Defensive Security Project
by: Bastion Brigade

Group Members: Carlos Brown, Collin Janecka, Logan Cain, Rafael Ramirez, & Samantha Hernandez

Table of Contents

This document contains the following resources:

01

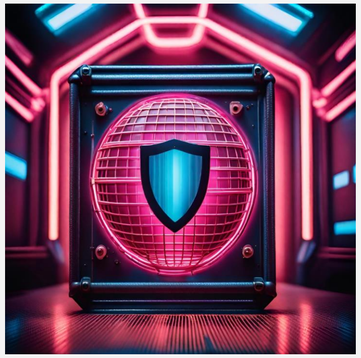
Monitoring Environment

02

Attack Analysis

03

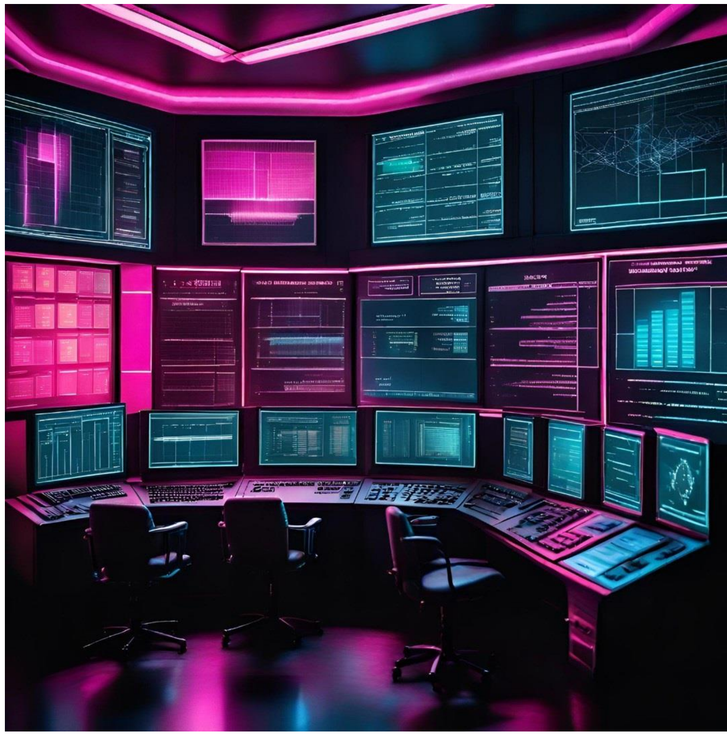
Project Summary & Future Mitigations



Monitoring Environment

Scenario

- We Have assumed the role of a SOC Analyst at a 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 businesses.
- As a SOC Analyst you are tasked with using splunk to monitor potential attacks on your systems and applications.
- You have been provided the following VSI products to monitor
- An Apache web server, which hosts the administrative webpage
- A Windows operating system, which runs VSI''s back-end operations



Website Monitoring

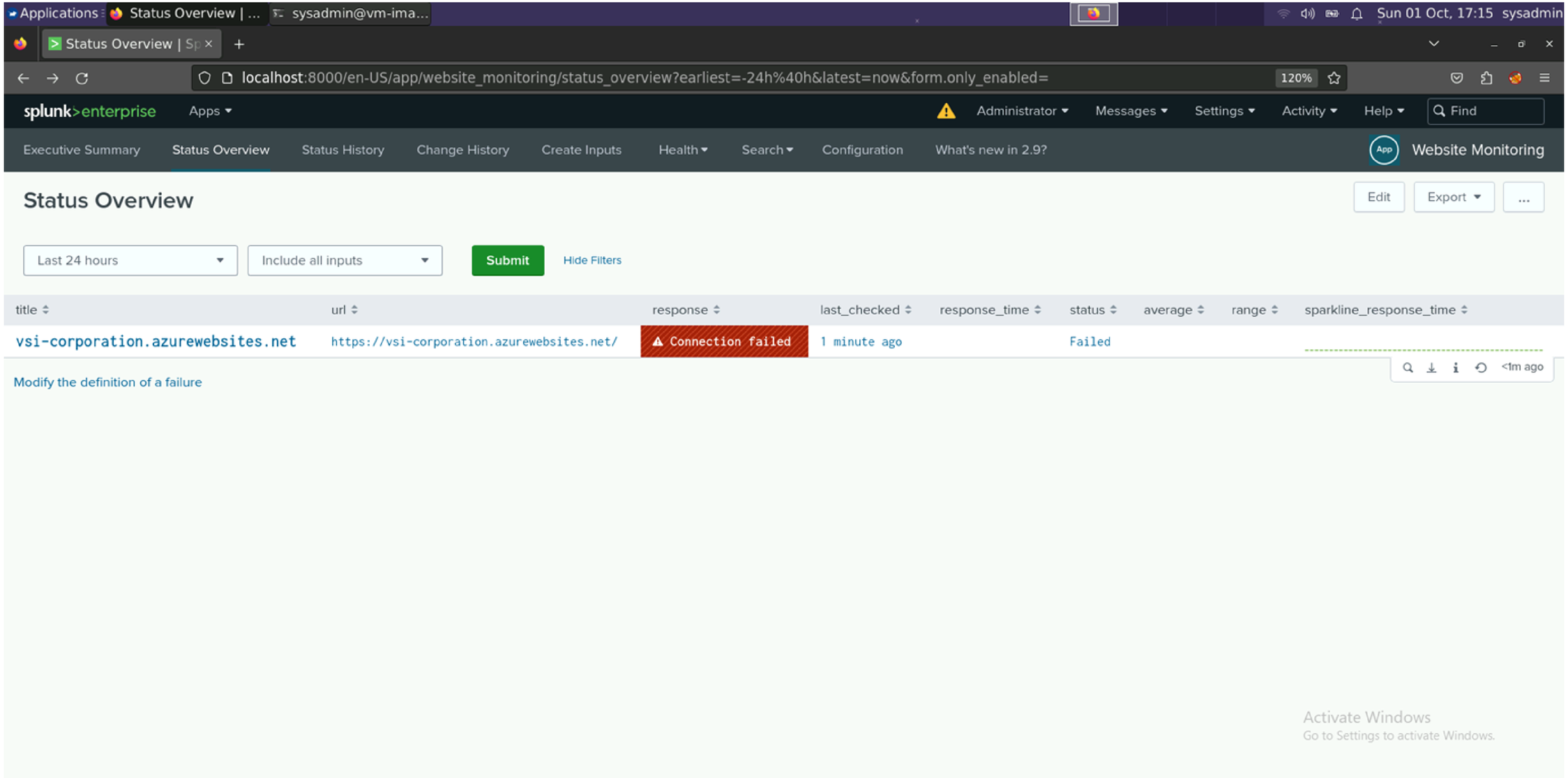
Website Monitoring

The website monitoring add-on app allows for a constant monitoring of a specific website at a given interval. This gives information such as; showing the average response time to the website, the history of the response time, the maximum response time to connect to the website, as well as the number of past failures of the website.

