Defensive Security Project
by: Zachary, Reza, Asnaf, Vincent

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- Playing the role of a SOC analysts for VSI (Virtual Space Industries). The team is tasked with using splunk to monitor against potential attacks on our system and applications from the competitor JobeCorp.

Website Monitoring: Add-on

Website Monitoring

- **The add-on monitors websites by url to detect downtime and performance problems through Splunk. It’s quite easy to use.**

- **Website monitoring allows you to see the status history of each website inputted by time, as well as the response time. It’s a great way to detect how well the traffic of each website is performing.**

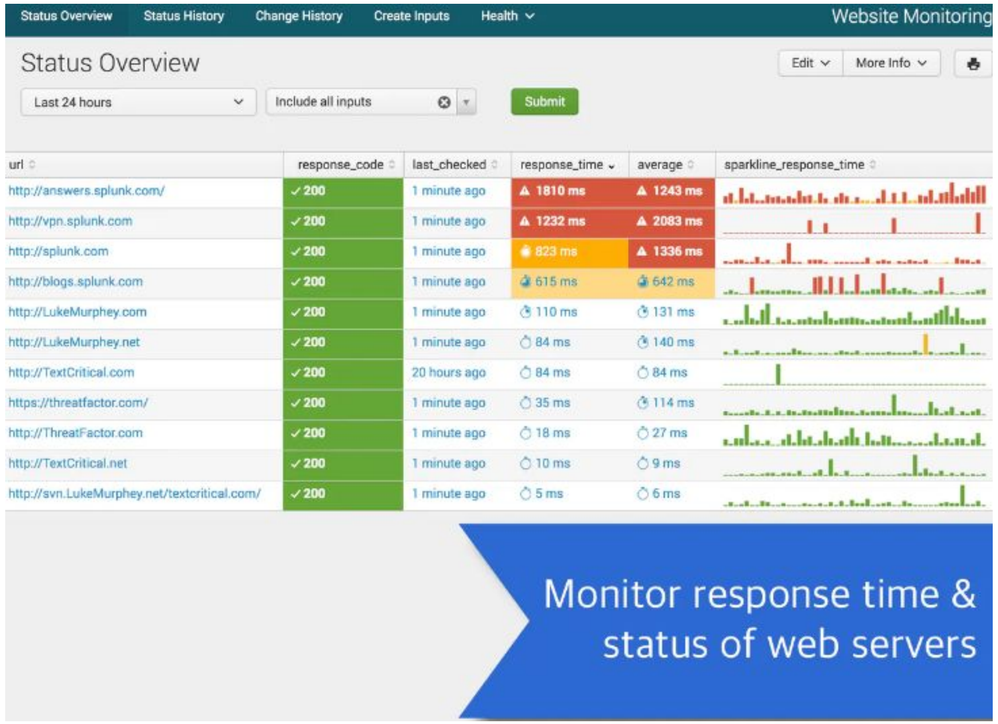
Website Monitoring

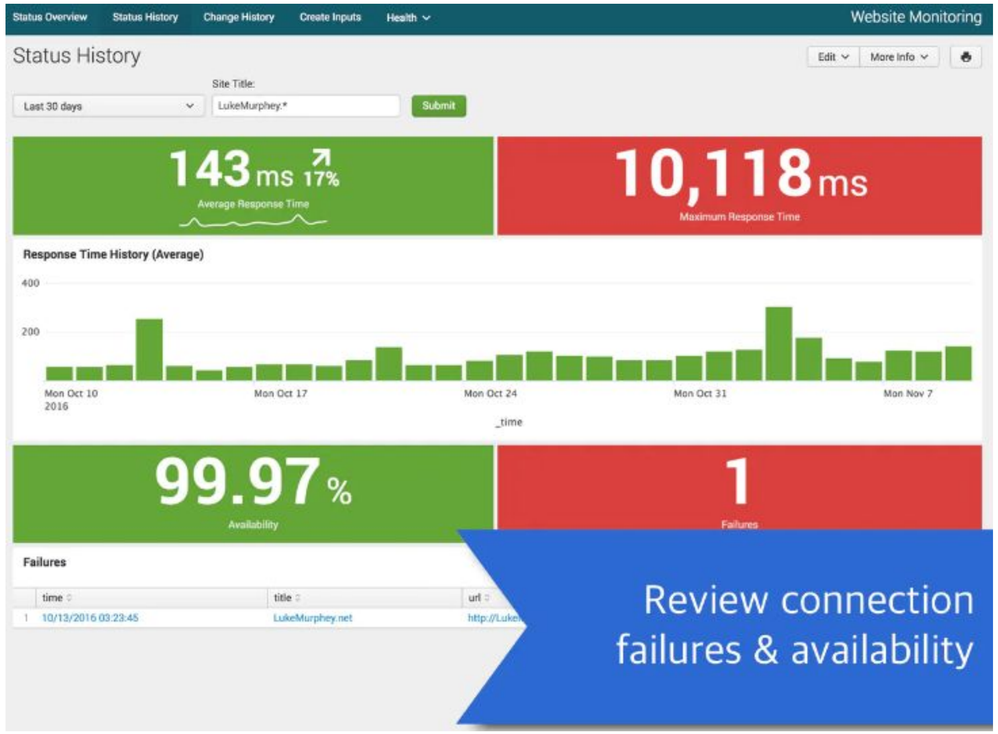
- **Let’s say a team of coding engineers are working on a project through the Azure portal, but as soon as they were about to complete their project, the portal started to massively slow down, causing their project to be incomplete until the issue is fixed.**

- **By inputting portal.azure.com through the app via Splunk, an admin can gather the data of when the site started to cause problems, as well as monitor what issues occurred in certain times within the domain inputted. Through the Website Monitoring Add-on you can see the response code, the response time and when the site started to change it’s response speed (by ms units).**

- **This tool is great for further data collection when monitoring each website is being used.**

Website Monitoring





Logs Analyzed

1 Windows Logs

The Data for these logs contain the (baseline) normal activity for VSI.

2 Apache Logs

The Data for these logs represented an attack against VSI, which triggered custom alerts.

