Defensive Security Project
by: Evan Kraft, Omar Rayo, & Adam Franklin

Scenario

- Our company, Virtual Space Industries(VSI) has been tasked to use Splunk to monitor against potential attacks
- One of our competitors, JobeCorp has been rumored to be launching cyber attacks against VSI
- We analyzed Windows and Apache logs to help develop risk mitigation tactics for VSI to deploy

Table of Contents

This document contains the following resources:

VSI Corporation Website Monitoring

By: Luke Murphey

[Website Monitoring]

The "Website Monitoring" add-on for Splunk is a tool that enables the monitoring and analysis of website performance and availability using Splunk's data analytics platform. It allows organizations to track and measure various aspects of website performance, such as response time, availability, and error rates.

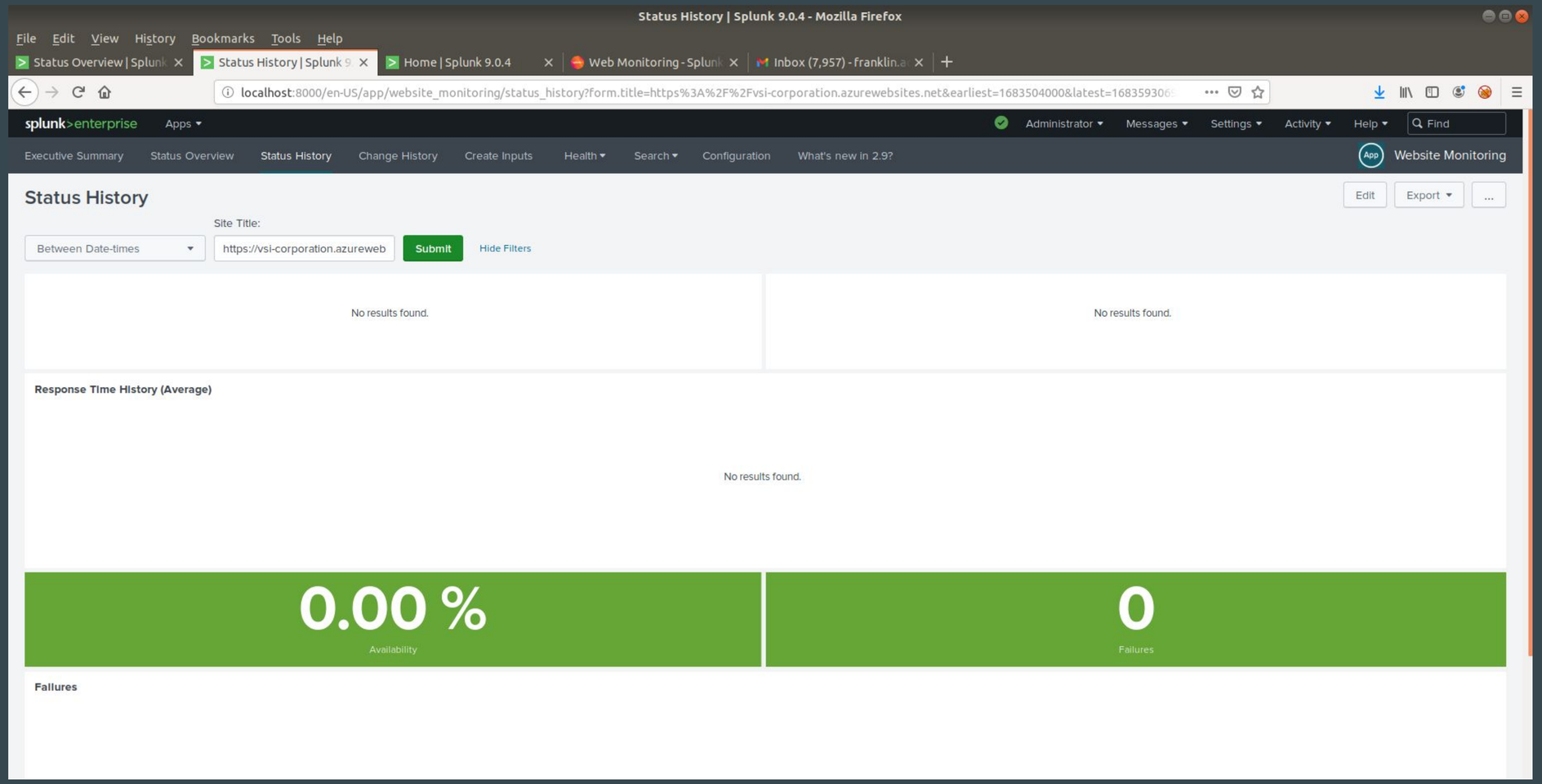
With the Website Monitoring add-on, users can configure monitors to periodically check specific URLs or endpoints of their websites. These monitors simulate user interactions and collect data on metrics like response time, DNS resolution, SSL handshake, and HTTP status codes. The add-on supports monitoring HTTP, HTTPS, and other protocols.

The collected data is put into Splunk, where it can be analyzed, visualized, and correlated with other data. This provides valuable insights into website performance, helps identify performance bottlenecks, troubleshoot issues, and optimize website availability and user experience.

[Website Monitoring]

Imagine VSI Corporation utilizes the "Website Monitoring" add-on for Splunk to monitor an online store. One day, they notice a sudden increase in website response time and a high number of errors being returned. With the add-on's real-time alerts, the IT team is immediately notified and investigates the issue. They identify a server overload caused by unexpected traffic. Prompt action is taken to optimize server resources, resolving the performance issue swiftly. As a result, VSI Corporation can ensure a smooth shopping experience, preventing potential revenue loss and maintaining customer satisfaction.

[Website Monitoring]



Logs Analyzed

1 Windows Logs

The Windows Logs show system performance and data that can be narrowed down into different categories. For example, user logins and account management.

2 Apache Logs

The apache logs shows the Client’s Ip. They also show data of what devices and browsers that the clients are using. The logs also show the method and https status code which are helpful for building a report.