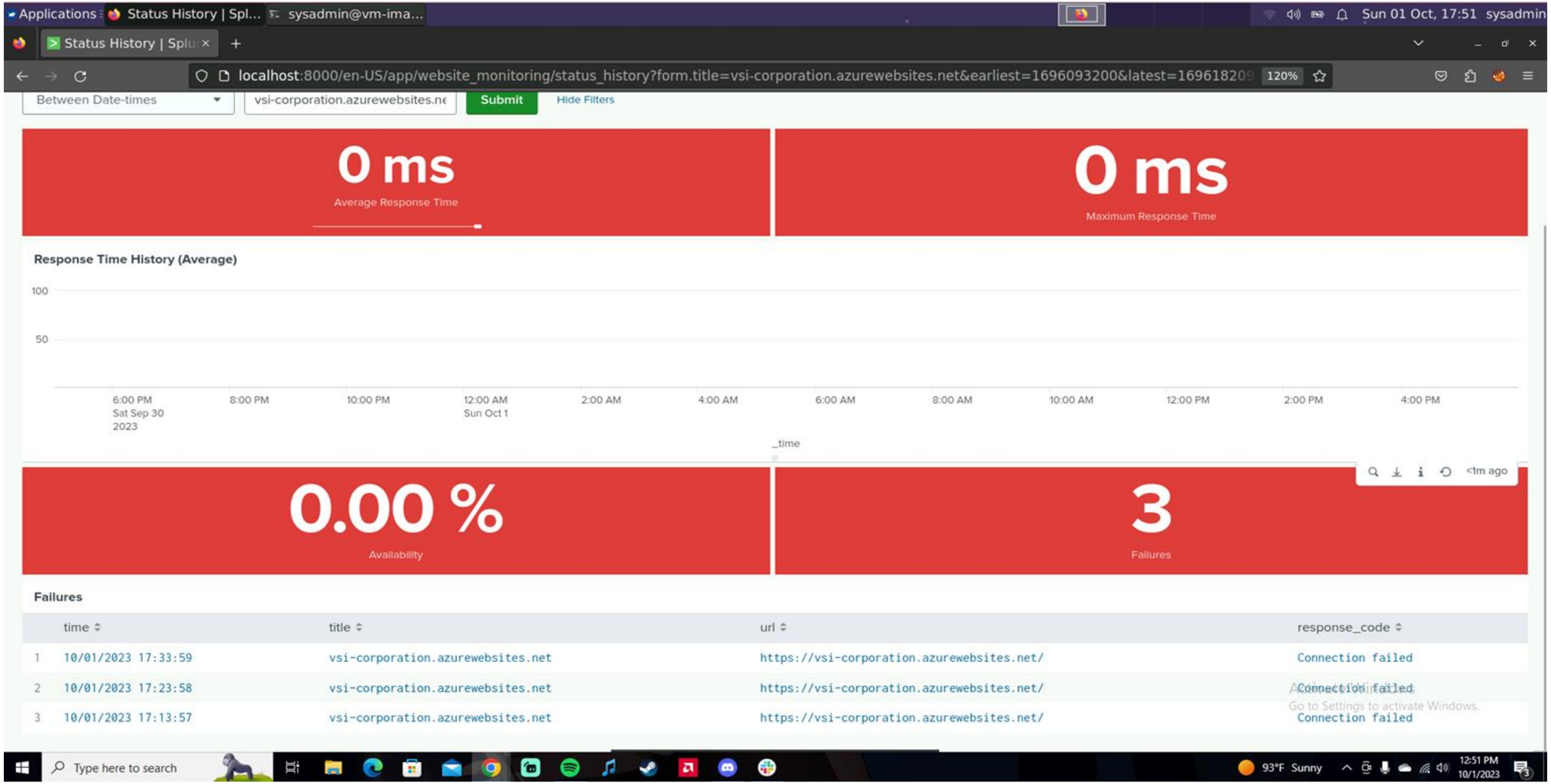
Website Monitoring

This app allows VSI to monitor their website and be able to react faster if they were to be attacked using a DDoS attack. Since JobeCorp is known to attack their competitors using DDoS attacks, this app will give VSI the ability to see if they are being attacked JobeCorp or any other competitor quickly and react accordingly.

Website Monitoring



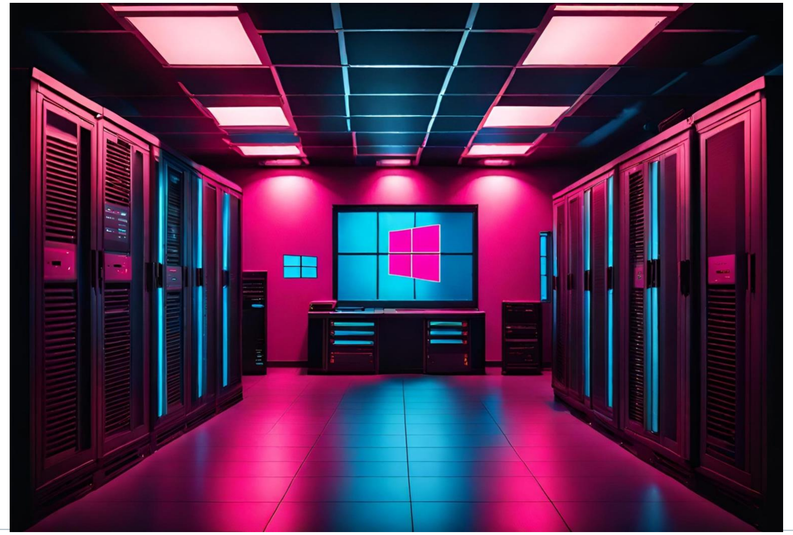
Website Monitoring



Logs Analyzed

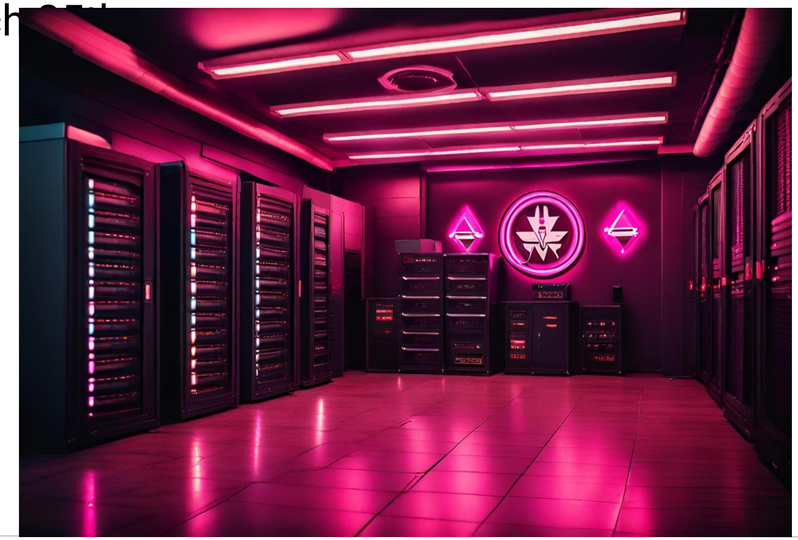
1 Windows Logs

The Windows logs show the logs from the Windows Domain Controller for VSI from the 24th of March and from the attack on March 25th.



