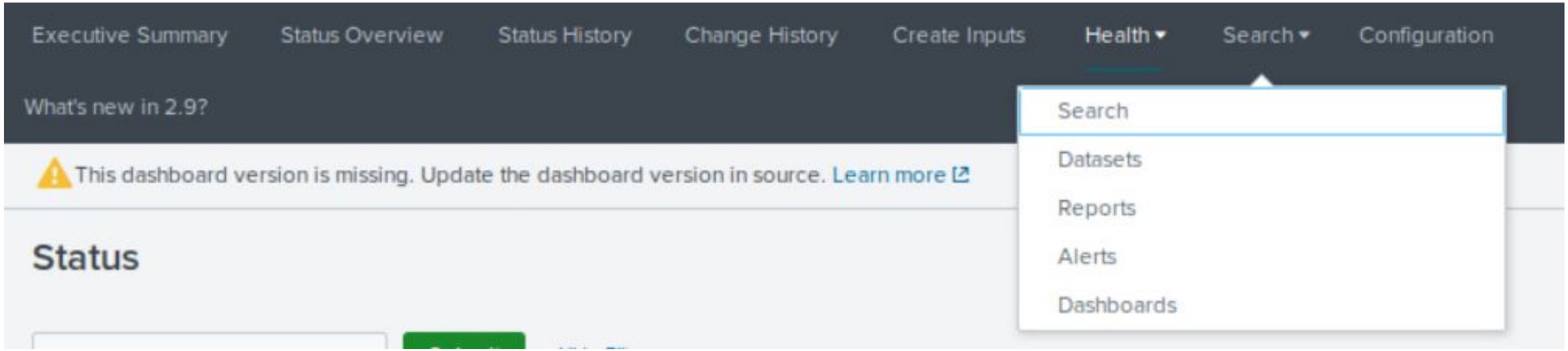
Last 24 hours | Submit | Hide Filters

Executing Threads



Results

Website Monitoring



Logs Analyzed

1 Windows Logs

- Windows Logs contained user and user account data
- Logs were created to view and monitor:
  - Account Signature Data
  - Severity Levels
  - Success and Failure of Windows Activities

2 Apache Logs

- Apache Logs contained HTTP methods and activity
- IP locations and addresses
  - Countries
- Response codes

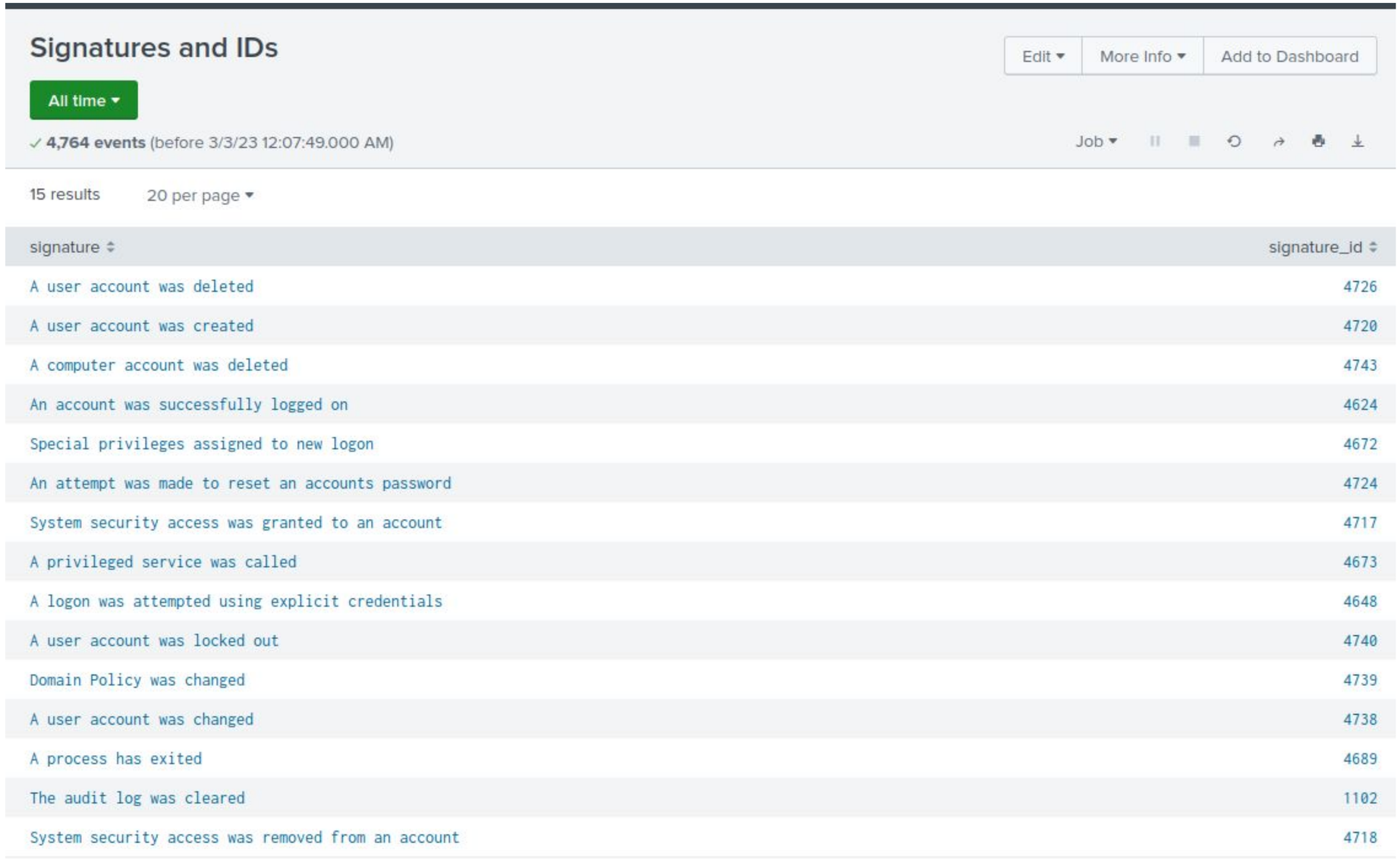
Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signatures & Signature IDs	A report allowing VSI to view and display the ID number associated with the specific signature for Windows activity.
Severity Levels	A report allowing VSI to quickly understand the severity levels of the windows logs being viewed.
Success & Failure of Windows Activities	A report allowing VSI to view whether a suspicious level of failed activities has occurred on the server.

Images of Reports—Windows



Signatures and IDs

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 3/3/23 12:07:49.000 AM)

Job ▾

15 results | 20 per page ▾

signature ⇕	signature_id ⇕
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718

Images of Reports—Windows

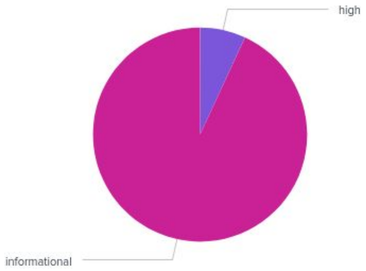
Severity Levels

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 3/3/23 12:37:15.000 AM)

Job ▾



2 results 20 per page ▾

severity	count	perc
high	329	6.91
informational	4435	93.09

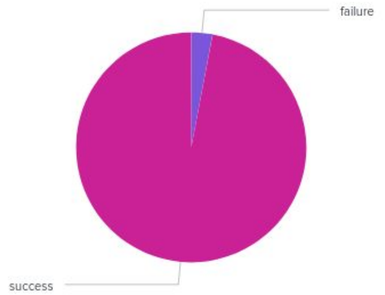
Successes vs Failures

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 3/3/23 12:48:38.000 AM)

Job ▾



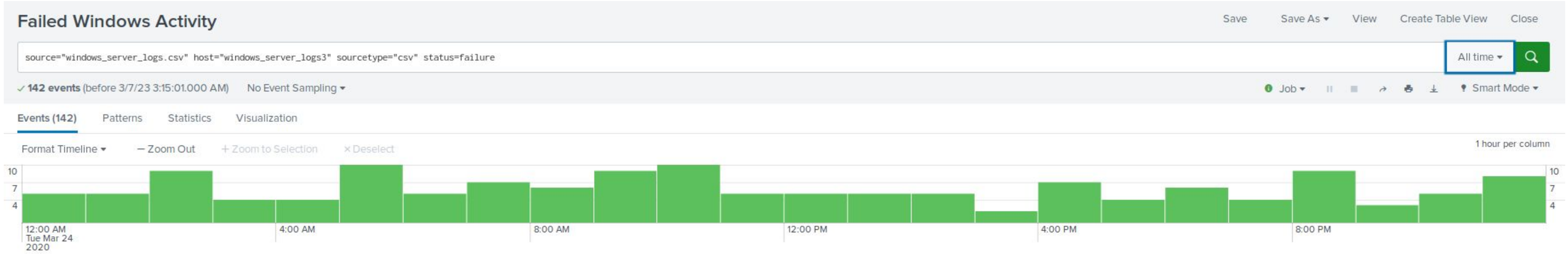
2 results 20 per page ▾

status	count
failure	142
success	4622

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	An alert that notifies on results of failed Windows activity on an hourly basis	6 failed events	>7 failed events



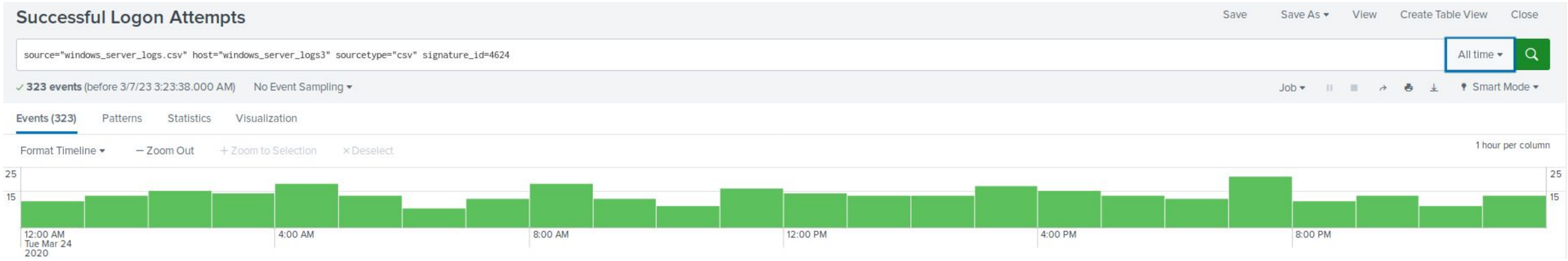
<u>JUSTIFICATION</u>:

- **Baseline was set based upon a total of 142 failed events (all time) with an average number of failures per hour = 6 failed events.**

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logon Attempts	An alert that notifies on results of successful logon attempts (based on corresponding signature ID and hourly basis)	13 successful attempts	>16 successful attempts

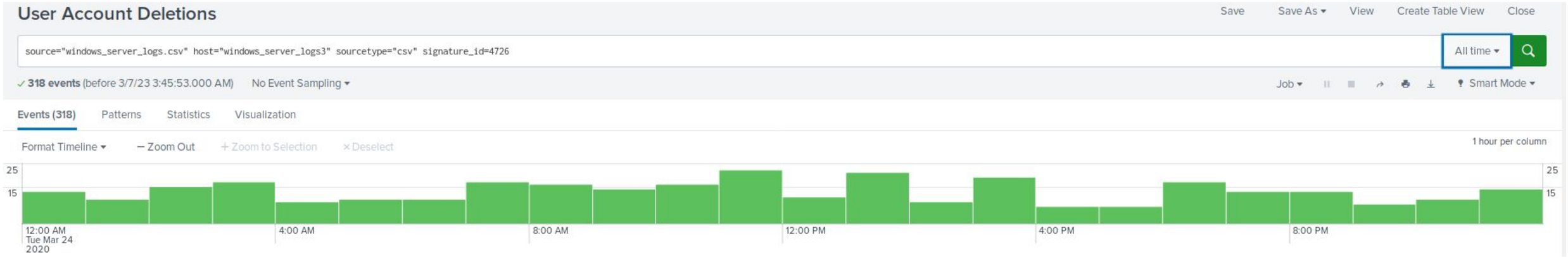


<u>JUSTIFICATION</u>: Baseline was set based upon a total of 323 successful attempts (all time) with an average number of successful attempts per hour = 13 attempts.