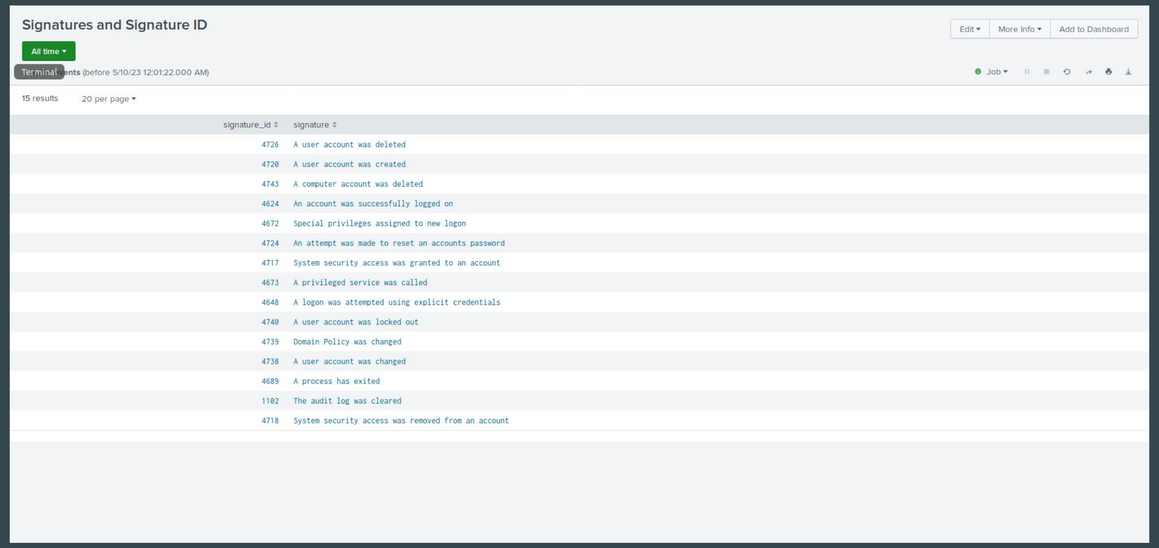
Windows Logs

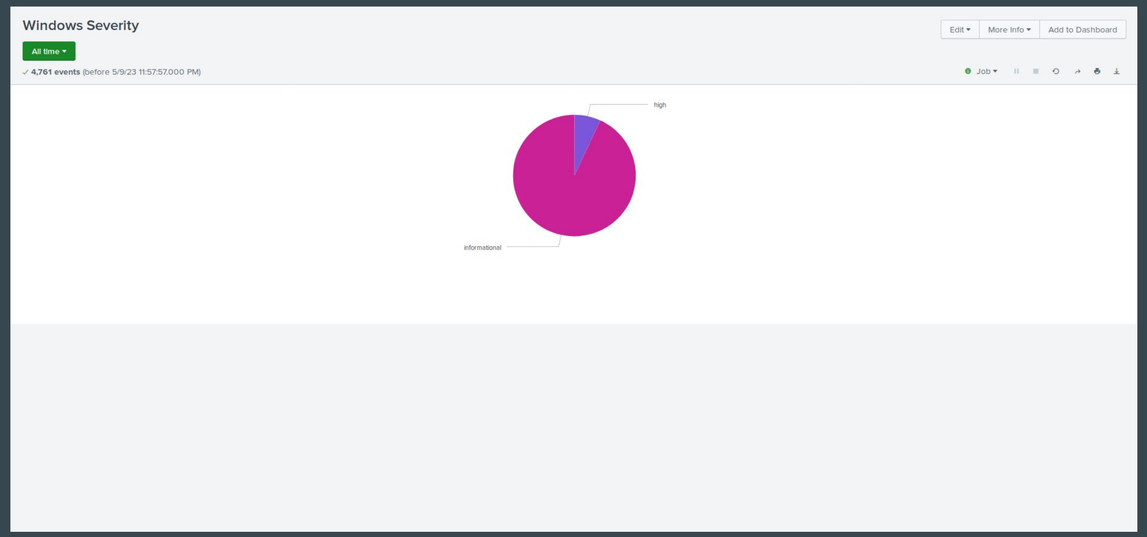
Reports—Windows

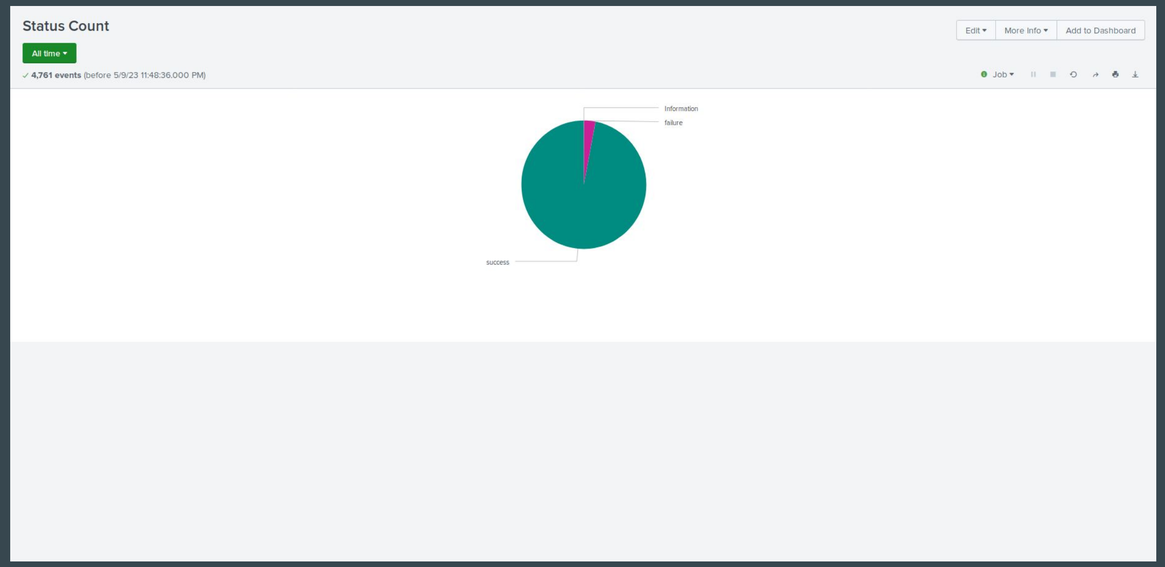
Designed the following reports:

Report Name	Report Description
Signatures and Signature ID	Displays the ID number associated with a specific signature
Windows Severity	Displays severity level of logs and count of each
Status Count	Displays comparison between success and failure of activities

Images of Reports—Windows







Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Failed Windows Activity	This alert will be triggered when the threshold of hourly failed Windows activities has been reached	5	8

JUSTIFICATION: The average of failed logins was around 5 and 8 or above is to us considered an outlier

Alerts—Windows

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Signature Count for “A user account was deleted”	This alert will be triggered when “A user account was deleted” reaches its hourly threshold	10	20

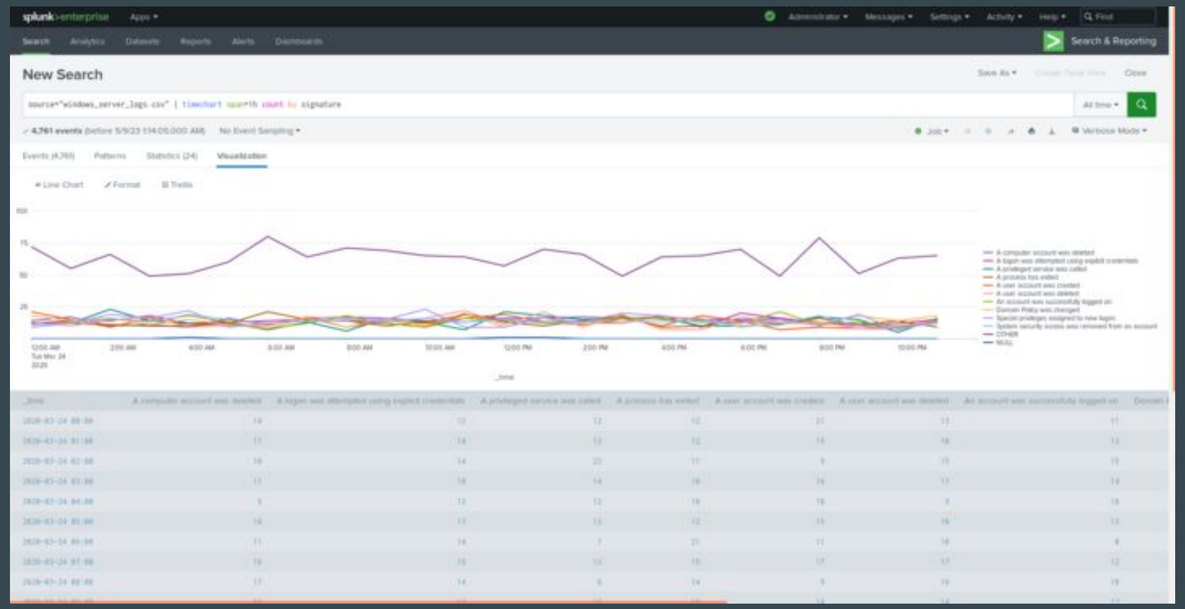
JUSTIFICATION: The average times a user account was deleted occurred was around 10. We consider 20 to be highly suspicious