Windows Logs

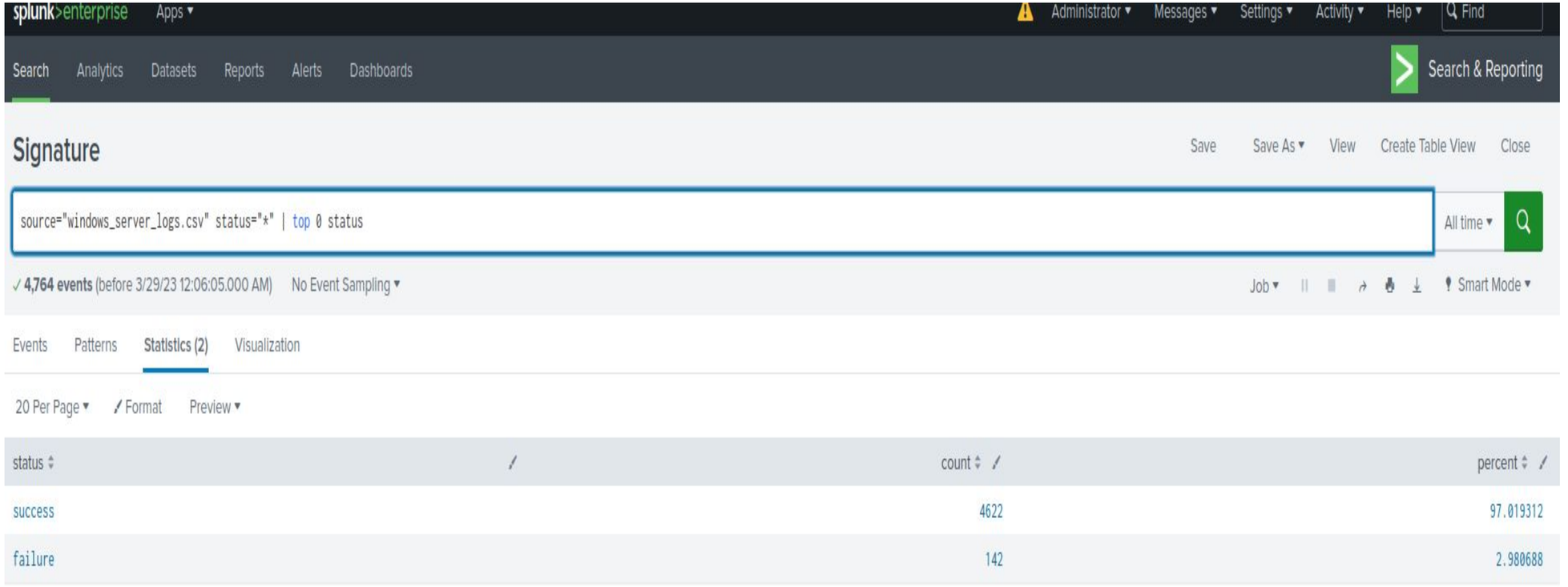
Reports—Windows

Designed the following Reports:

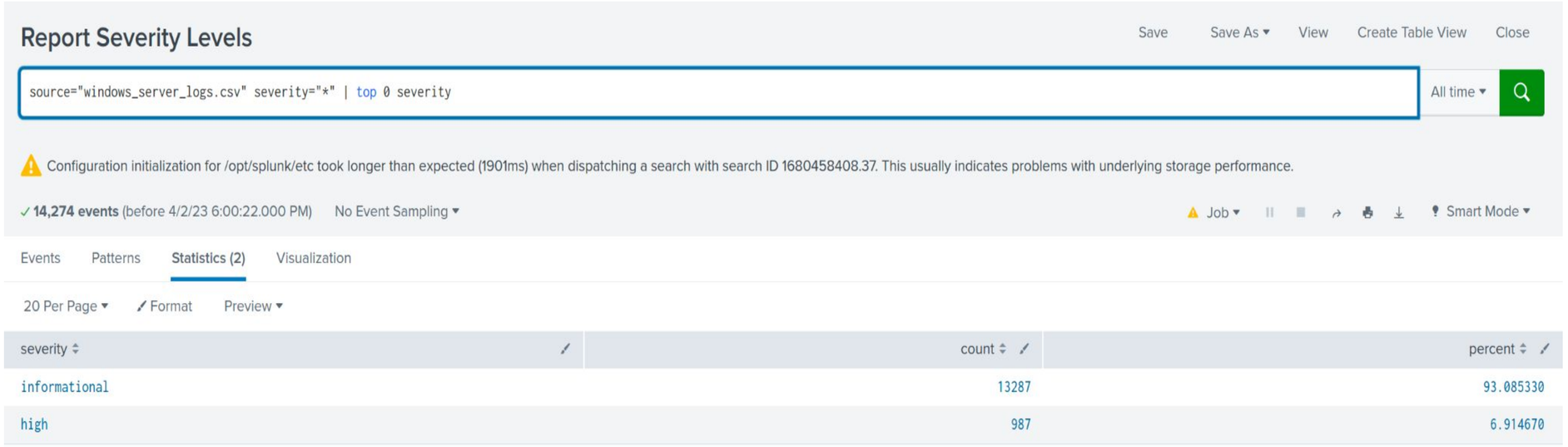
Windows Activity, Severity Level, Signature

Report Name	Report Description
Windows Activity Status	This report showed the success and failure of Windows activities
Windows Severity Level	This report shows the severity levels of the window logs
Windows Signature	Report of Signatures of Windows Activity

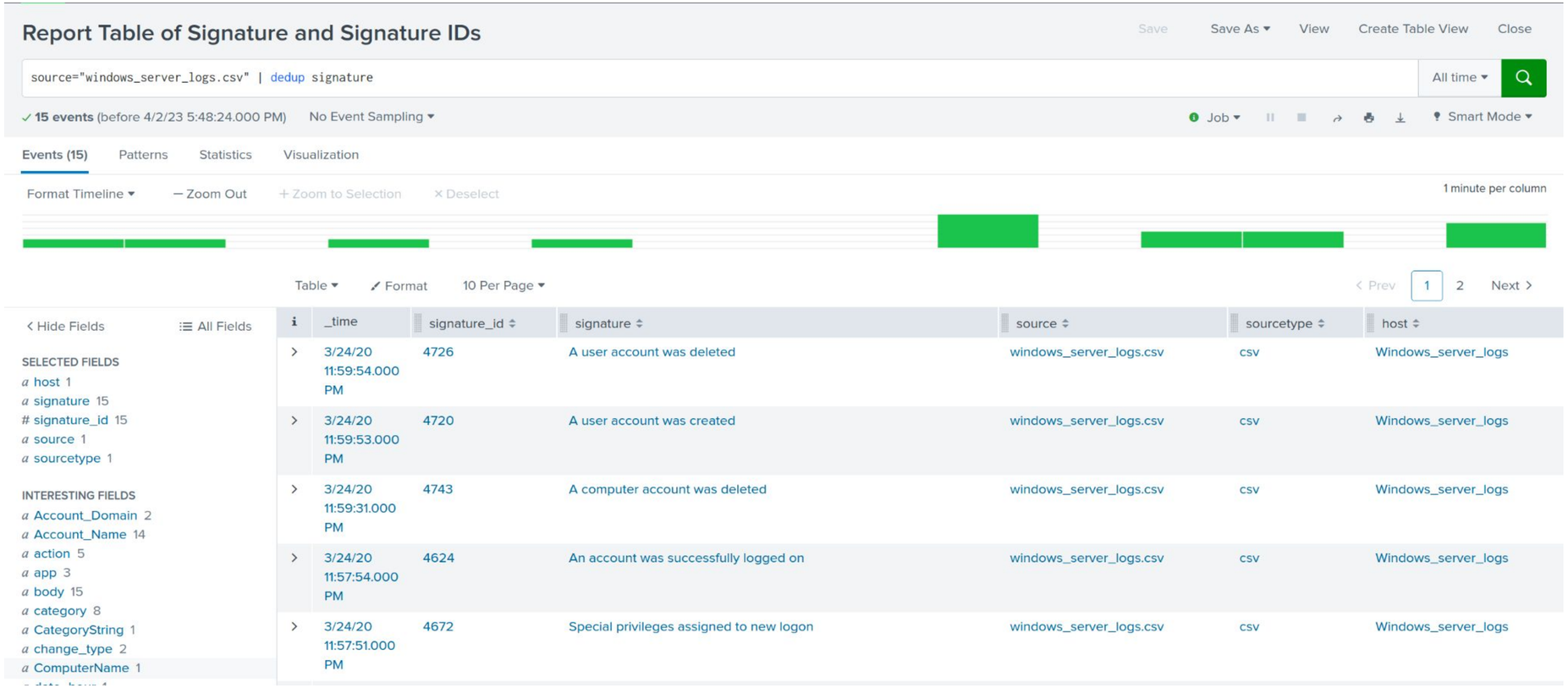
Images of Reports—Windows



Images of Reports—Windows (cont.)