Alerts—Windows

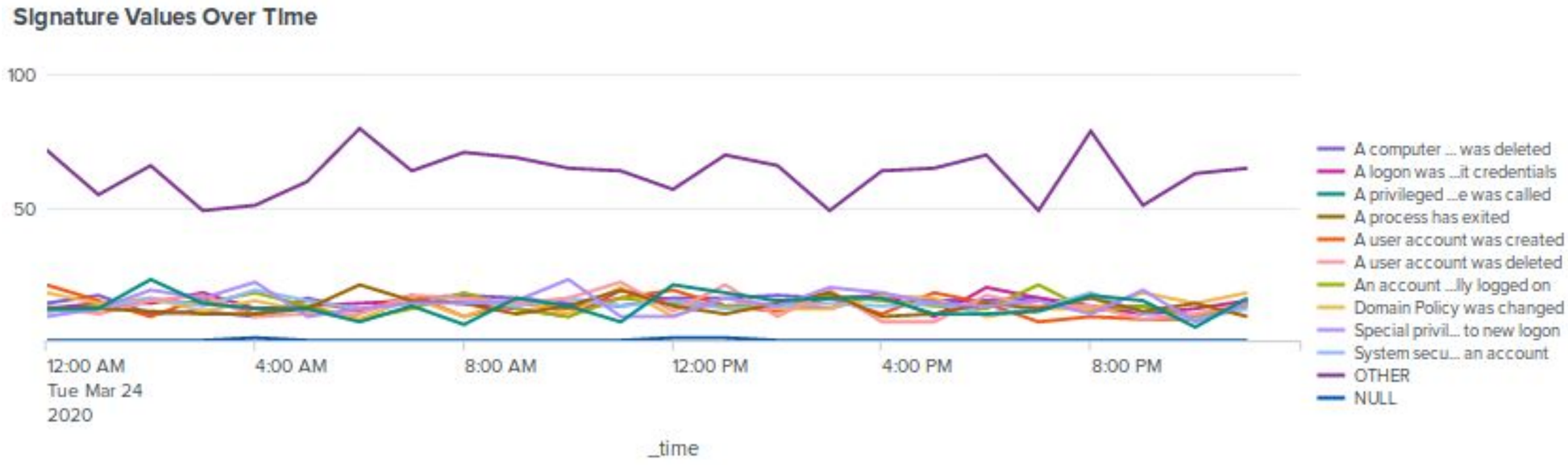
Designed the following alerts:

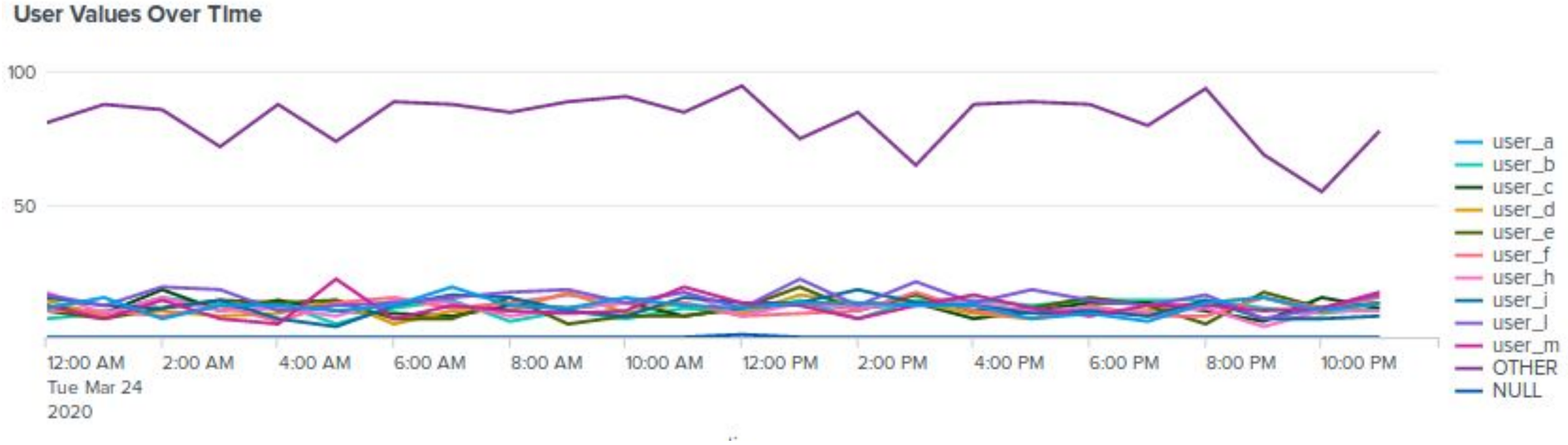
Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deletions	An alert that notifies on results of how many user accounts are being deleted on an hourly basis	13 account deletions	>15 account deletions



<u>JUSTIFICATION</u>: Baseline was set based upon a total of 318 account deletions (all time) with an average number of account deletions per hour = 13 deletions.

Dashboards—Windows

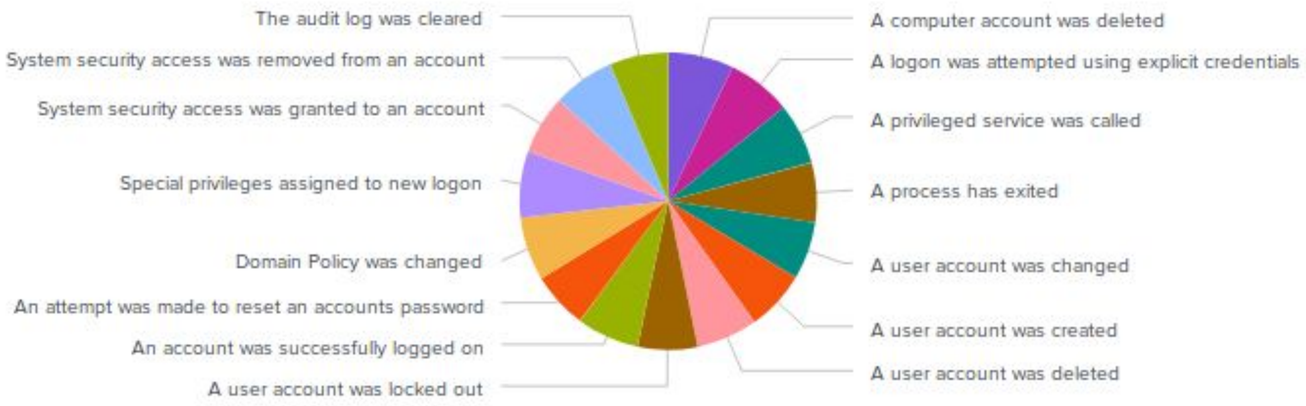




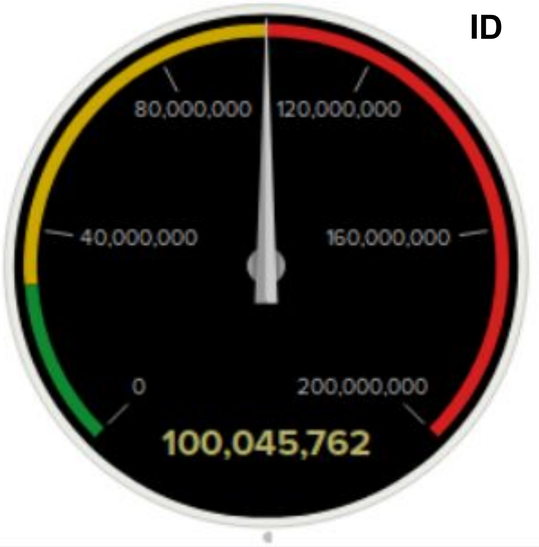
Dashboards—Windows

Signatures for Accounts

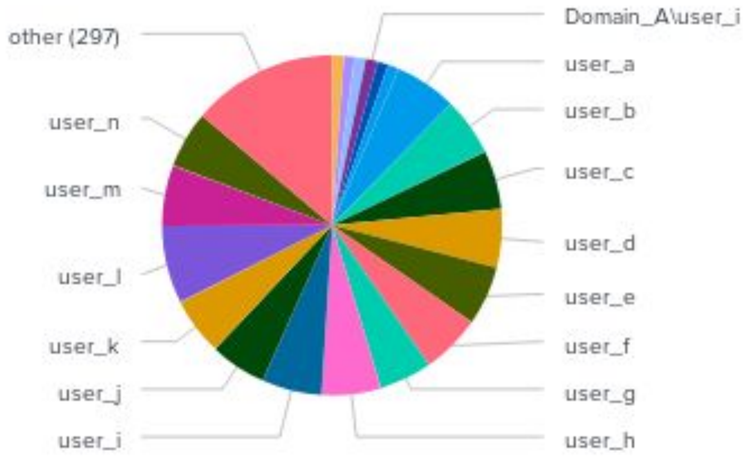
Account Status Logs



ID



User Count (Chart View)



142

Apache Logs

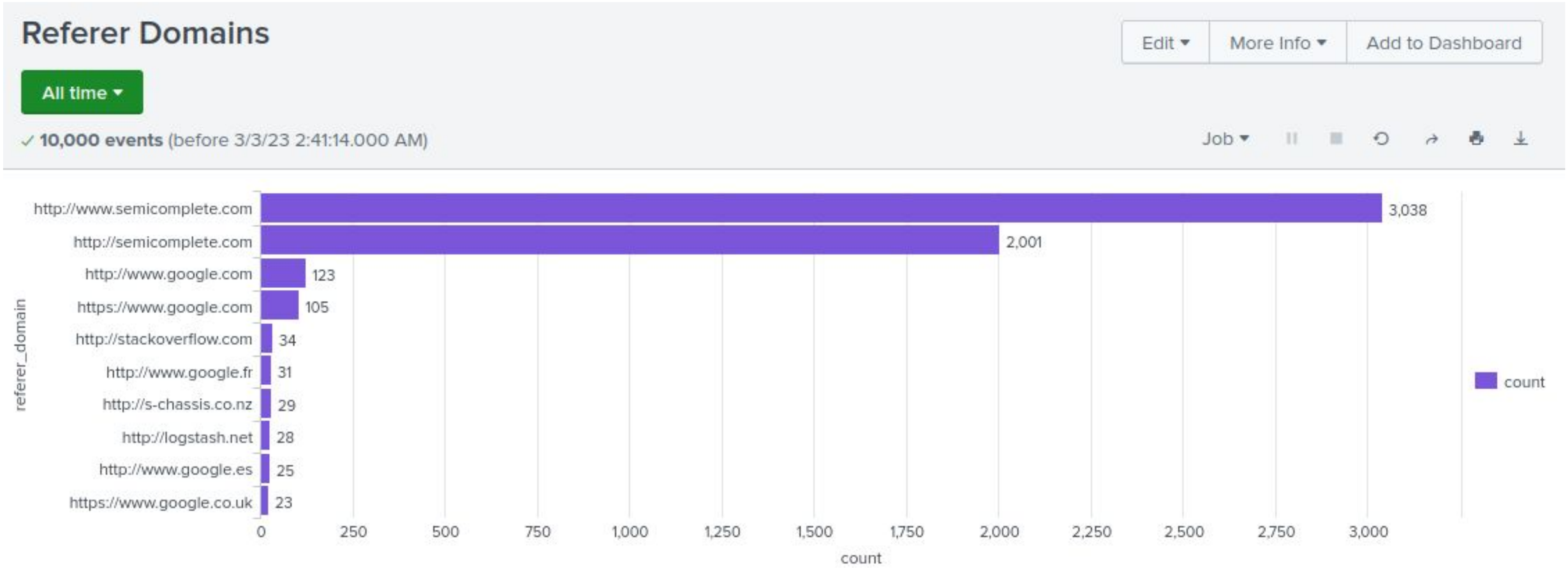
Reports—Apache

Designed the following reports:

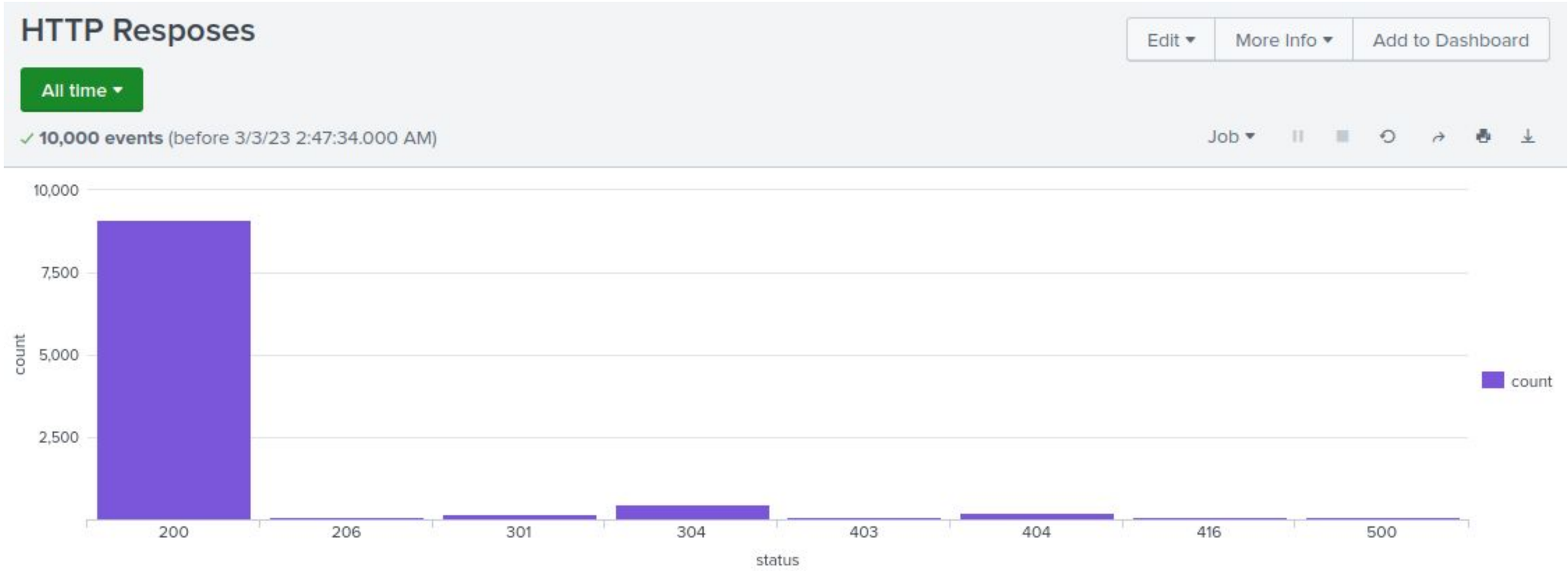
Report Name	Report Description
HTTP Methods	Table of the different HTTP methods (GET, POST, HEAD, etc.)
Referrer Domains	A bar chart that shows the top 10 domains that refer to VSI’s website
HTTP Response Codes	A column chart shows the count of each HTTP response code.

