Defensive Security Project
by: Jordan, Eric, Jaz, Franc, & Joel

Table of Contents

This document contains the following resources:

Monitoring Environment

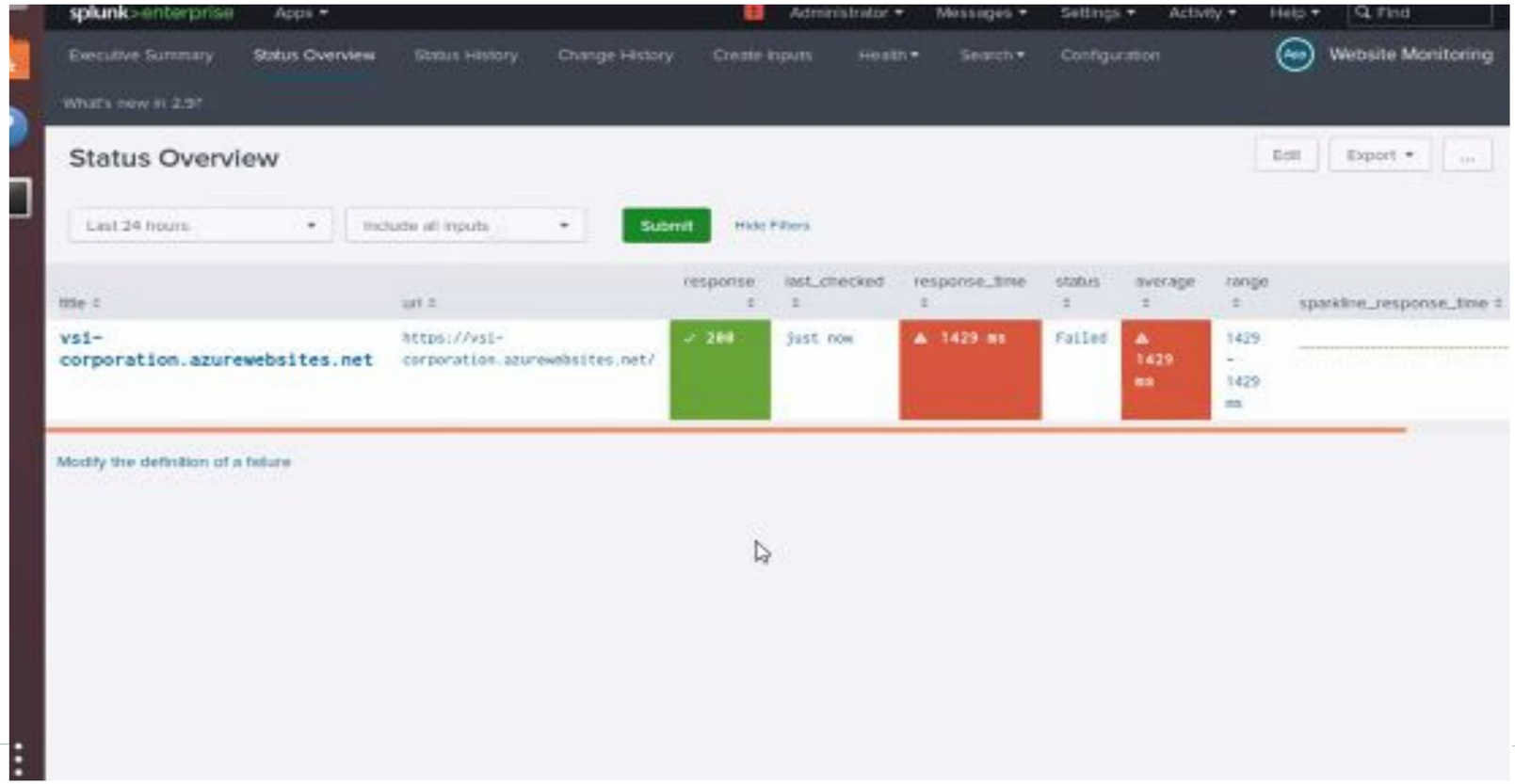
Scenario

- We are employed at a small company called Virtual Space Industries (VSI) as SOC Analysts
- There are rumors that a competitor might disrupt our business
- We are tasked with using SPLUNK against to monitor against our potential attacks

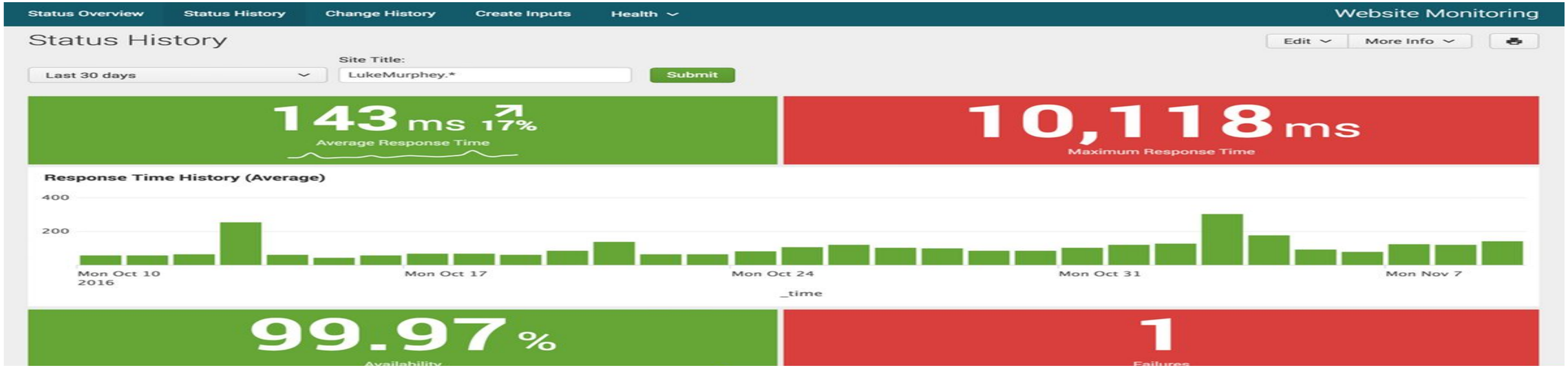
“Add-On” App
WEBSITE MONITORING

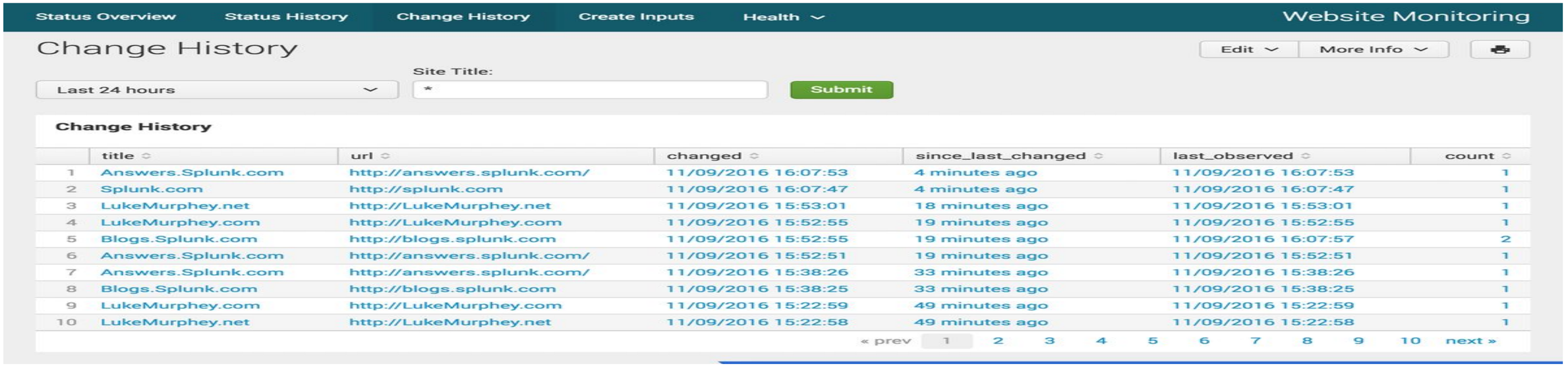
Website Monitoring

- **Monitor websites to detect downtime and performance issues**
- **You can define the websites you would like to monitor**
- **This app uses a modular input that can easily be set up in minutes.**
- **This add-on will help check the availability, performance, and function of a website or web service.**



Website Monitoring





Website Monitoring

Why would web monitoring be important?

1. **To avoid losing money/customers**
2. **To safeguard your content and data**
3. **To identify problems with your site or hosting**
4. **To understand how visitors are interacting with your website**

Logs Analyzed

1 Windows Logs

Signature_ID

Signature

User

Status

Severity

2 Apache Logs

IP Addresses

Https

Windows Logs

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity	level of failed Windows activity	7	failed logins is > 10

JUSTIFICATION: The average was about 7 failed logins so we decided more than 10 failed log ins would trigger an alert.

