



Defensive Security Project

by: Stokely De Freitas

Table of Contents

This document contains the following resources:

01

**Monitoring
Environment**

02

Attack Analysis

03

**Project Summary
& Future
Mitigations**

Monitoring Environment

Scenario

- VSI received credible information that a competitor, JobeCorp maybe planning to launch a cyber attack. Impacting VSI daily operations.
- The SOC management team reviewed a variety of SIEM tools and based on functionality selected Splunk as its preferred option.
- The tool was used to baseline the current environment, prior, to the suspected attack. Reports were generated and alerts configured to notify the SOC team of any threshold violations.
- The baselines generated for the current environment will be used to determine the effectiveness of the alerts and the type of attack triggering the notification.



Add-On “Number Display”

Summary of Add-On “Number Display”

Number Display is a collection of ultra-configurable, single-statistic visualizations for Splunk. It includes the following styles: gauge, horseshoe, spinner, shapes (rectangle, hexagon, circle, ring, donut). Bringing life to the dashboards through animated number changes and subtle pulse animations.

Benefit of Add-On “Number Display”

This add-on was selected optimizing the appearance of the data being presented, while increasing the efficiency and enhancing the source data by creating a rich data set.

Image of Add-On “Number Display”

The image below is a representation on how the data will be displayed

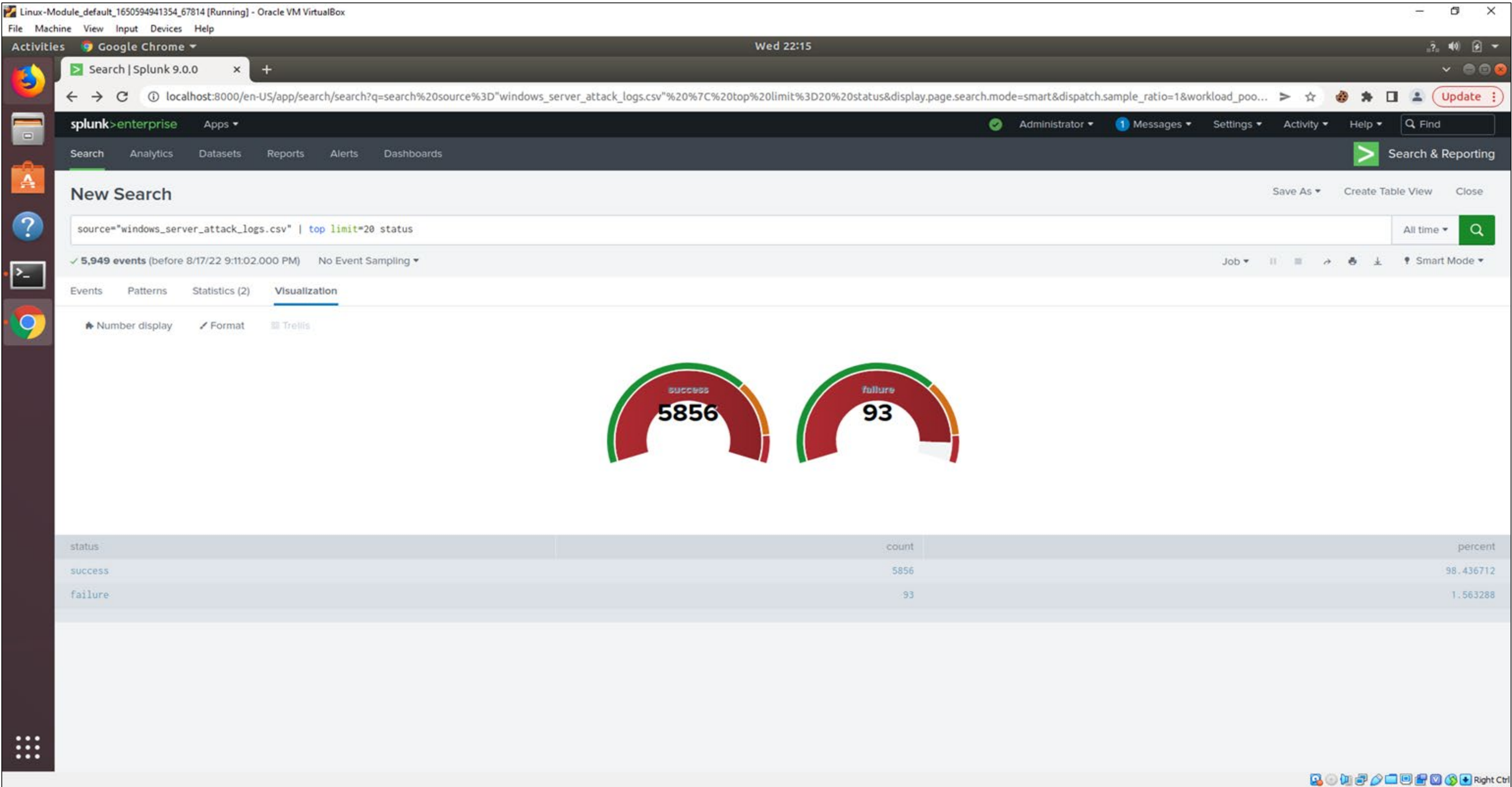


Fig.1 – Add-On: Number Display

Logs Analyzed

1

Windows Logs

Two sets of Windows logs were analyzed during this exercise, the pre-attack logs and the post attack logs. Every attempt will be made to quickly identify suspicious activities such as successful & failed logon attempts and deleted user accounts. This will also determine the effectiveness of the alerts.

2

Apache Logs

Two sets of Windows logs were analyzed during this exercise, the pre-attack logs and the post attack logs. Special attention would be placed on reviewing the HTTP methods (GET, POST, HEAD, etc..). Focus will be placed on determining the origins of the attack and the overall impact to the environment.

Windows Logs

Reports—Windows

| Report Name | Report Description |
|-----------------------------------|--|
| Window Server Log Table Signature | This is a report with a table of signatures with associated Signature_ID |
| Window Server Log Top Severity | This is a report that provides the count and percent of the severity. |
| Window Server Log top status | This is a report that provides a comparison between the success and failure of Windows activities. |