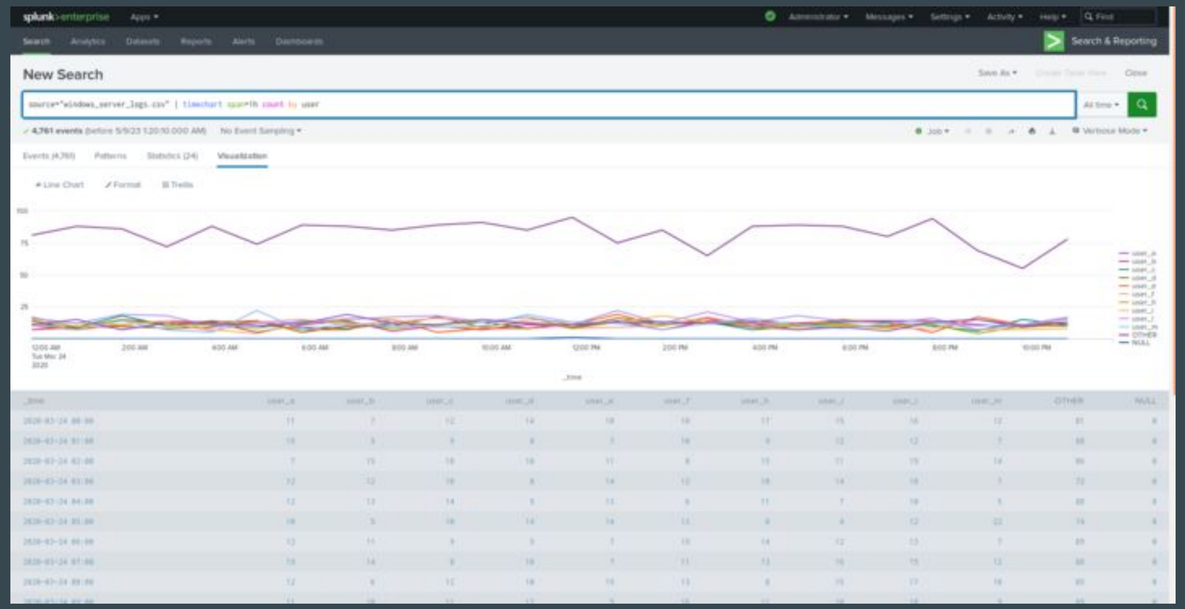
Alerts—Windows

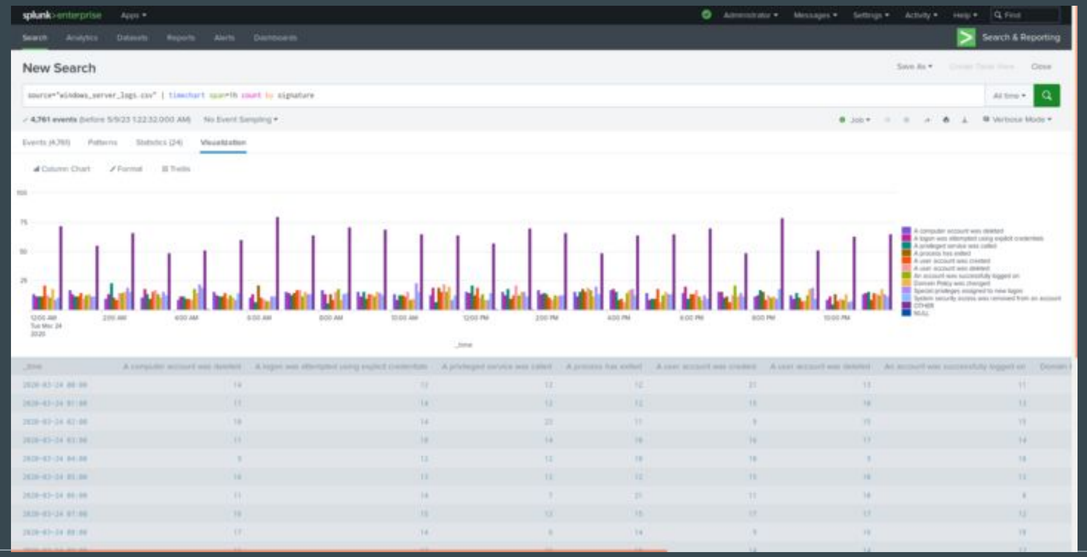
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Signature Count for “An account was successfully logged on”	An alert will be triggered when a threshold for how many times “an account was successfully logged on” has be reached in an hour	10	15

JUSTIFICATION: 10 was about the average times an account was successfully logged on. 15 was a number we determined was suspicious