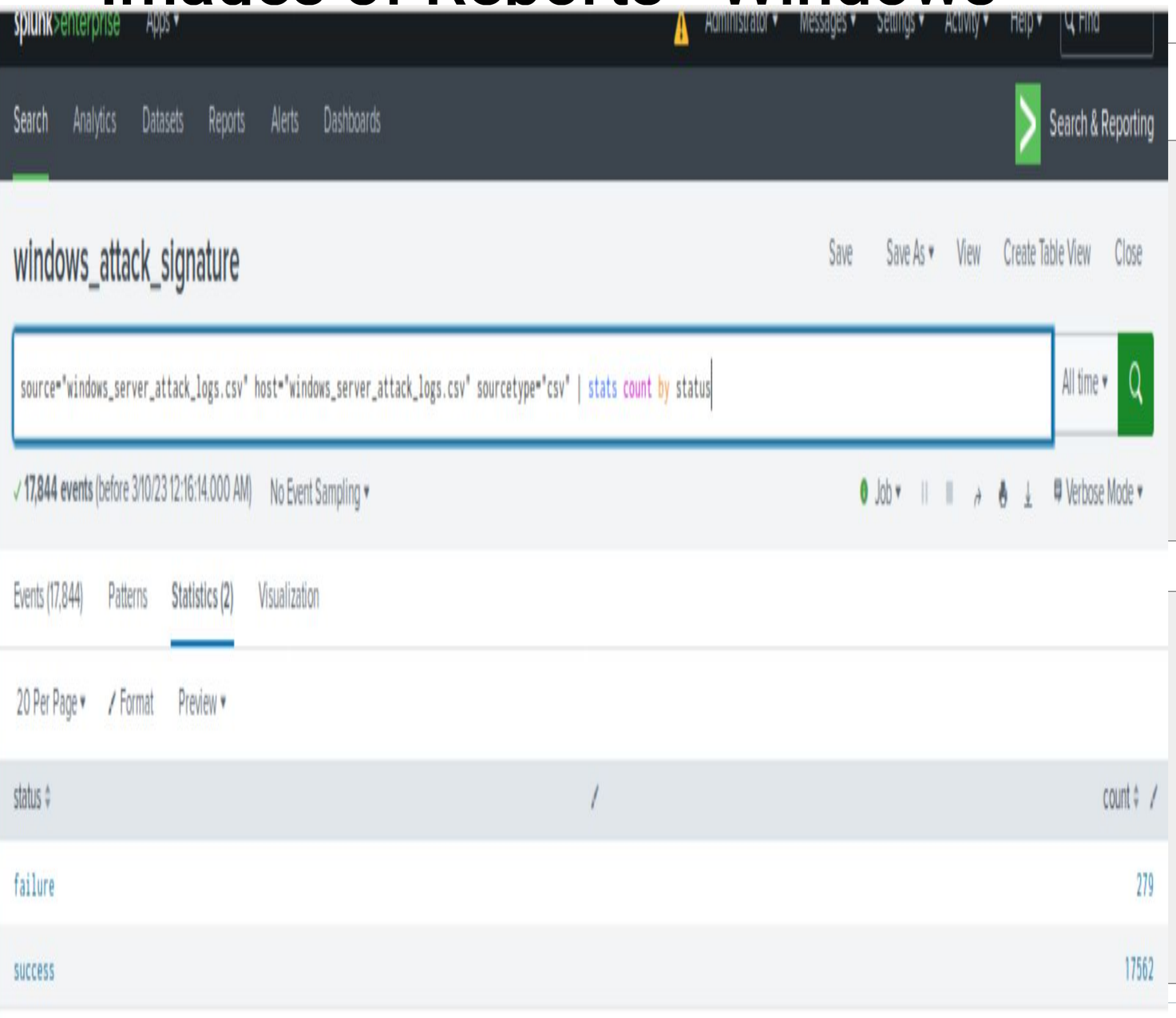
Alerts—Windows

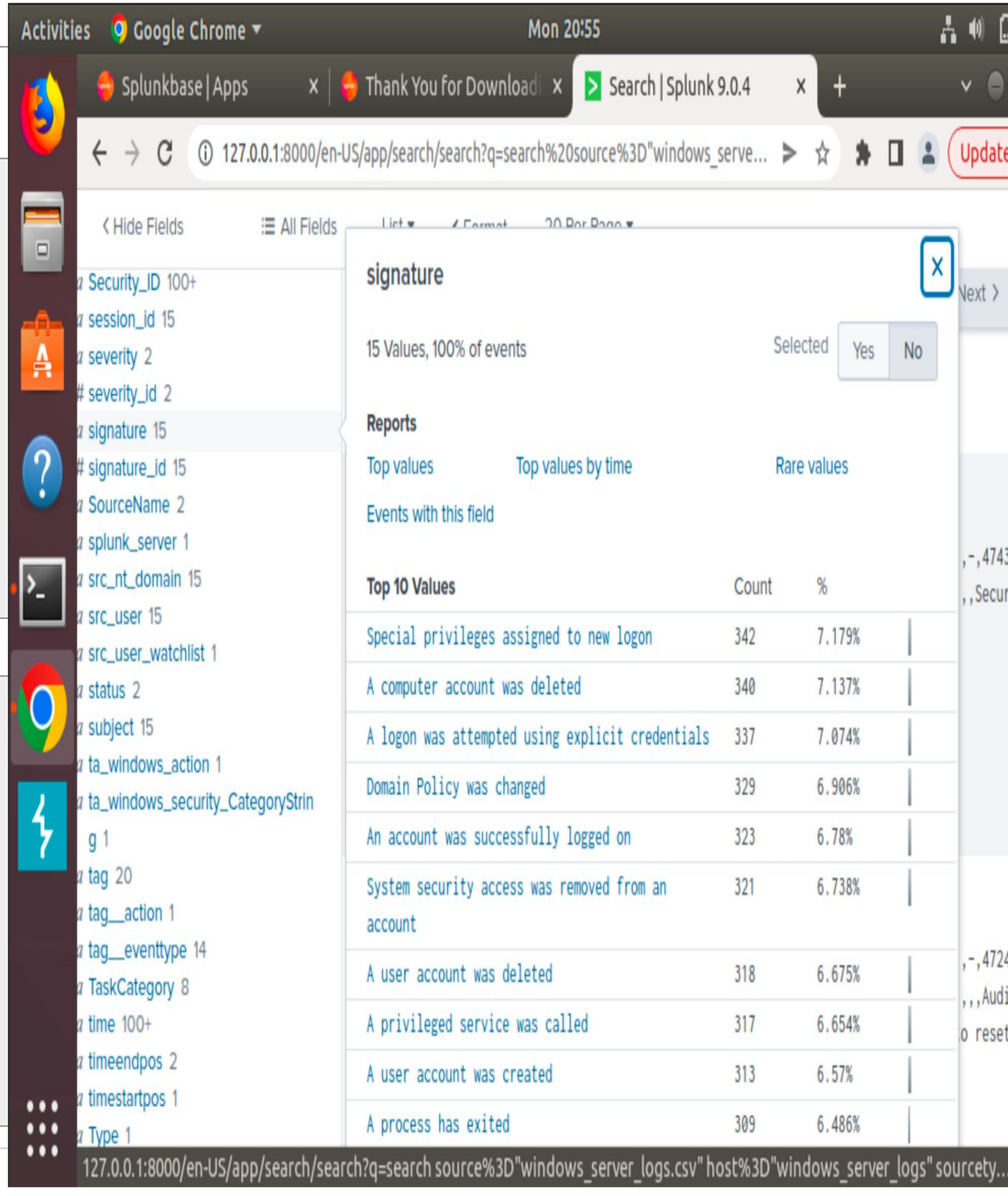
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful logins Alert	when a user account successfully logged on	10	Successful logins is >15

JUSTIFICATION: With a baseline of 10 successful logins per hour, we added an alert that would trigger with a threshold of 15 successful logins.