Images of Reports—Windows

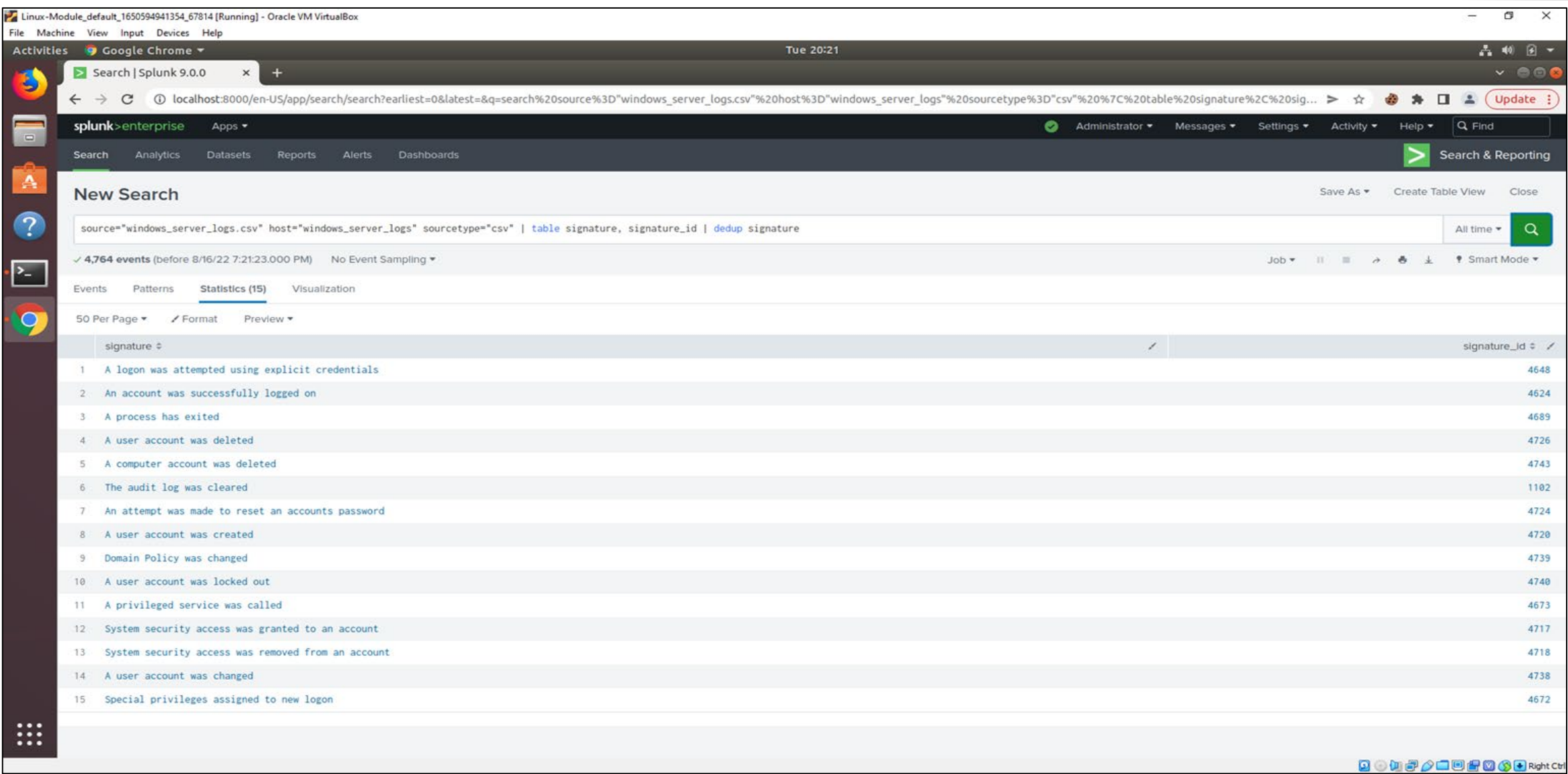


Fig.2 – Dataset: Signature

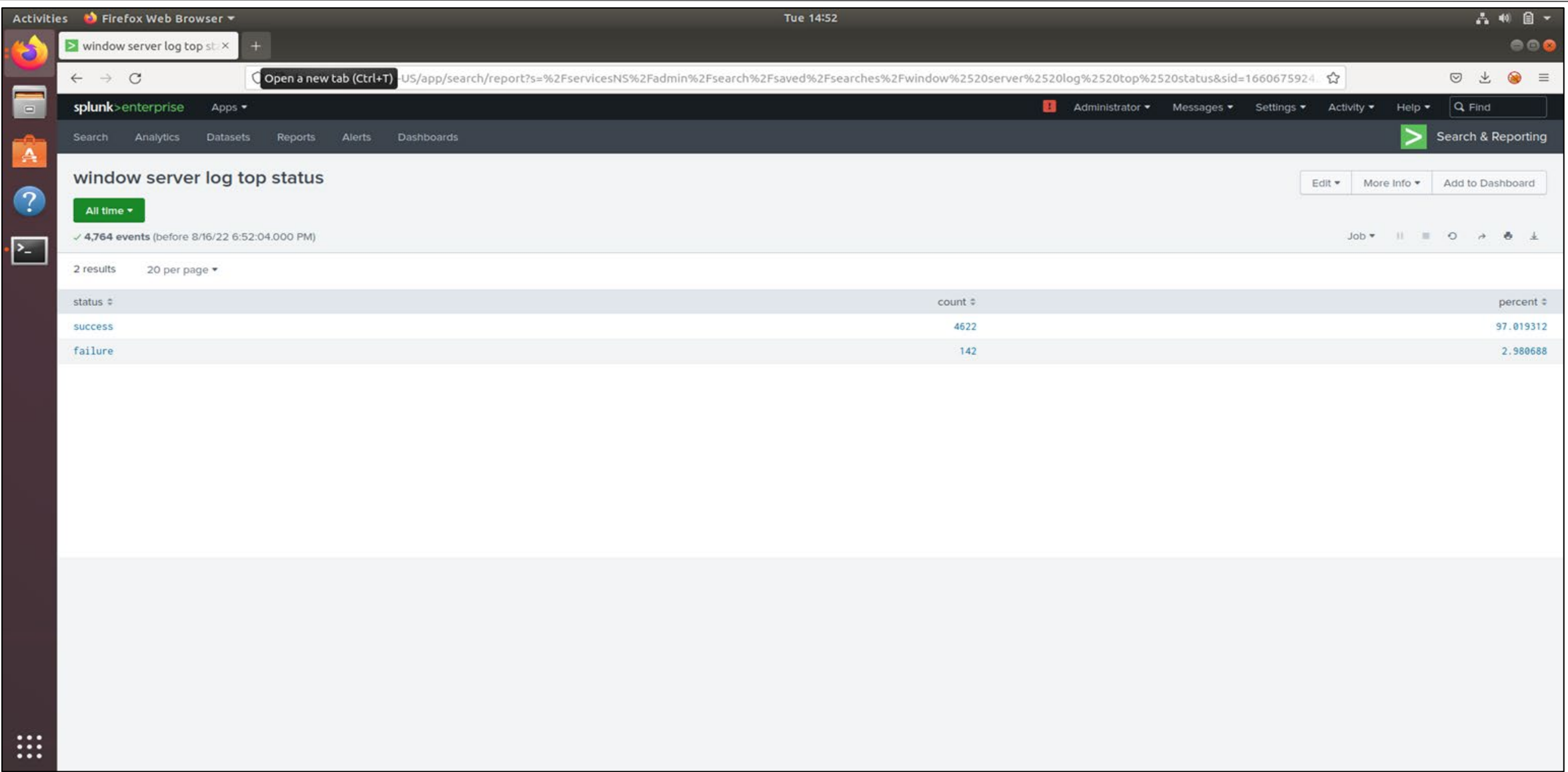


Fig.3 – Dataset: Status

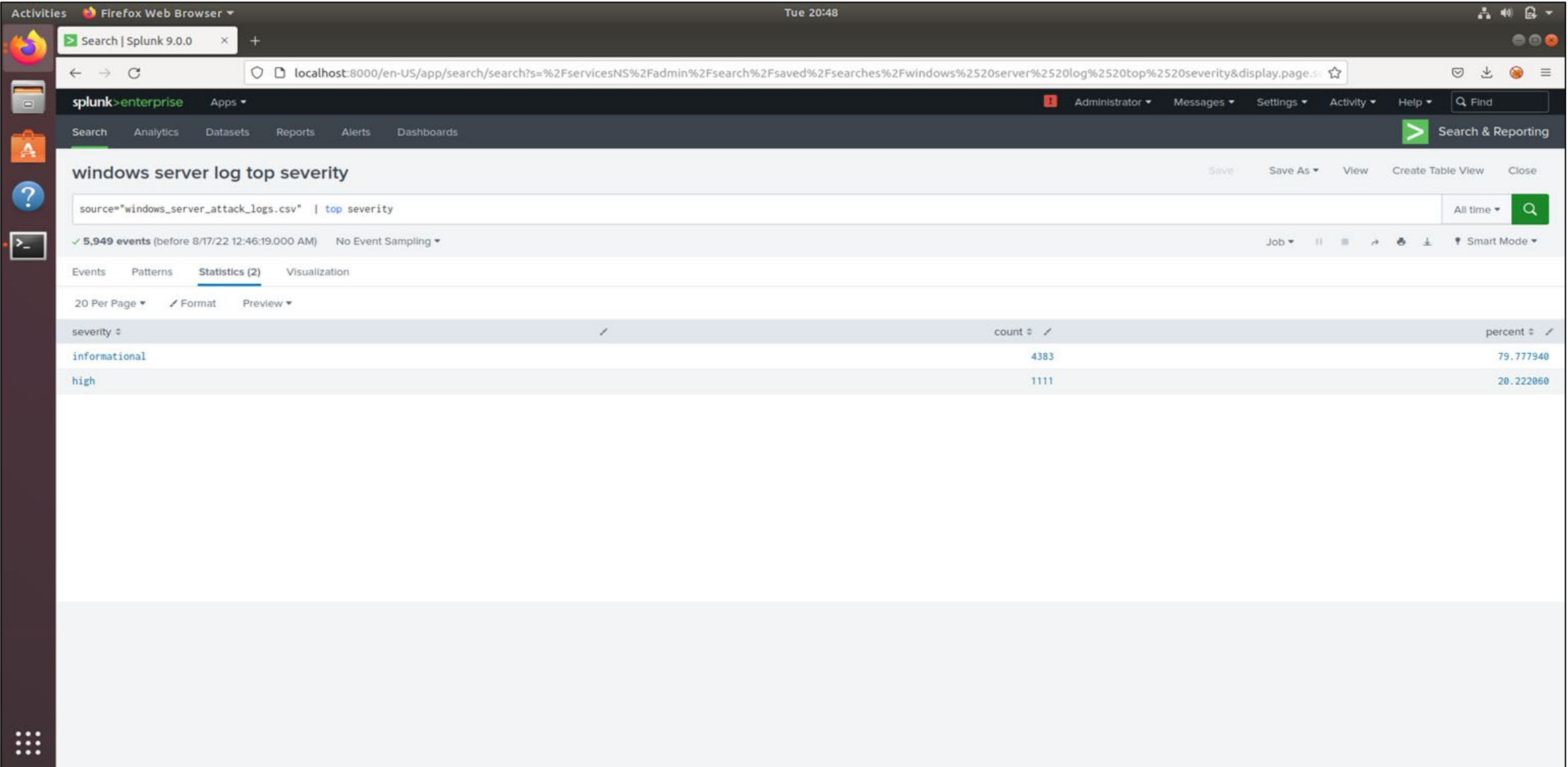


Fig.4 – Dataset: Severity

Alerts—Windows

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|-------------------------|--|----------------|-----------------|
| Failed Windows Activity | This alert triggers failed windows activities, reporting hourly. | 5 | 20 |

A review of all alerts were performed, and our observation determined a baseline of five (5) alerts per hour seemed consistent. Therefore, an alert threshold of twenty (20) was considered effective without subjecting the SOC team to “alert fatigue”.

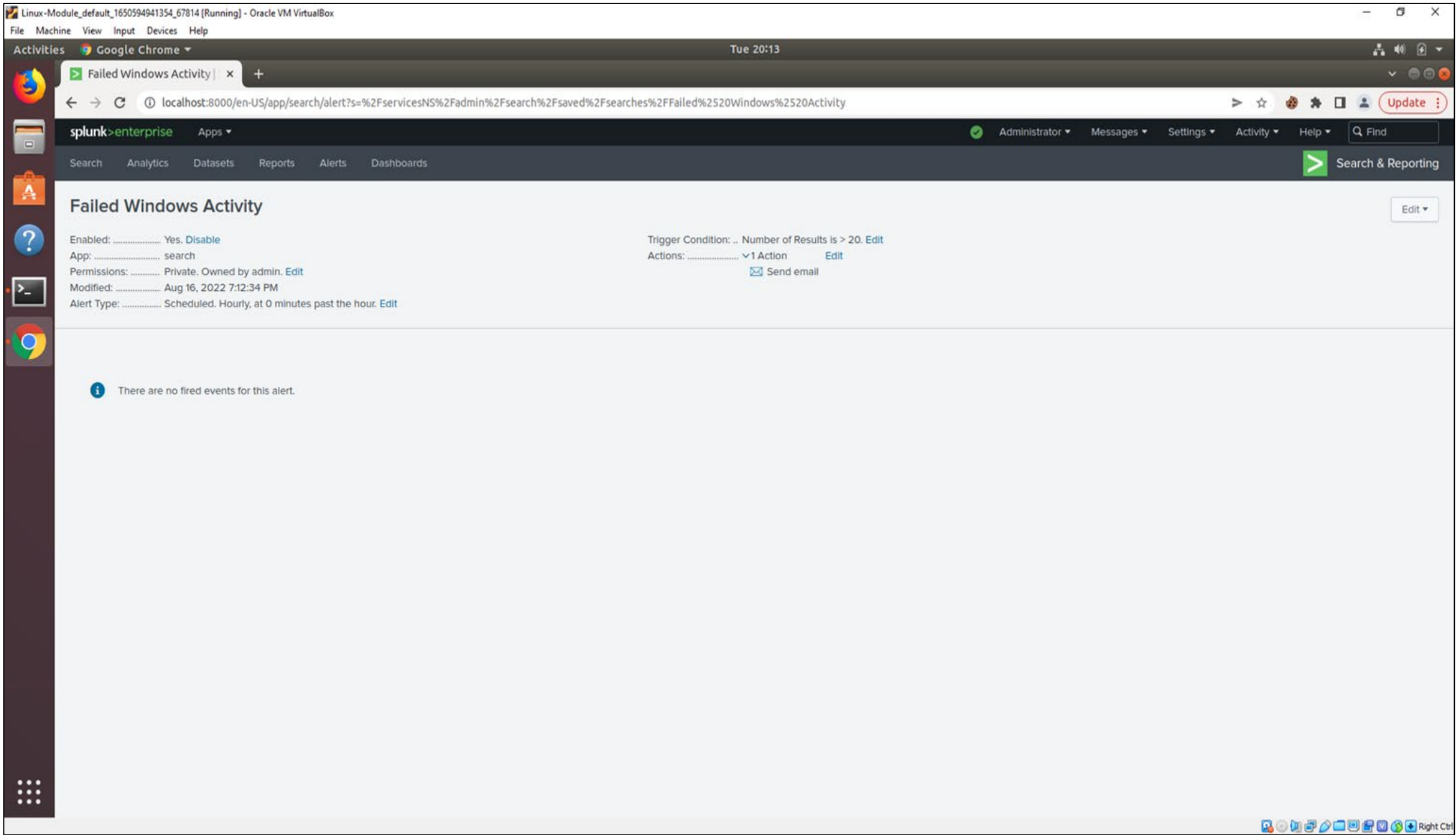


Fig.5 – Failed Windows Activity

Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---------------------------------|---|----------------|-----------------|
| Successfully Logged on Accounts | An alert that triggers for successfully logged on accounts when the threshold has been reached. | 12 | 30 |

A review of all alerts were performed, and our observation determined a baseline of twelve (12) alerts per hour seemed consistent. Therefore, an alert threshold of thirty (30) was considered effective without subjecting the SOC team to “alert fatigue”.

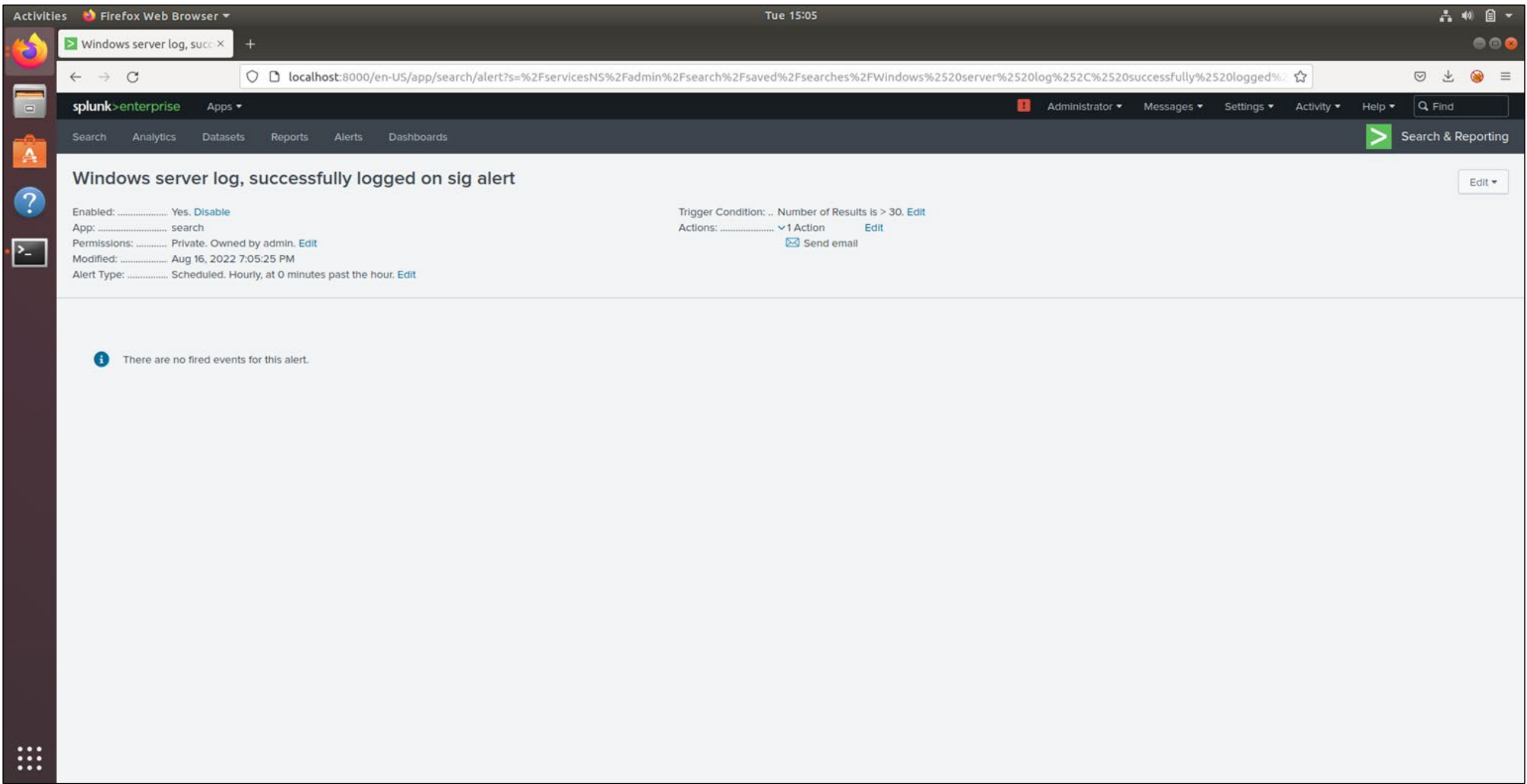


Fig.6 – Dataset: Successfully Logged On

Alerts—Windows

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|-------------------------------|---|----------------|-----------------|
| Signature_ID Windows Activity | This alert triggers “a user account was deleted”, reporting hourly. | 12 | 20 |

A review of all alerts were performed, and our observation determined a baseline of twelve (12) alerts per hour seemed consistent. Therefore, an alert threshold of twenty (20) was considered effective without subjecting the SOC team to “alert fatigue”.