Images of Reports—Windows (cont.)



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Failed Activity	This alert tracks the different type of signatures that have failed.	160	260

JUSTIFICATION: We do not see any events that are lower than 160 per hr. Major spikes that occurred were over 800+ events.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Signature Success Logged On	The alert is triggered due suspiciously low event account logins	20	5

JUSTIFICATION: Baseline normal activity was 14-20 pr hr. We saw a drop of activity between 2-4 an hr with only one user logging in. Then in the next hr we saw that same user with him only being logged in multiple times.

Alerts—Windows

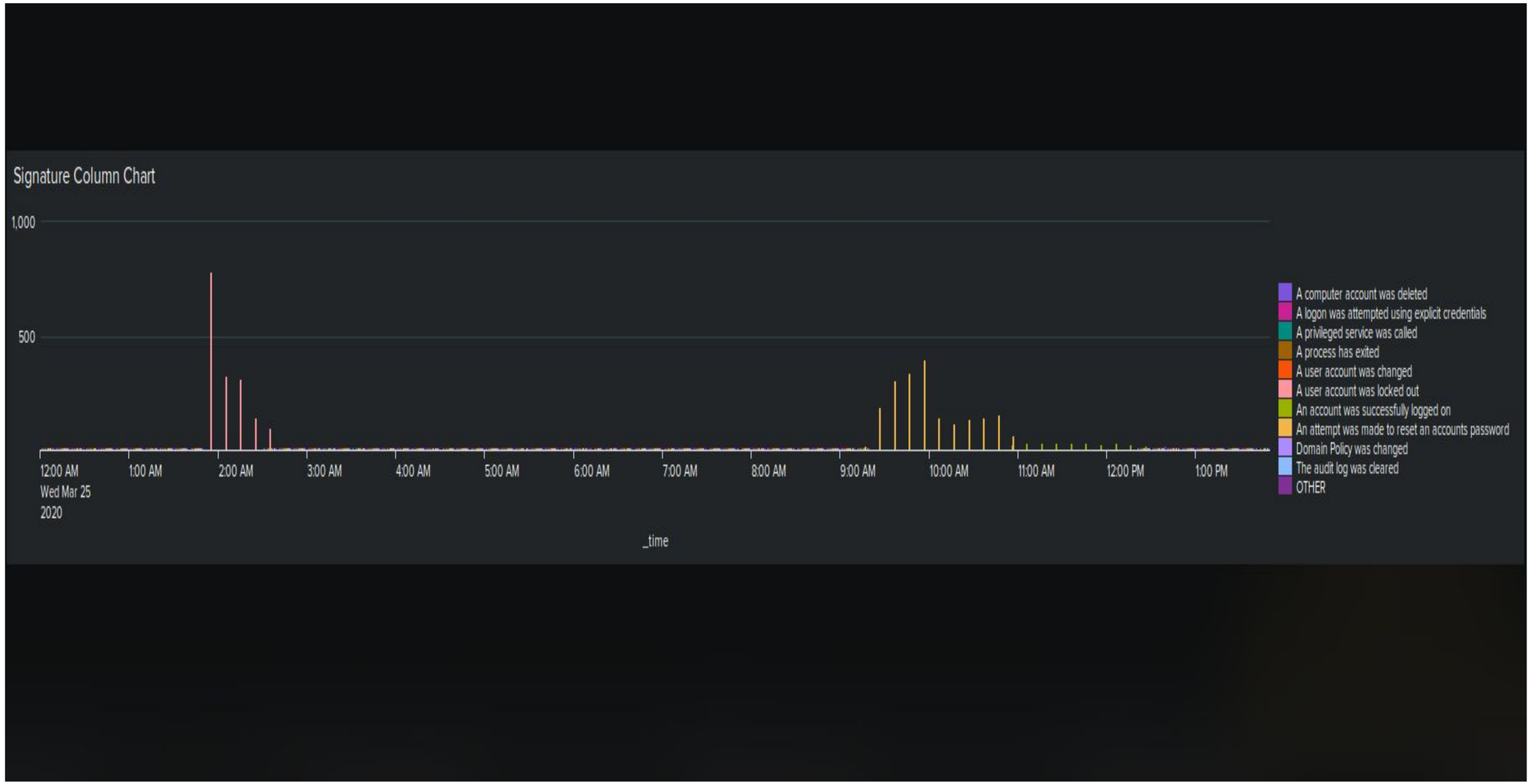
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
A user account was deleted	Alert will be triggered when user account is deleted more than threshold.	12	30

JUSTIFICATION: The average deleted accounts was 12.

Dashboards—Windows

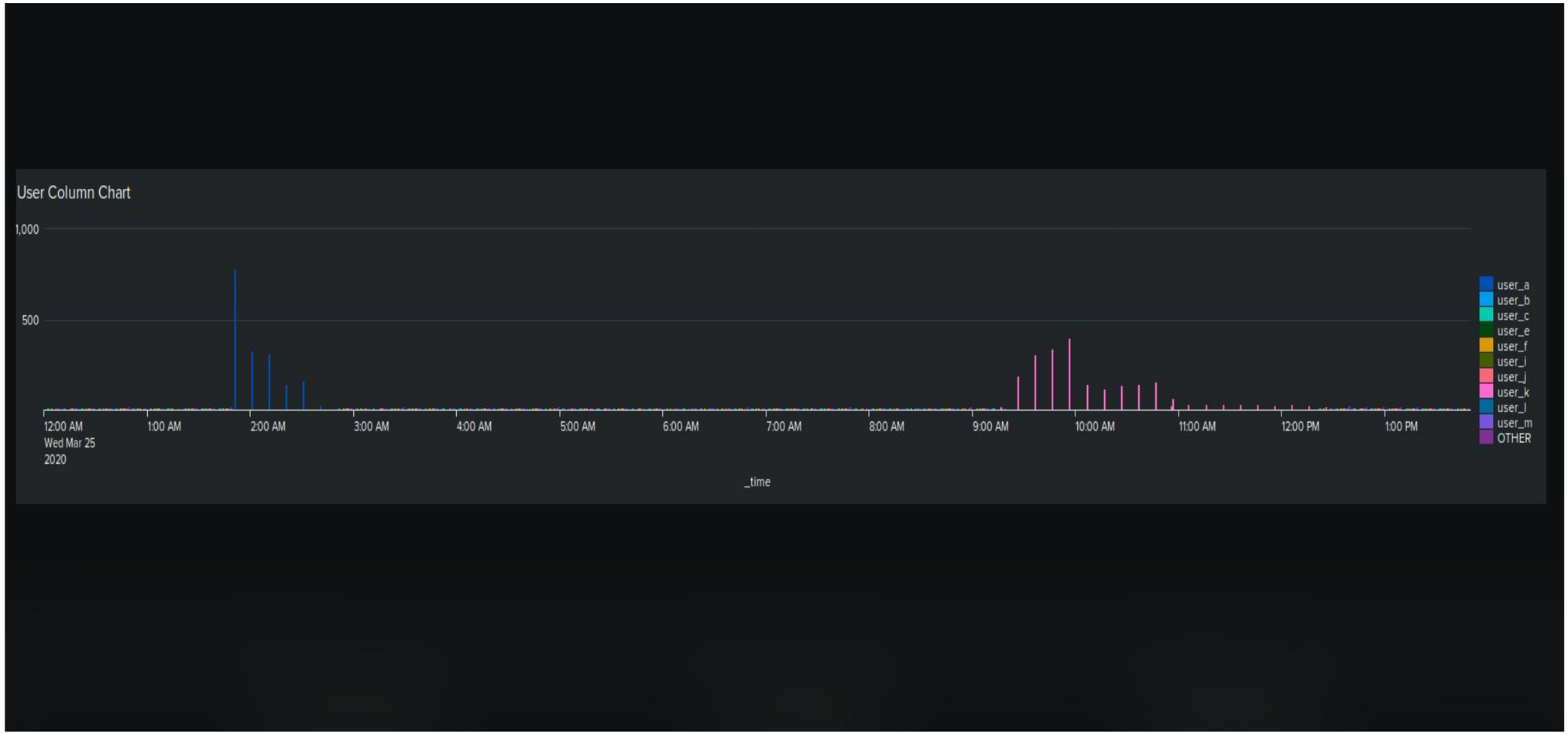
Dashboards—Windows (cont.)