Images of Reports—Windows





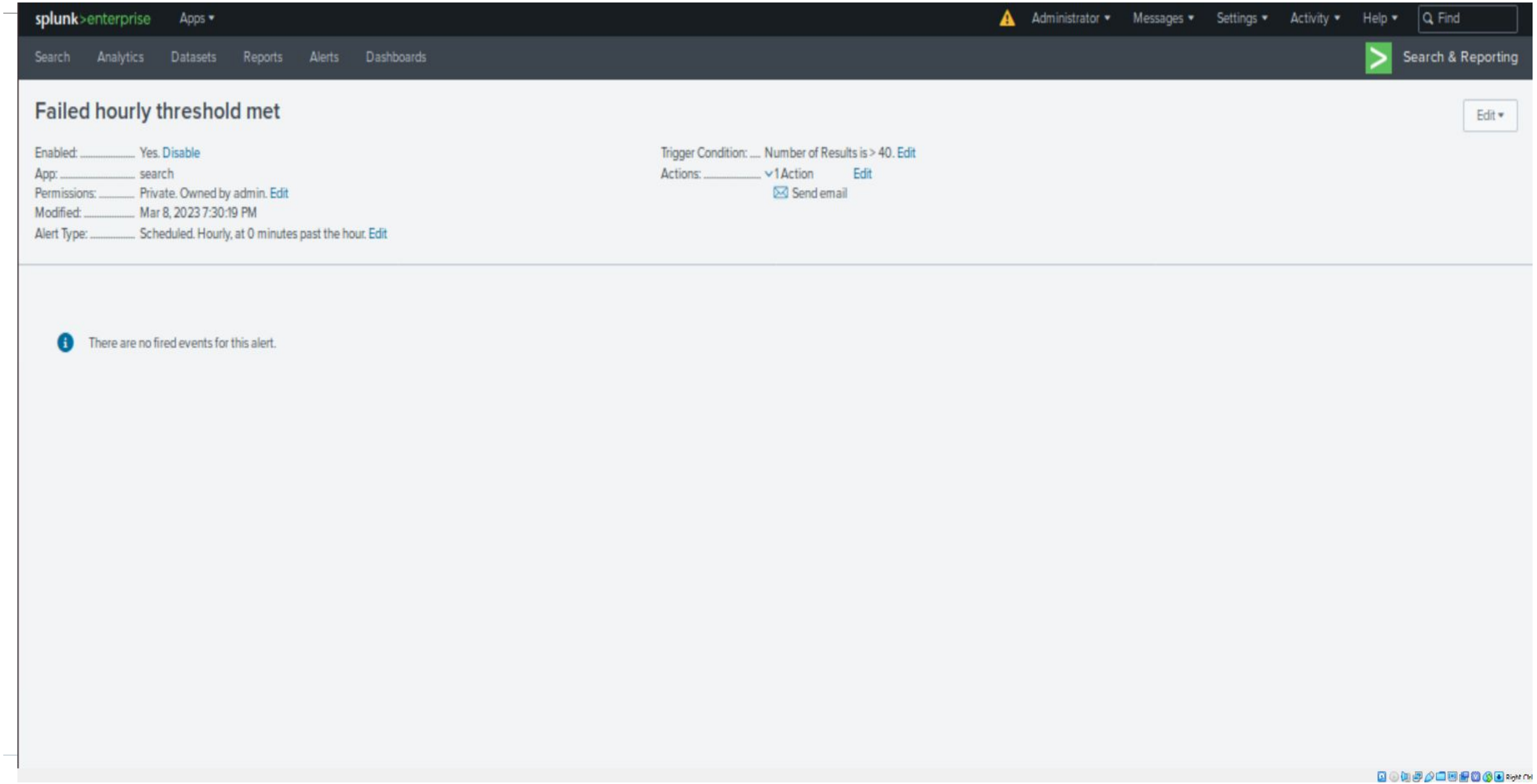
Alerts—Windows

Designed the following alerts:

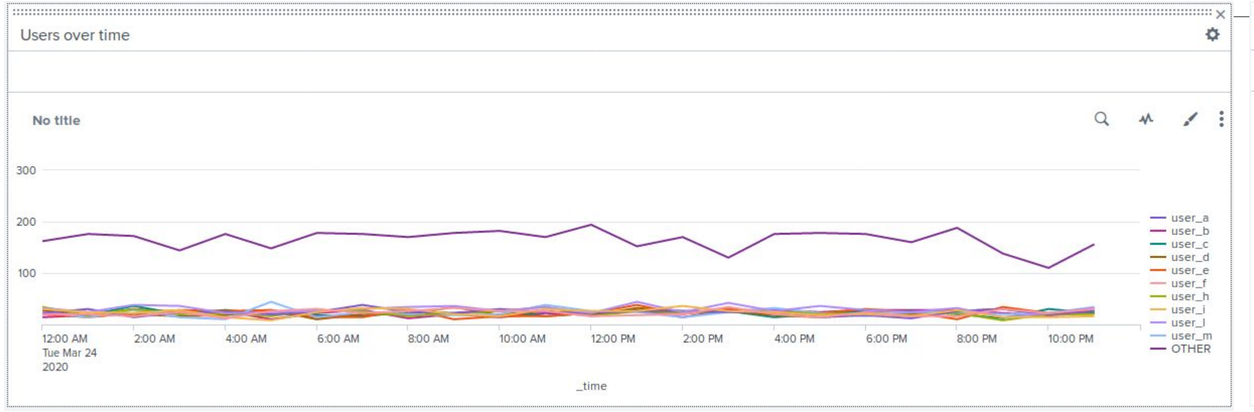
Alert Name	Alert Description	Alert Baseline	Alert Threshold
User account deletion	when deleted account users are greater than 20	11	>20

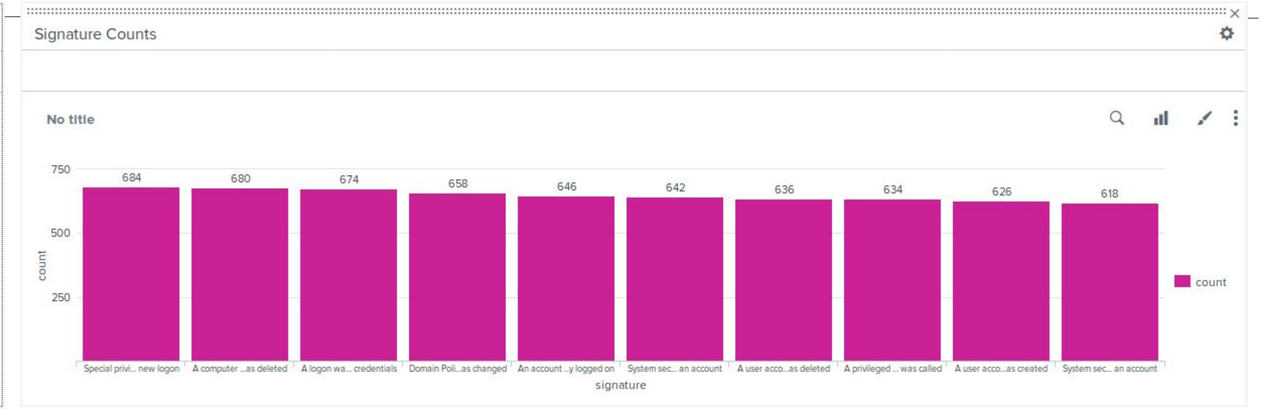
JUSTIFICATION: The baseline showed an average of 11 user accounts deleted, so the threshold of 20 user account deletions will trigger the alert.