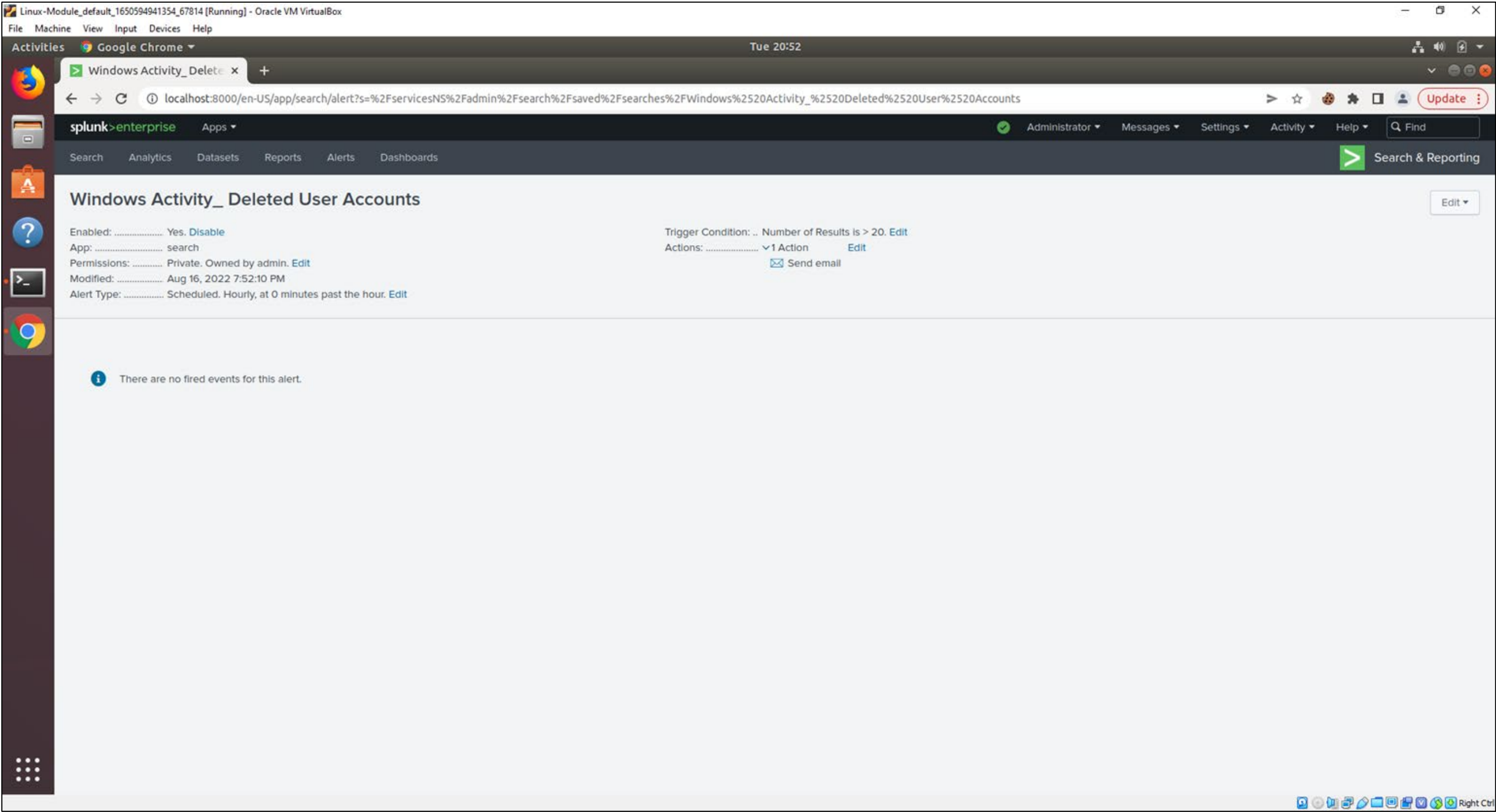


Fig.7 – Dataset: Successfully Logged On

Dashboards—Windows

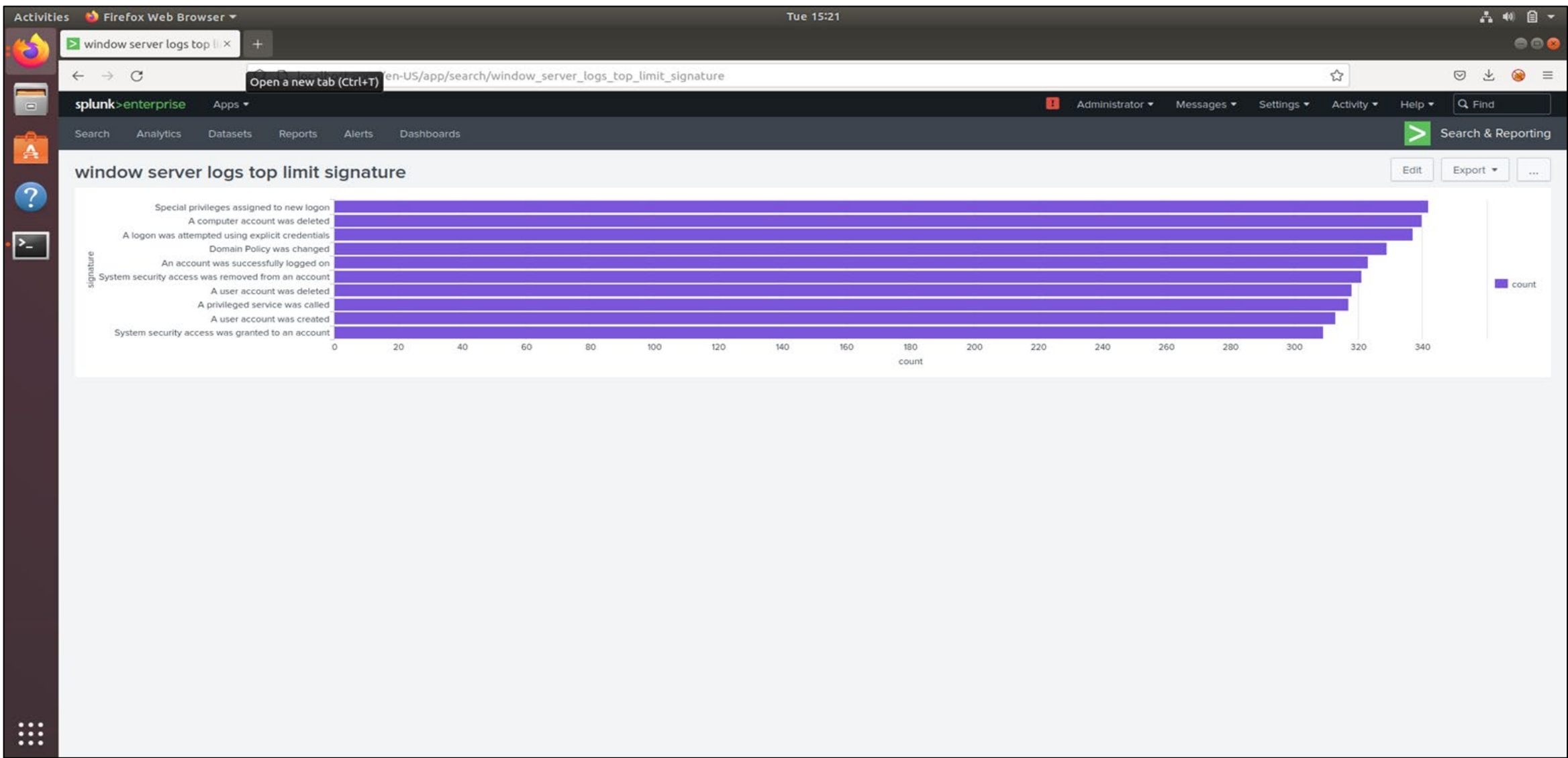


Fig.8 – Bar Chart

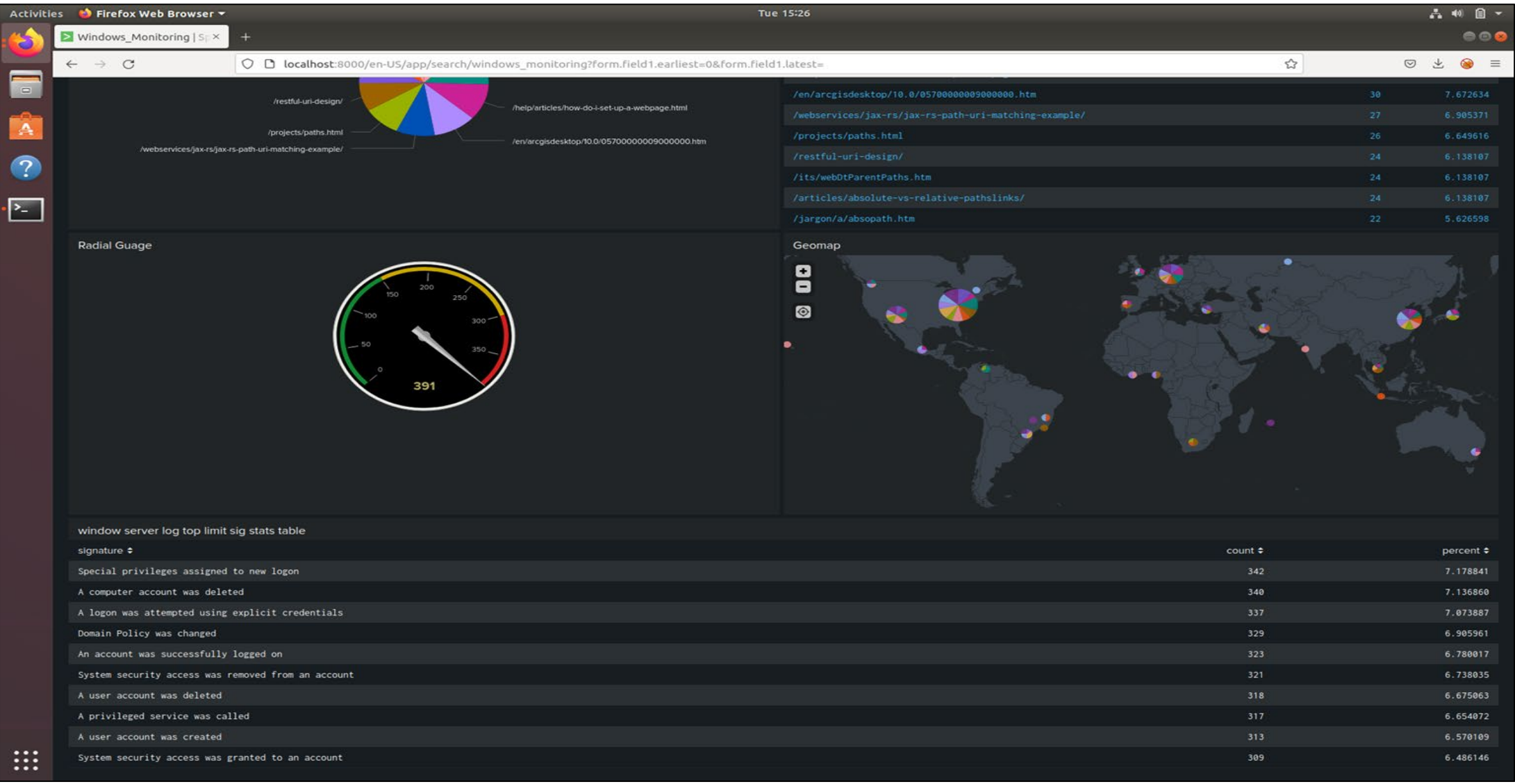


Fig.9 – Compiled Dashboard

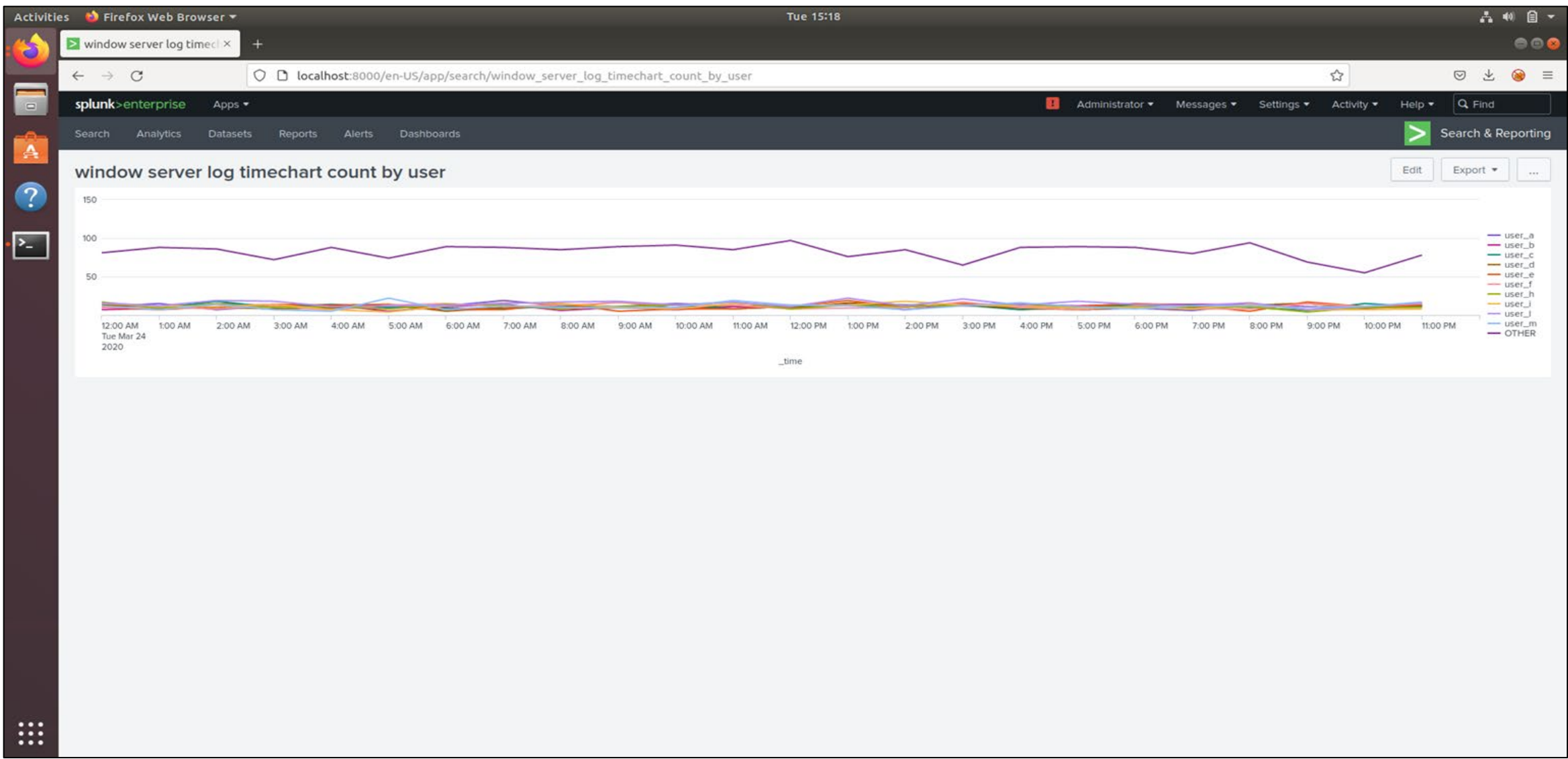


Fig.10 – Count by User Line Chart

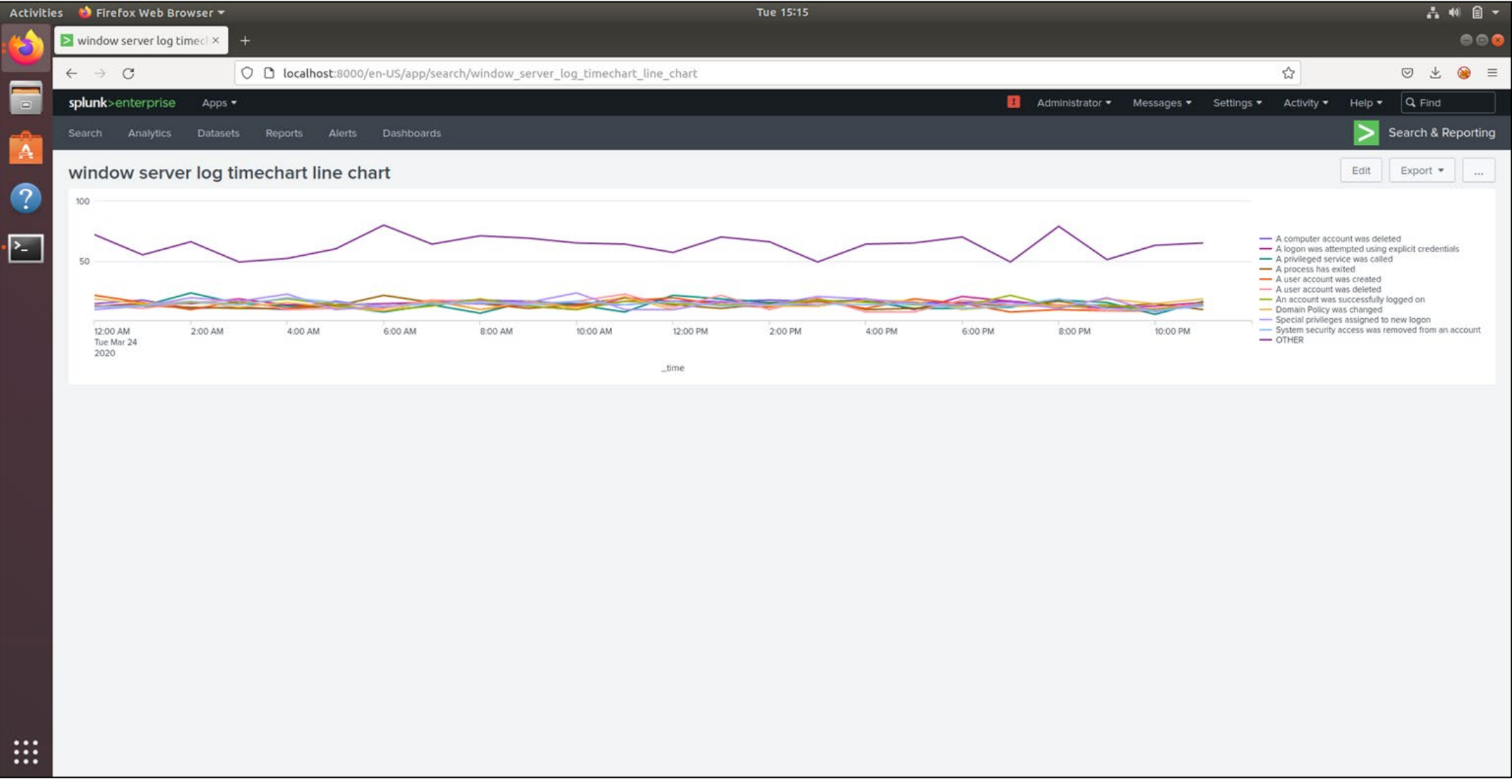


Fig.11 – Time Interval Line Chart

Dashboards—Windows

| Stats Table Top 10 Users | | | |
|--------------------------|--------|---------|-----------|
| | user ↕ | count ↕ | percent ↕ |
| 1 | user_l | 354 | 7.430730 |
| 2 | user_a | 282 | 5.919395 |
| 3 | user_m | 275 | 5.772460 |
| 4 | user_i | 271 | 5.688497 |
| 5 | user_f | 270 | 5.667506 |
| 6 | user_h | 269 | 5.646516 |
| 7 | user_e | 269 | 5.646516 |
| 8 | user_c | 267 | 5.604534 |
| 9 | user_d | 264 | 5.541562 |
| 10 | user_b | 263 | 5.520571 |