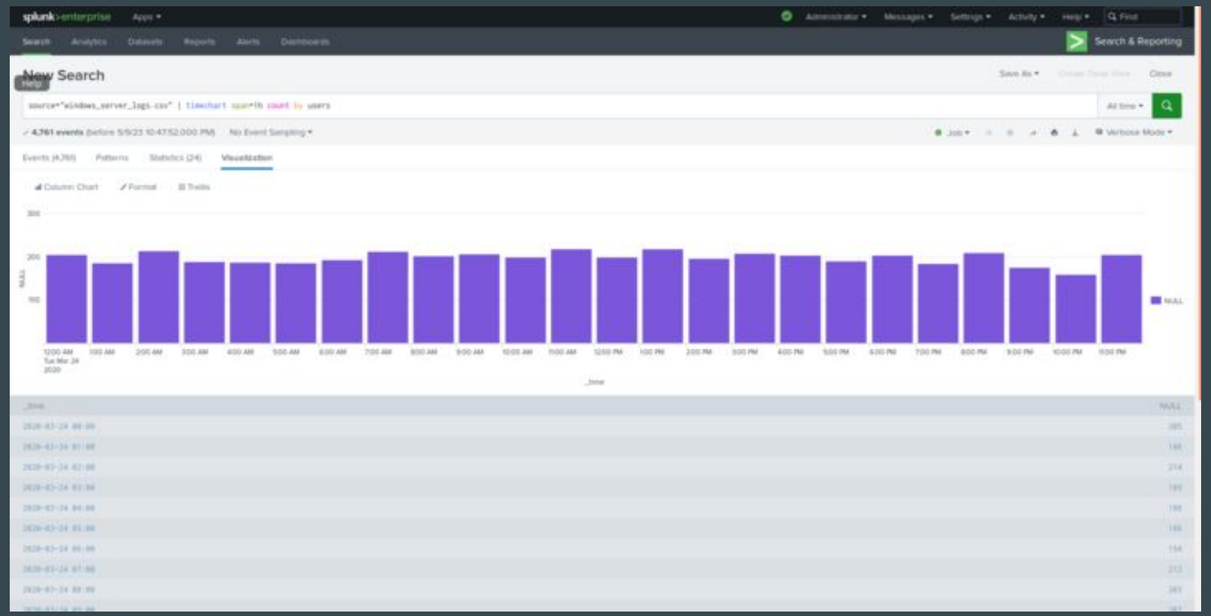
Dashboards—Windows

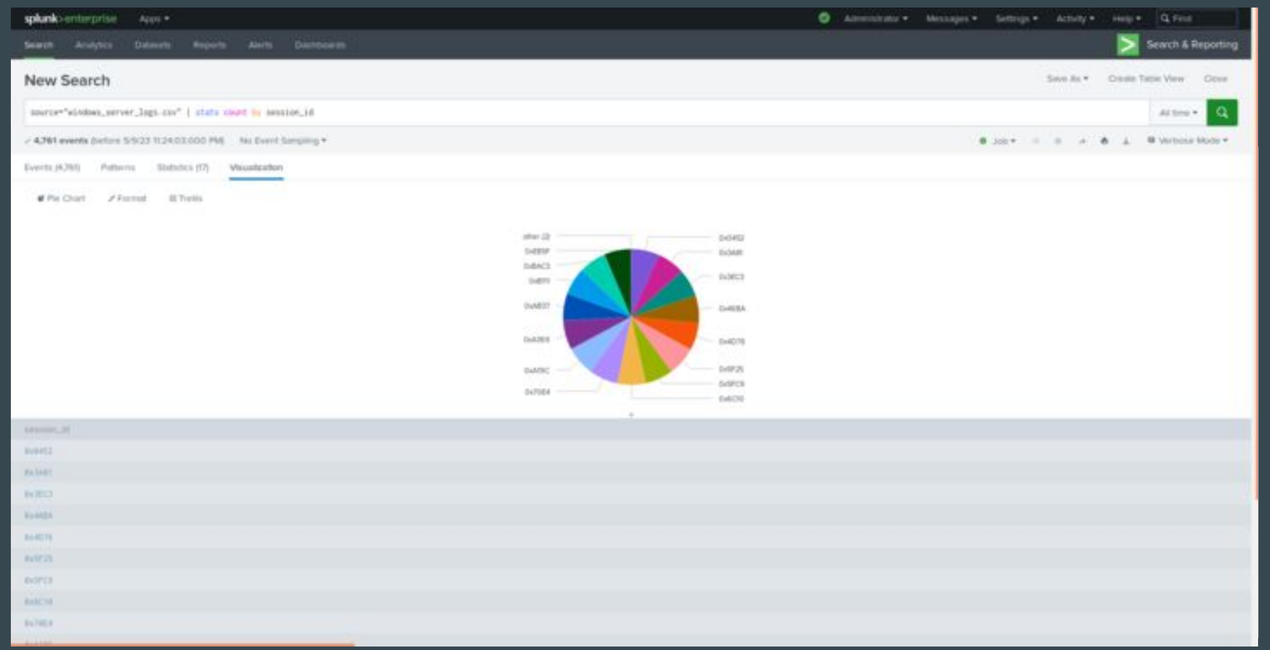






Dashboards—Windows





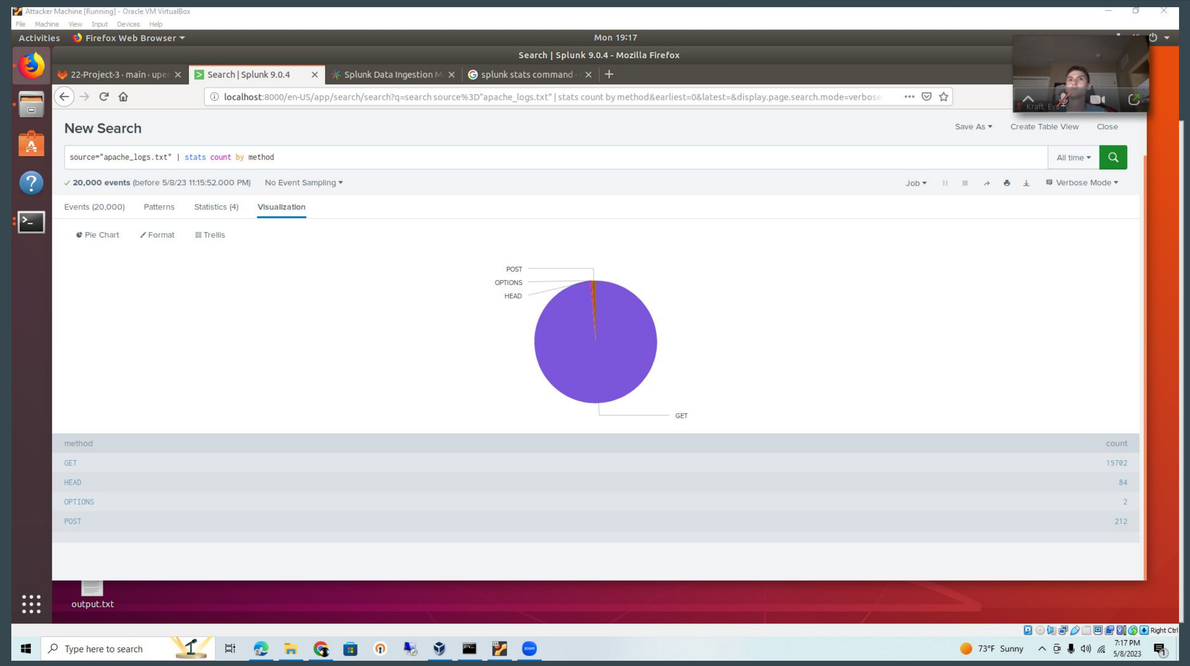
Apache Logs

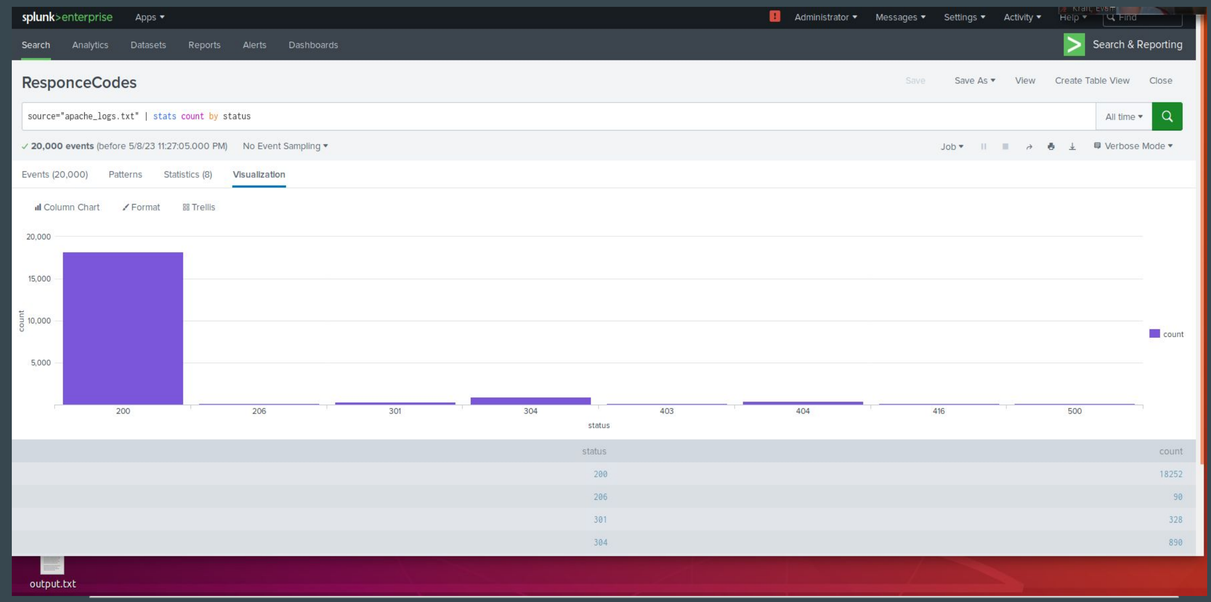
Reports—Apache

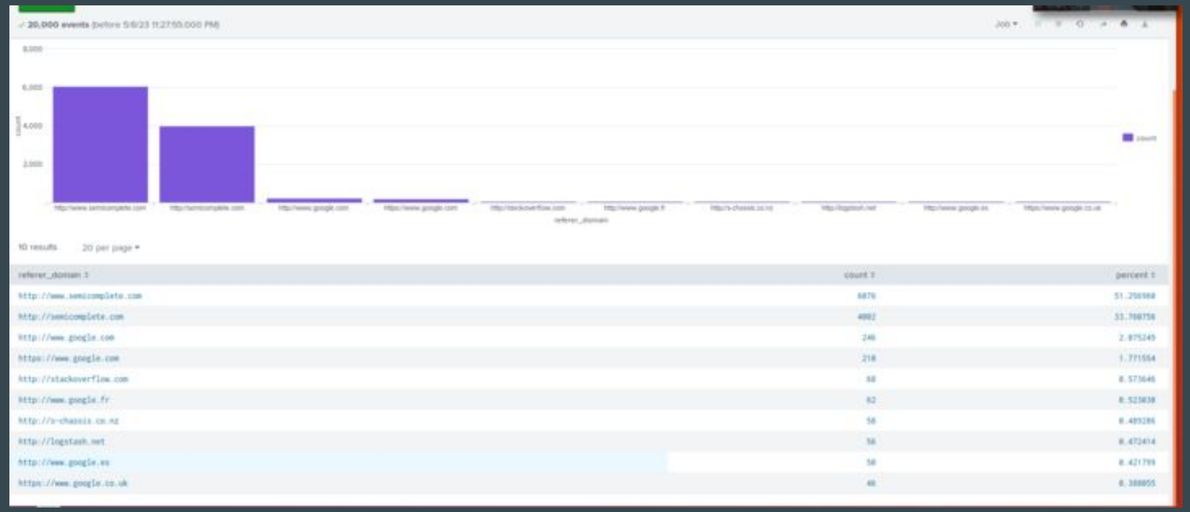
Designed the following reports:

Report Name	Report Description
HTTP Methods	Provides the type of HTTP activity being requested
Top 10 Domains	Ranking the top 10 domains that refer to VSI’s website
Response Codes	Displays response codes and insight on suspicious responses

Images of Reports—Apache







Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert_Japan_Request_per_hour	This alert is for when Japan’s activity reaches its threshold	14	20

JUSTIFICATION: The reason for the threshold was because the high was 58 and then after the high we saw a range from 2-14. This threshold seemed like a good indicator for suspicious activity.