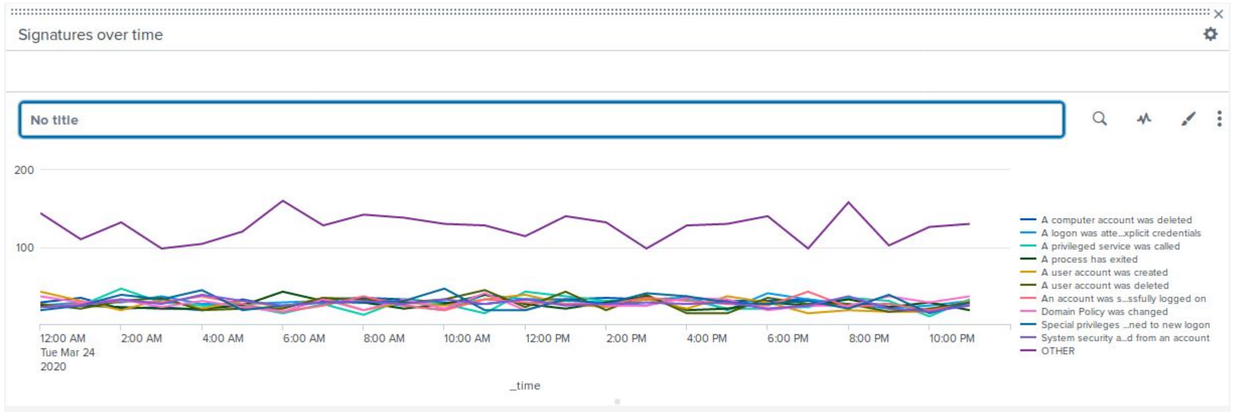
Dashboards—Windows



Dashboard - Windows







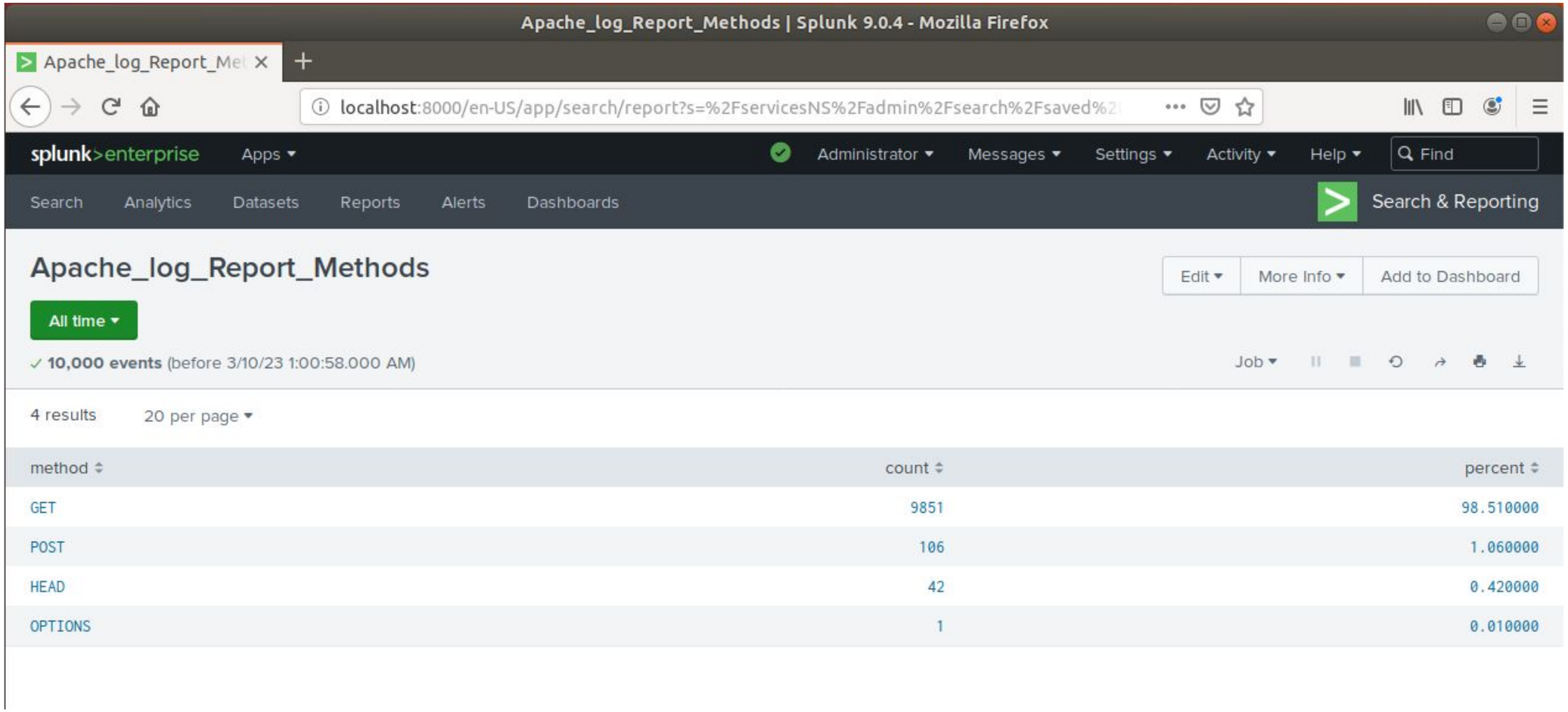
Apache Logs

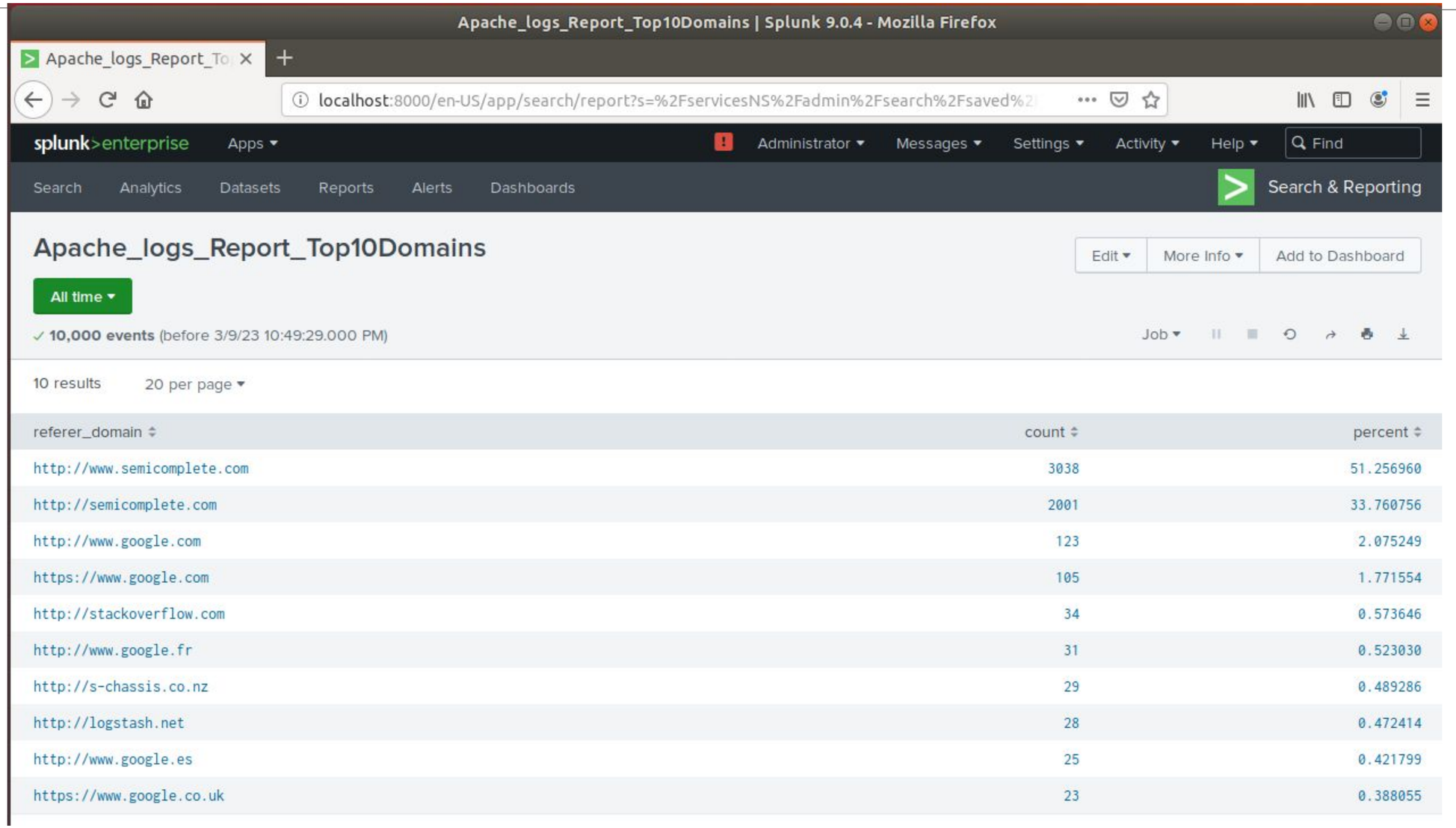
Reports—Apache

Designed the following reports:

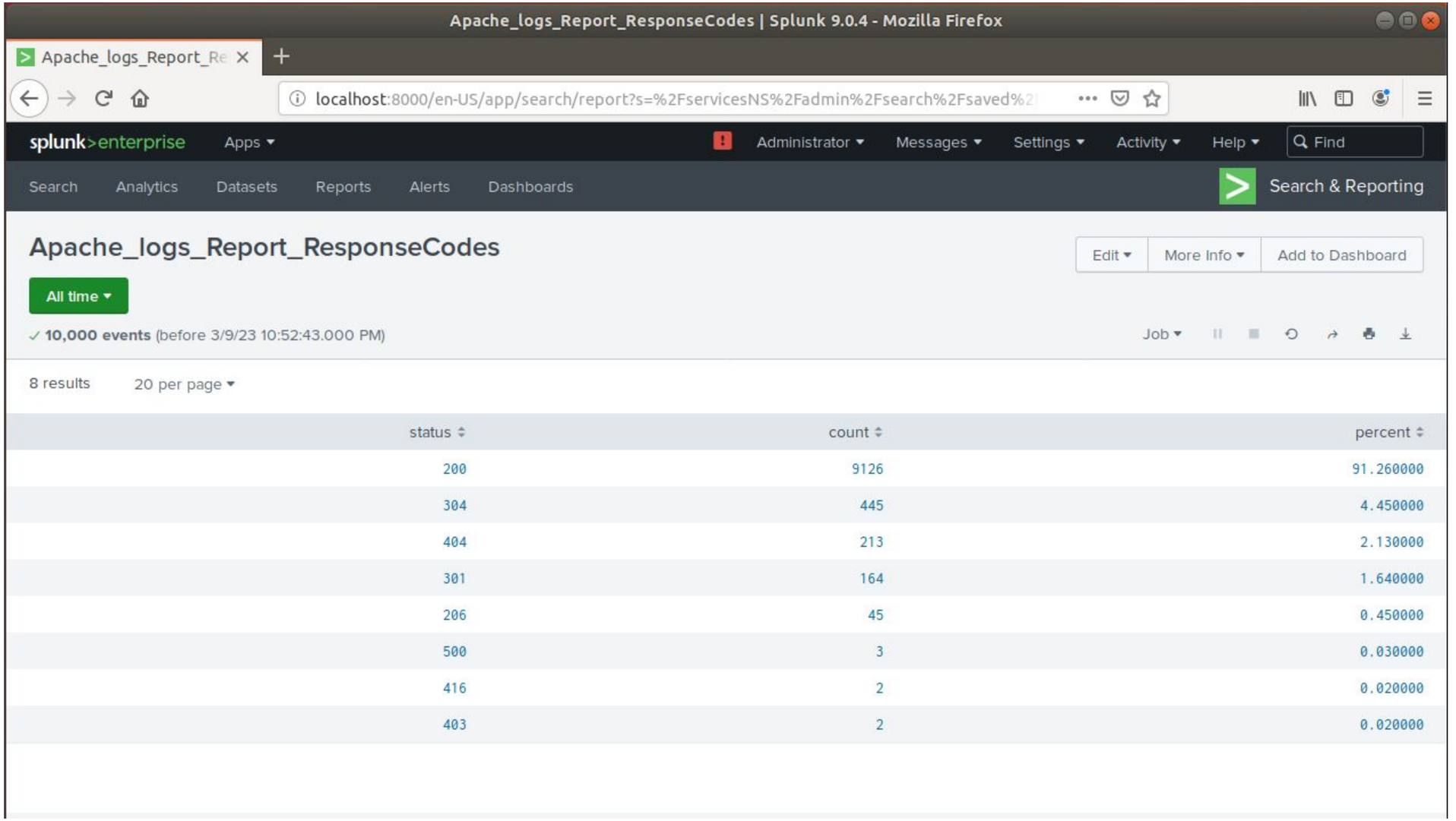
Report Name	Report Description
Apache HTTP Methods	Provides insight into the type of HTTP activity that is being requested against VSI's web server
Apache Top 10 Domains	Highlights the top ten domains that refer to VSI's website
Apache Total Response Codes	Highlights the total number of each response code, and can help with analyzing for suspicious levels of HTTP responses

Images of Reports—Apache





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


Apache_logs_Report_ResponseCodes | Splunk 9.0.4 - Mozilla Firefox
Apache_logs_Report_Re
localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Apache_logs_Report_ResponseCodes
Edit
More Info
Add to Dashboard
All time
✓ 10,000 events (before 3/9/23 10:52:43.000 PM)
Job
8 results
20 per page
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