Fig.12 – Top 10 Users

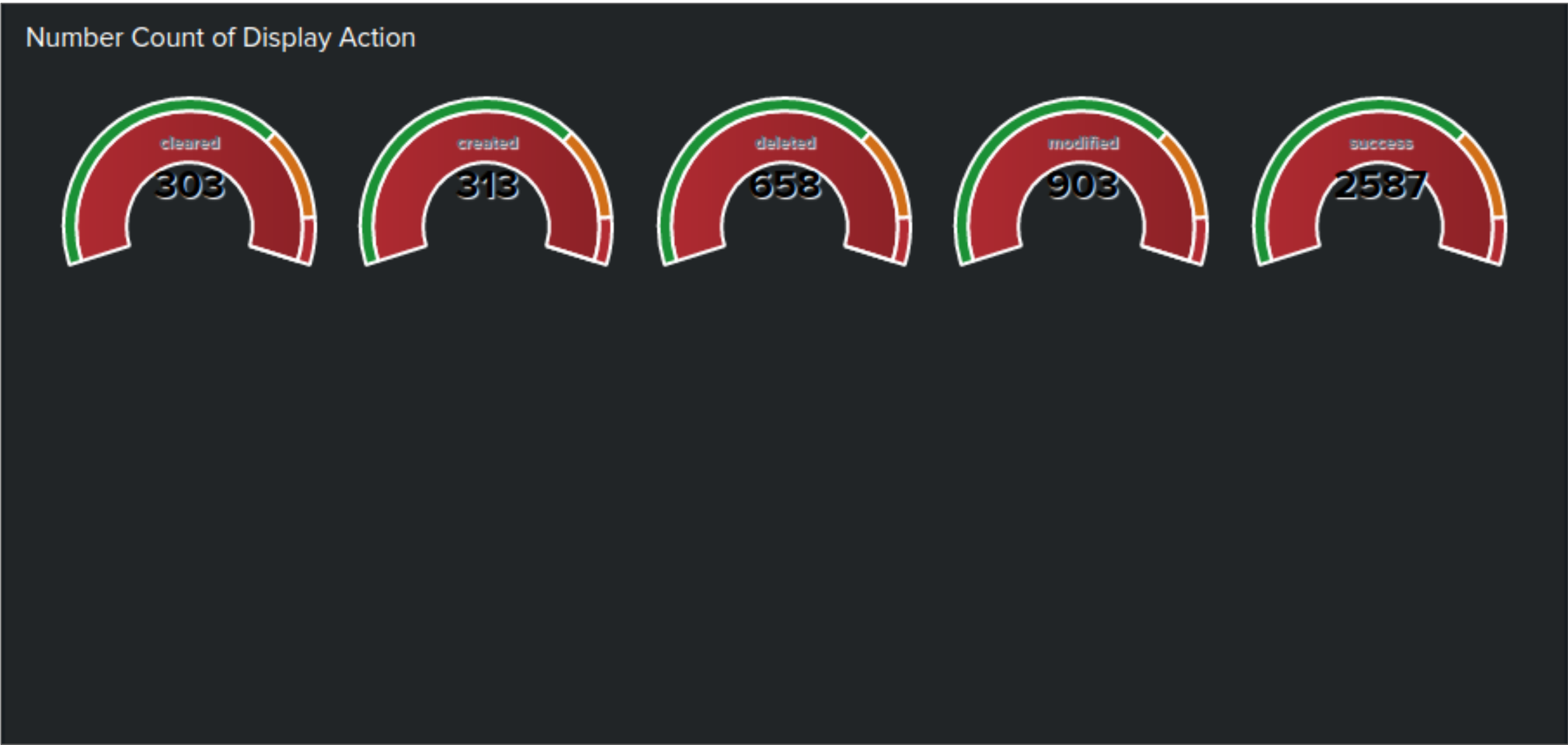


Fig.13 – Number Count of Display Action

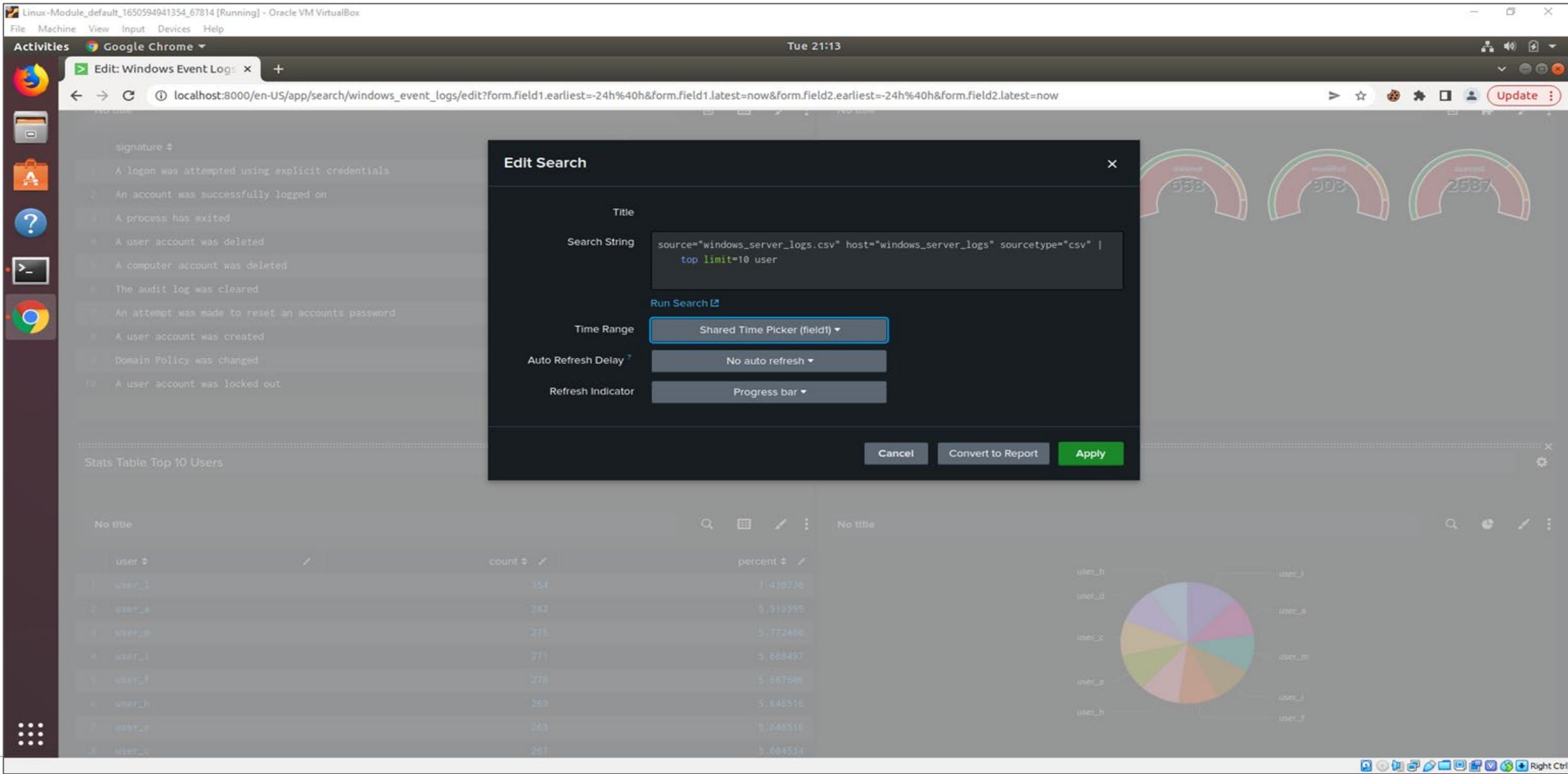


Fig.14 – Dashboard Configuration

Apache Logs

Reports—Apache

| Report Name | Report Description |
|---------------------------|-------------------------------------|
| Apache HTTP Reports Table | Report analysis for Methods |
| Apache Referrer Domain | Analysis of referrer Domains |
| Apache HTTP Response | Analysis of the HTTP response codes |

Images of Reports—Apache

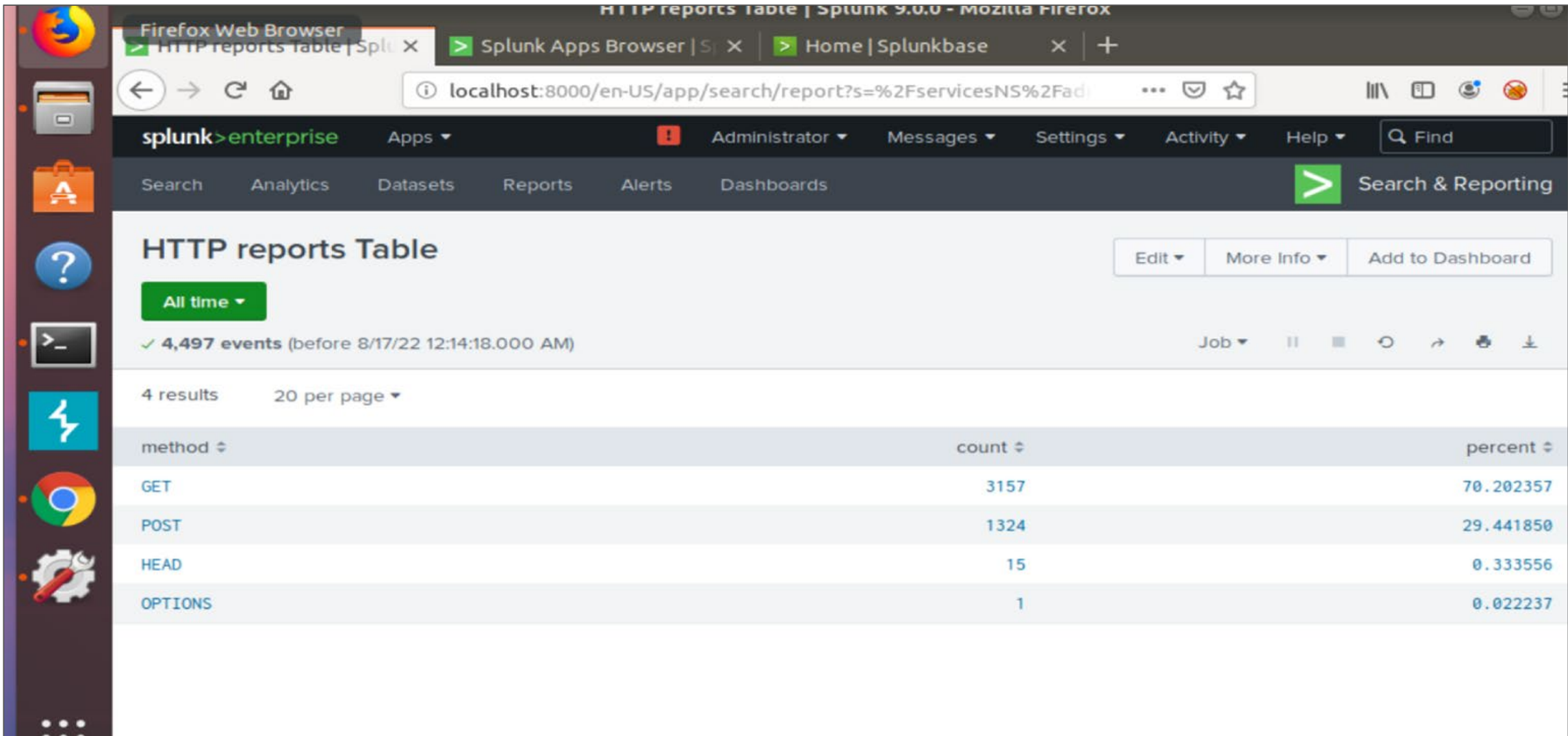


Fig.15 – HTTP Method Count & Percentages

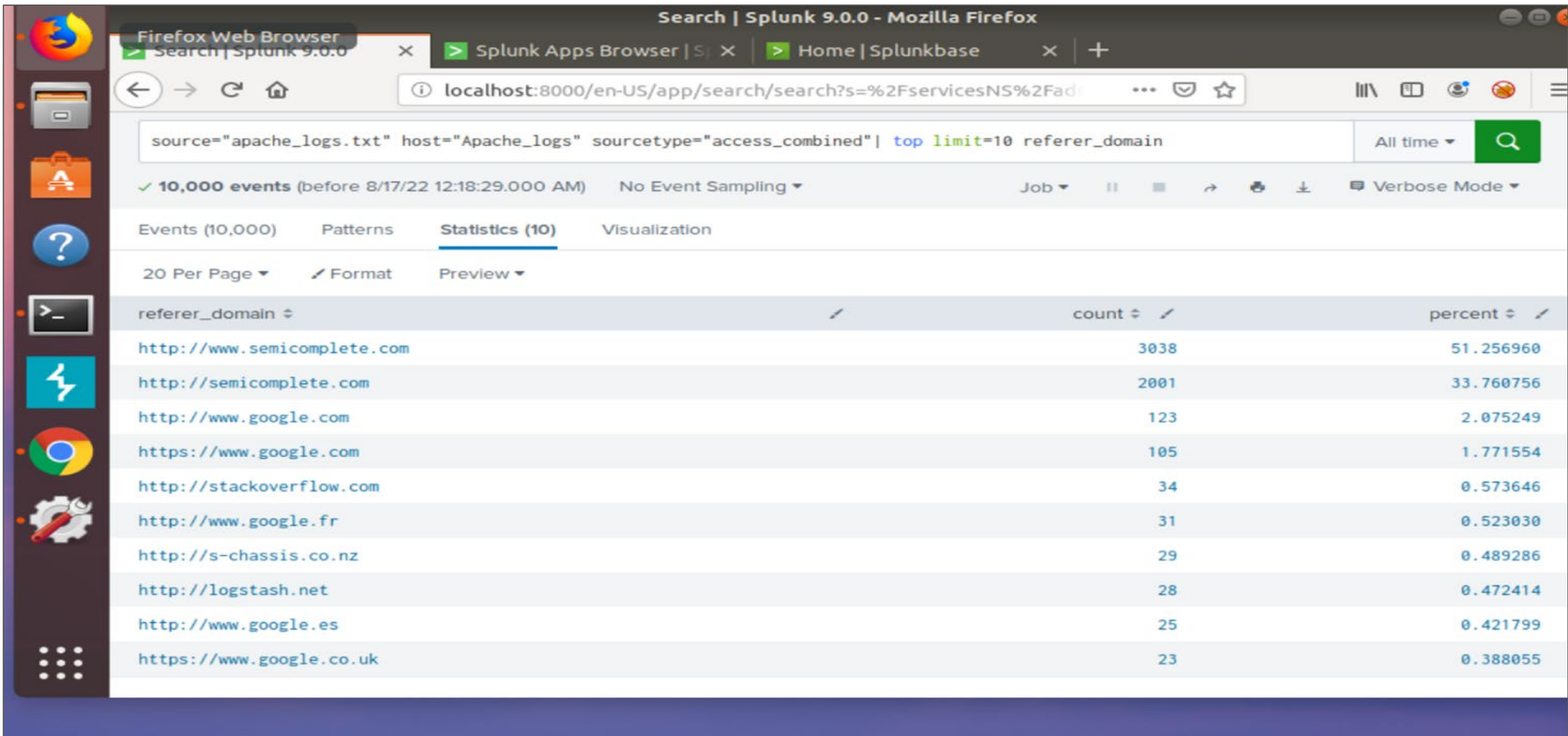


Fig.16 – Top 10 “referer_domain”

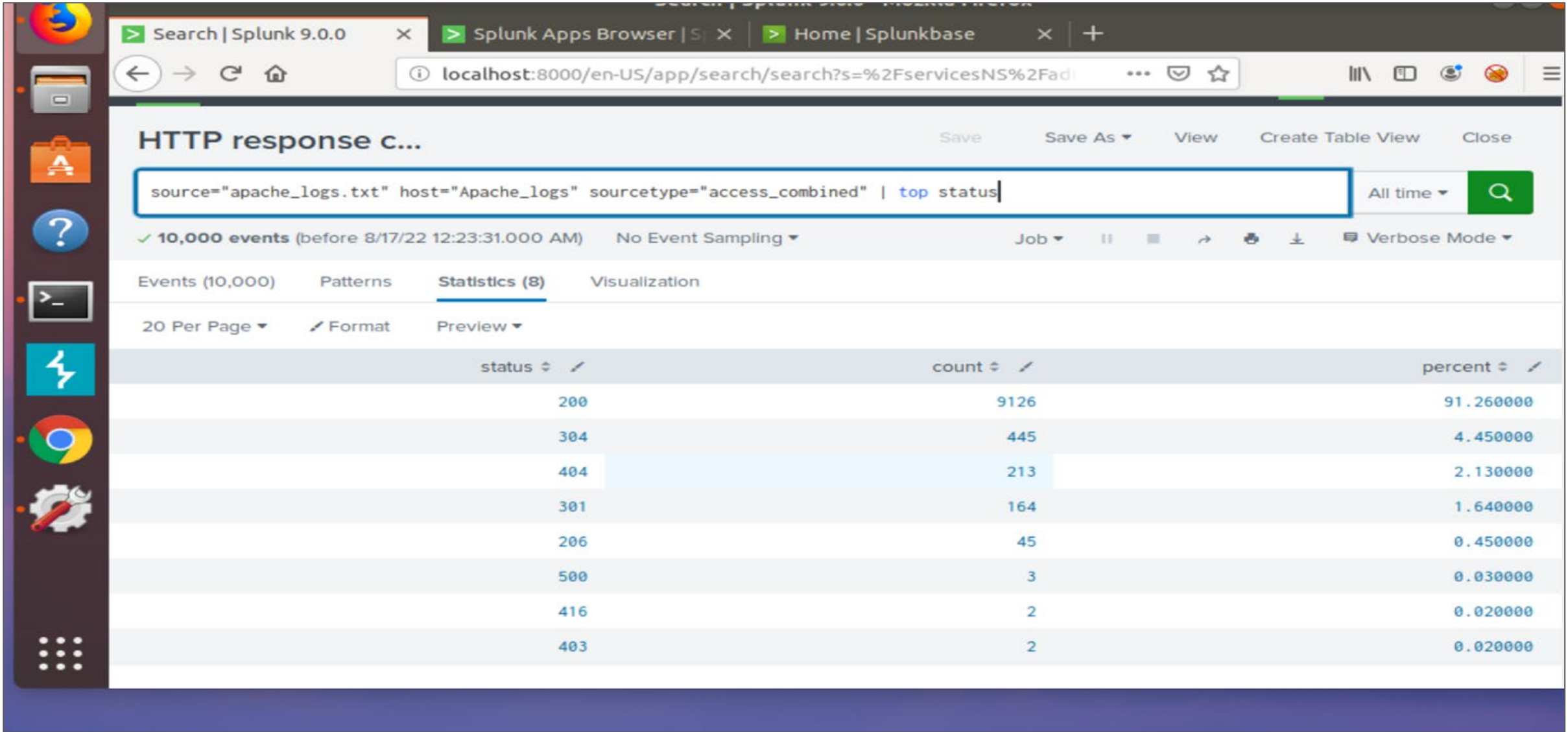


Fig.17 – Status Count & Percentage

Alerts—Apache

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|--|---|----------------|-----------------|
| Alert analysis of international activity | Alert for international activity per hour | 146 | 220 |

A review of all alerts were performed, and our observation determined a baseline of one hundred and forty-six (146) alerts per hour seemed consistent. Therefore, an alert threshold of two hundred and twenty (220) was considered effective without subjecting the SOC team to “alert fatigue”.