Dashboards—Windows (cont.)

Dashboards—Windows (cont.)

Dashboards—Windows (cont.)



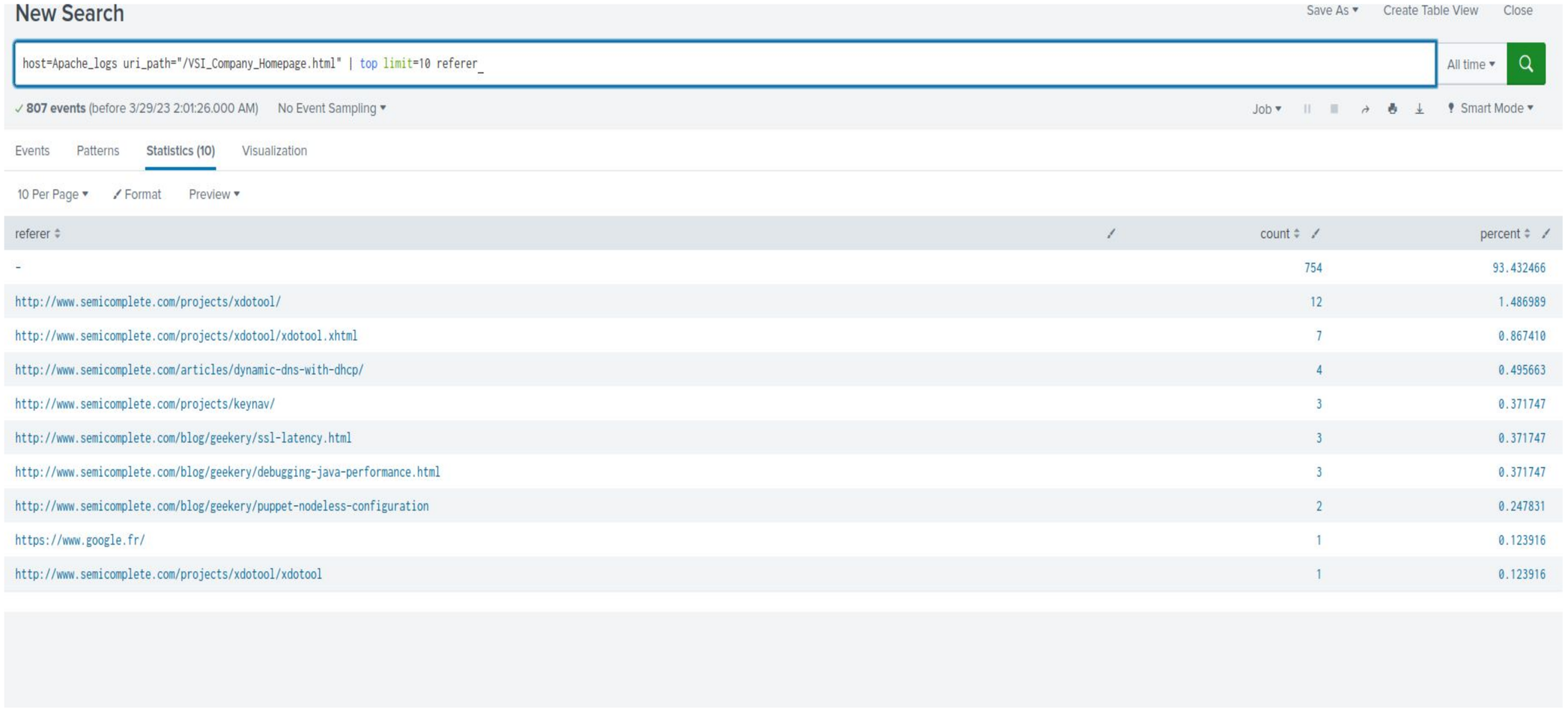
Apache Logs

Reports—Apache

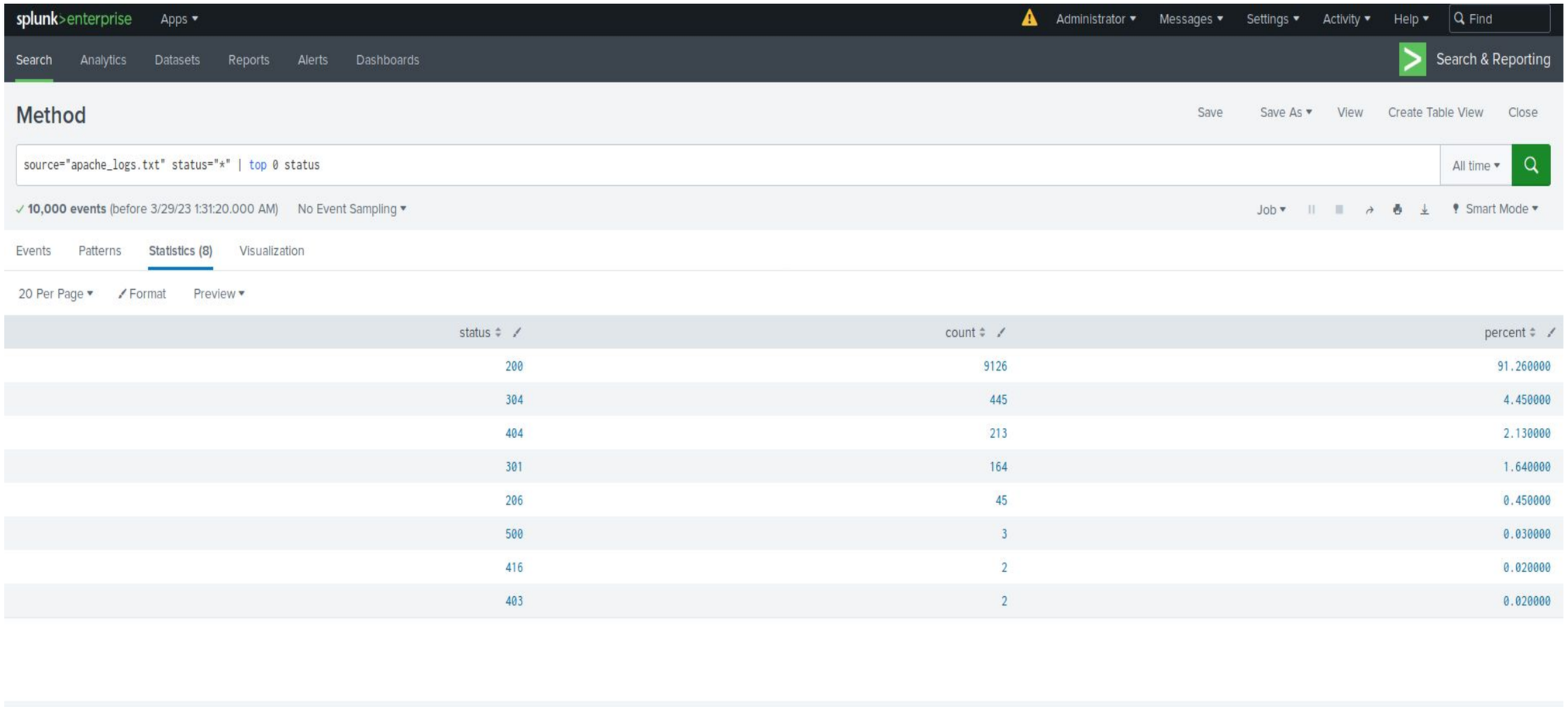
Designed the following reports:

Report Name	Report Description
Referrer Report	Report of top 10 domains that went to the VSI Homepage
HTTP Response code	Report of HTTP responses
HTTP Methods	Report of the type of HTTP activity on the VSI web server

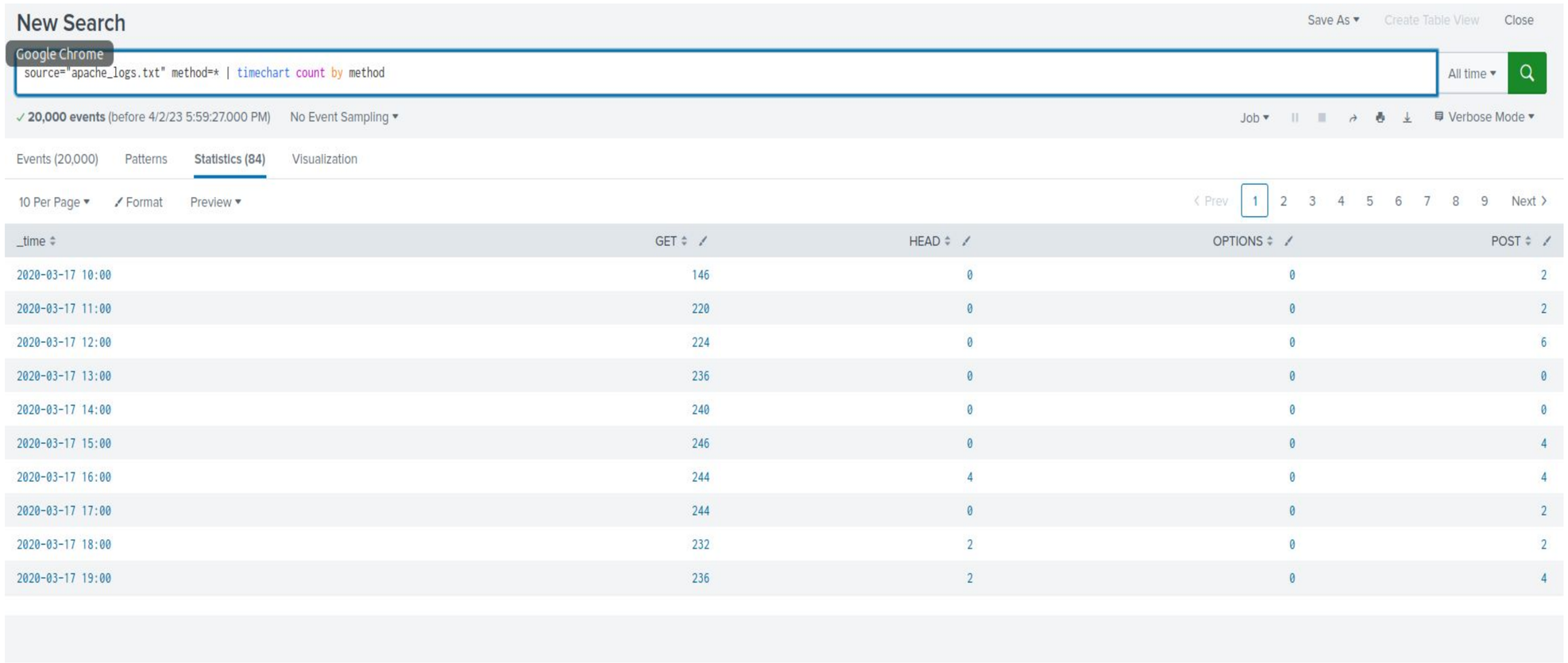
Images of Reports—Apache



Images of Reports—Apache (cont.)



Images of Reports—Apache (cont.)



_time	GET	HEAD	OPTIONS	POST
2020-03-17 10:00	146	0	0	2
2020-03-17 11:00	220	0	0	2
2020-03-17 12:00	224	0	0	6
2020-03-17 13:00	236	0	0	0
2020-03-17 14:00	240	0	0	0
2020-03-17 15:00	246	0	0	4
2020-03-17 16:00	244	4	0	4
2020-03-17 17:00	244	0	0	2
2020-03-17 18:00	232	2	0	2
2020-03-17 19:00	236	2	0	4

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST	This alert is for hourly count of when the HTTP POST method is used	The baseline would be 3	Our Alert Threshold would be 30

JUSTIFICATION: We had our baseline at 3 because thats the lowest the logs go and our threshold would be 30 because the highest event we had was 21 events