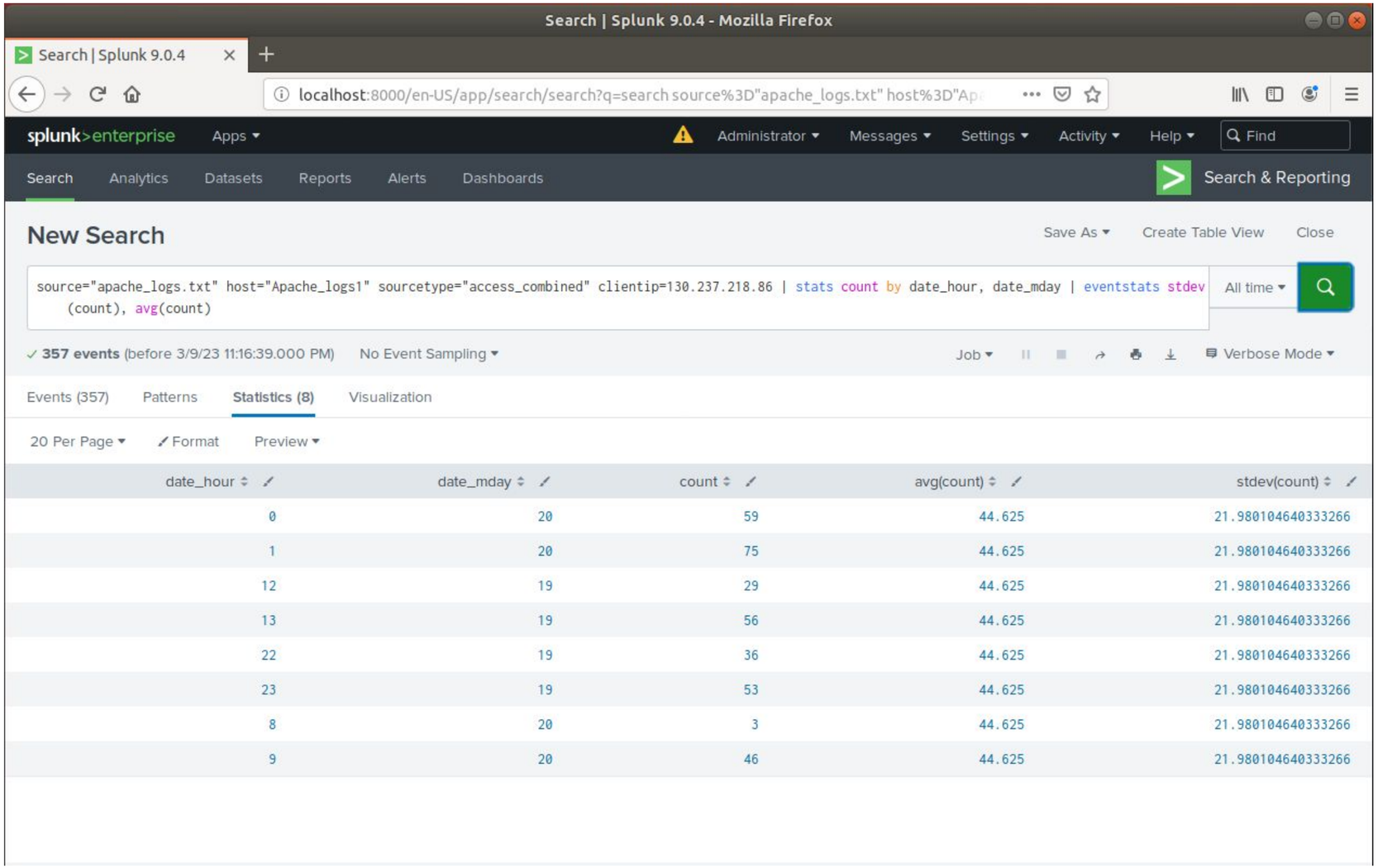
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Logs on ClientIP-Germany	This alert is triggered when the hourly activity in Germany surpasses the threshold	~44	>88

Justification: The normal activity showed us hourly activity in Germany ranging from 3 to 75 with an average baseline of 44. We decided to set the threshold at 88 because with the standard deviation at 21.9 we doubled the standard deviation (~44) and added it to the baseline (~44).

Germany Hourly Activity Alert

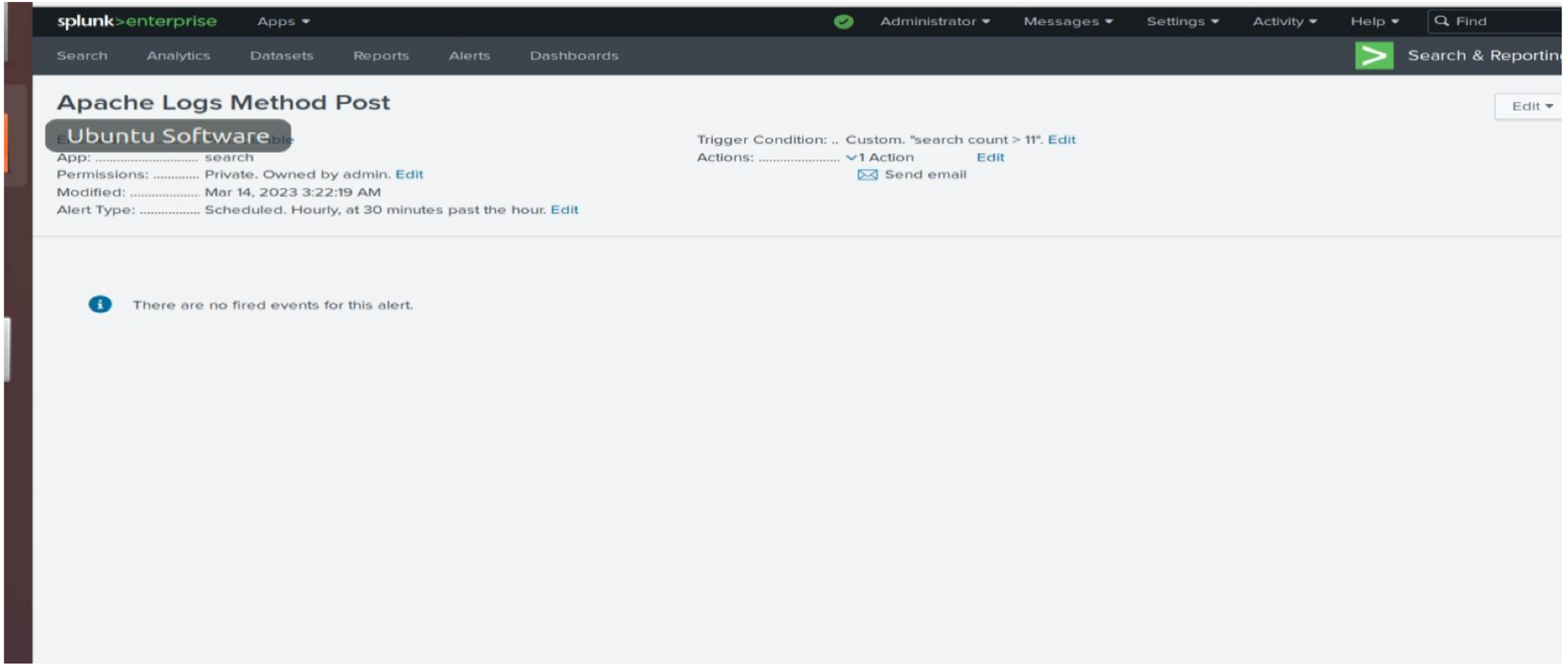


date_hour	date_mday	count	avg(count)	stdev(count)
0	20	59	44.625	21.980104640333266
1	20	75	44.625	21.980104640333266
12	19	29	44.625	21.980104640333266
13	19	56	44.625	21.980104640333266
22	19	36	44.625	21.980104640333266
23	19	53	44.625	21.980104640333266
8	20	3	44.625	21.980104640333266
9	20	46	44.625	21.980104640333266