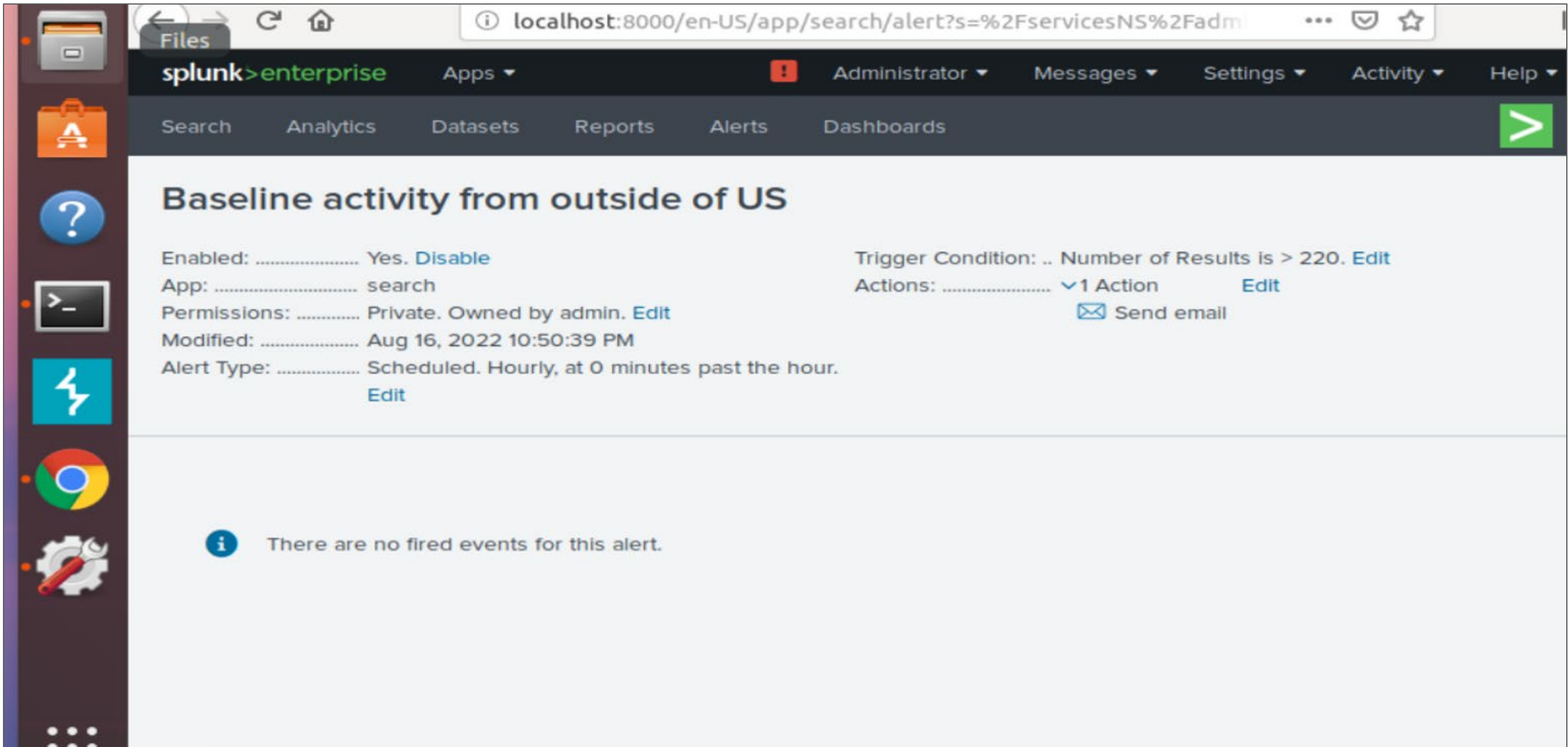


Fig.18 – Baseline Activity from Outside the US

Alerts—Apache

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|--------------------------|------------------------------------|----------------|-----------------|
| Alert HTTP POST activity | Alert of HTTP POST volume per hour | 10 | 18 |

A review of all alerts were performed, and our observation determined a baseline of ten (10) alerts per hour seemed consistent. Therefore, an alert threshold of eighteen (18) was considered effective without subjecting the SOC team to “alert fatigue”.