Images of Reports—Apache

Images of Reports—Apache



Images of Reports—Apache



Alerts—Apache

Designed the following alerts:

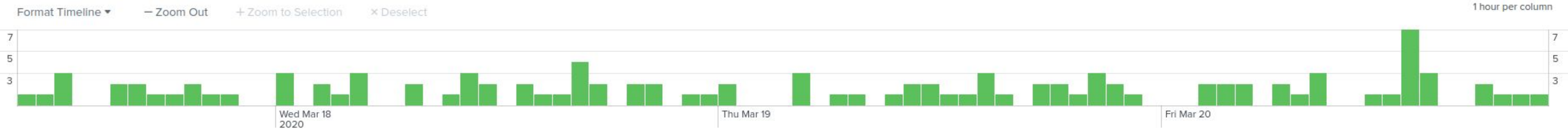
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Activity Outside of US	An alert for hourly activity from any country besides the United States	90	> 120

JUSTIFICATION: The baseline the average and the threshold was highest value for “normal” activity

Alerts—Apache

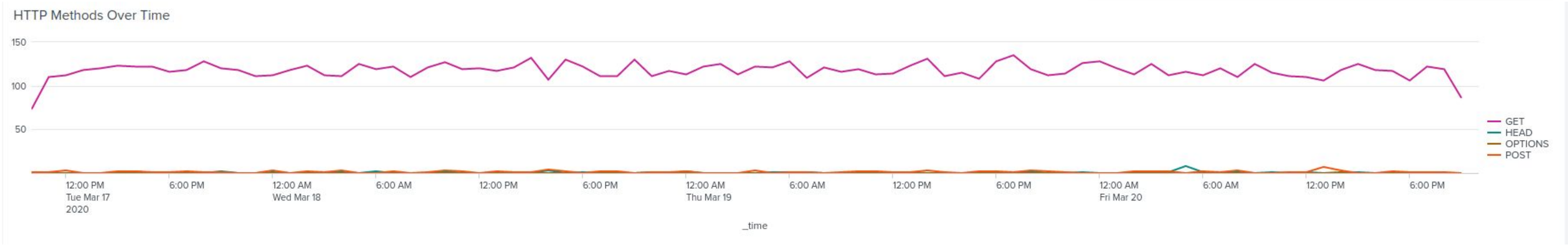
Designed the following alerts:

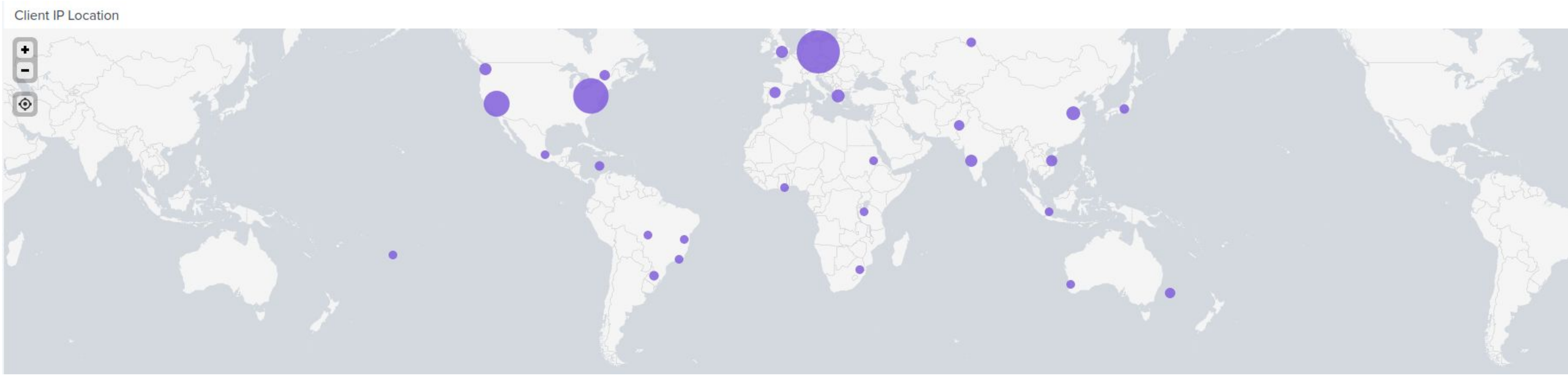
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Request	An alert for hourly count of the HTTP POST method	3	> 5



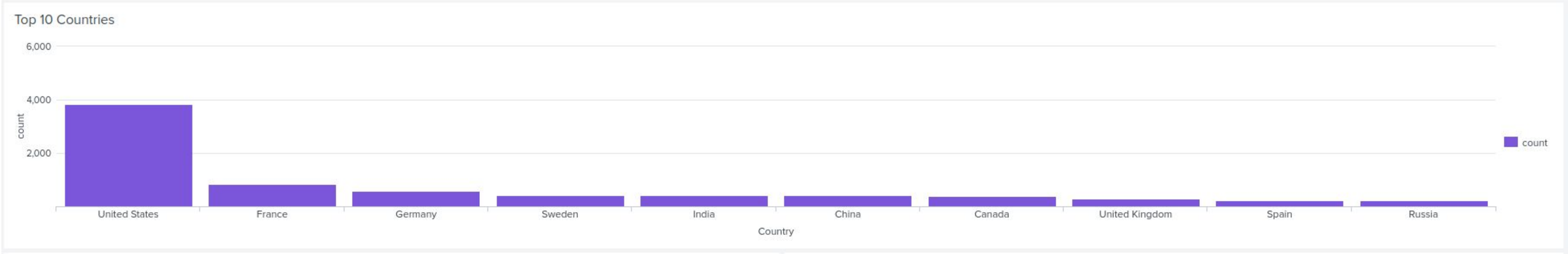
JUSTIFICATION: The baseline was set at 3 because it was the number of events that occurred the most common max over time. The threshold was determined at 5 because that was the average number of events.

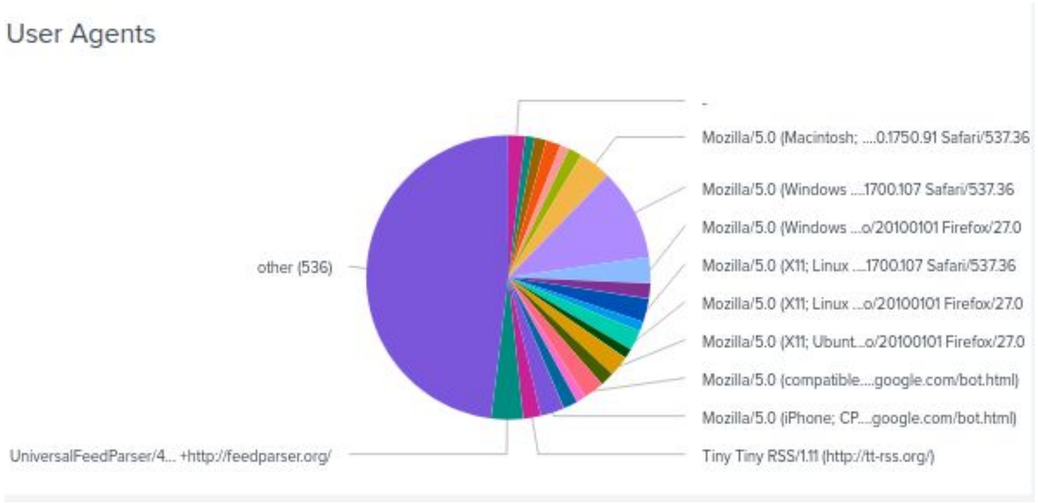
Dashboards—Apache





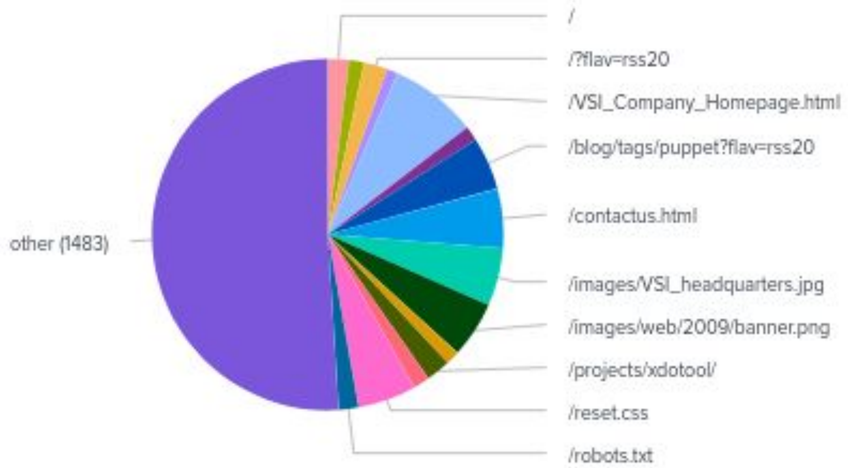
Dashboards—Apache





Dashboards—Apache

URIs



Total HTTP Post Methods

Attack Analysis

Attack Summary—Windows

- An increase in Windows logs containing the “high” and “informational” severity levels was determined
- An increase in Successful Windows Activities, and decrease in Failed Windows Activities was determined

Attack Summary—Windows (Reports)

- Success went from 97% to 98%, for an increase of 1%
- Failure went from 3% to 2%, for a decrease of 1%

Severity Levels — Before Attack

Edit ▾ | More Info ▾ | Add to Dashboard

✓ **4,761 events** (before 3/7/23 12:31:13.000 AM) — Job ▾

2 results — 20 per page ▾

severity	count	perc
high	329	6.91
informational	4429	93.09

Severity Levels — After Attack

Save | Save As ▾ | View | Create Table View | Close

```
source="windows_server_attack_logs.csverc | eval perc=round(count*100/perc,2)
```

All time ▾

✓ **5,948 events** (before 3/7/23 12:28:36.000 — Job ▾ — Smart Mode ▾

Events | Patterns | **Statistics (2)** | Vi

20 Per Page ▾ | Format | Preview ▾

severity	count	perc
high	1111	20.23
informational	4381	79.77

Success & Failure of Windows Activities — Before Attack

✓ **4,758 events** (before 3/7/23 12:34:06.000 AM)

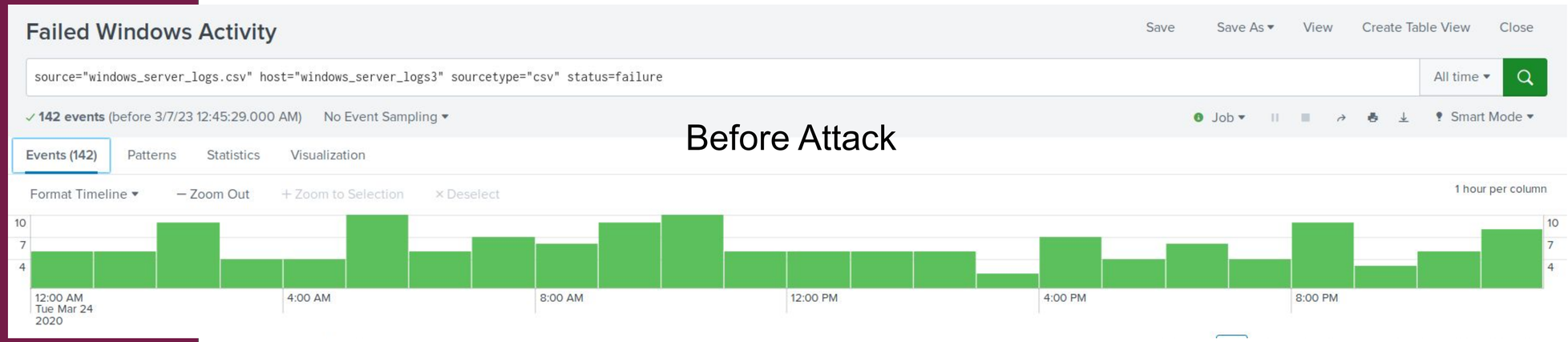
status	count	perc
failure	142	2.98
success	4616	97.02