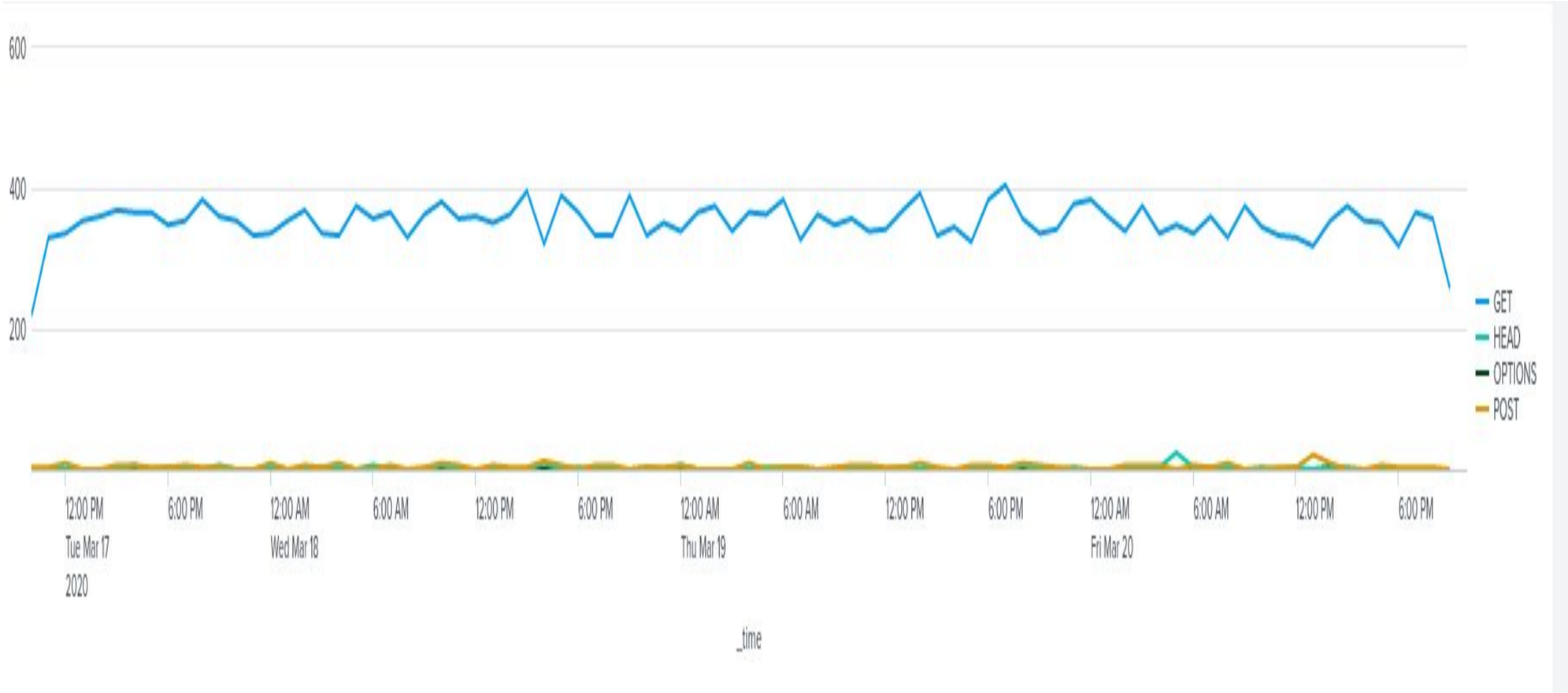
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly International activity	This alert showed hourly activity from every country except United States	The baseline was 75	The Threshold would be 160

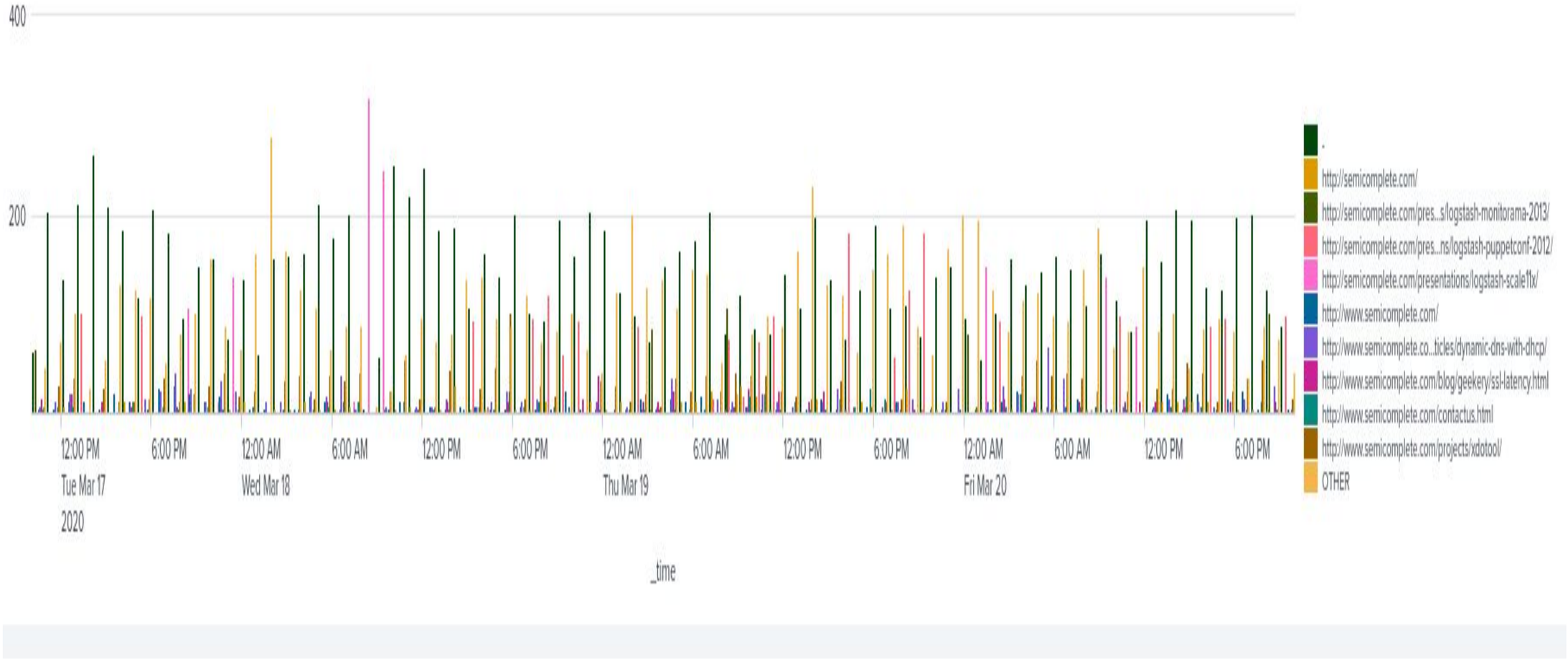
JUSTIFICATION: Our baseline was 75 because that was the lowest event and our Threshold was 160 because the highest event we had was 160