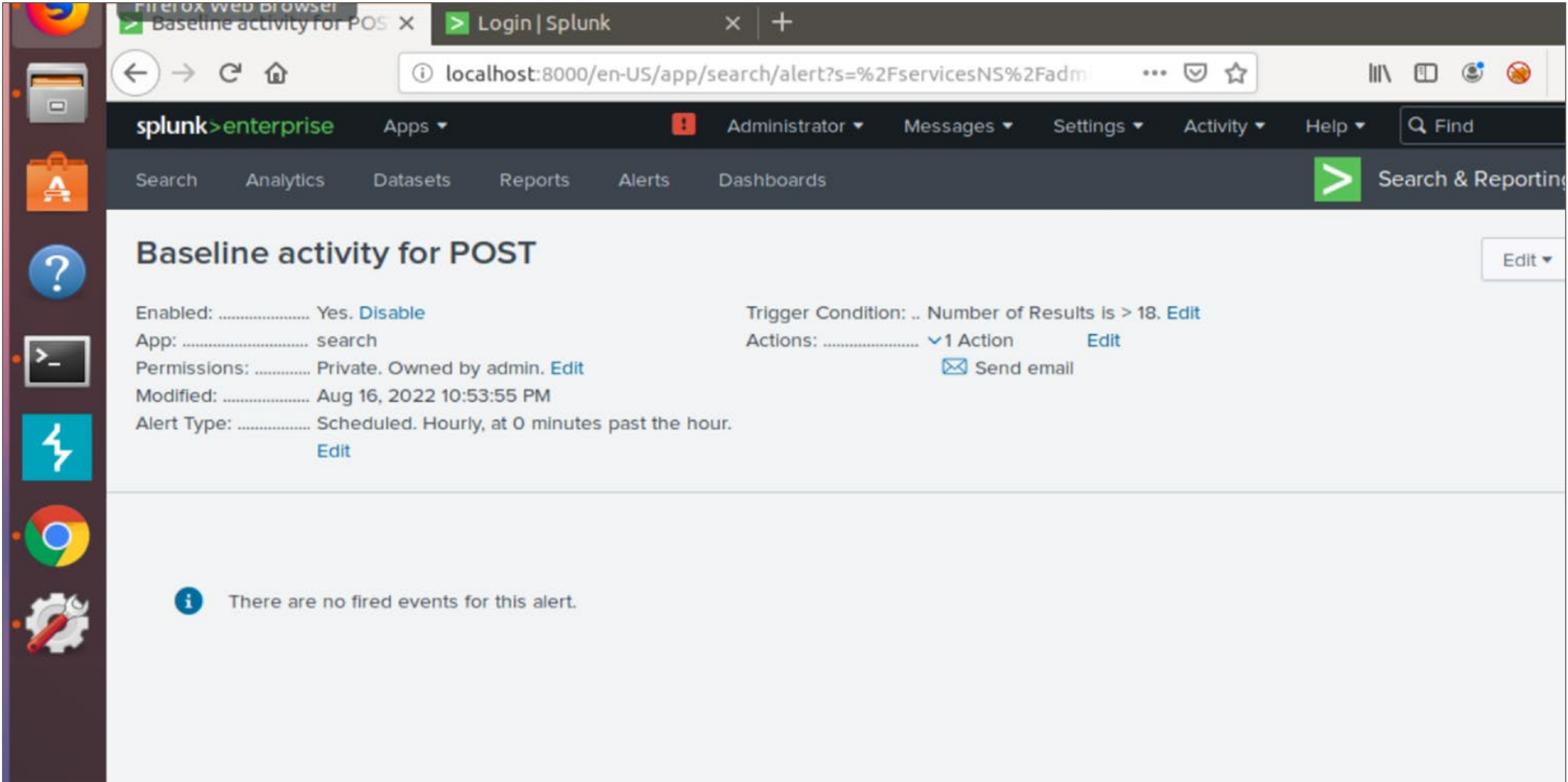


Fig.19 – Baseline Activity for POST

Dashboards—Apache

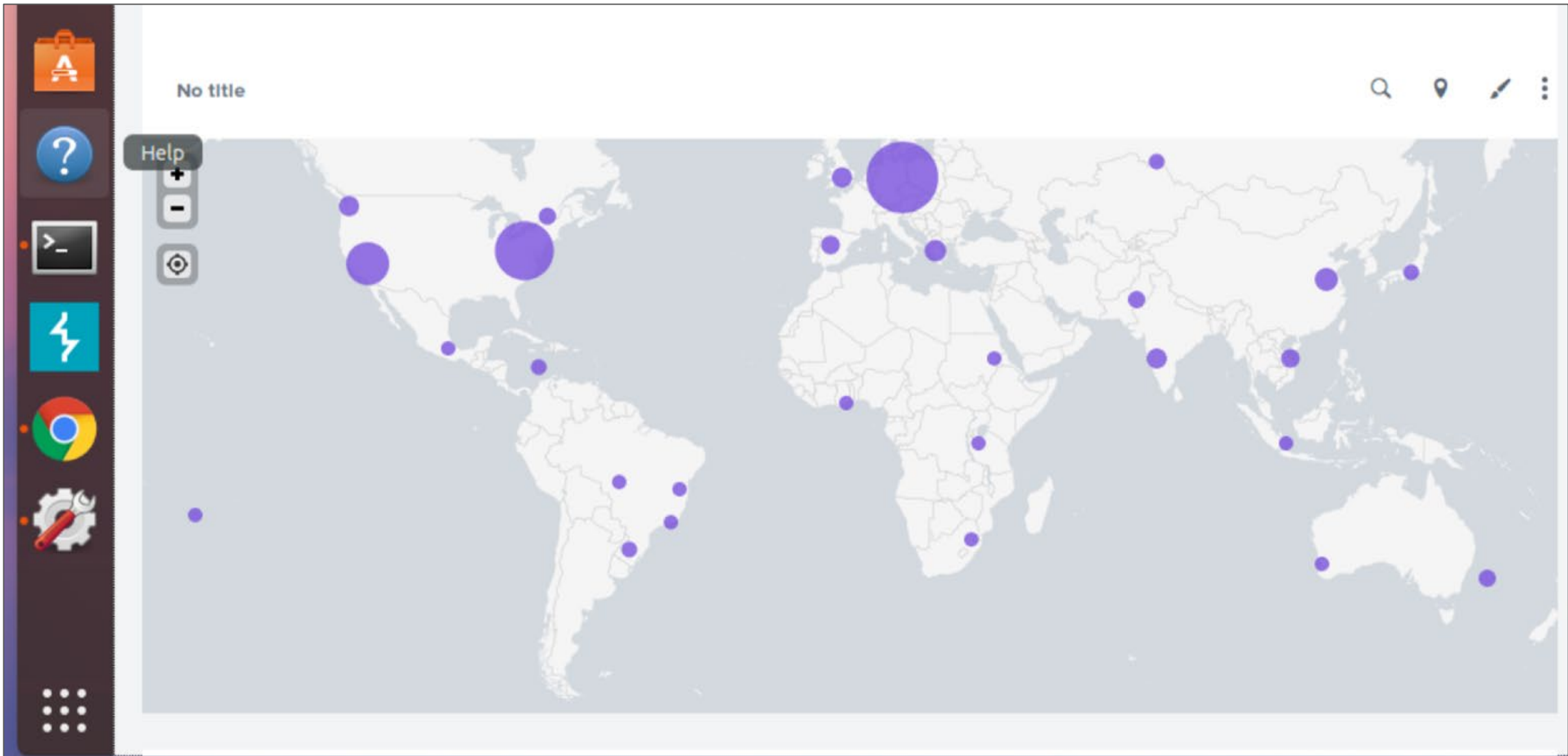


Fig.20 – Internet Connection by Continent



Fig.21 – Line Chart of HTTP Methods based on Type

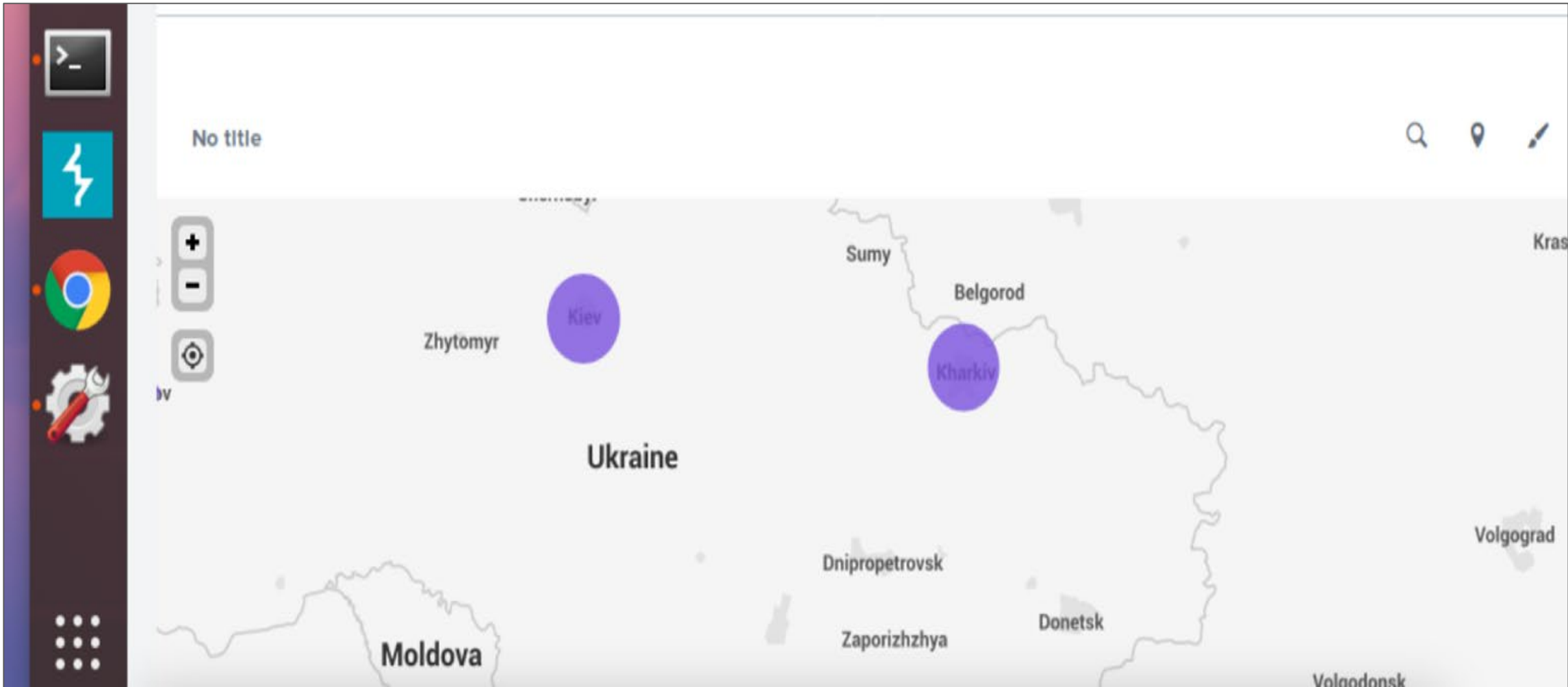


Fig.22 – Origins of Attack

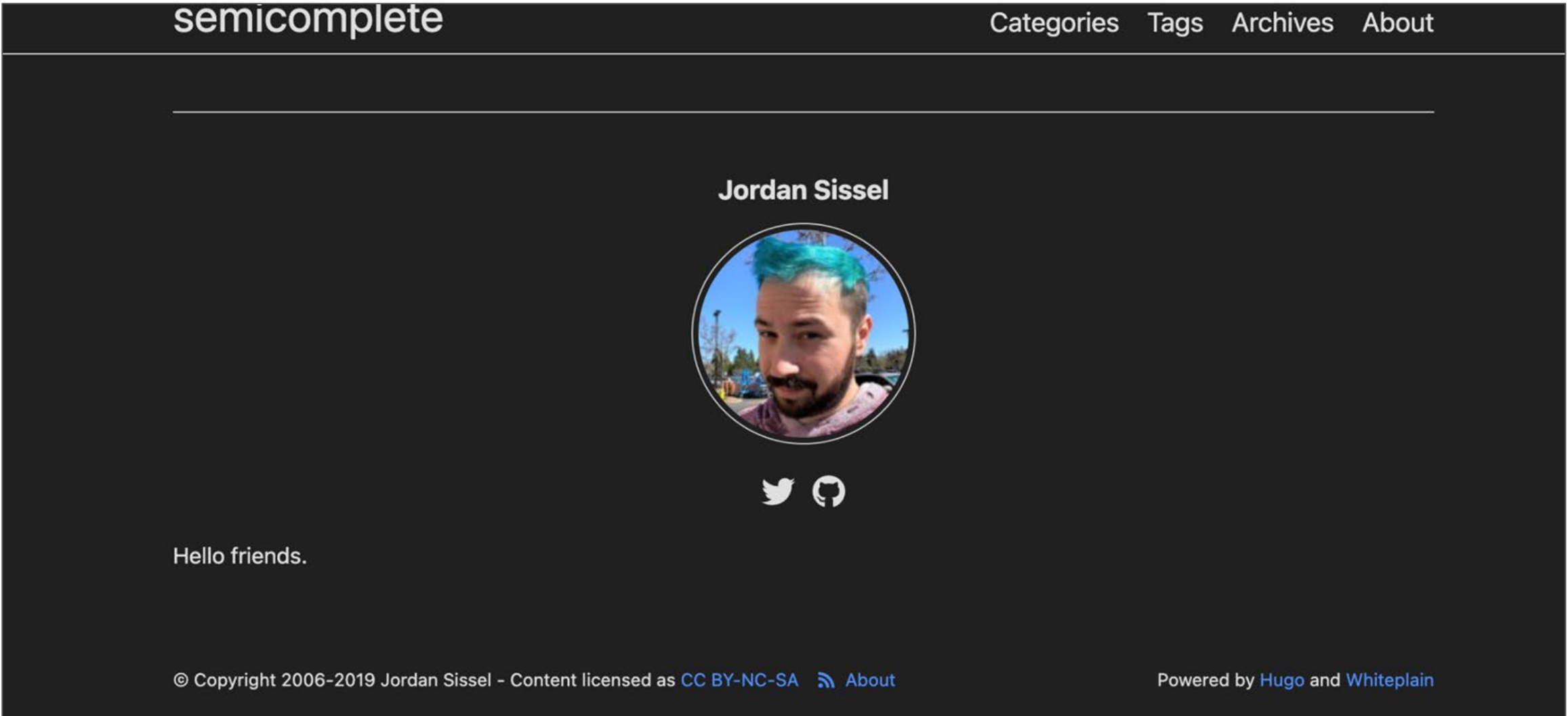


Fig.23 – Suspicious Site Associated with Attack

Dashboards—Apache

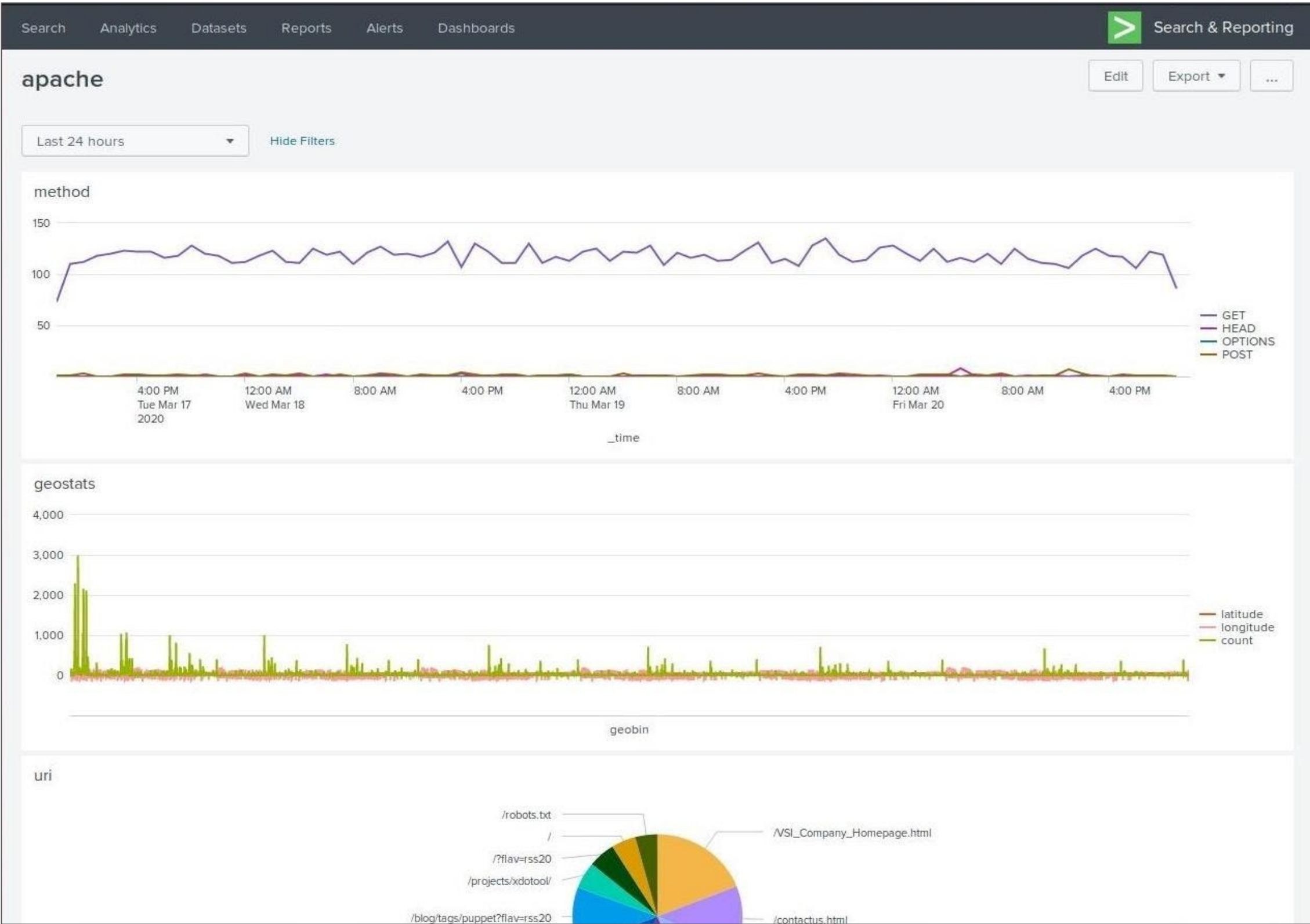