After Attack

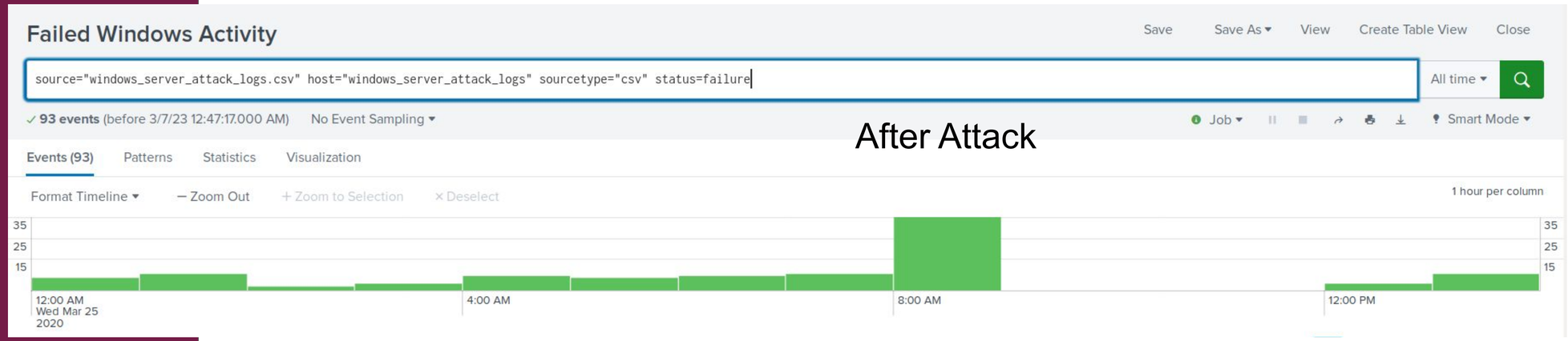
status	count	perc
failure	93	1.56
success	5854	98.44

Attack Summary—Windows (Alerts)

- An increase of failed events (35) detected at 8AM on 3/25/20



Before Attack

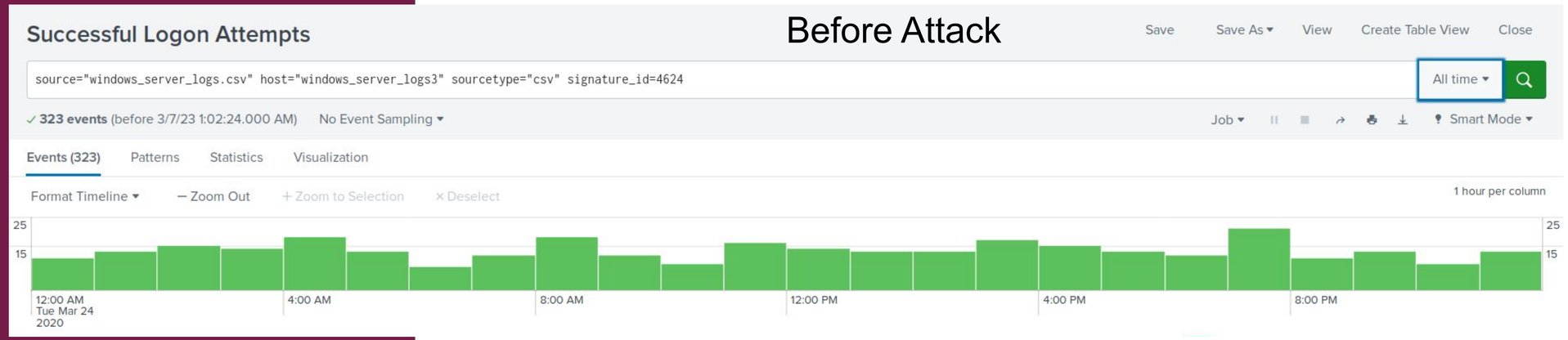


After Attack

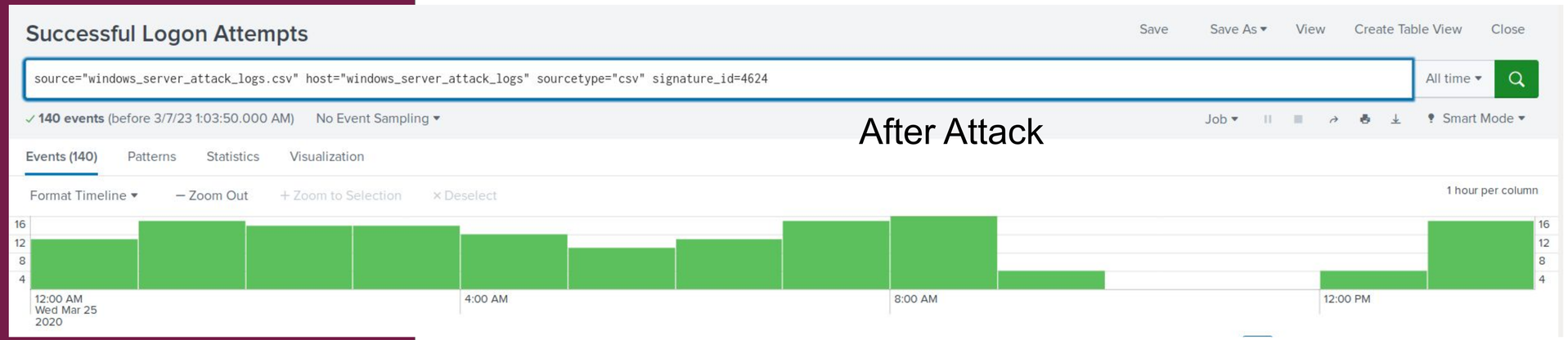
Attack Summary—Windows (Alerts)

- Successful login attempts drastically decreased between 9AM and 12PM on 3/25/20

Before Attack

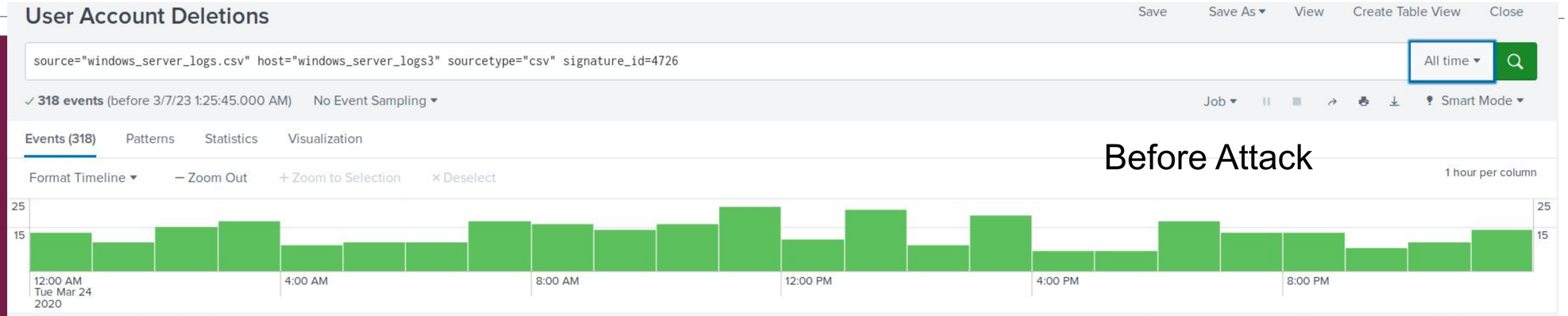


After Attack

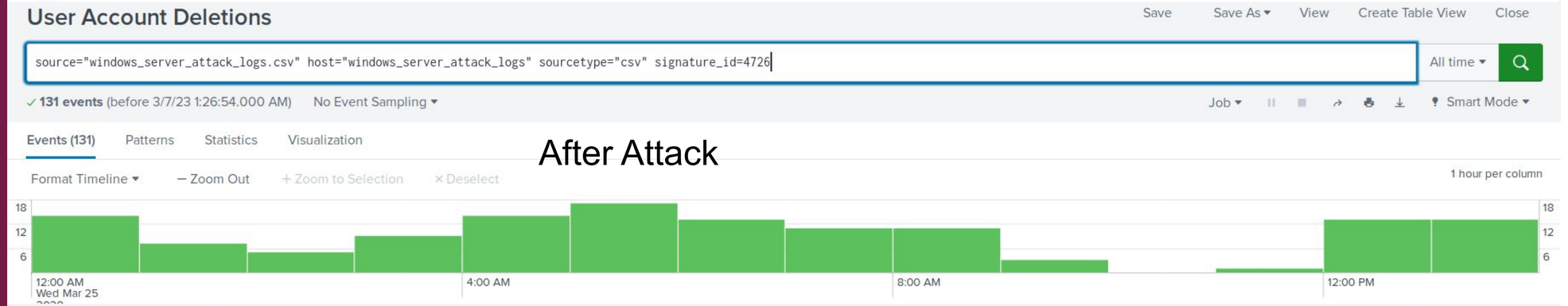


Attack Summary—Windows (Alerts)

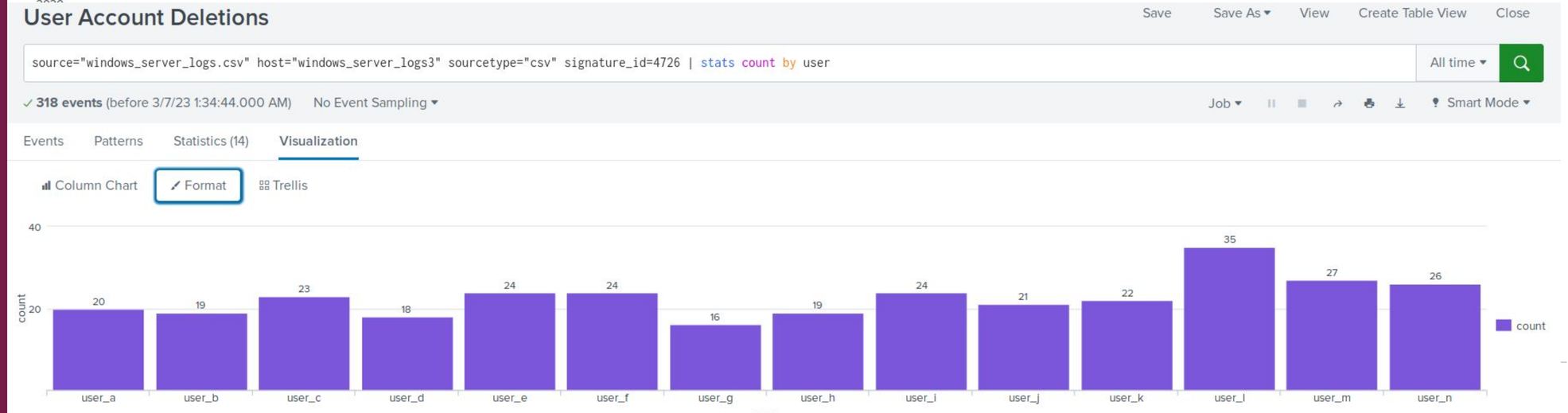
- Decrease in user account deletions was observed



Before Attack



After Attack



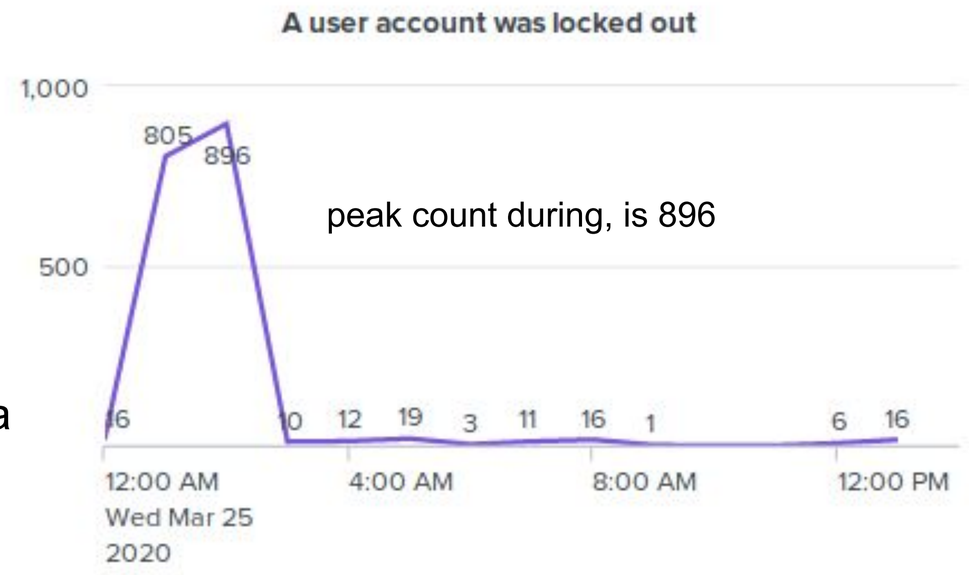
Attack Summary—Windows (Dashboards)