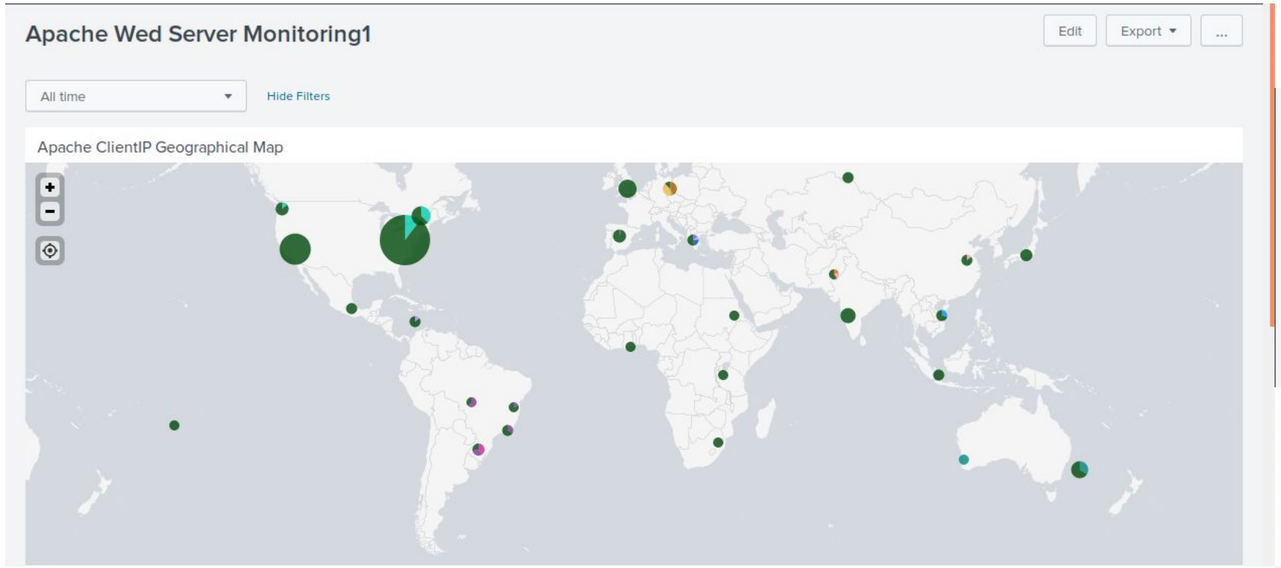
Alerts—Apache

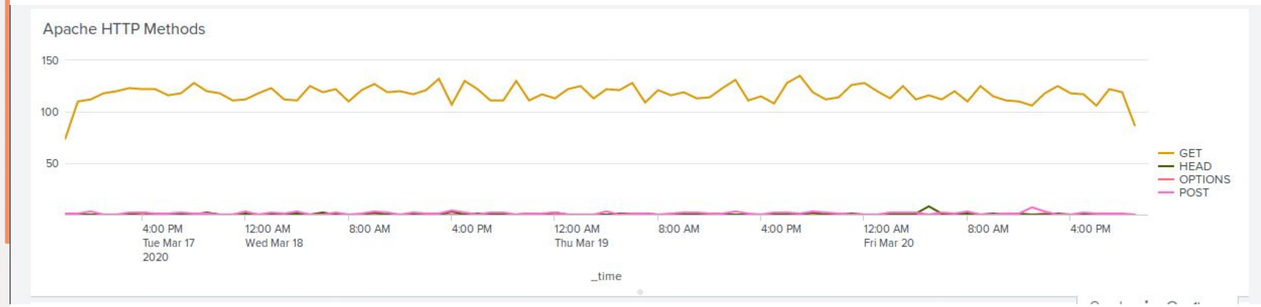
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Logs on POST Method	When the amount of POST request exceed the count of threshold (11) we will send an alert email to SOC management whenever the hourly rate is exceeded.	5	>11

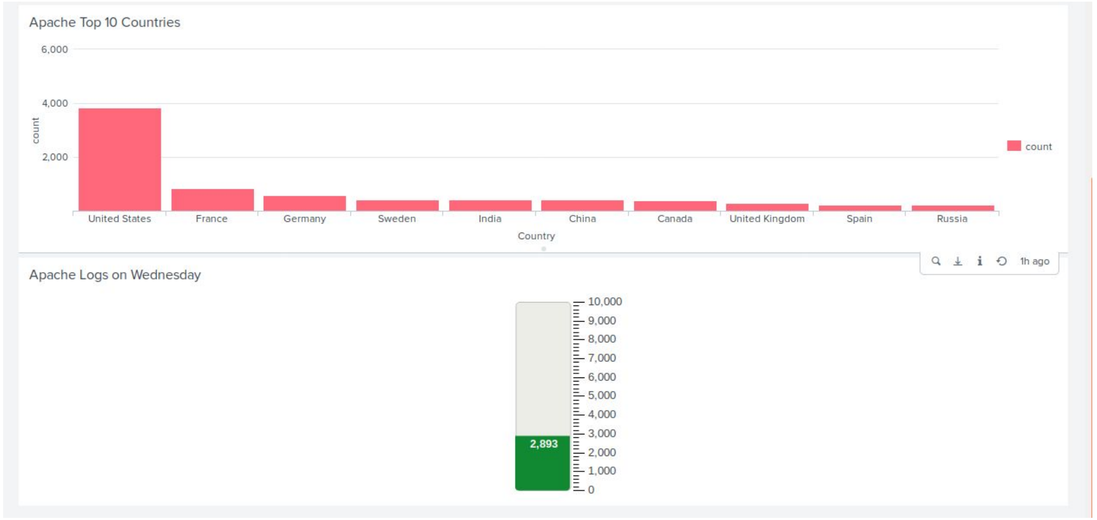
Justification: With the baseline being at 5 and our threshold being at 11 the alert would’ve been triggered. I got 11 for my threshold with standard deviation of my baseline number(5) and that number was 12. With that I chose 11 to be my threshold because I felt that 12 was to much of a risk.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reportin
Apache Logs Method Post
Edit
Ubuntu Software
App: search
Permissions: Private. Owned by admin. Edit
Modified: Mar 14, 2023 3:22:19 AM
Alert Type: Scheduled. Hourly, at 30 minutes past the hour. Edit
Trigger Condition: Custom. "search count > 11". Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.

Dashboards—Apache







Attack Analysis

Attack Summary—Windows

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

- It appeared that Users A and K were working together performing a brute force attack on the Windows Server.
- User A performed their attack from 0140am-0240am. During this time they were performing a bruteforce attack and our threshold alert was tripped.
- User K performed their part of the attack from 0910am-1100am and were attempting to reset account passwords.
- User J started rapidly logging on from 1000am-0100pm

Attack Summary—Windows

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

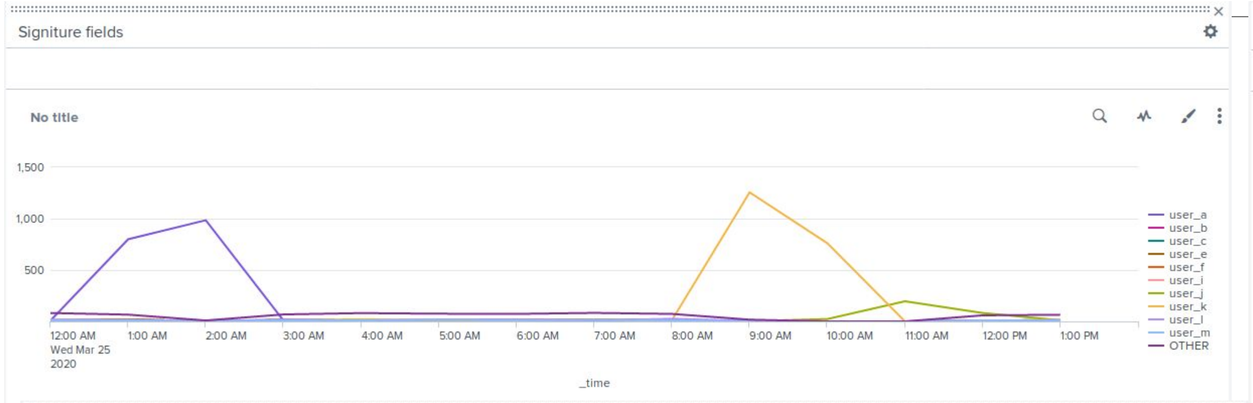
- Our failure alert worked properly. Since our threshold was set at >25.
- Our success alert also worked properly and was tripped since our threshold was set at >300.

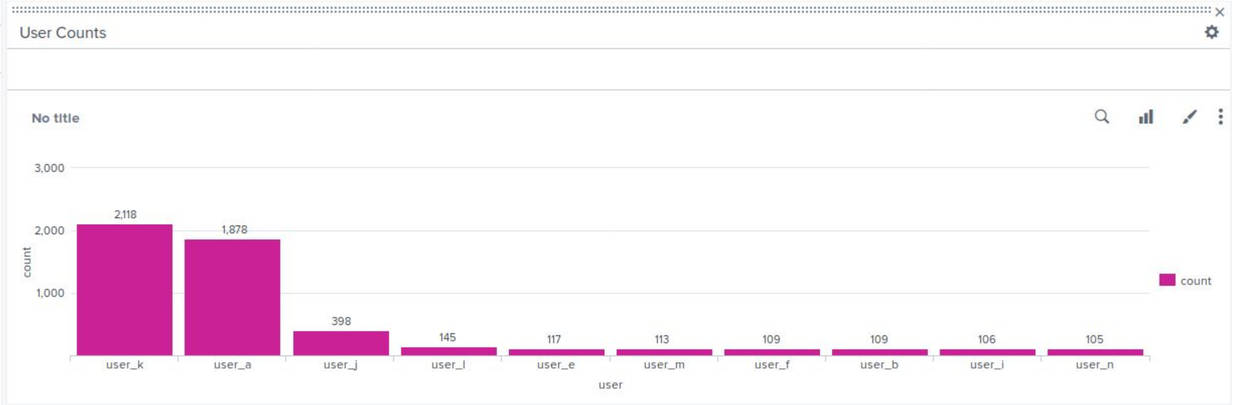
Attack Summary—Windows

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

- The Windows attack logs show an increase in activity on our “User Counts” and “Signature counts” graphs
- There is also more activity for certain users in successful account logins, attempted reset of passwords, and users accounts being locked out
- User_j and primarily logging in, and users “a” and “k” had high signature counts of attempting password resets/accounts locked out

Screenshots of Windows Attack Dashboard





Attack Summary—Apache

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

- We noticed a increase in HTTP POST request. From a count of 106 to 1,324 on the 25th of March.

- The team found a significant decrease in website referrals from the Apache logs to Apache attack logs.

- There was a increase in international traffic from Germany on the 25th of March. With an increase of 404 response codes showing there was a DDoS attack.