Dashboards—Apache

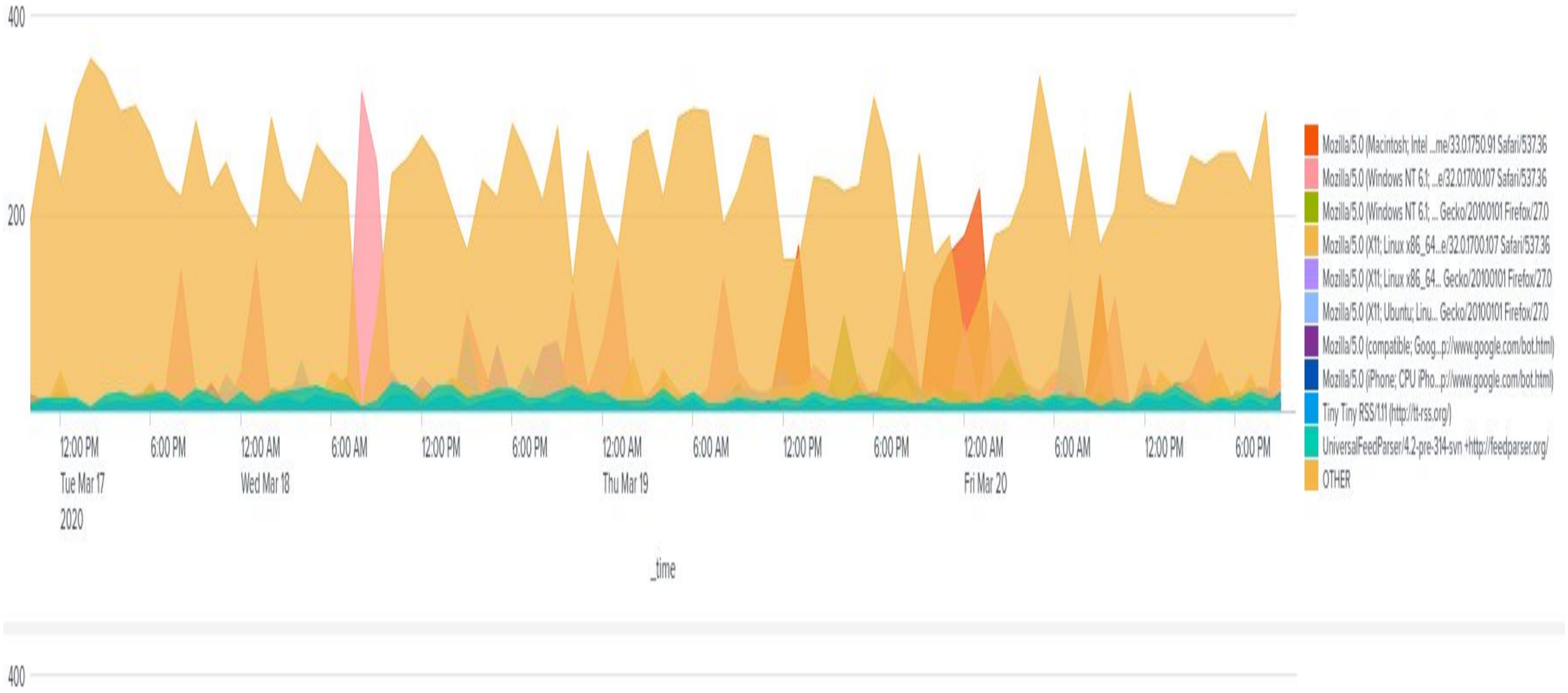


Dashboards—Apache (cont.)

Dashboards—Apache (cont.)



Dashboards—Apache (cont.)



Attack Analysis

Attack Summary—Windows

- Severity Percentage increased by 15 percent when switching logs and we also noticed a decrease in the failure percentage from 2.9 percent to 1.5 percent

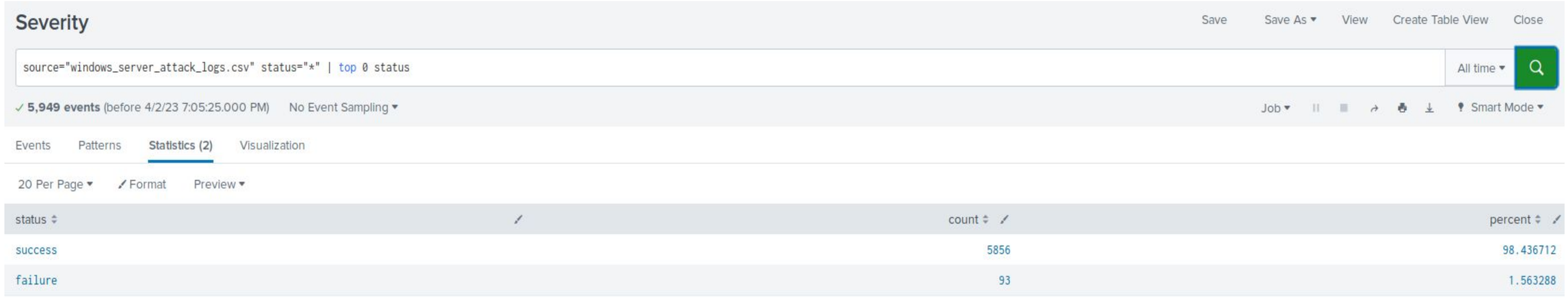
Attack Summary—Windows

- There was 1,980 failed events from 1am to 2am and 2,077 failed events from 9am to 10am. Our threshold would still be correct because our threshold was 260 events an hr.

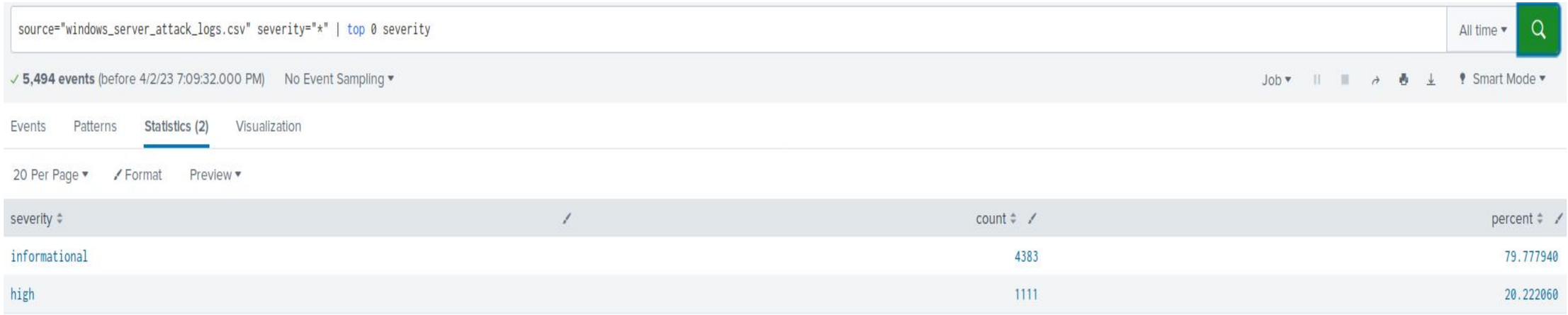
Attack Summary—Windows

- We had a spike of signatures with “user being locked out” between 12am and 3am and “resetting an account password” between 8am and 11am
- For the signature “user being locked out” UserA and UserK stood out with UserA peak with 785 events at 1:50AM and UserK peak with 397 events at 9:50AM

Screenshots of Attack Logs



Screenshots of Attack Logs (cont.)