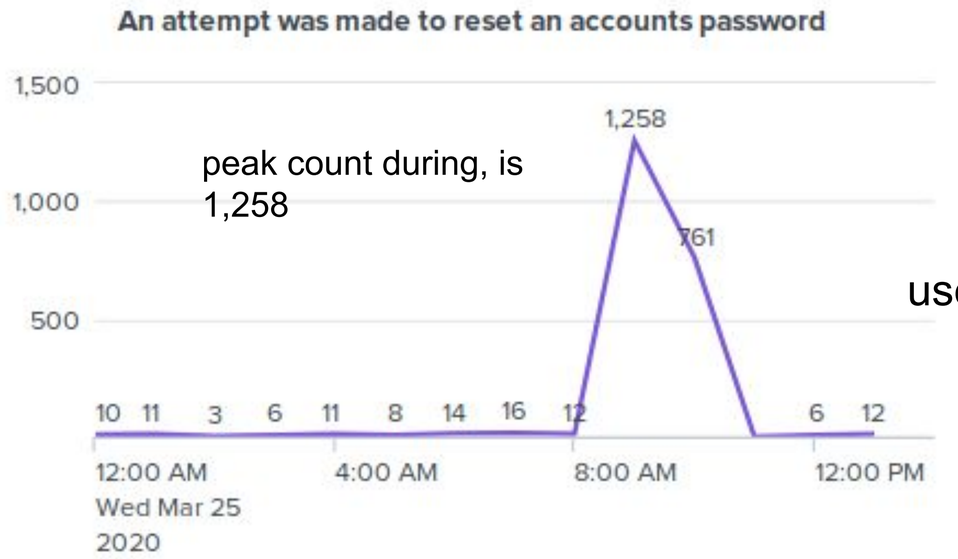
- A cyber attack occurred on March 25th, 2020
  - Time Chart of Signatures and Users:
    - “A user account was locked out” - 12AM to 3AM
    - “An attempt was made to reset an accounts password” - 8AM to 11AM
  - Increased account activity for user_a between 12AM to 3AM
  - Increased account activity for user_j between 8AM to 11AM

Attack Summary—Windows (Dashboards)

- Time chart of Signatures and Users
  - “A user account was locked out” - 12AM to 3AM
  - “An attempt was made to reset an accounts password” - 8AM to 11AM

user_a

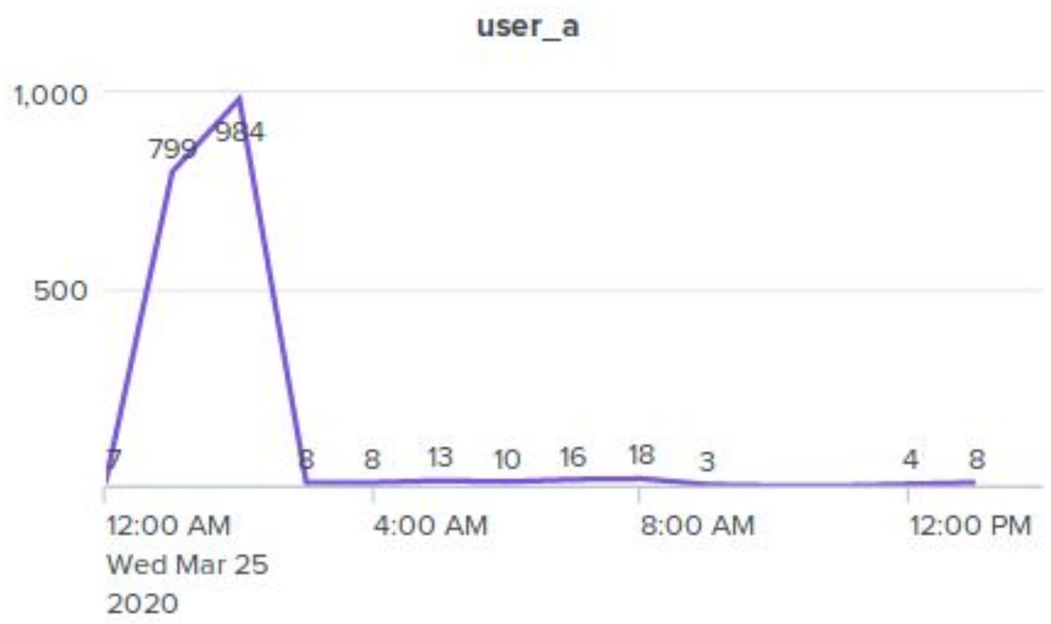


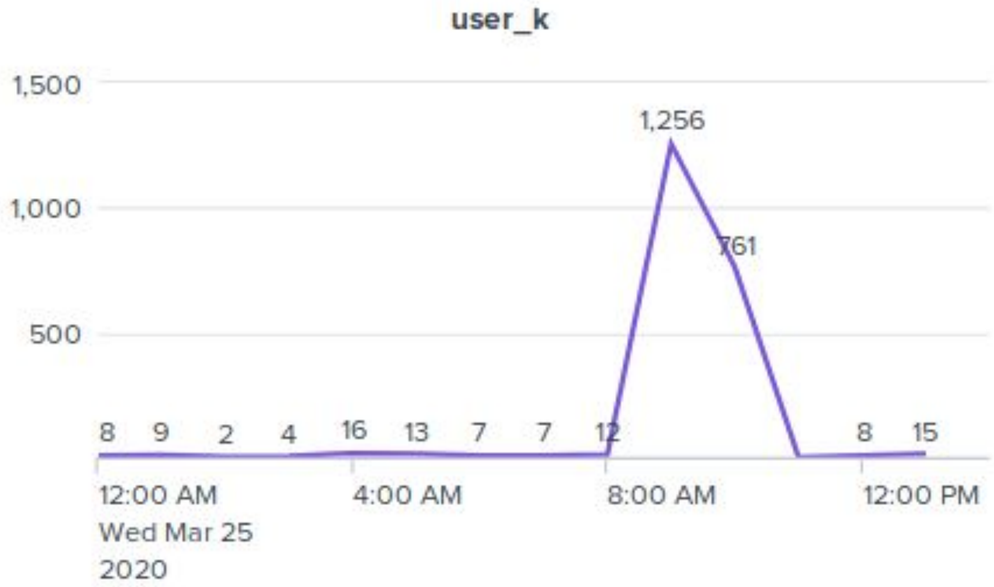


user_k

Attack Summary—Windows (Dashboards)