Fig.24 – Dashboard (Method Line Chart & geostats Bar Chart)

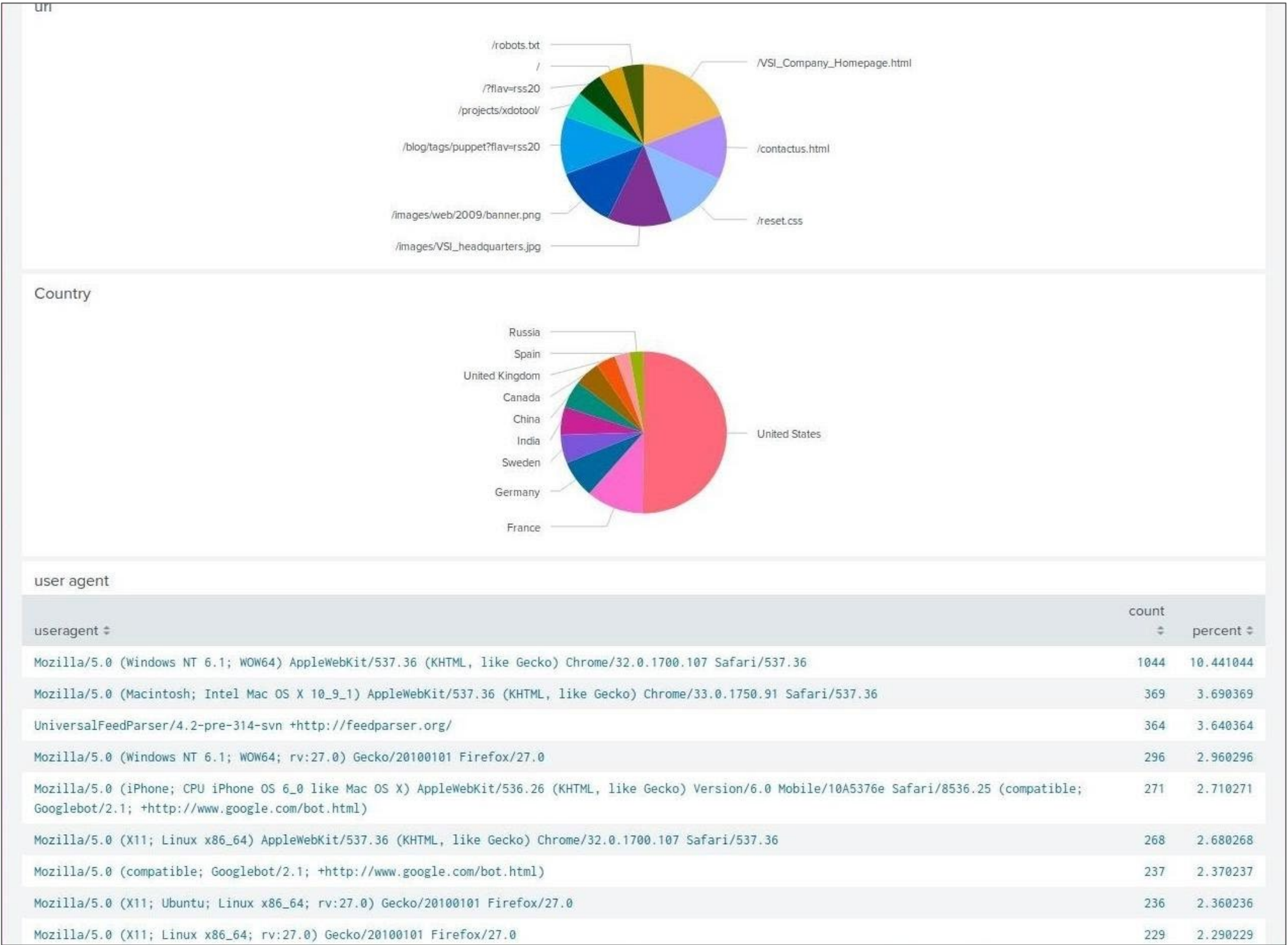


Fig.25 – URI & Country Pie Chart

Attack Analysis

Attack Summary—Windows

Accounts deletions were observed during the analysis of the log files. As well as several other additional activities, such as account creation, accounts modified where access was granted. Some accounts were also given special privileges, with data confirming successfully logons.