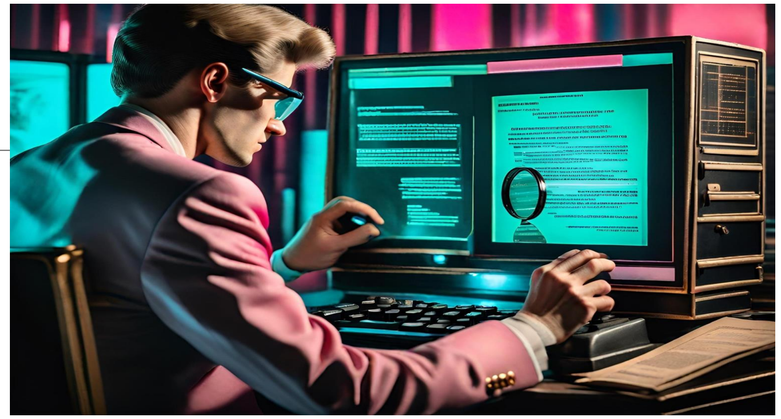
2 Apache Logs

The Apache logs show the various HTTP methods that were recorded on VSI's website on March 18th and HTTP methods that were recorded during the attack on their website on March



Windows Logs

Reports—Windows



Designed the following reports:

Report Name	Report Description
Signature and Signature IDs	This report shows the ID number associated with the specific signature for Windows activity.
Severity Levels	This report shows the severity levels of the Windows logs with their count and percentage.
Success and Failures	This report will show if there is a suspicious level of failed activities on the VSI server.

Images of Reports—Windows

Signatures and Signature IDs

Edit ▾ | More Info ▾ | Add to Dashboard

A report that shows ID number associated with specific signatures for Windows activity

All time ▾

✓ **15 events** (before 9/28/23 12:22:31.000 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

Images of Reports—Windows

Severity Levels Report

Edit ▾ | More Info ▾ | Add to Dashboard

The severity levels of the Windows logs being viewed

All time ▾

✓ **4,764 events** (before 9/28/23 12:46:30.000 AM)

Job ▾

2 results | 20 per page ▾

severity	count	percentage
high	329	6.905961376994123
informational	4435	93.09403862300589

Images of Reports—Windows

Success and Failure Attempts

Edit ▾ | More Info ▾ | Add to Dashboard

This report will show if there is a suspicious level of failed activities on the server

All time ▾

✓ **4,764 events** (before 9/28/23 1:00:40.000 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
Failure Attempts Reached 	Hourly level of failed Windows activity has reached the threshold	5	8

JUSTIFICATION: The average amount of failed attempts was around 5 which would be our baseline and the spikes were around 9 or 10, so we placed our threshold to be anything above 8.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins 	Alert is made when the signature “an account was successfully logged on” has reached its threshold	14	17

JUSTIFICATION: Our baseline is 14 because that’s about the average of successful logins we received and then our threshold is 17 because we have a few spikes that begin to take place over that amount.

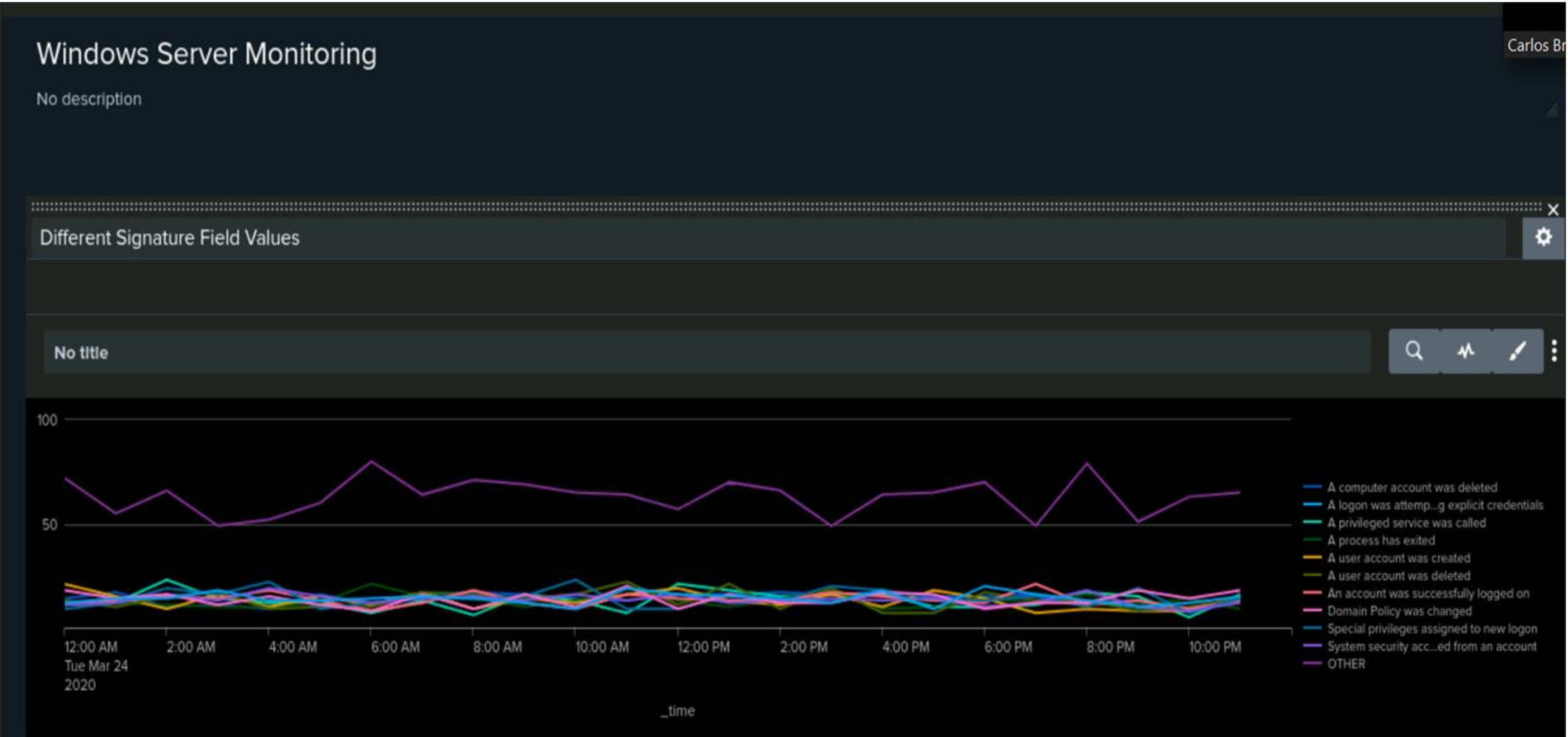
Alerts—Windows

Designed the following alerts:

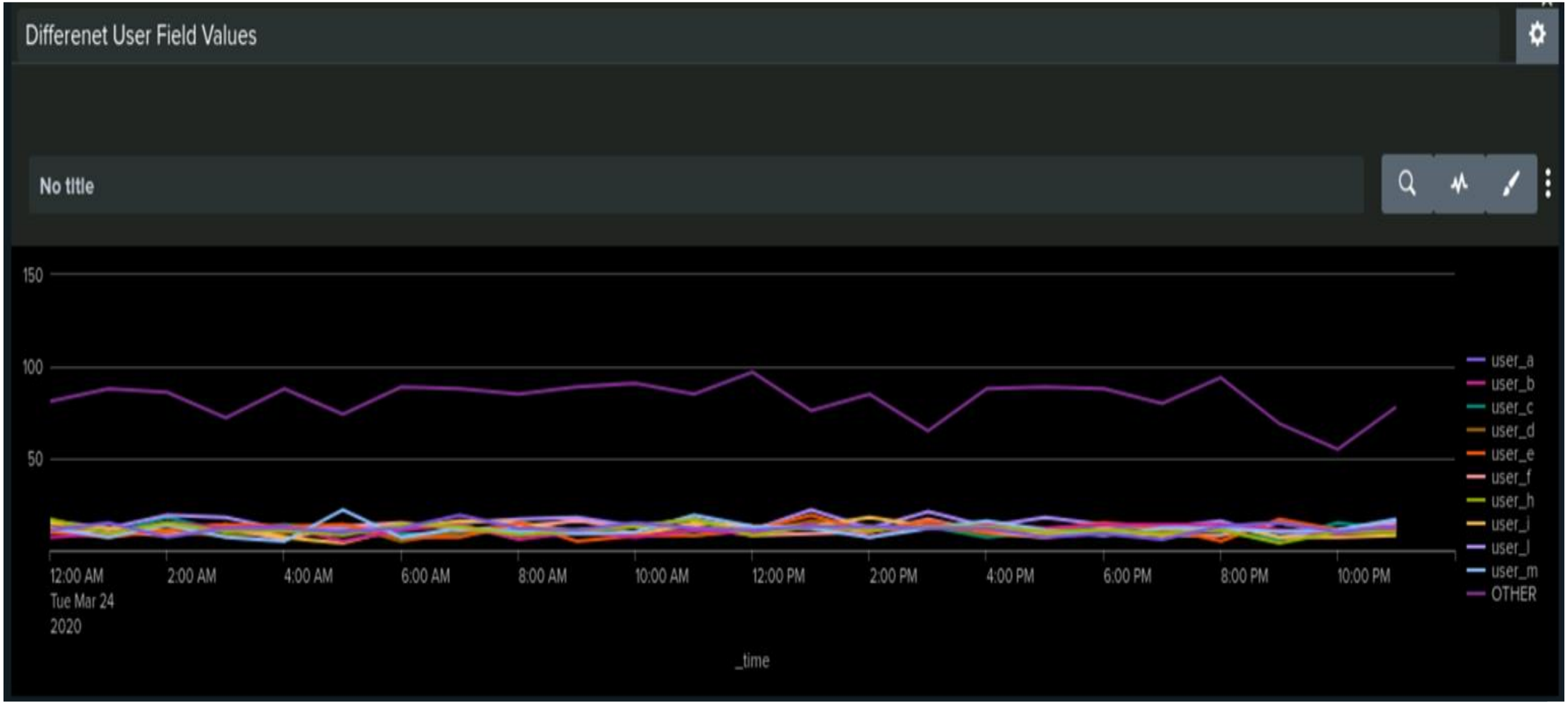
Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted 	Alert is made when the hourly count of the signature “a user account was deleted” has reached its threshold.	10	17

JUSTIFICATION: The amount of user Accounts deleted mostly stays under 10, so that is what determined our baseline. Then there are spikes that occurred once it meets the 17 threshold.