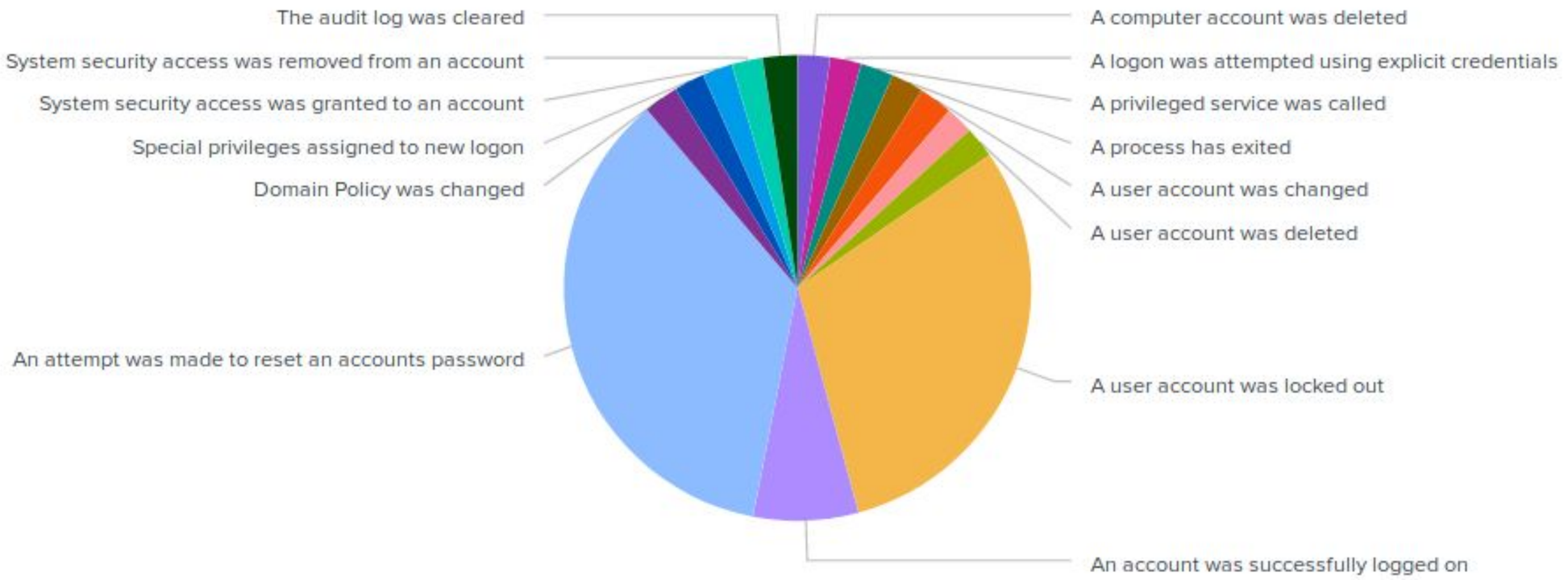
- Time chart of Signatures and Users





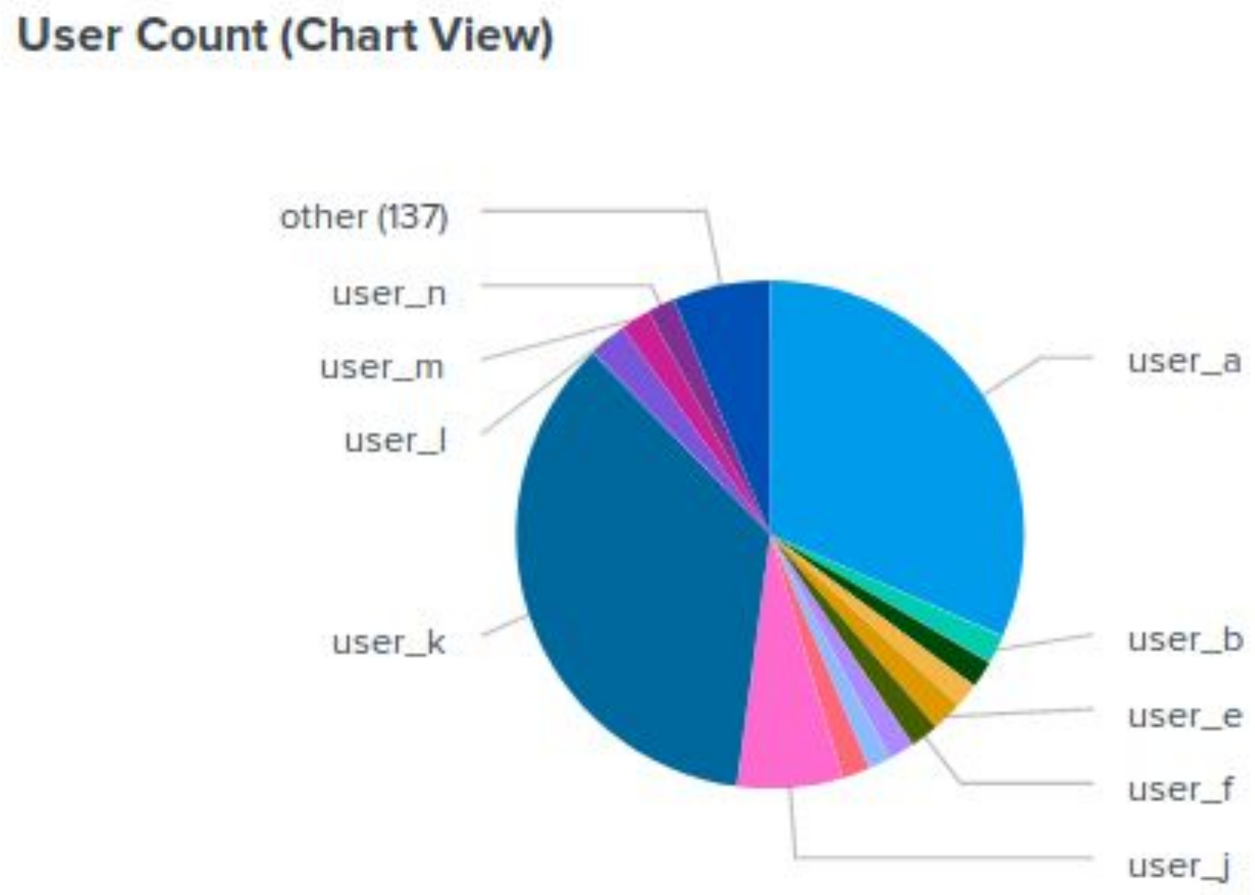
Attack Summary—Windows

- Time Chart of Signatures - Pie Chart



Attack Summary—Windows

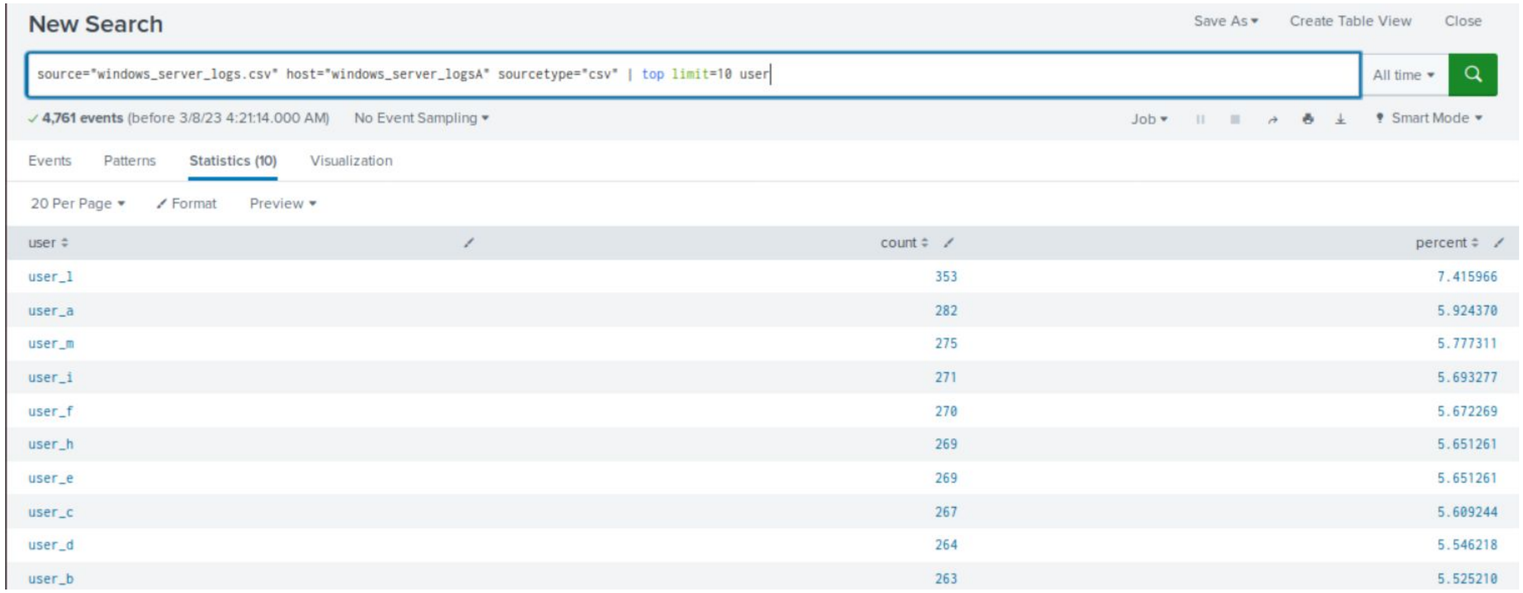
- Time Chart of Users - Pie Chart



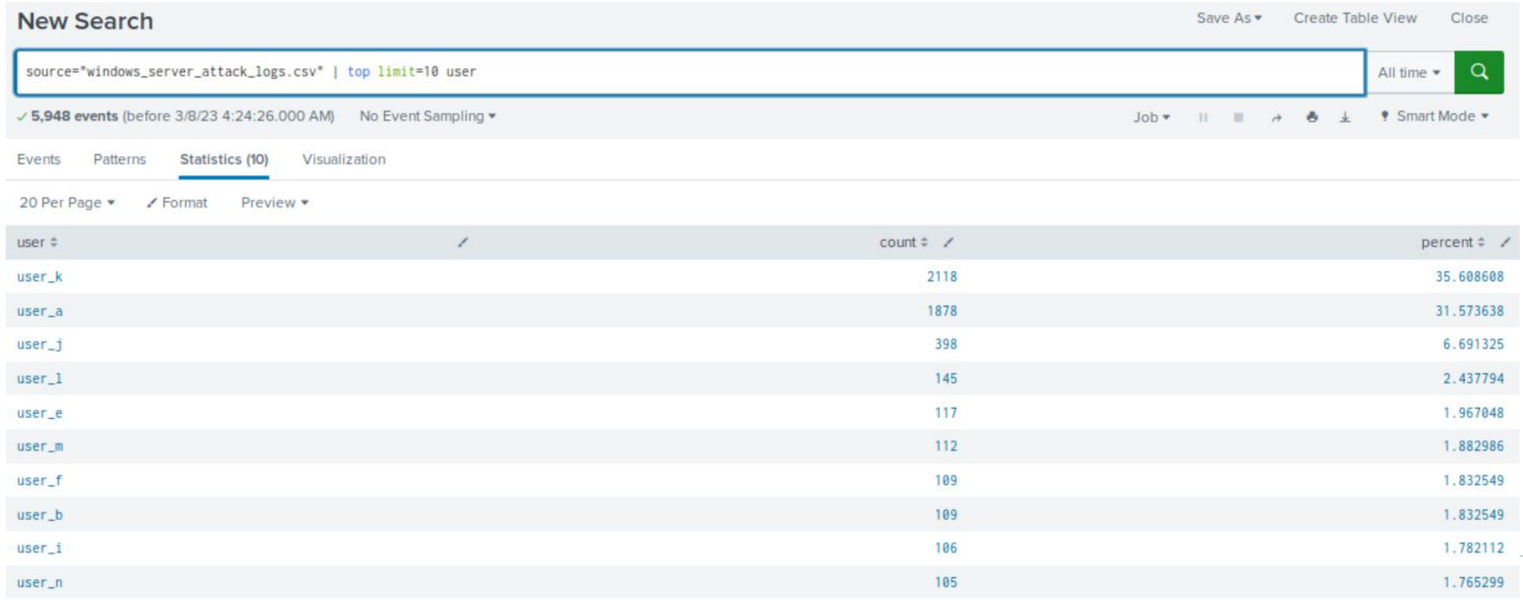
Attack Summary—Windows (Dashboards)

- Users Statistical Charts

Before Attack



user	count	percent
user_l	353	7.415966
user_a	282	5.924370
user_m	275	5.777311
user_i	271	5.693277
user_f	270	5.672269
user_h	269	5.651261
user_e	269	5.651261
user_c	267	5.609244
user_d	264	5.546218
user_b	263	5.525210



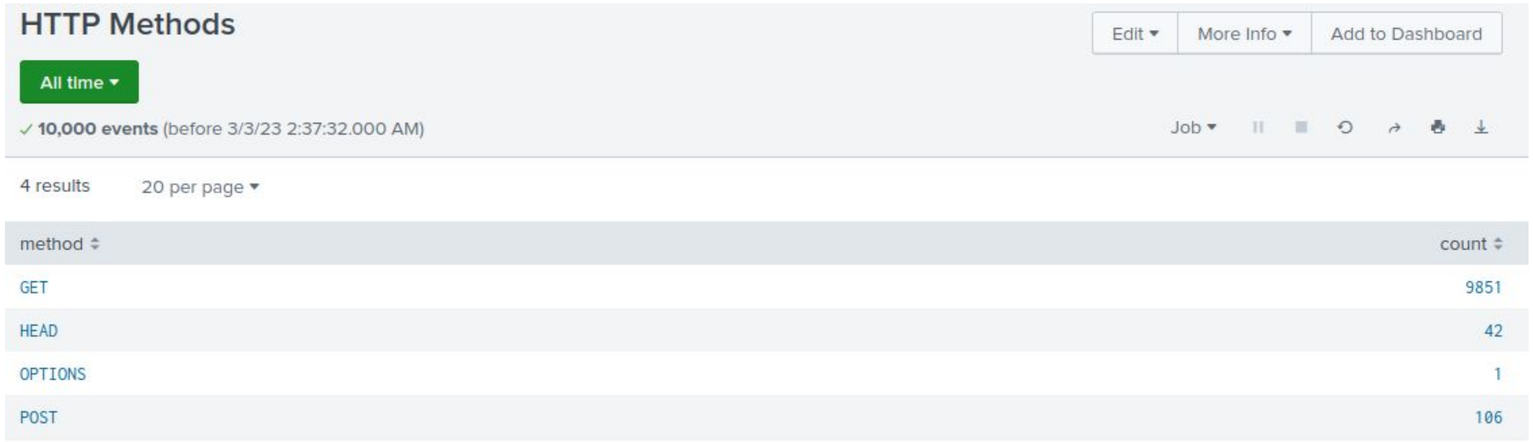
user	count	percent
user_k	2118	35.608608
user_a	1878	31.573638
user_j	398	6.691325
user_l	145	2.437794
user_e	117	1.967048
user_m	112	1.882986
user_f	109	1.832549
user_b	109	1.832549
user_i	106	1.782112
user_n	105	1.765299

After Attack

Report Attack Summary—Apache

- The HTTP POST method Increased
- There were fewer Referrer Domains
- Increase of HTTP 404 response codes