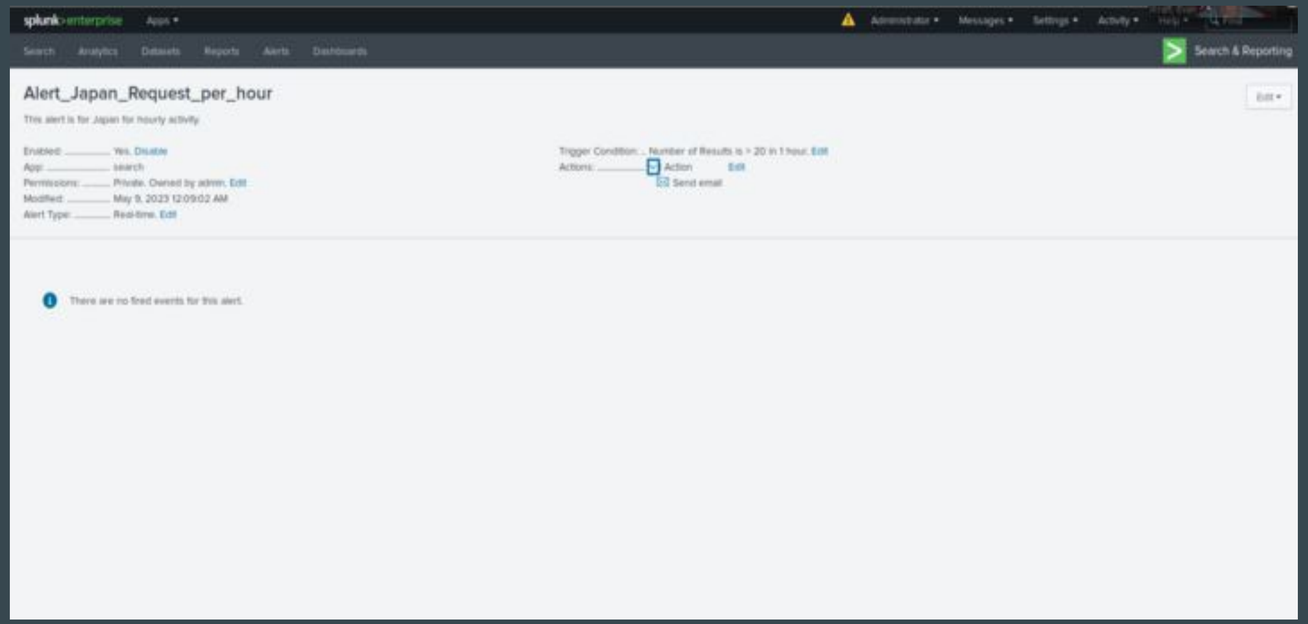
Alerts—Apache

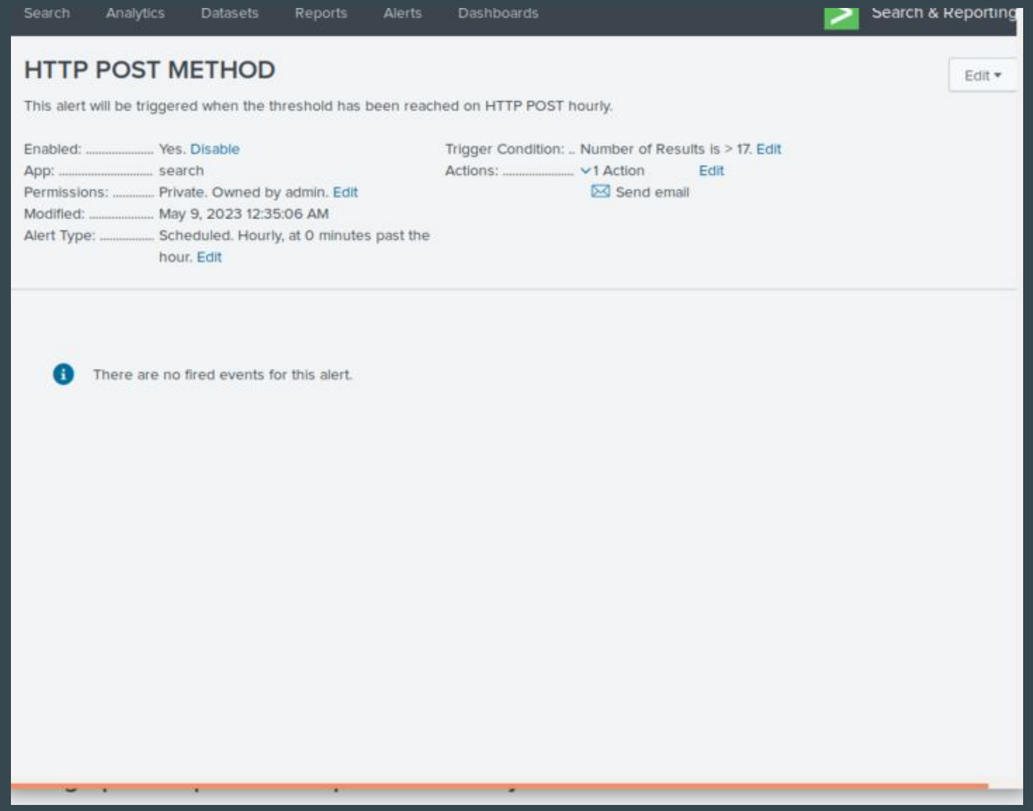
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Method	This alert will be triggered when the threshold of HTTP POST requests is reached	13	17

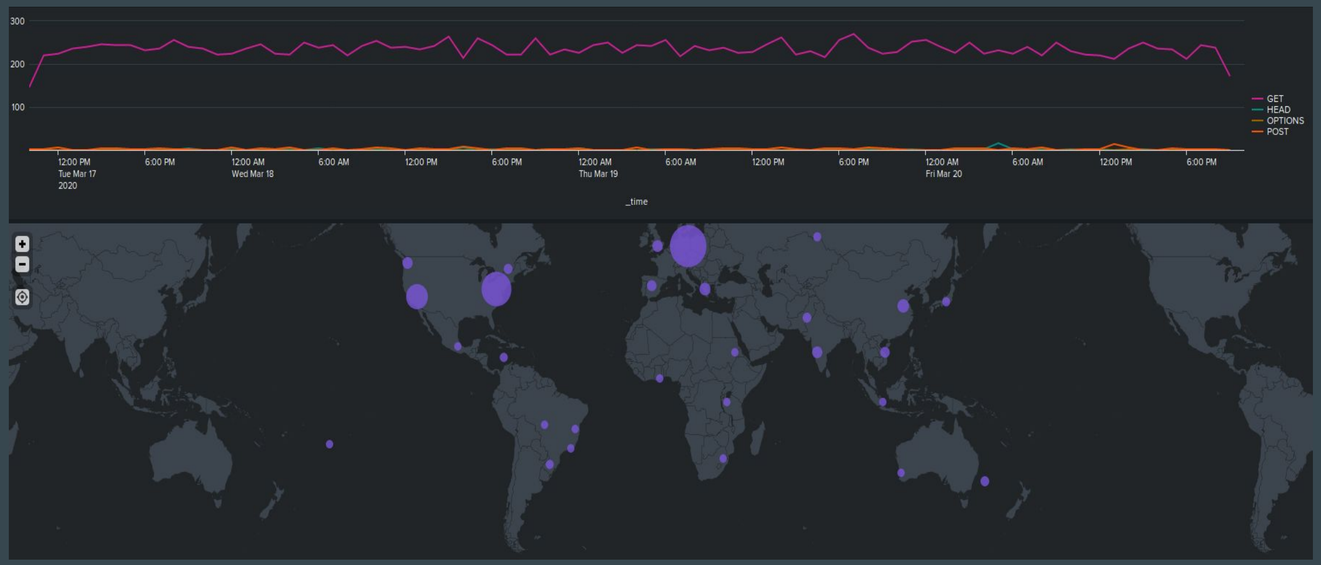
JUSTIFICATION:The reason for having 17 for the threshold is because we saw a high of 20. Anything lower than 17 seemed to be normal.