Attack Summary—Apache

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

Apache Logs compared to Apache attack logs

- We noticed a 28% decrease from the apache_logs to the apache_attacker_logs in the GET request. But a 28% increase in POST request. When you're receiving a HTTP response flood like this it most likely intels a DDoS attack. Our alert threshold was set to 11 requests with the baseline being 5. With this alert threshold in place it would detect this attack against the Apache servers.
- There was a difference between the two Apache logs with a decent increase of international client activity from Ukraine during the time of the attack from 791 to 1425 on March 25th.

Attack Summary—Apache

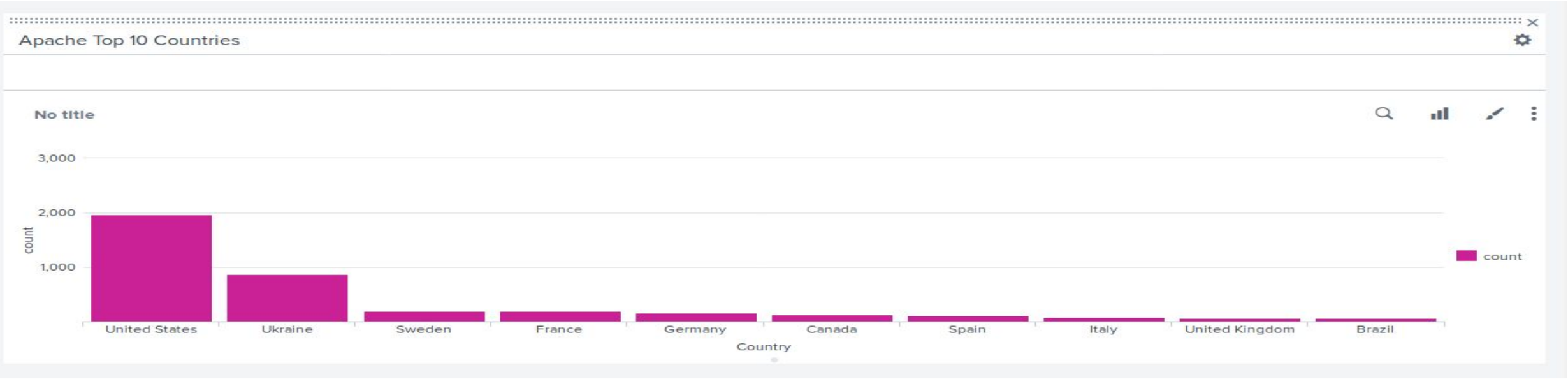
Summarize your findings from your dashboards when analyzing the attack logs.

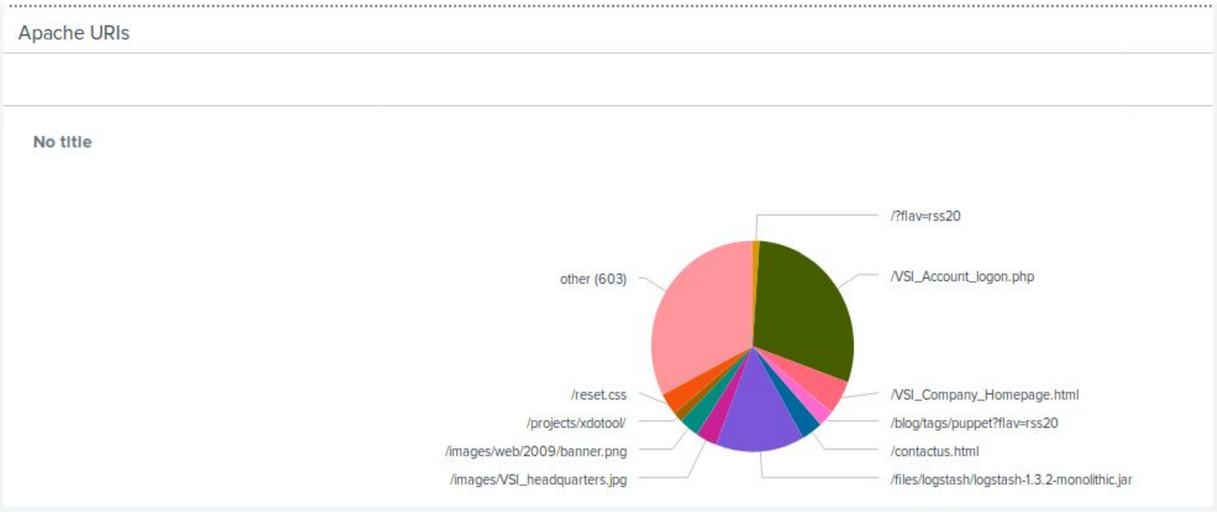
- After comparing the original dashboard to the dashboard containing the attack log data we realized a significant increase in HTTP POST requests that happened between the hours of 5:00 pm and 7:00 pm.

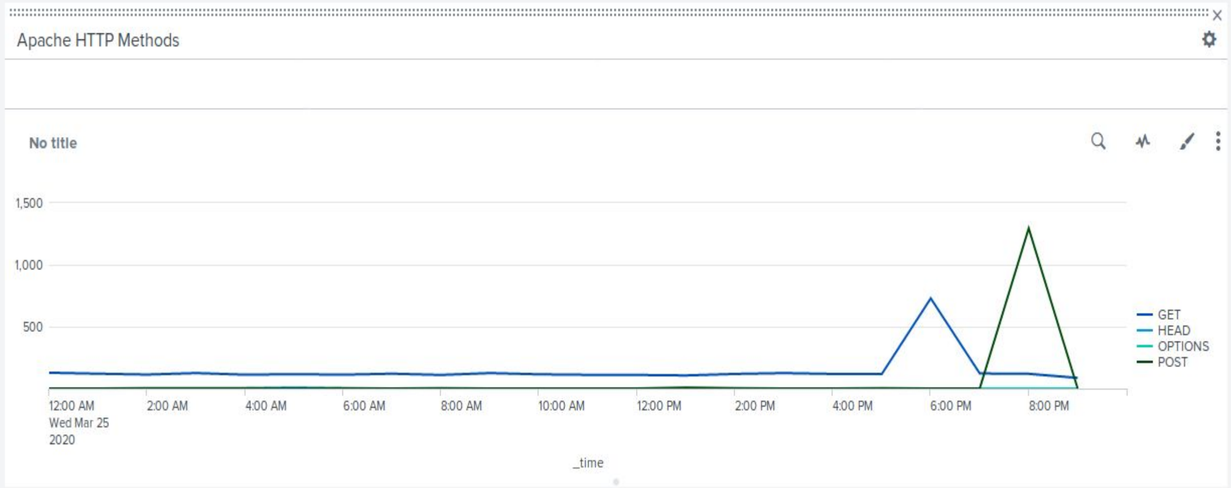
- We noticed that on our URI graph the number one URI was “/VSI_Account_logon.php” as opposed to just “/VSI_Company_Homepage.html” which was the primary URI before the attack.

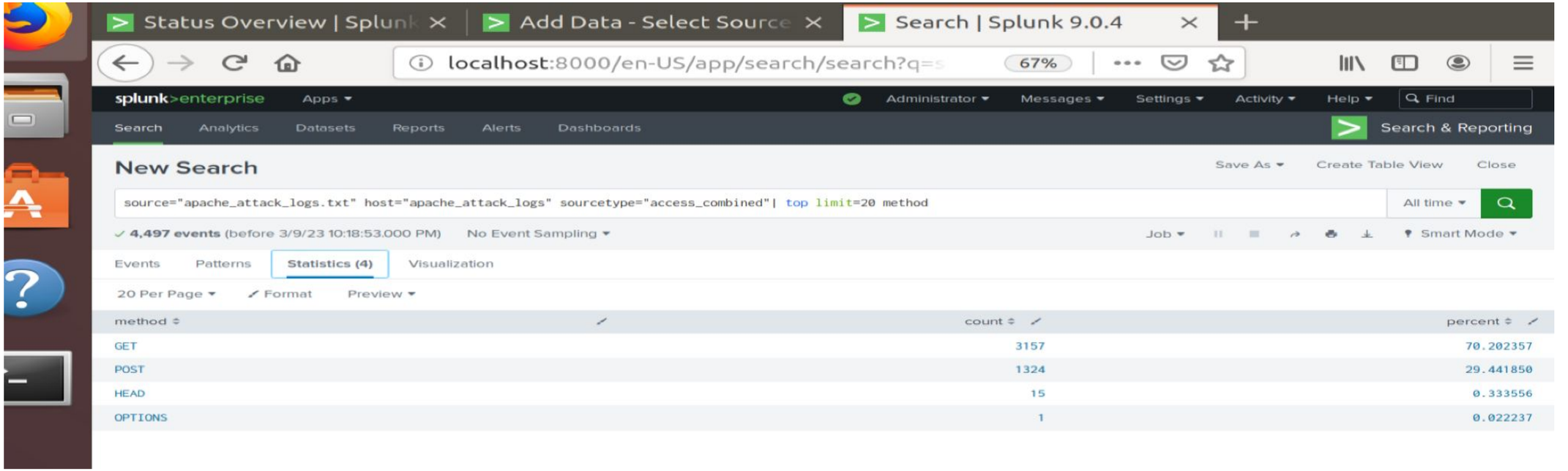
- For the top ten countries, we noticed that Ukraine, which was not in the top ten before, now had the second most behind the United States.