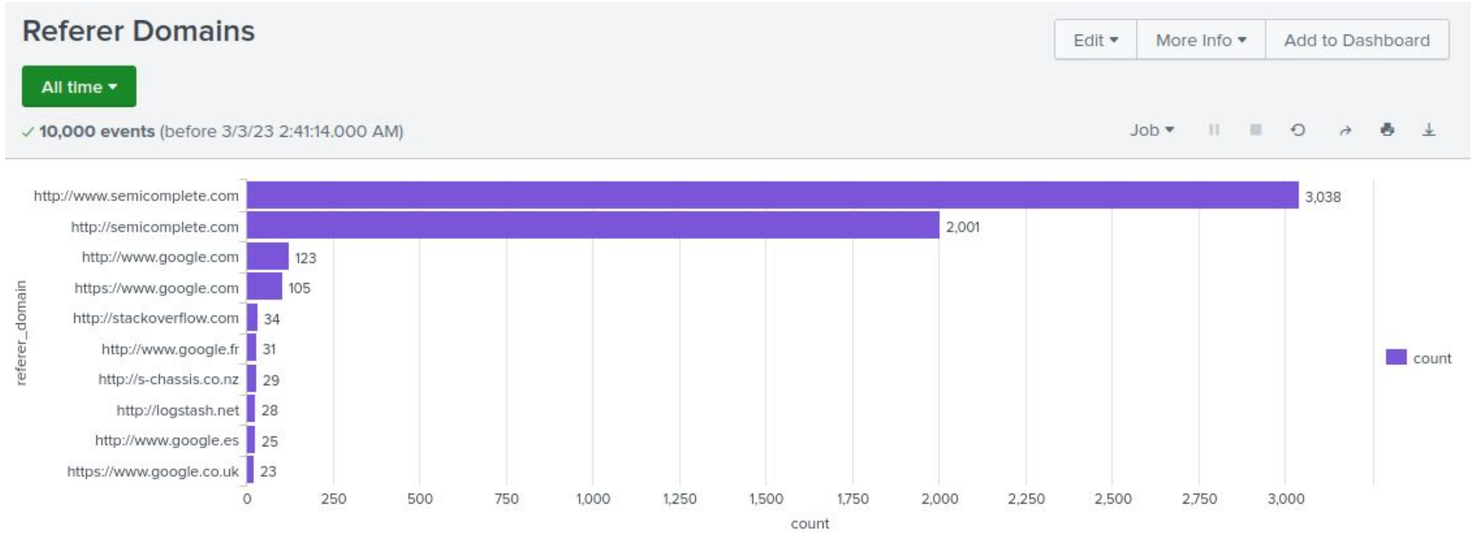
Report Attack Images—Apache



Before Attack

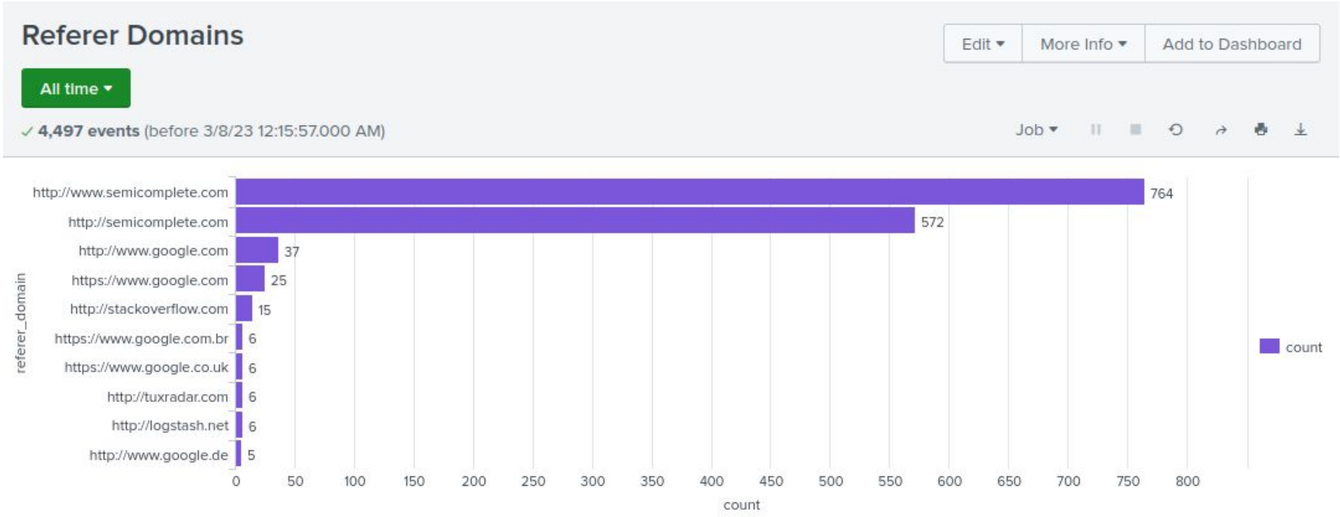
After Attack

Report Attack Images—Apache

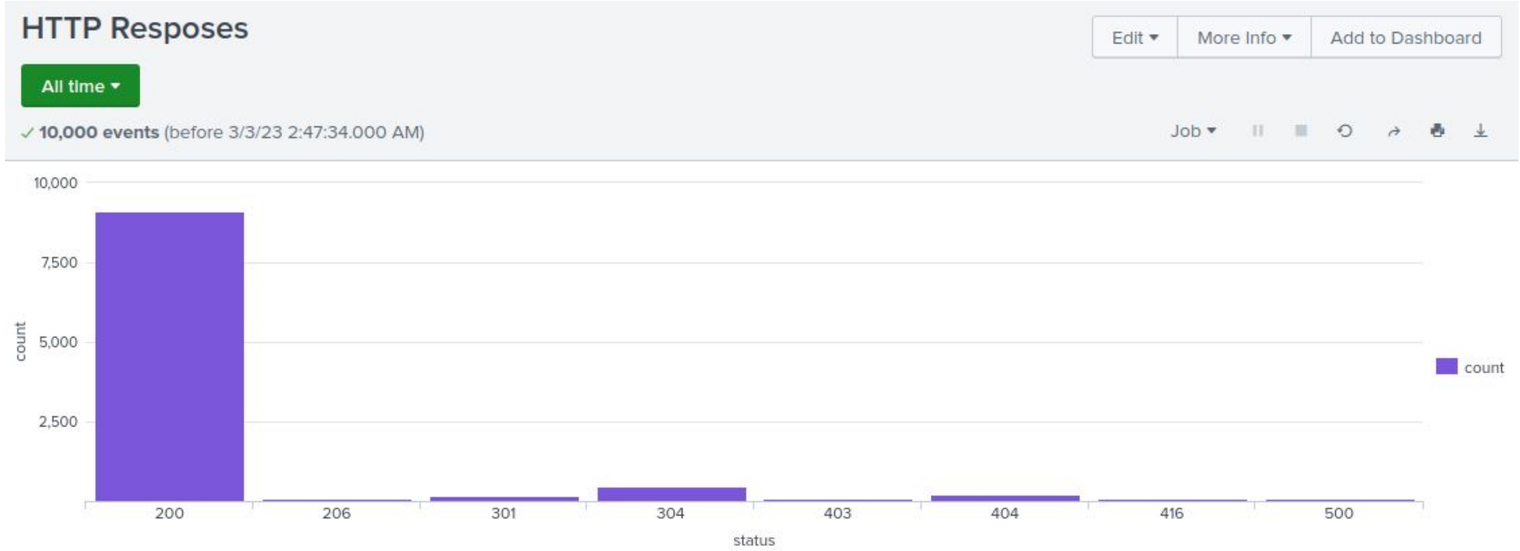


Before Attack

After Attack

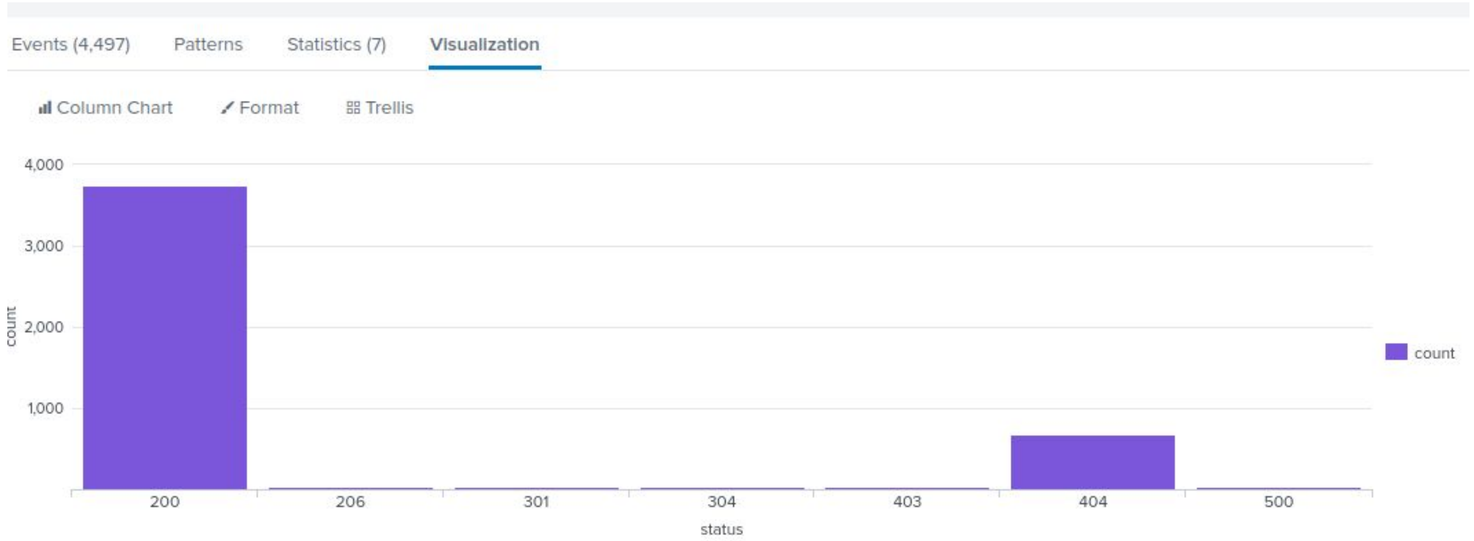


Report Attack Images—Apache



Before Attack

After Attack

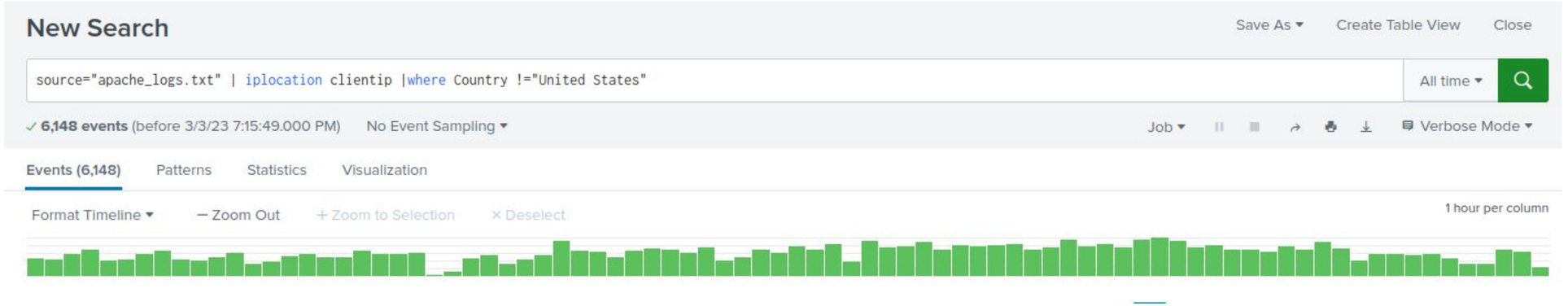


Alert Attack Summary—Apache

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

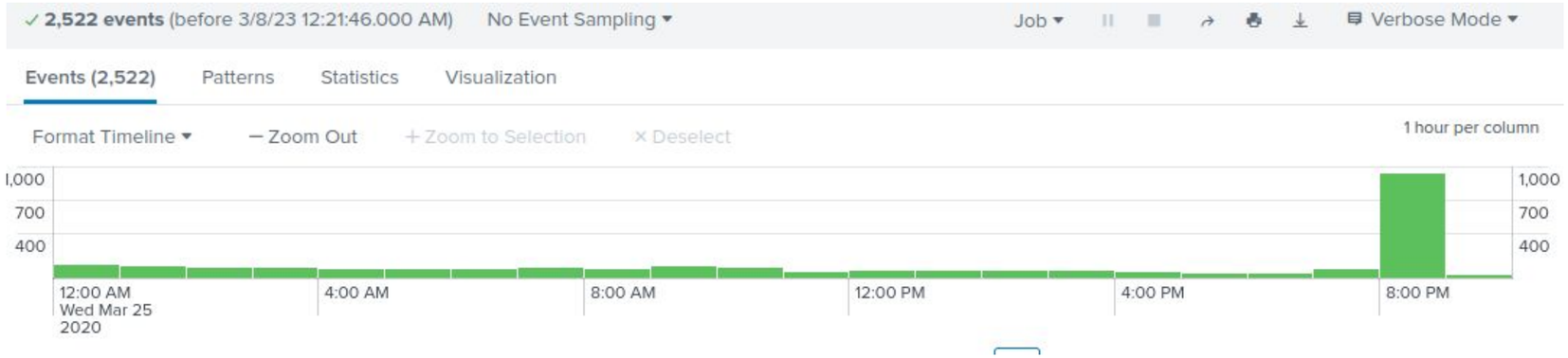
- Spike of international activity during an hour block Starting at 8:00pm
  - threshold would correctly alert
- Spike in HTTP POST activity that surpassed threshold
  - 8:00pm