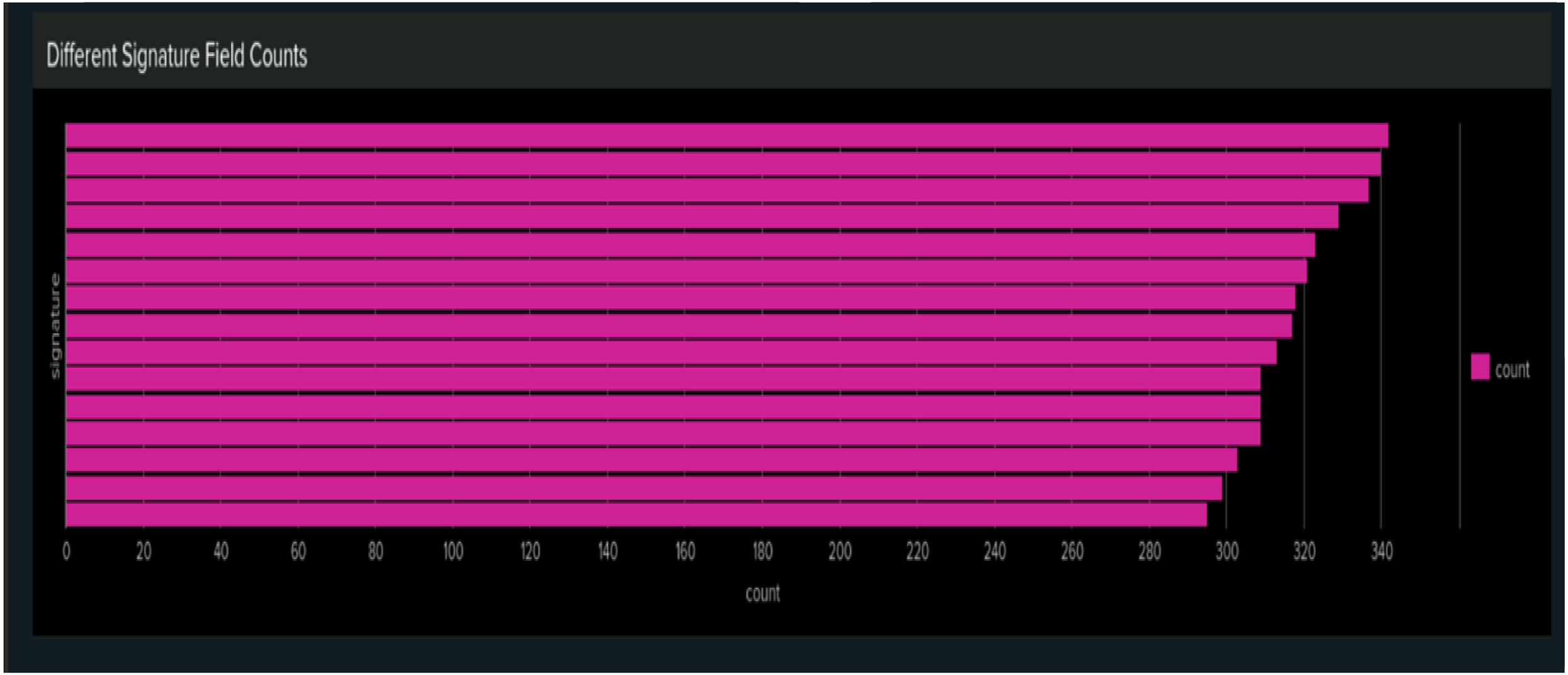
Dashboards—Windows



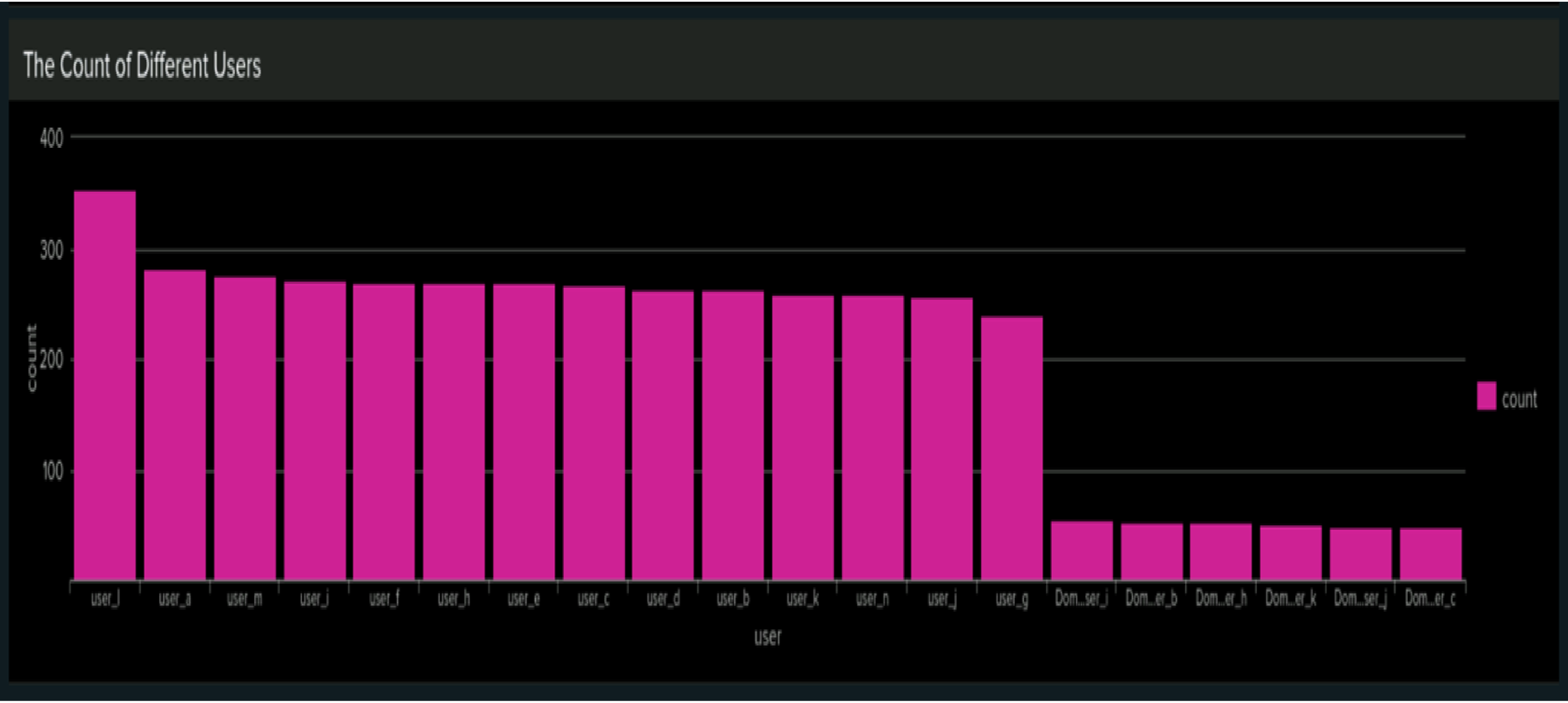
Dashboards—Windows



Dashboards—Windows



Dashboards—Windows



Apache Logs

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP Methods	Report Shows the type of HTTP Activity that is requested against the The VSI server
Top 10 Domains	Shows the 10 Domains that refer to VSI website
Count of HTTP Response Code	Shows total count of HTTP response code for each

Images of Reports-Apache

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

HTTP Methods

Edit More Info Add to Dashboard

All time

✓ **10,000 events** (before 9/29/23 2:27:13.000 AM)

Job

4 results 20 per page

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

Images of Reports—Apache

New Search

Save As ▾ Create Table View Close

```
source="apache_logs.txt"|top limit=10 referer_domain
```

All time

✓ **10,000 events** (before 9/28/23 2:25:41.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (10)** Visualization

20 Per Page ▾ Format Preview ▾

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

Images of Reports -Apache

New Search

Save As ▾ Create Table View Close

```
source="apache_logs.txt"|top limit=20 status
```

All time ▾

✓ **10,000 events** (before 9/28/23 2:27:42.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (8)** Visualization

20 Per Page ▾ Format Preview ▾

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

Alerts—Apache

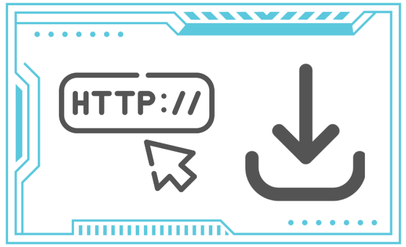
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Activity 	Alert is made when the hourly count of “non-US activity” meets the threshold.	80	170

JUSTIFICATION: The Non-US Activity showcased a range of counts, with the typical activity ranging from 100-170, with some counts falling below 100. Opted for the baseline of 80 to account for these low values, and a threshold of 170 to target any spikes that are outside of normal activity.

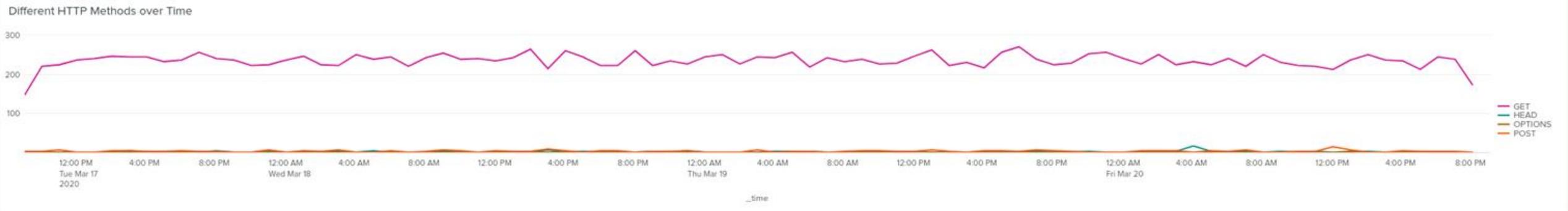
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Method 	Alert is made when the hourly count of the “HTTP POST Method” reaches the threshold.	2	7

JUSTIFICATION: Typical HTTP POST Method activity was at two (2) events per hour with spikes of six (6)+. Using this information, the baseline was set at two (2) and the threshold was set at seven (7) to flag any activity that is outside of the normal parameters.