Screenshots of Attack Dashboard

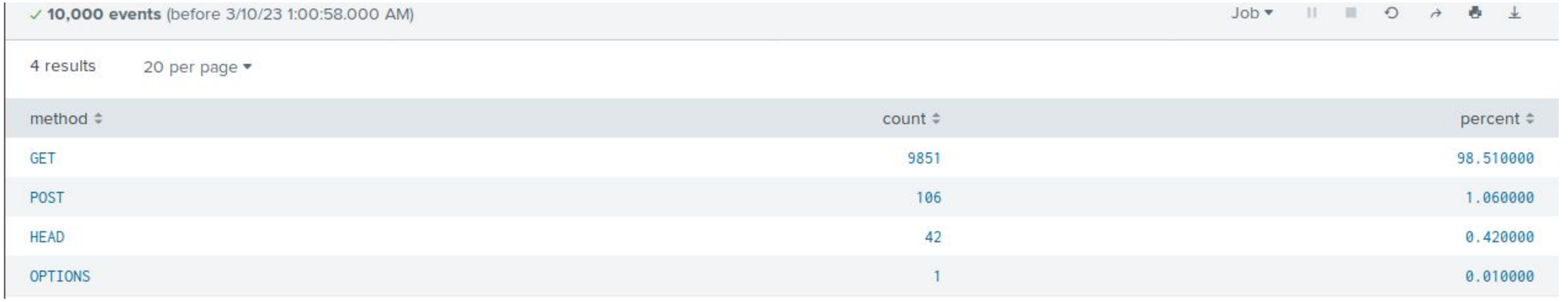


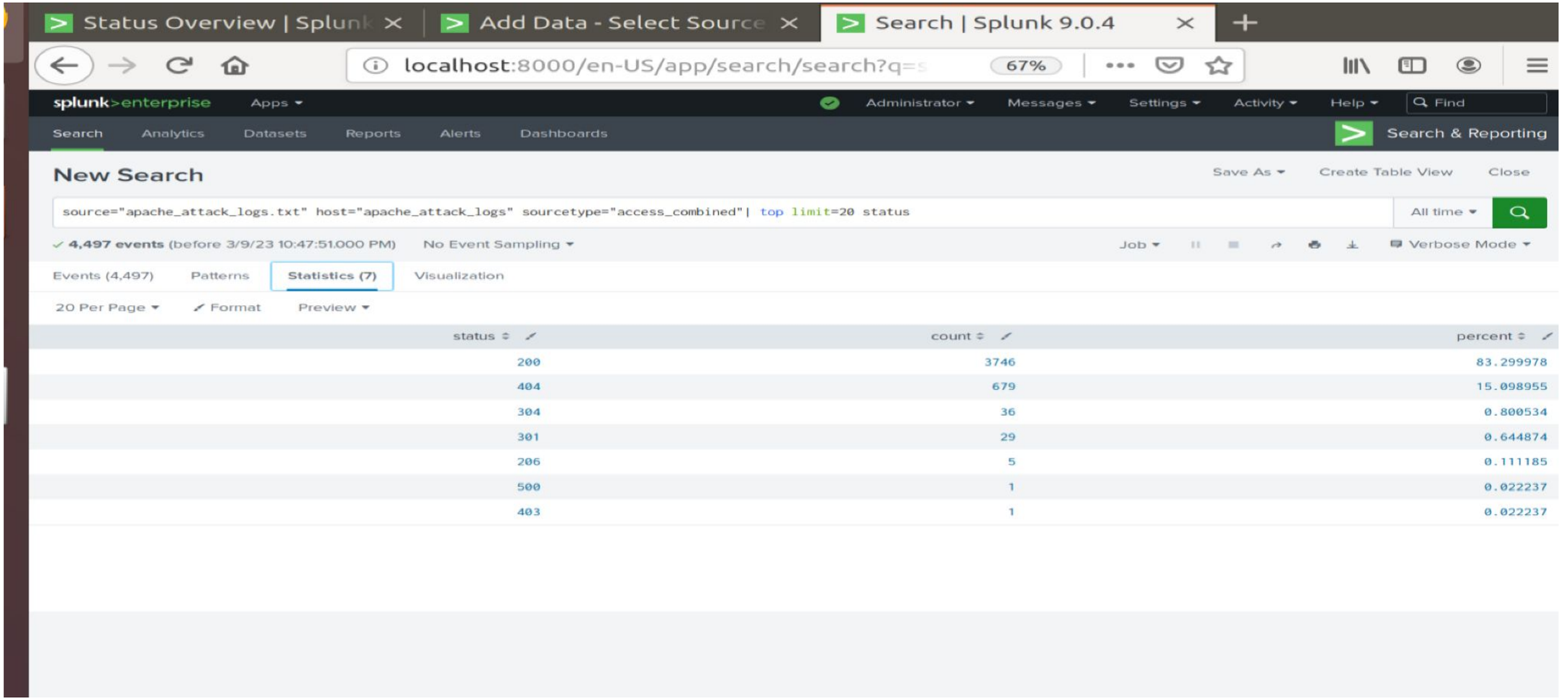




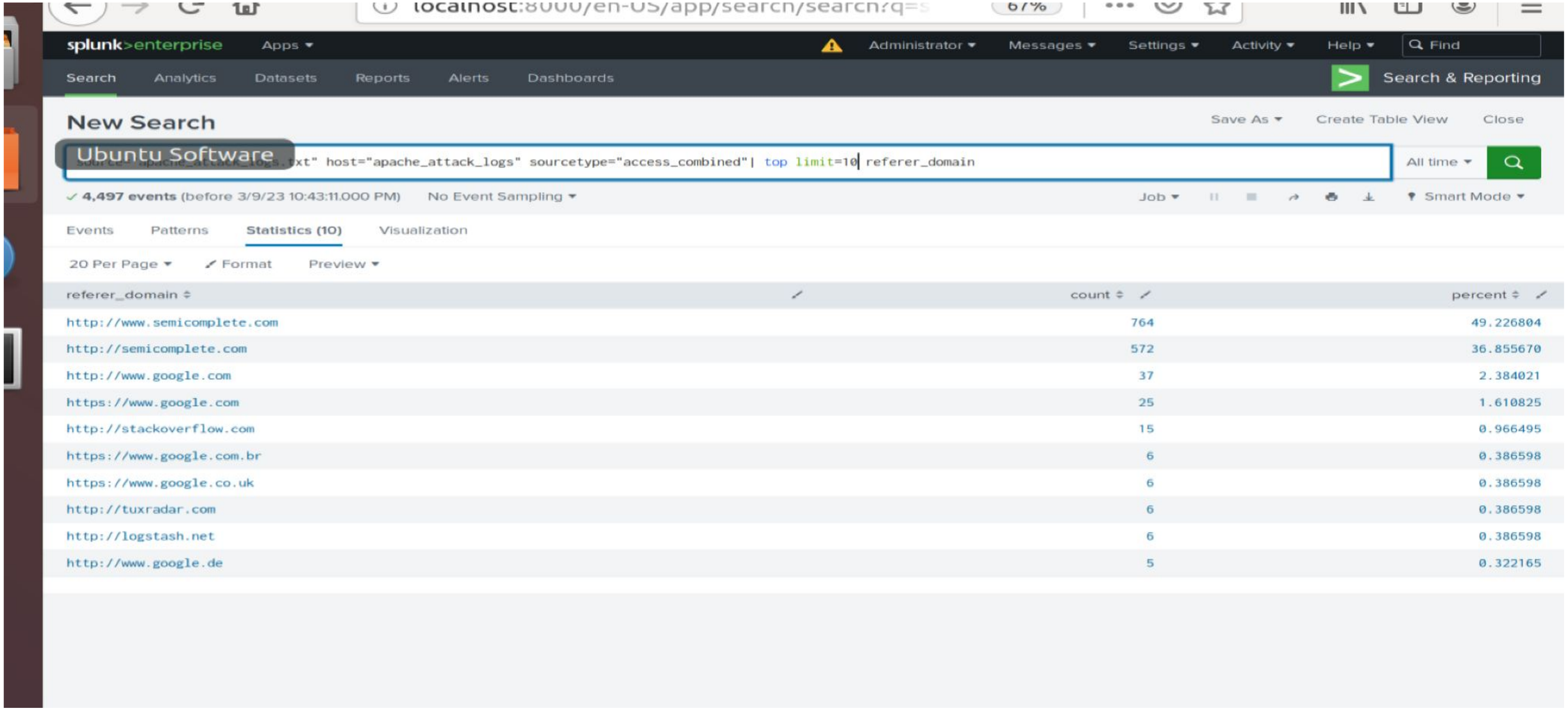


Compared to average statistics:





status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
Ubuntu Software
txt" host="apache_attack_logs" sourcetype="access_combined"| top limit=10 referer_domain
All time
4,497 events (before 3/9/23 10:43:11.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (10)
Visualization
20 Per Page
Format
Preview
referer_domain
count
percent
http://www.semicomplete.com 764 49.226804
http://semicomplete.com 572 36.855670
http://www.google.com 37 2.384021
https://www.google.com 25 1.610825
http://stackoverflow.com 15 0.966495
https://www.google.com.br 6 0.386598
https://www.google.co.uk 6 0.386598
http://tuxradar.com 6 0.386598
http://logstash.net 6 0.386598
http://www.google.de 5 0.322165

Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
- Brute force attacks took place in Windows.
- DDoS attacks took place on Apache.

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

- User accounts should be locked out after 5 incorrect attempts
- Consecutive brute forcing attempts from the same IP Address should be locked out permanently
- Implementing multi- factor authentication