Alert Attack Images—Apache

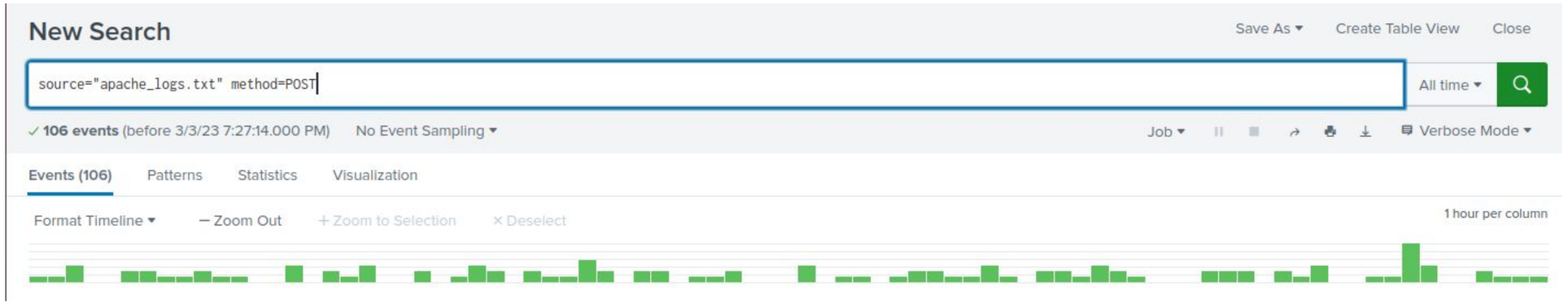


Before Attack

After Attack

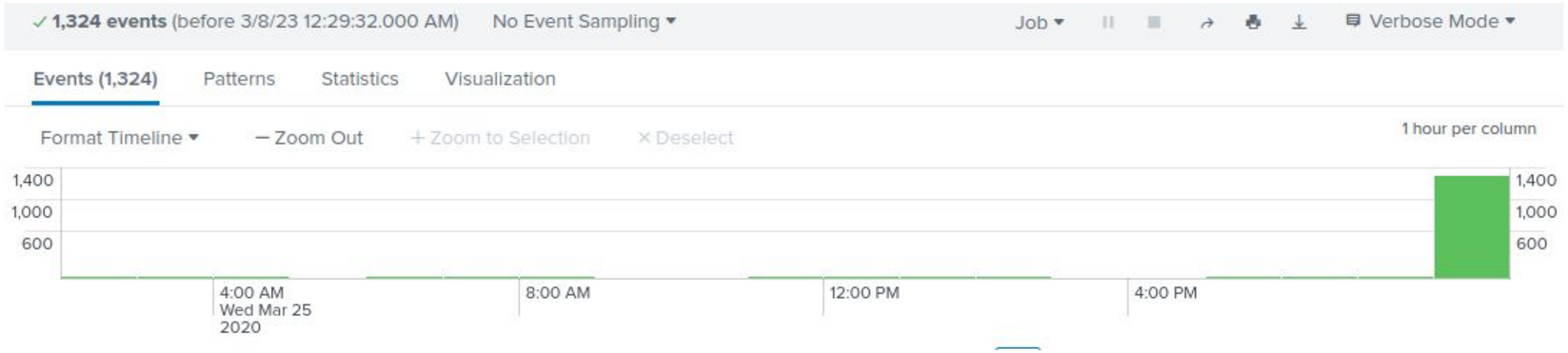


Alert Attack Images—Apache



Before Attack

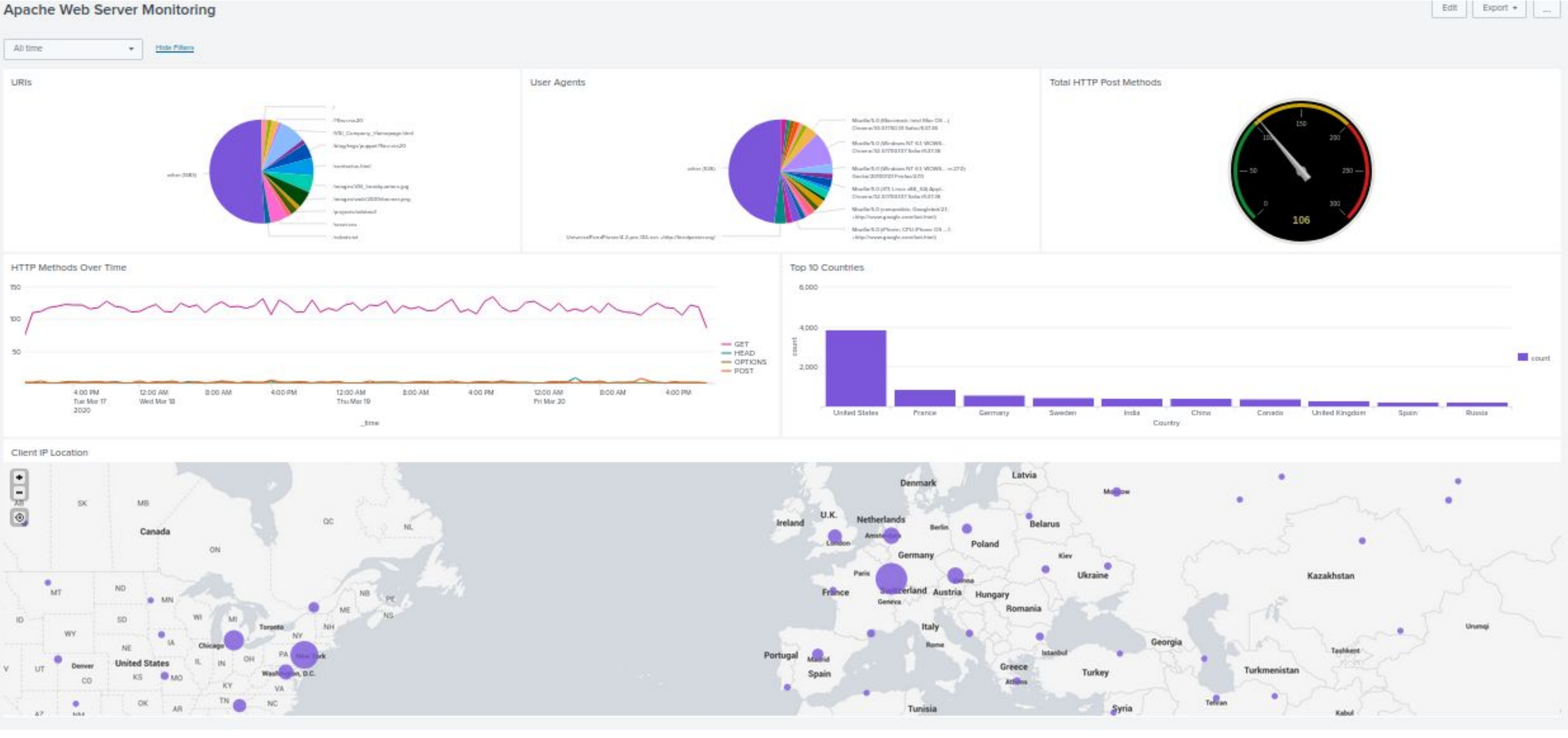
After Attack



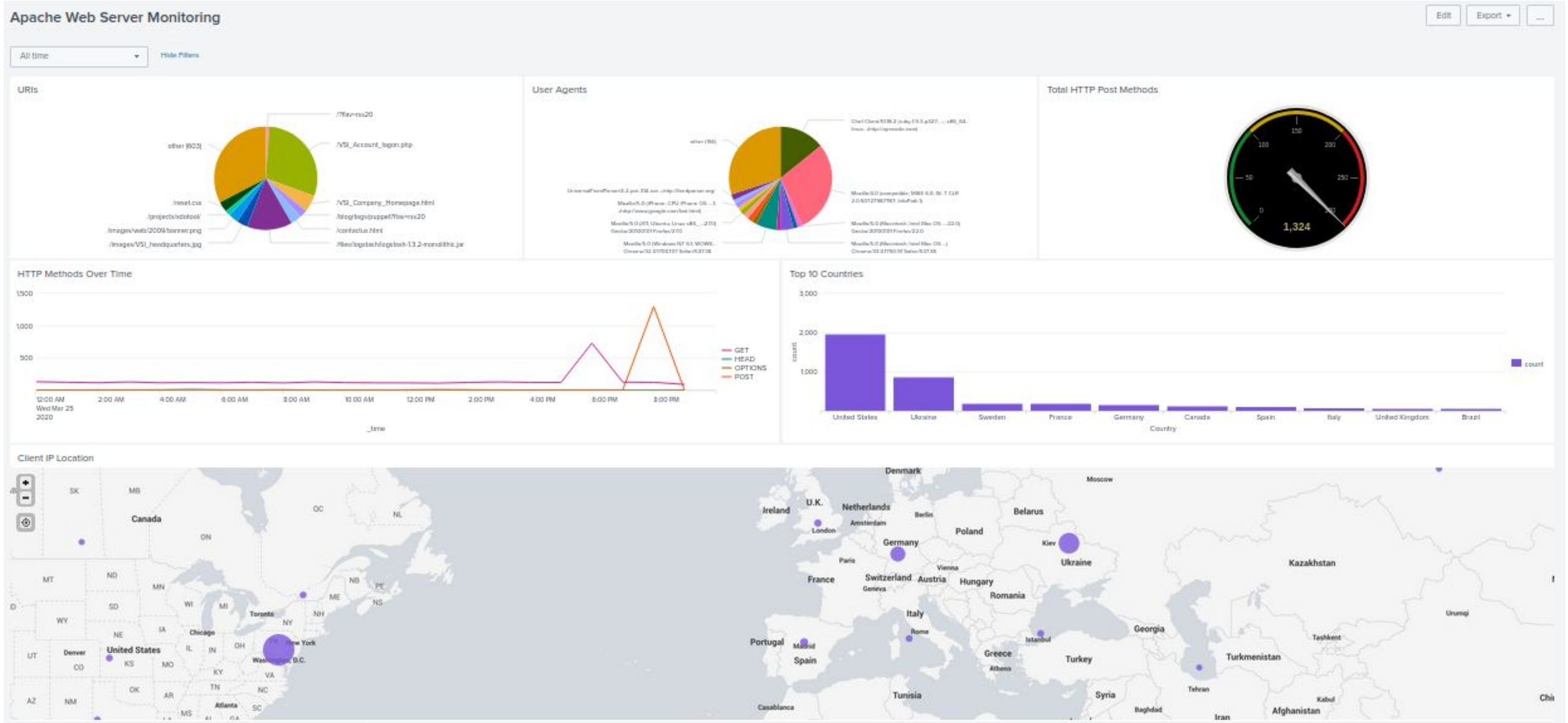
Dashboard Attack Summary—Apache

- Time Chart for HTTP Methods developed peaks for POST and GET methods
  - Peaks formed from 5:00pm to 9:00pm March 25 2020
  - 729 for GET method and 1296 for POST method
- High volume of activity from a country
  - Ukraine
- A dramatic change in URI’s
  - /VSI_Account_logon.php

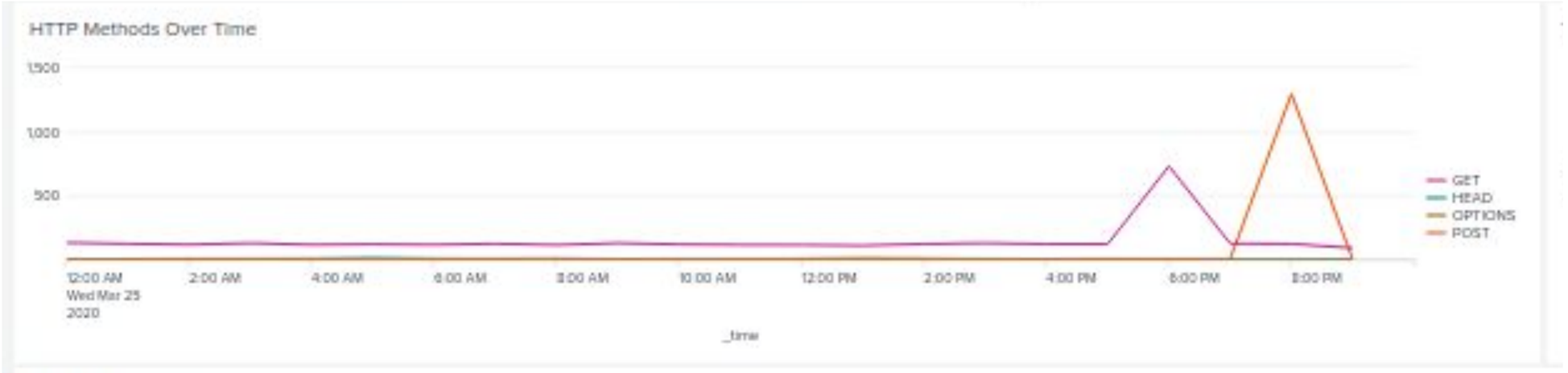
Dashboard Attack Images



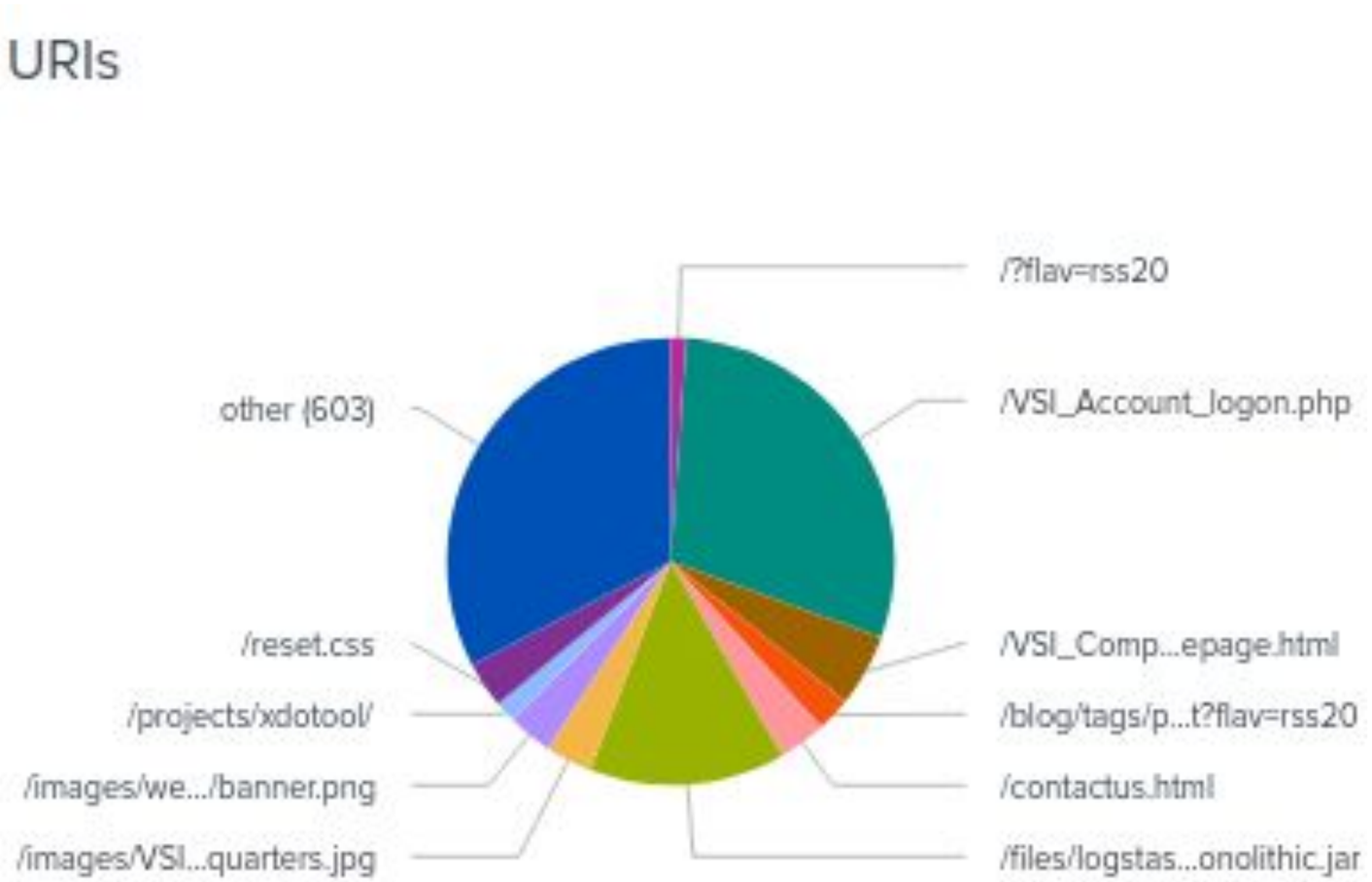
Dashboard Attack Images



Dashboard Attack Images



Dashboard Attack Images



Summary and Future Mitigations

Project 3 Summary

- Overall findings from the attack that took place:
  - A cyber attack occurred against VSI on March 25th, 2020
  - Windows logs suggest there was a brute force attack and a distributed denial of service (DDOS) attack
  - Apache logs suggest there was a brute force attack
- To protect VSI from future attacks, the following mitigations are recommended:
  - New passwords with two-factor authentication should be implemented for user_a and user_j
  - Implement a firewall rule that blocks all incoming traffic with a source IP address originating from Ukraine
  - Utilize Web Monitoring Add-on App for continuous monitoring