Attack Summary—Apache

- The GET method jumped from average 73-120 to high 300s
- The HTTP response codes changed the code 200 got a 8% decrease , code 304 got a 4% decrease, and code 404 got a 11% increase

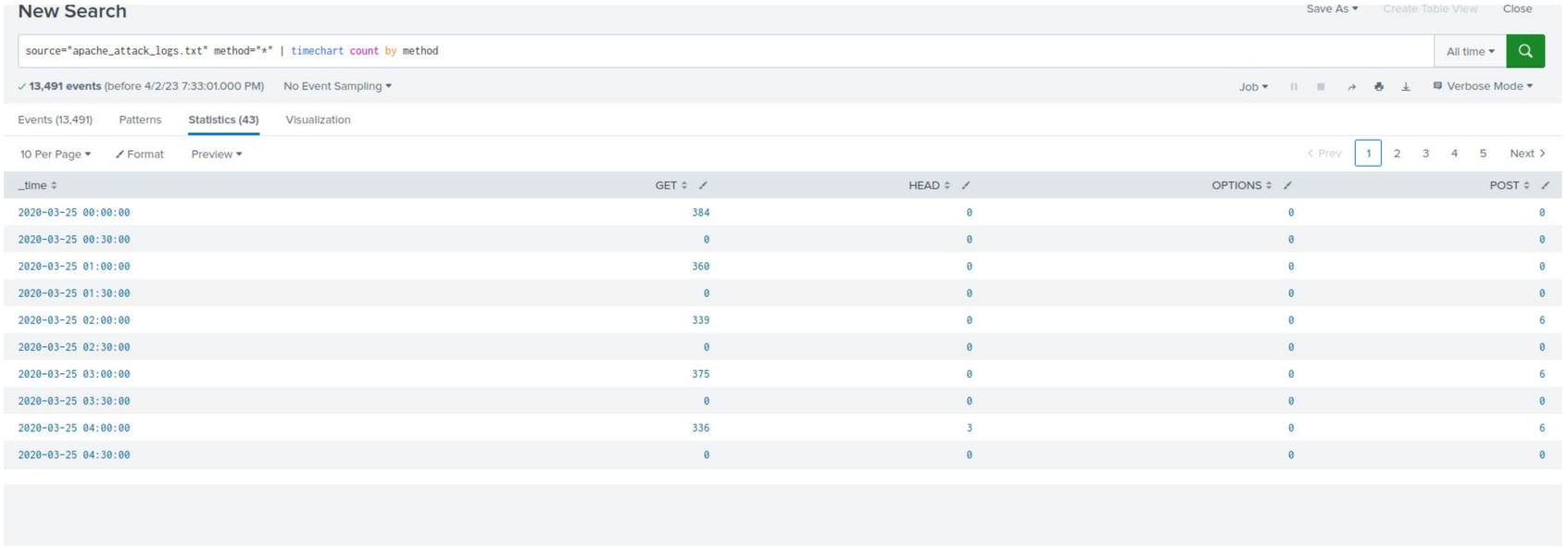
Attack Summary—Apache

- We noticed that there was more activity from Brazil and Other which occurred from 6pm to 8pm. Our alert would be still triggered because our alert was 160 events an hr.

Attack Summary—Apache

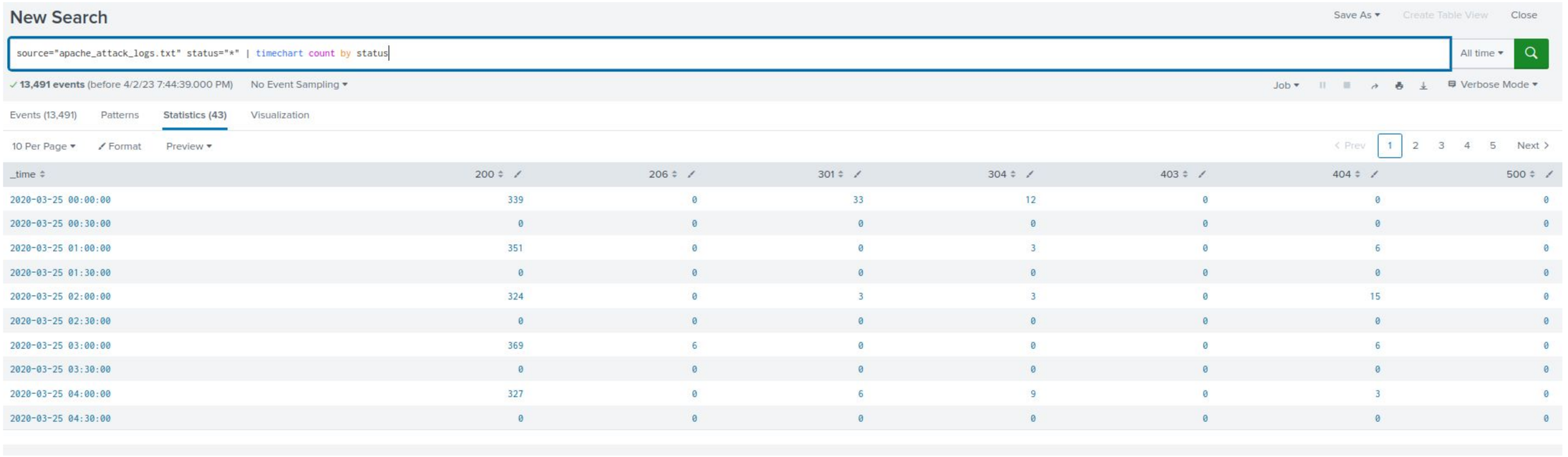
- We noticed that the POST method was used in the attacks and it started at 7pm and ended at 9pm. The peak event count for POST was 1,296 events in an hr.
- We noticed on our cluster map that more data was added into the Europe section, where Germany gained a total of 571 and France had a count of 753.

Screenshots of Attack Logs



_time	GET	HEAD	OPTIONS	POST
2020-03-25 00:00:00	384	0	0	0
2020-03-25 00:30:00	0	0	0	0
2020-03-25 01:00:00	360	0	0	0
2020-03-25 01:30:00	0	0	0	0
2020-03-25 02:00:00	339	0	0	6
2020-03-25 02:30:00	0	0	0	0
2020-03-25 03:00:00	375	0	0	6
2020-03-25 03:30:00	0	0	0	0
2020-03-25 04:00:00	336	3	0	6
2020-03-25 04:30:00	0	0	0	0

Screenshots of Attack Logs (cont.)



_time	200	206	301	304	403	404	500
2020-03-25 00:00:00	339	0	33	12	0	0	0
2020-03-25 00:30:00	0	0	0	0	0	0	0
2020-03-25 01:00:00	351	0	0	3	0	6	0
2020-03-25 01:30:00	0	0	0	0	0	0	0
2020-03-25 02:00:00	324	0	3	3	0	15	0
2020-03-25 02:30:00	0	0	0	0	0	0	0
2020-03-25 03:00:00	369	6	0	0	0	6	0
2020-03-25 03:30:00	0	0	0	0	0	0	0
2020-03-25 04:00:00	327	0	6	9	0	3	0
2020-03-25 04:30:00	0	0	0	0	0	0	0

Summary and Future Mitigations

Project 3 Summary

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

  We found severity levels increased during this attack. The POST method was the most common during this attack with 1,296 events using it. The most common signatures during this attack was “user locked out” and “resetting an account password”

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

  Regarding signatures, we could limit how many login tries someone was allowed to have. We would also remove sensitive data from the HTTP source.