Dashboards—Apache

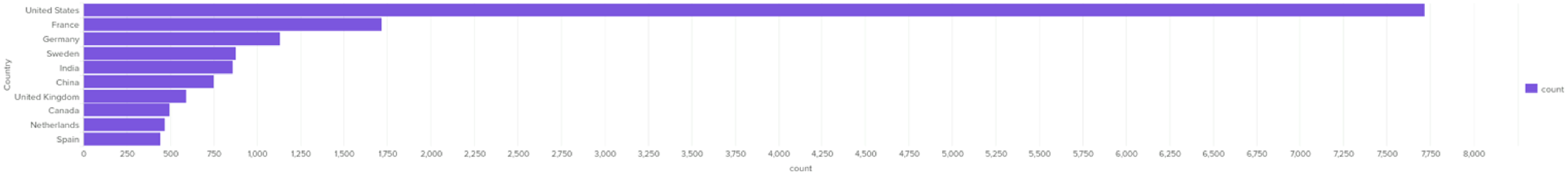


Dashboards—Apache

Bar Chart of Different URI Counts

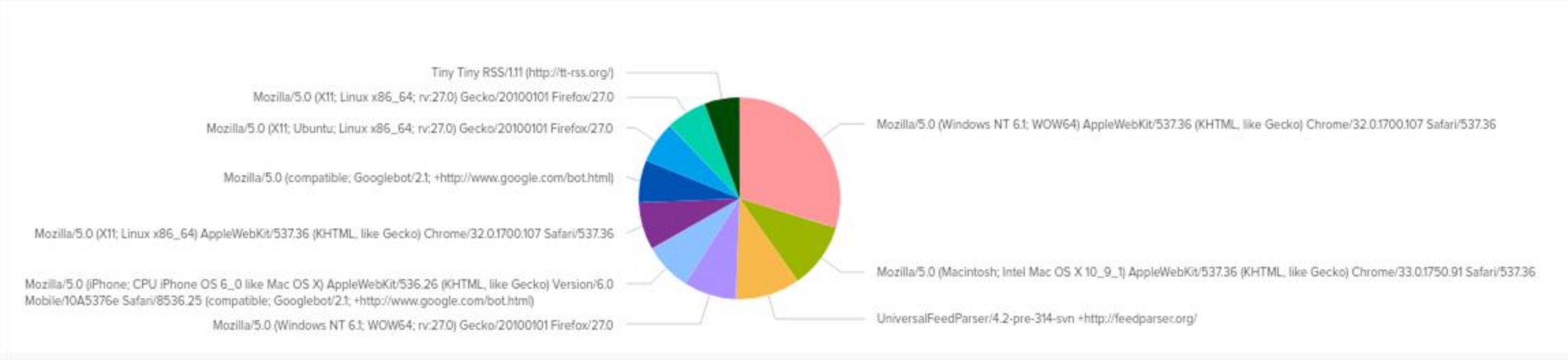
Single Value Representation of HTTP Successes

Bar Chart of Top 10 Countries



Dashboards—Apache

Different User Agents



Attack Analysis

Attack Summary—Windows

- Our Summary from analyzing the Windows attack logs showed that Windows had more high severity levels than informational. There were also more successes than failures after the attack. Alerts also showed suspicious volume of failed activities.
- There were 35 failed logins that occurred at 8am on 03/25/2020. Our threshold was successful. No changes are recommended.

Attack Summary—Windows

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

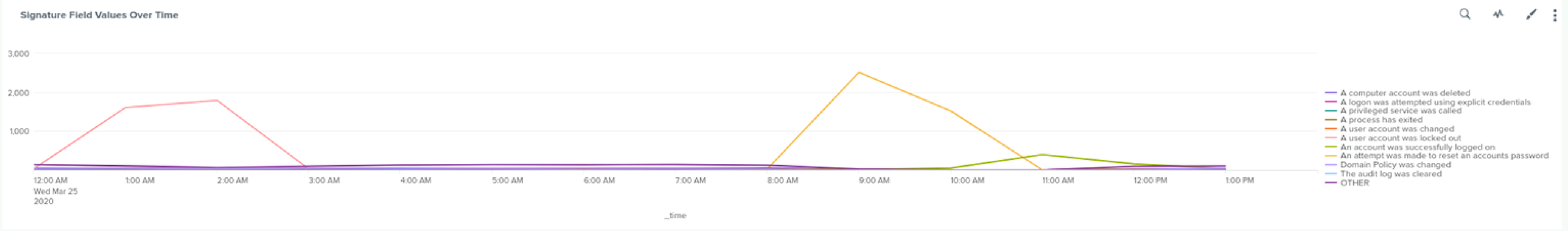
- Our thresholds for the alerts were correct in order to recognize that the attacks were happening without giving any false positives.

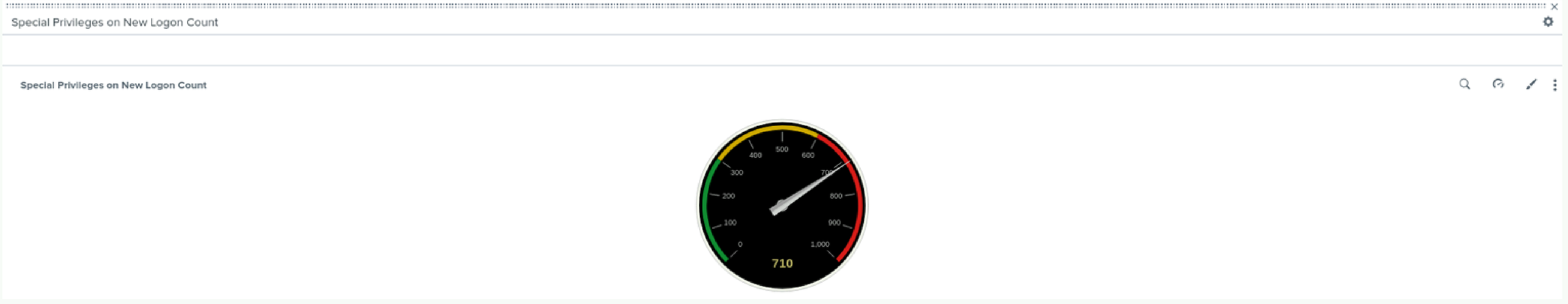
Attack Summary—Windows

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

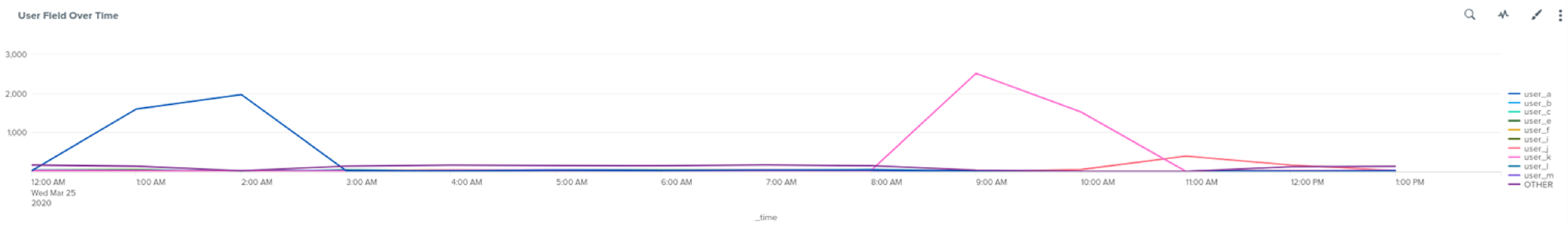
- When comparing the two dashboards from before the attack and the dashboard during the attack. The dashboards do a great job of visualizing the spikes of certain information.