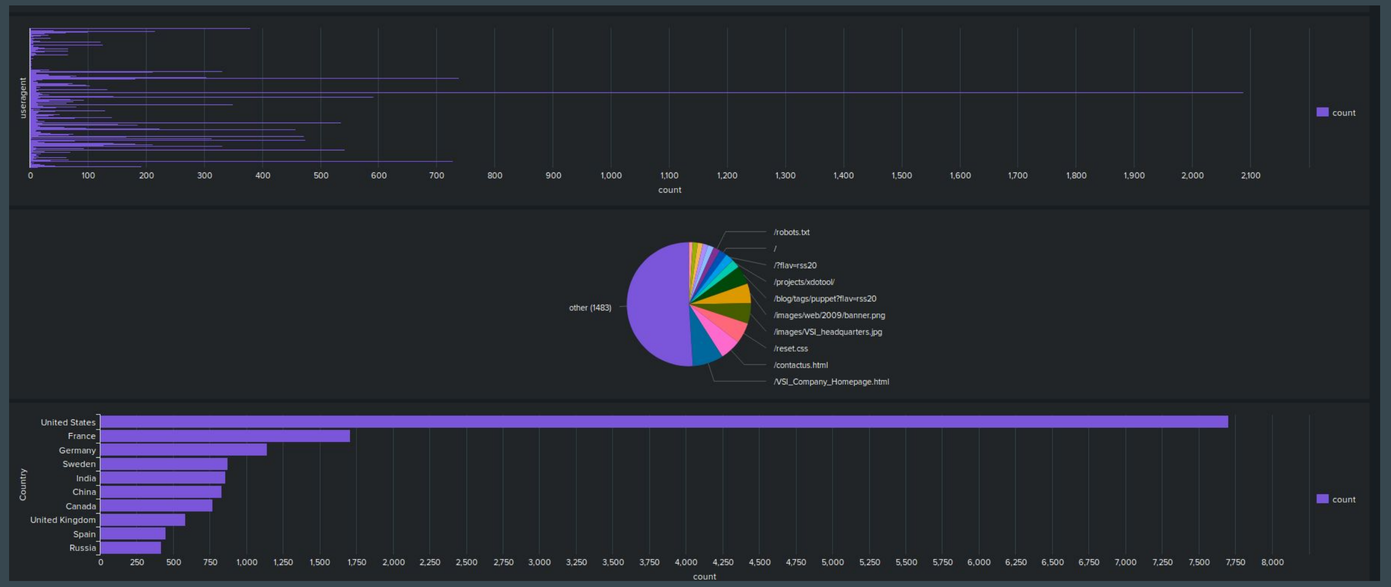
Alerts—Apache





Dashboards—Apache





Attack Analysis

Attack Summary—Windows

Findings from our reports when analyzing the attack logs.

- User_a and User_k had a suspicious amount of activity that was in big clusters
- Their activity in the prior logs was significantly lower and spread out in time

Attack Summary—Windows

Findings from our alerts when analyzing the attack logs.

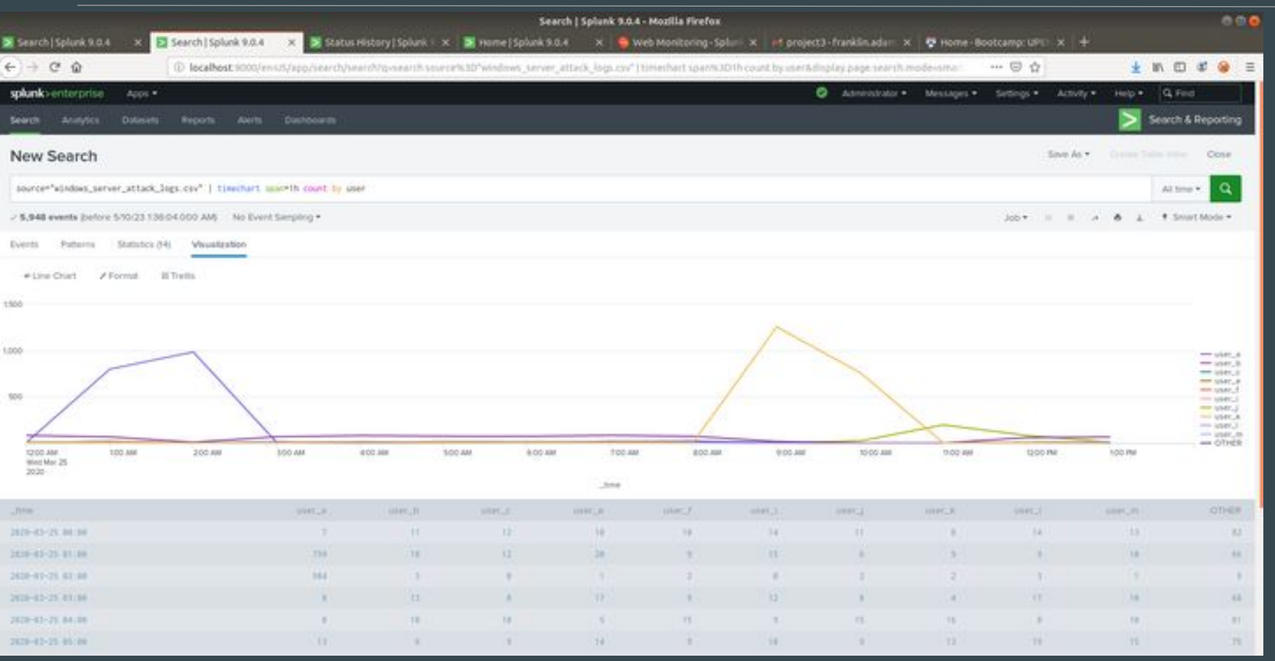
- Our initial thresholds could be increased as that threshold was only surpassed by 2 users and all of their suspicious activity was much higher than the baseline

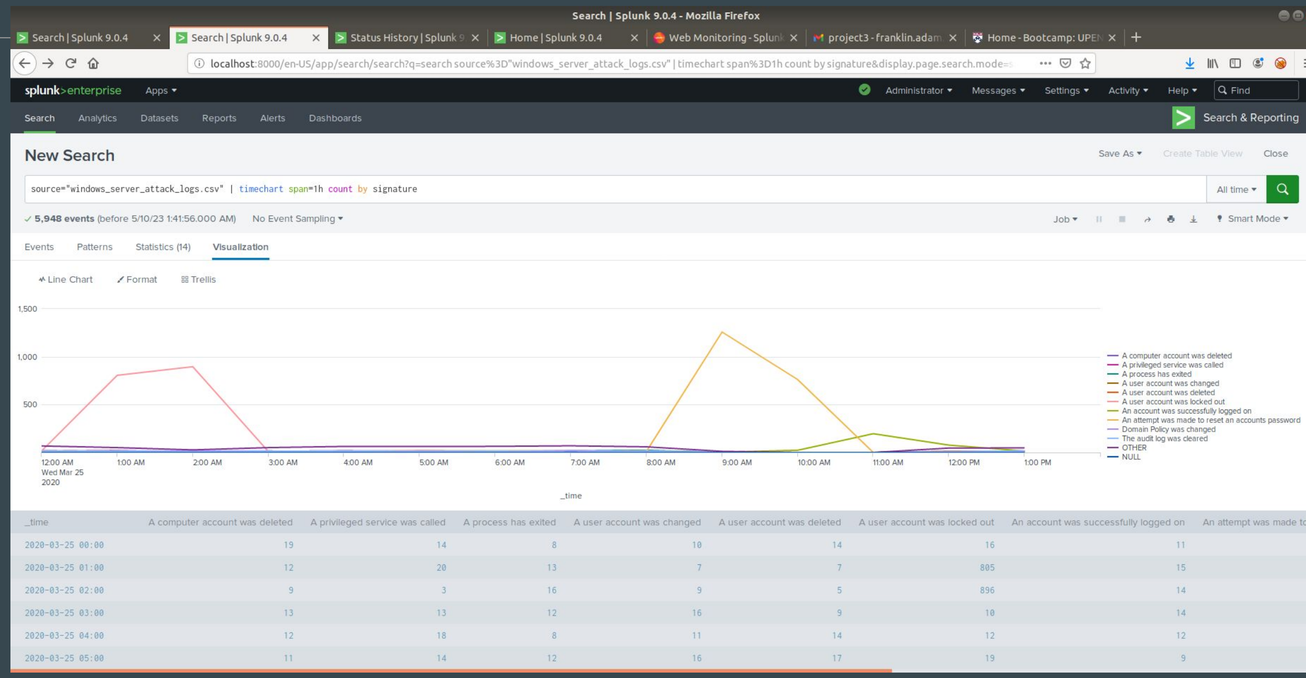
Attack Summary—Windows

Findings from our dashboards when analyzing the attack logs.