Account management password policy changes during the attack were concerning and would require further investigation. We also observed excessive user account lockout and attempted password resets. A user account was deleted during the attack with the audit logs cleared, this is an indication of the attacker attempting to hide their tracks. It was then observed that special privileges were assigned to new login after the account was created.

Attack Summary—Windows

During the attack, which peaked at specific times on 24th & 25th March 2020, the SOC team was alerted to suspicious activities on the network. This activity was in the form of failed login attempts which exceeded an estimated 35 attempts per hour. The alerts configured within the SIEM tool alerted the SOC team to the suspicious activity, due the threshold violations set within the alert. Based on our observations we are confident in the thresholds used and would not modify.

Attack Summary—Windows

The dashboards provided a wealth of evidence. Based on the reports and alerts we were able to identify the exact time and date of the attack. At approximately Tuesday March 24th, 2020, at 8pm we observed the attacker using the following account “user_a”, to gain unauthorized access to network resources. One thousand (1000) represents the attempts to gain access via this specific user. The large volume of logon attempts coupled with the limited frame suggest that this was a brute force attack, specifically the credential stuffing technique. The alert triggered was “A user account was locked out”.

Activity on the network returned to within normal operating parameters until Wednesday March 25th, 2020, at 4am. The activity on the network spiked under the following account “user_k”, with approximately one thousand two hundred (1200) attempts to change account password. This is extremely suspicious, as members of staff are not required to be logged in at this time of the day. This activity supports our suspicions that access to the network was gained, and the attacker was attempting to secure a legitimate account providing the ability to traverse and login back into the network later, without alerting the SOC team.

“Fig.26 - Windows Attack Logs Users & Signatures” below will support our findings and conclusion.

Screenshots of Attack Logs

A graphical representation showing each user's peaked activity and the associated activity signature.

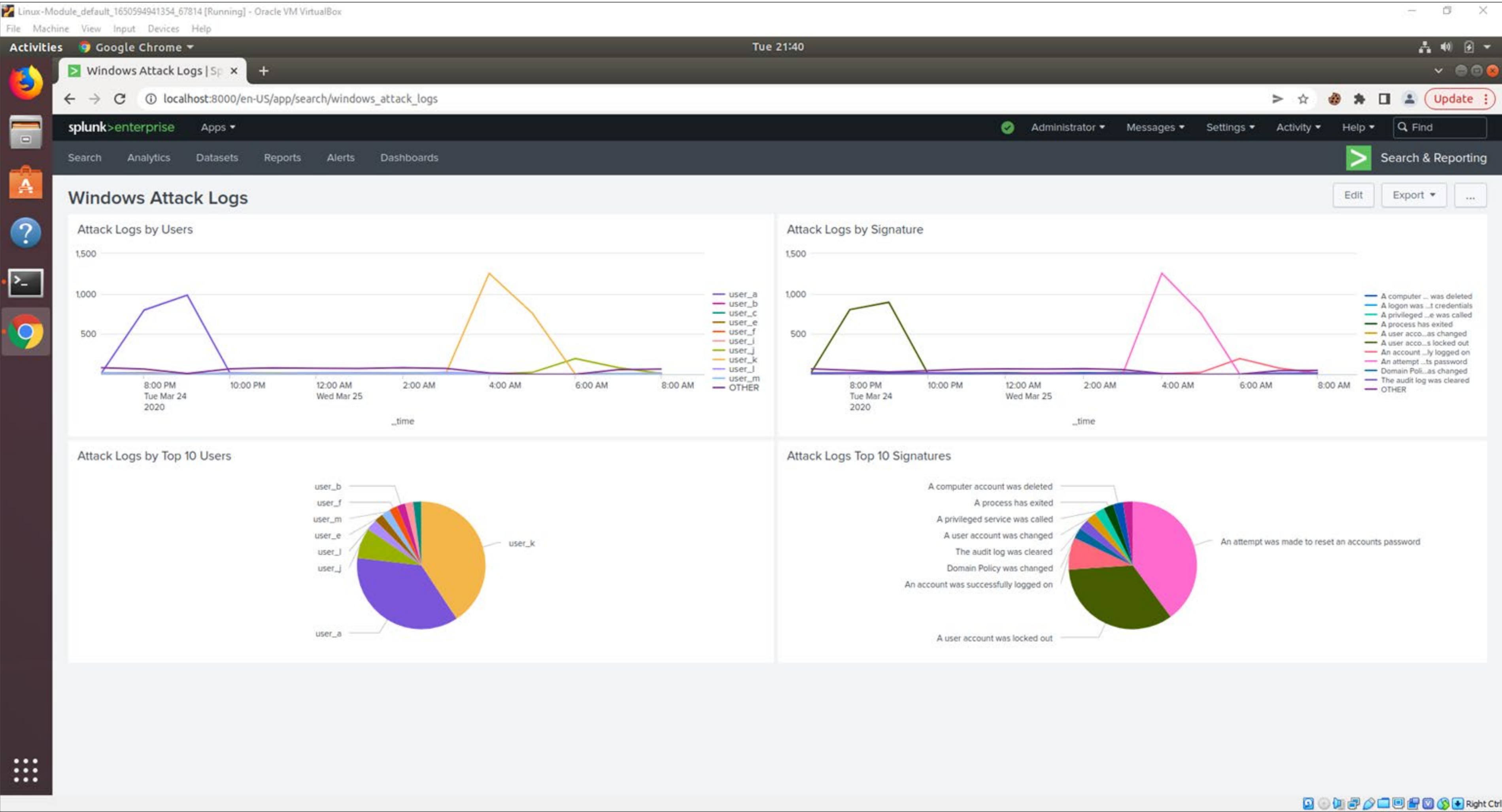


Fig.26 – Windows Attack Logs Users & Signatures

Attack Summary—Apache

In the first attack we noticed a change in the HTTP methods GET and POST. Both request had significant spike counts. This spike count as detailed in the report had a correlation to another defined alert set for the “referrer_domain”.

A single domain seemed to be the origin of the high alerts observed within the report.

Attack Summary—Apache

HTTP method GET originating from international addresses count spiked to 939 events on Wednesday 25th 2020 between 4:30pm – 6:30pm. This lasted for approximately two (2) hours, with activity peaking at 6pm and an event count of thirty-eight (38). This was followed by a steep decline to normalcy at 6:30pm

We also noticed similar activities with the HTTP method POST, count spiked of 1,296 events on Wednesday 25th 2020 between 6:30pm – 8:30pm. These results are in correlation with our information from the HTTP method analysis.

Attack Summary—Apache

We found from our Time Chart of the HTTP methods that there was an increase of the POST and GET methods. The suspicious POST events occurred between 7:00pm – 9:00pm with a total event count of 1,296. The suspicious GET events happened between 5:00pm – 7:00pm with an event count of 729.

The Cluster Map created showed that most of the activity originated from Ukraine. The specific cities identified in the attack was Kharkiv with an event count of 433 and Kyiv with an event count of 439.

Based on the information gathered we were able to determine it was a brute force attack against the VSI logon page.

Screenshots of Attack Logs

A graphical representation showing the GET & POST Apache attack logs along with the coordinates of where the attacks originated.



Fig.27 – Apache Attack Logs GET & POST

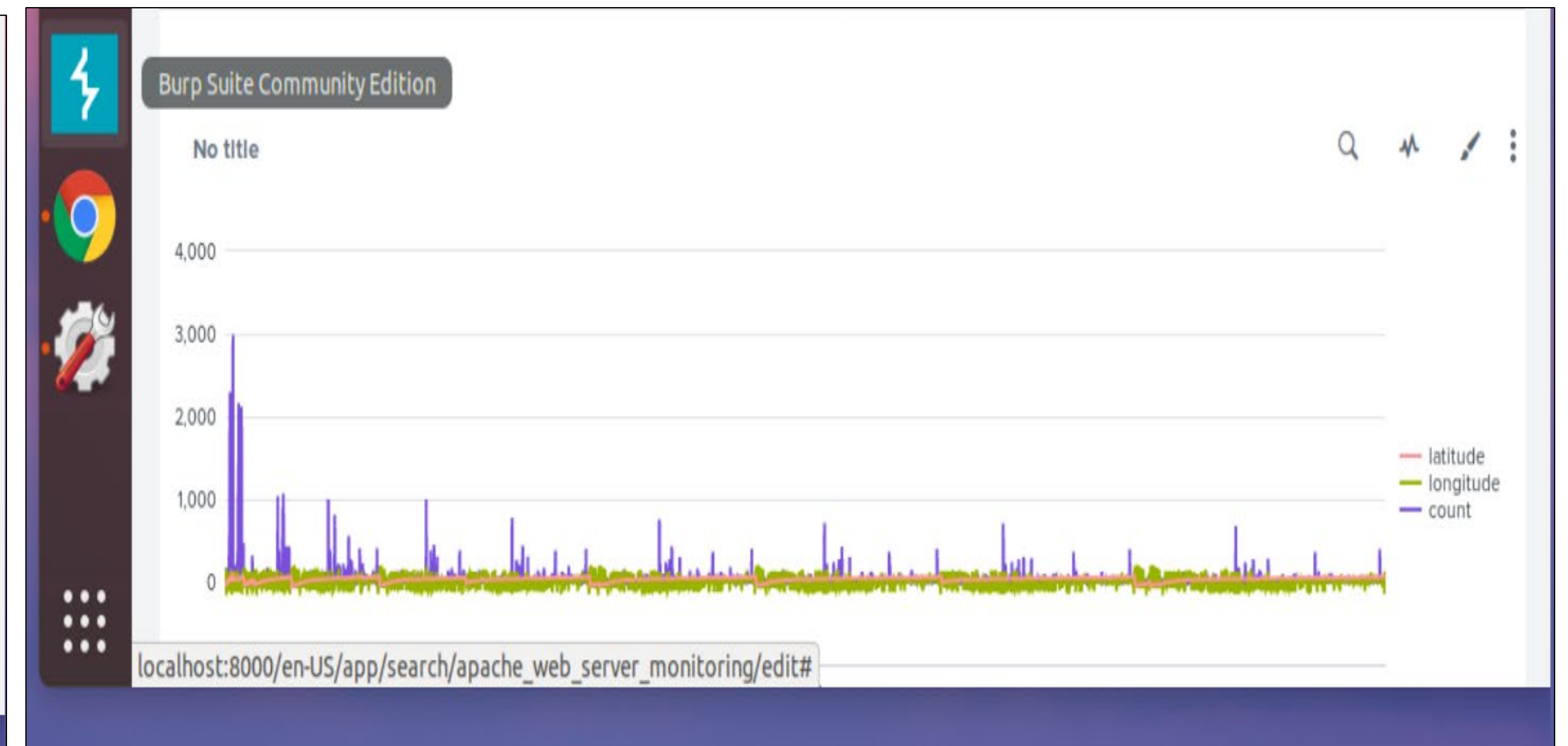


Fig.28 – Apache Attack Logs Latitude, Longitude & Count

Summary and Future Mitigations

Project 3 Summary

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

From our findings we found there were Brute Force and a Pre-hijacking attacks performed on the Apache and Windows servers.

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

Set web application firewall configurations. This can be set for blocking traffic from Ukraine.

Create complicated passwords for users. Set login rules for failed attempts.