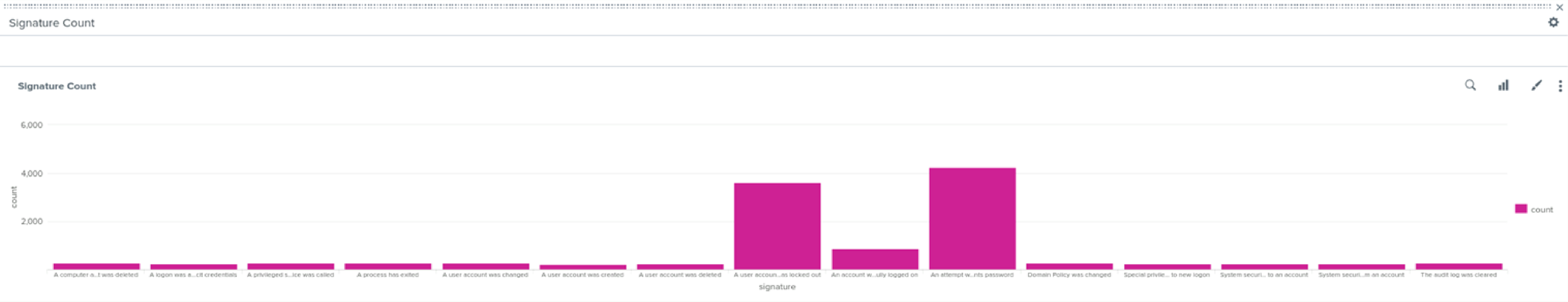
Screenshots of Windows Attack Logs



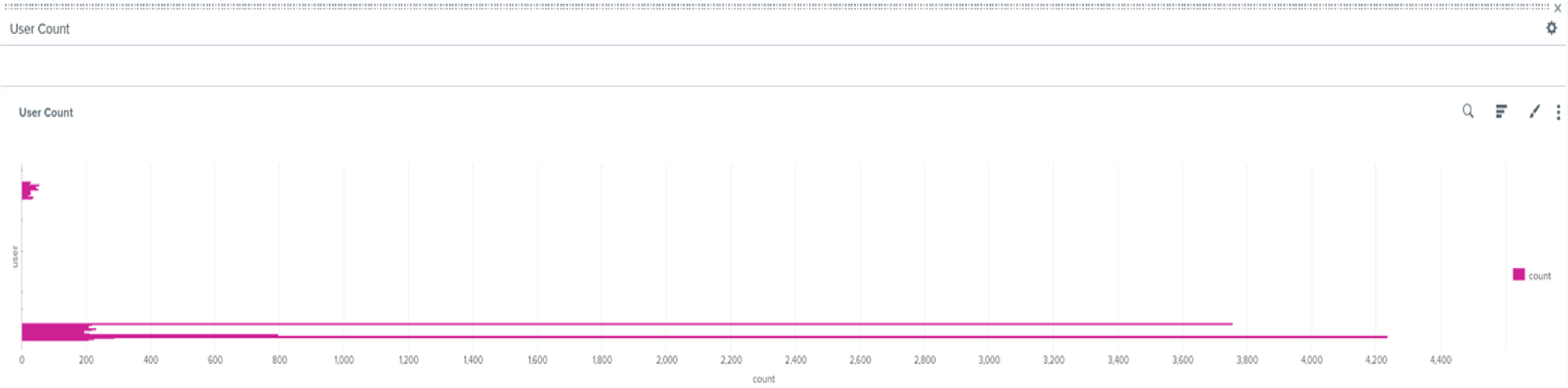


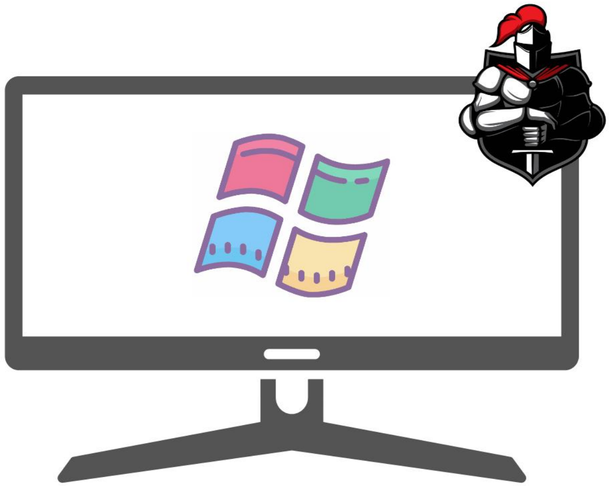
Screenshots of Windows Attack Logs

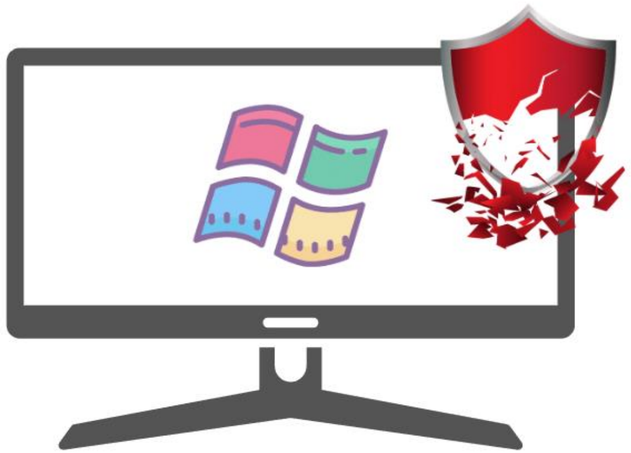




Screenshots of Windows Attack Logs



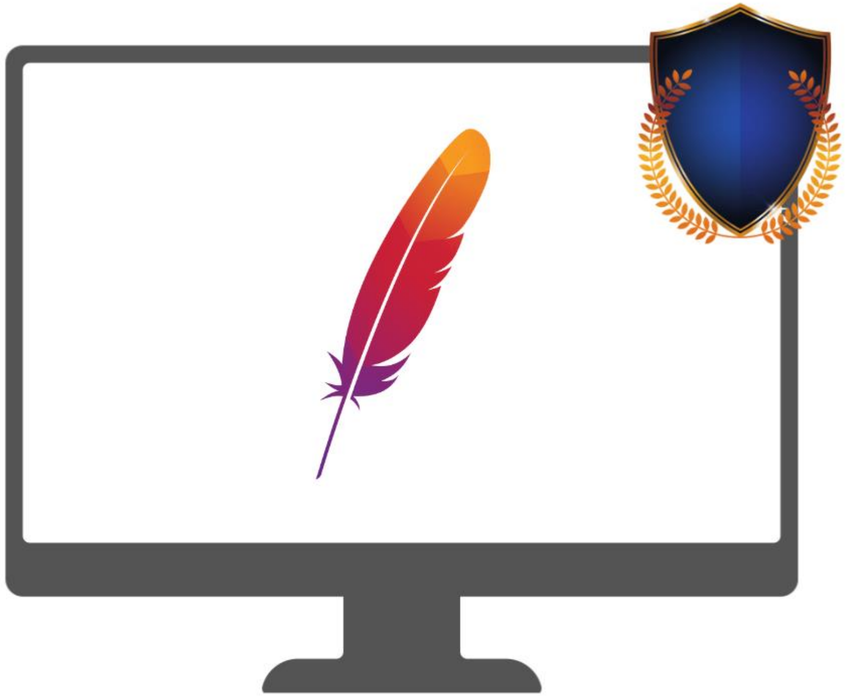




Attack Summary—Apache

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

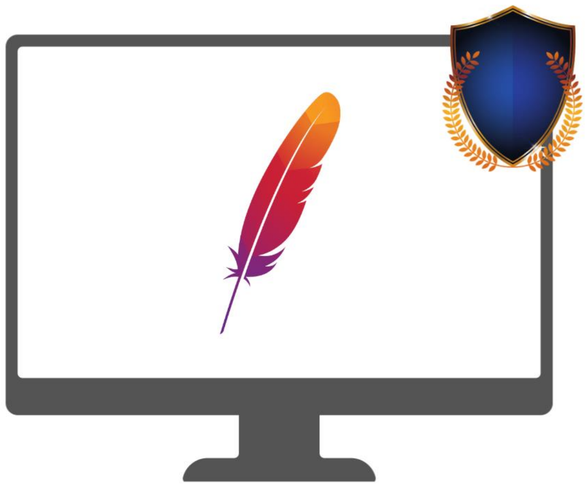
- The attack logs show that there was an attempted DDoS attack by sending a large amount of POST requests to the server