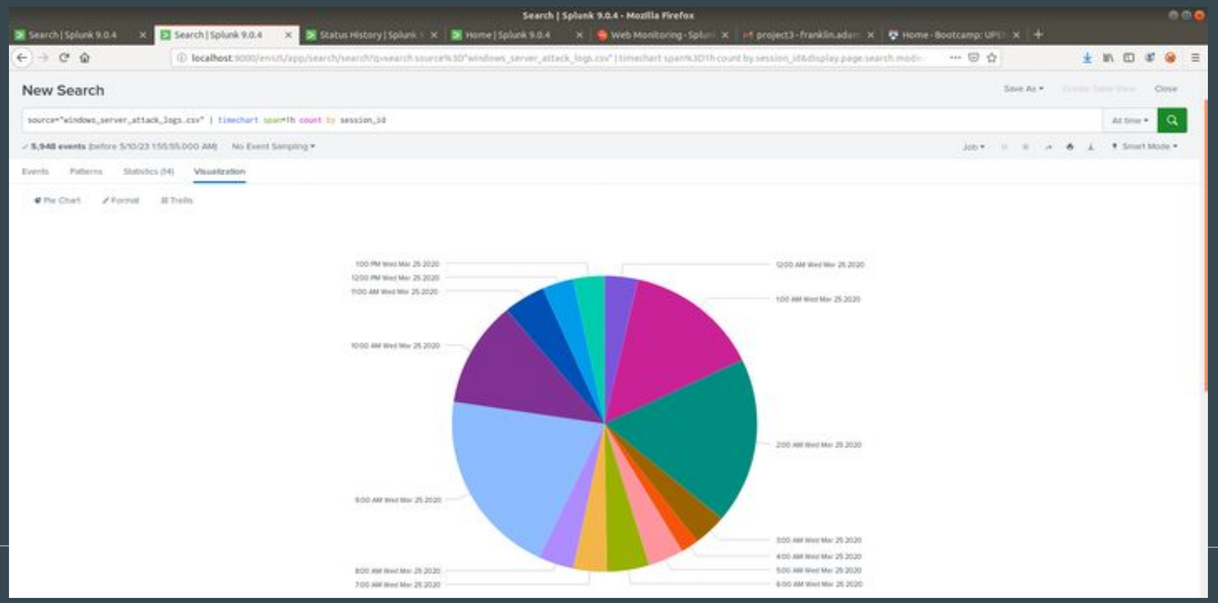
- Our findings seem to show that “user_a” had a large amount of account lockouts, possibly from login attempts.
- Additionally “user_k” had a large amount of attempts to reset a password that could be a similar type of brute force attack as seen with “user_a”.
- Both of these events lasted about 2-3 hours respectively.