Attack Summary—Apache

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

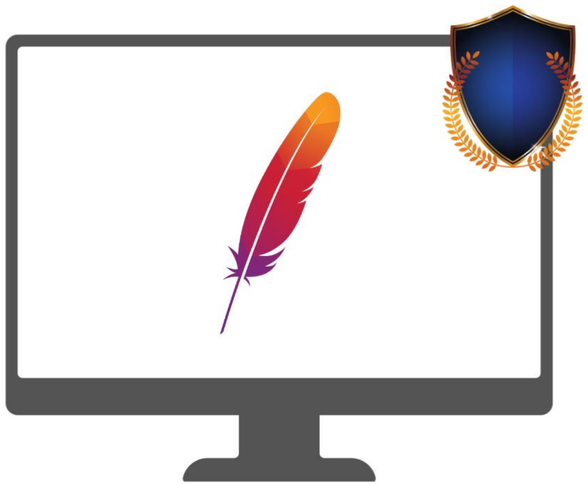
- The alert thresholds did well to alert the SOC team that an attack was happening without creating any false positives.
- The alerts showed that the POST method was rising much higher than it had on what was deemed a normal day



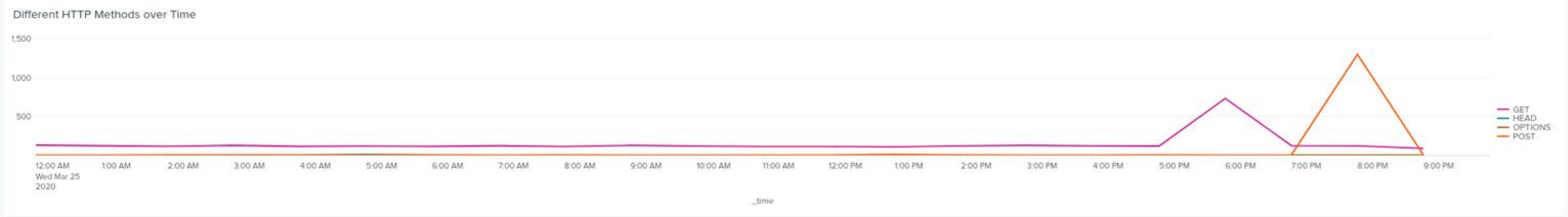
Attack Summary—Apache

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

- The dashboard helped visualize the breakdown of how the attack was happening through the POST method.
- The graphs on the dashboard also showed that there was a spike in account logon URIs that were being accessed.

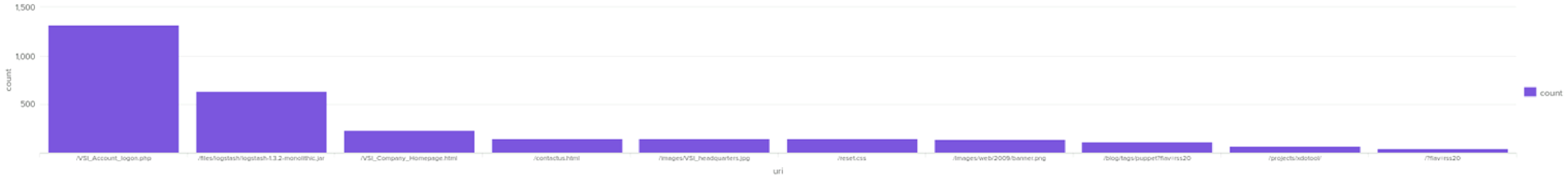


Screenshots of Apache Attack Logs

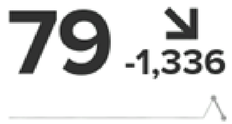


Screenshots of Apache Attack Logs

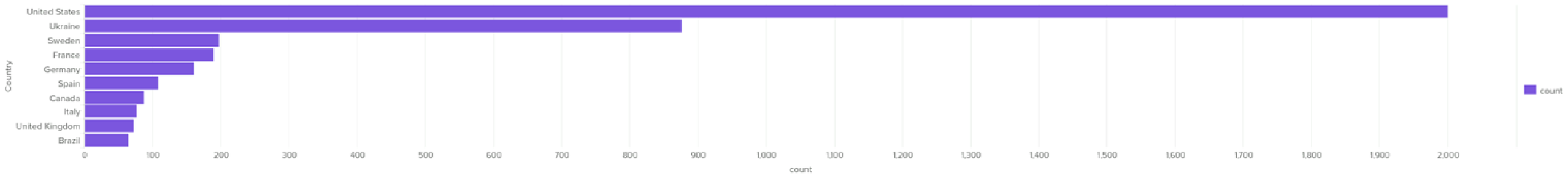
Bar Chart of Different URI Counts



Single Value Representation of HTTP Successes

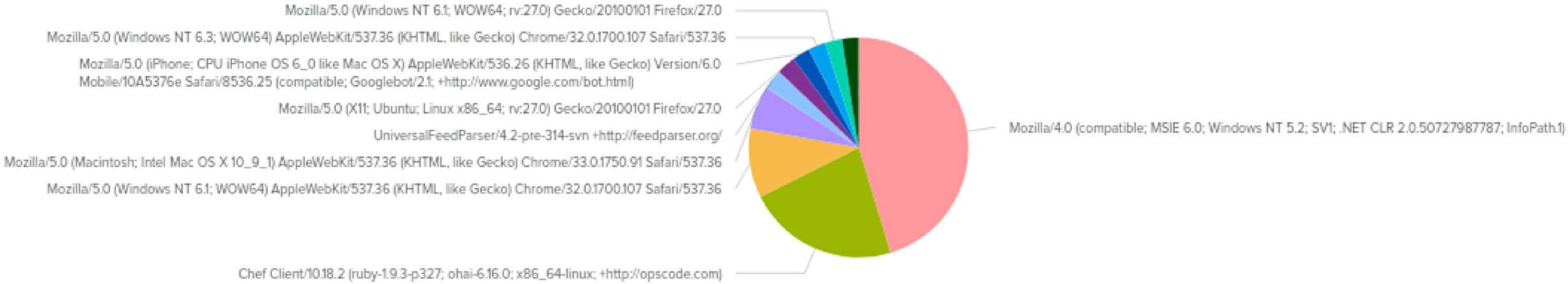


Bar Chart of Top 10 Countries



Screenshots of Apache Attack Logs

Different User Agents



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
  - Our findings found that on March 25th VSI had multiple attacks, mainly brute force attacks on their Windows and Apache Servers. We also detected password spamming attacks from different countries.
- To protect VSI from future attacks, what future mitigations would you recommend?
  - Set a limit on the amount of login attempts before users are locked out
  - To Prevent Brute Force attacks, enable Two-factor authentication.