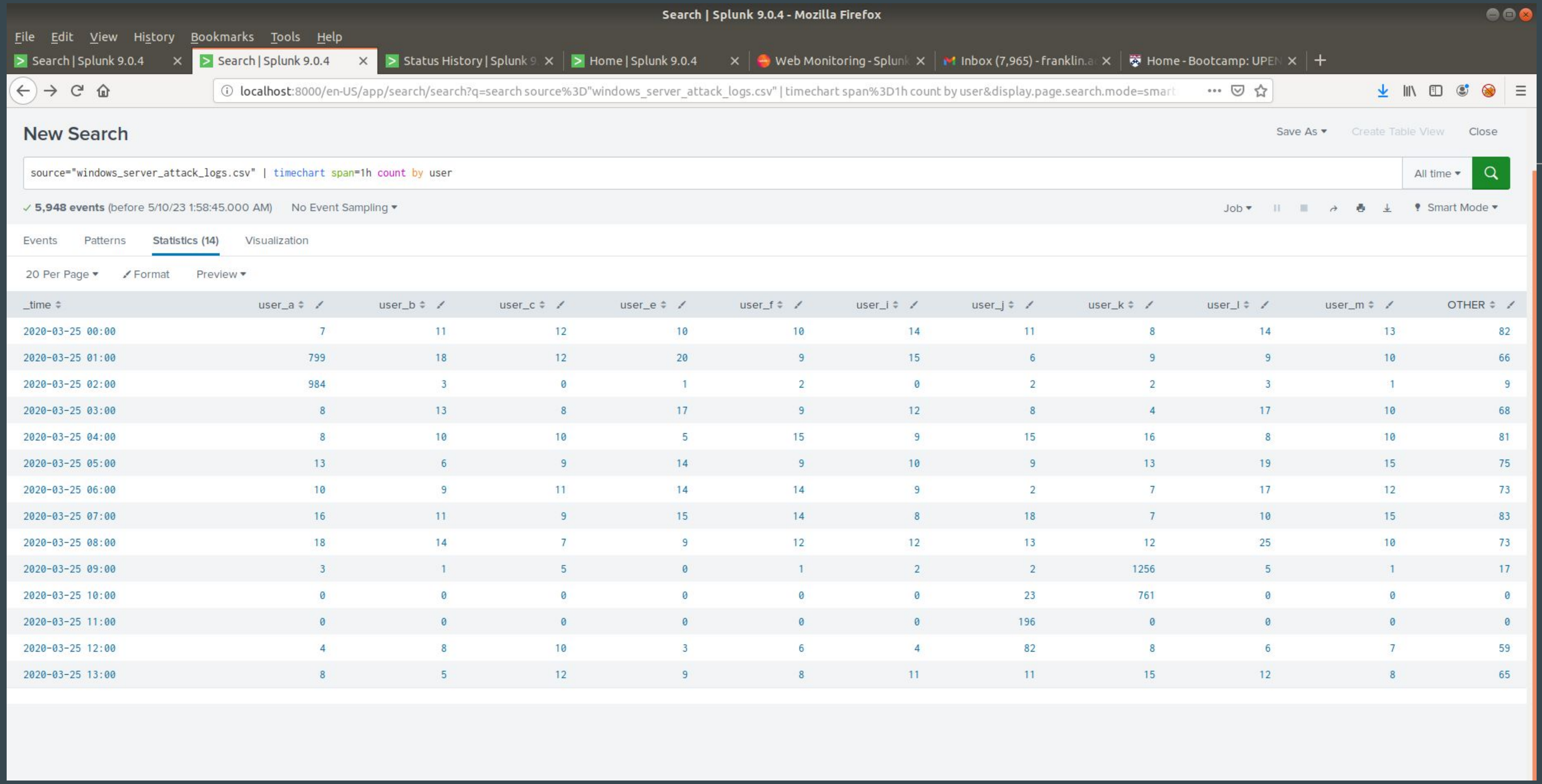
Screenshots of Attack Logs



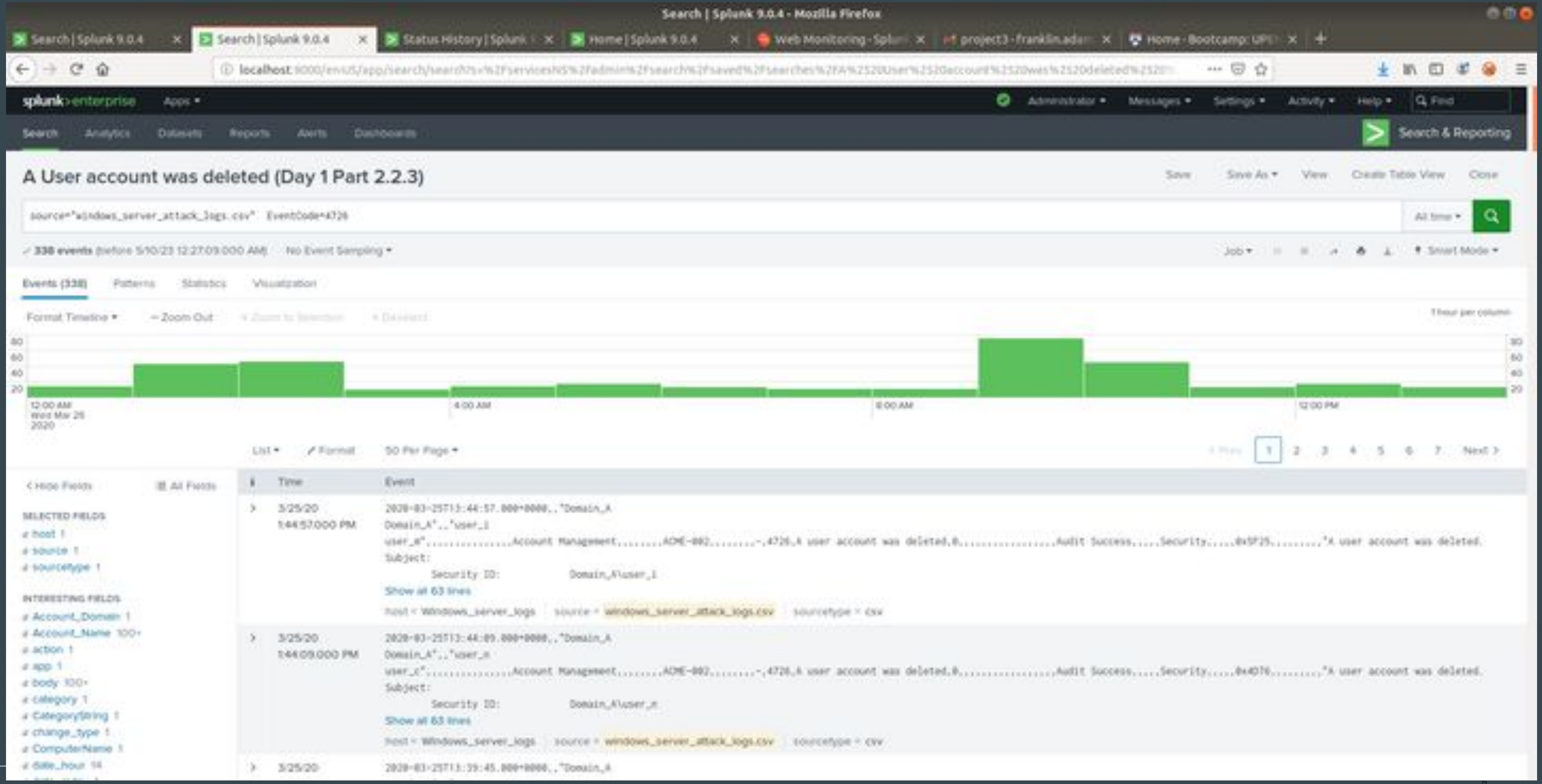


_time	A computer account was deleted	A privileged service was called	A process has exited	A user account was changed	A user account was deleted	A user account was locked out	An account was successfully logged on	An attempt was made to
2020-03-25 00:00	19	14	8	10	14	16	11	
2020-03-25 01:00	12	20	13	7	7	805	15	
2020-03-25 02:00	9	3	16	9	5	896	14	
2020-03-25 03:00	13	13	12	16	9	10	14	
2020-03-25 04:00	12	18	8	11	14	12	12	
2020-03-25 05:00	11	14	12	16	17	19	9	





_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	15	83
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	4	8	10	3	6	4	82	8	6	7	59
2020-03-25 13:00	8	5	12	9	8	11	11	15	12	8	65



Attack Summary—Apache

Findings from our reports when analyzing the attack logs.

- We found that HTTP methods POST and GET had a combined 2000+ requests. The time of both requests started at 6pm and end at 9pm. In the attack log we saw a significant decrease in user activity. We saw the amount of 404 errors rose. We received about 1296 POST requests at 8pm.

Attack Summary—Apache

Findings from our alerts when analyzing the attack logs. Were the thresholds correct?

- Our alert for outside IP was not configured properly.We did see that Ukraine had some very suspicious activity and rose to second most visited country. There were about 2000 event counts from 6pm to 8pm and the majority of the count came from Ukraine and the U.S. The HTTP POST alert would have been triggered with the attacks clearing the 17 count threshold.

Attack Summary—Apache

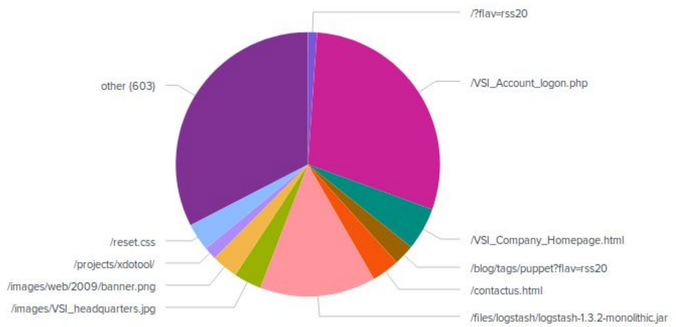
Findings from our dashboards when analyzing the attack logs.

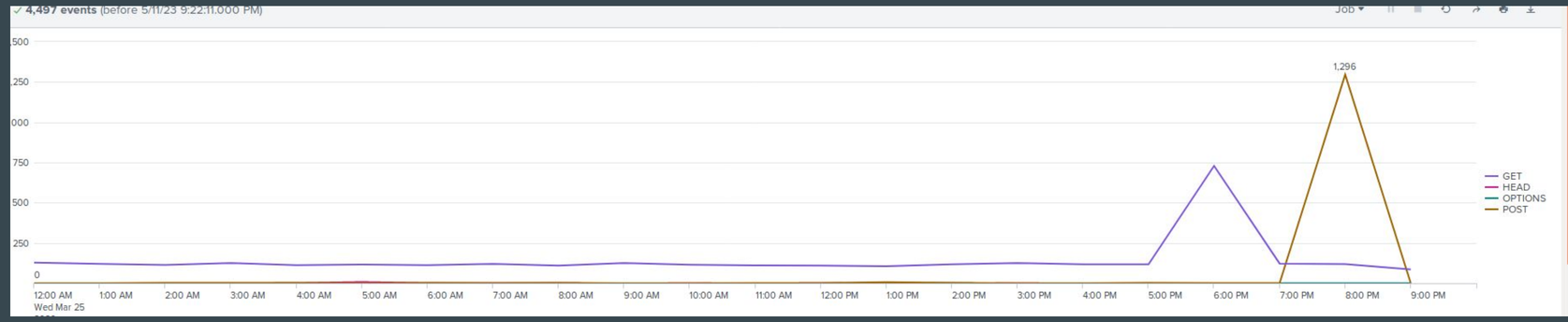
- The amount of HTTP GET and POST were visible and tightly connected by time and IP. The attack seem to be DOS or DDOS attack at first glance with the 404 error status it seemed like that was the attack method. Then when looking at the cluster map and URI data, I saw Ukraine rocket to second and the most visited uri was VSI_Account_logon.php went from 202 count at 1% to 29.42% at 1323 count.
- The attacker may have tried to do a brute force attack.

Screenshots of Attack Logs

/VSI_Account_logon.php	194.105.145.147	432
/VSI_Account_logon.php	194.146.132.138	432
/VSI_Account_logon.php	79.171.127.34	432

Country	count	percent
United States	1975	43.918168
Ukraine	877	19.501890
Sweden	198	4.402935
France	186	4.136091
Germany	161	3.580165
Canada	132	2.935290
Spain	110	2.446075
Italy	77	1.712253
United Kingdom	71	1.578830
	65	1.445408





Summary & Future Mitigations

Project 3 Summary

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

  In the logs we see that there may have been a brute force attack on the log in and also that the attacks may have been trying to exploit a vulnerability through our logstash. There is a known vulnerability that allows remote attackers to execute arbitrary commands via a crafted event. CVE-2014-4326

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

  Lock accounts after a defined number of incorrect passwords and we can also lock out an IP with multiple failed logins. We should also enforce passwords that more than 8 characters and contain special characters. We would also recommend utilizing at WAF (Web Application Firewall) and IDS (Intrusion Detection Services).