Defensive Security Project by: Stokely De Freitas

Table of Contents

This document contains the following resources:

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”

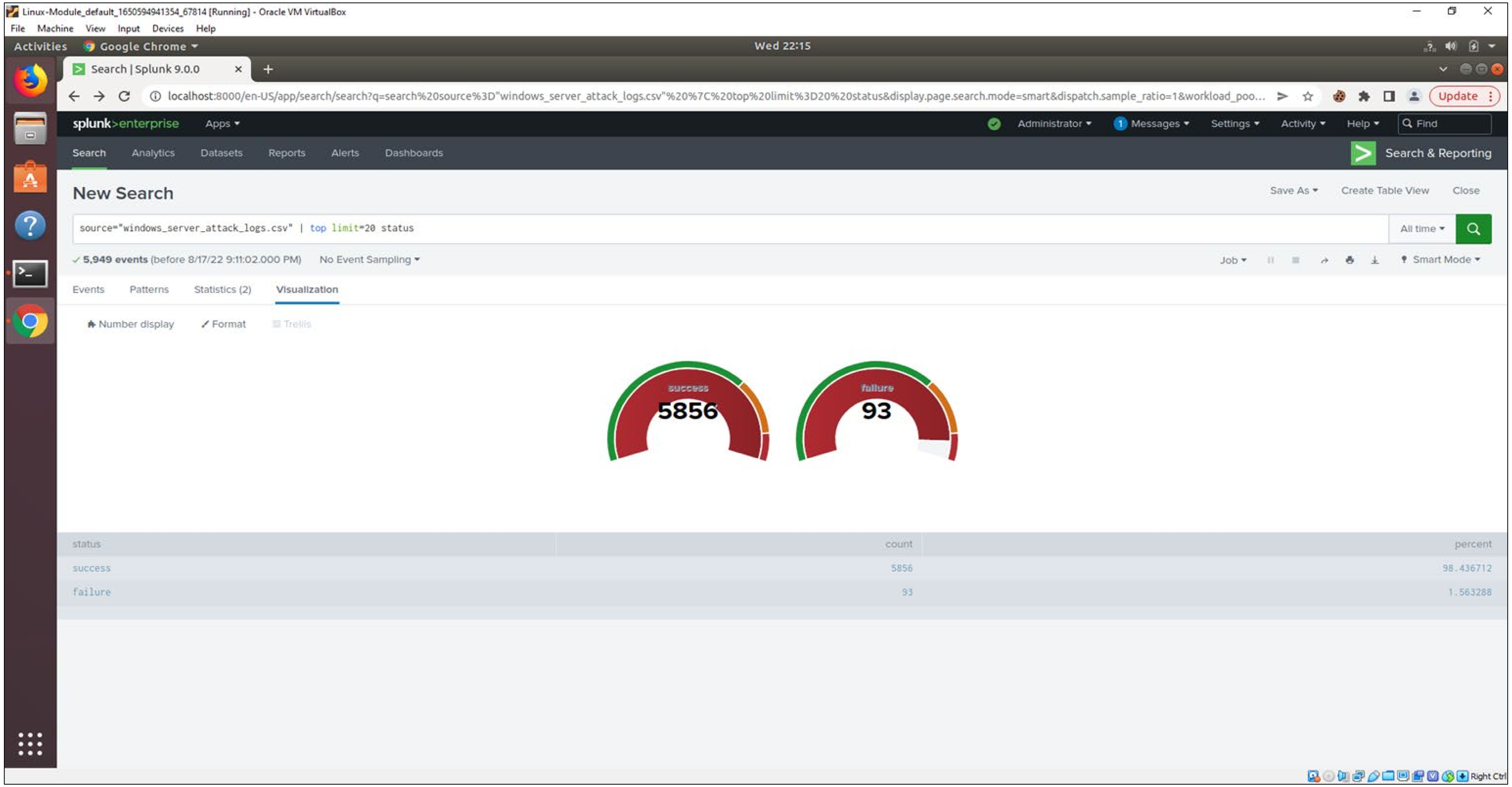
Number Display is a collection of ultra-configurable, single-statistic visualizations for Splunk. It includes the following styles: gauge, horseshoe, spinner, shapes (rectangle, hexagon, circle, ring, donut). Bringing life to the dashboards through animated number changes and subtle pulse animations.

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



```
source="windows_server_attack_logs.csv" | top limit=20 status
```

✓ 5,949 events (before 8/17/22 9:11:02.000 PM) No Event Sampling

status	count	percent
success	5856	98.436712
failure	93	1.563288

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

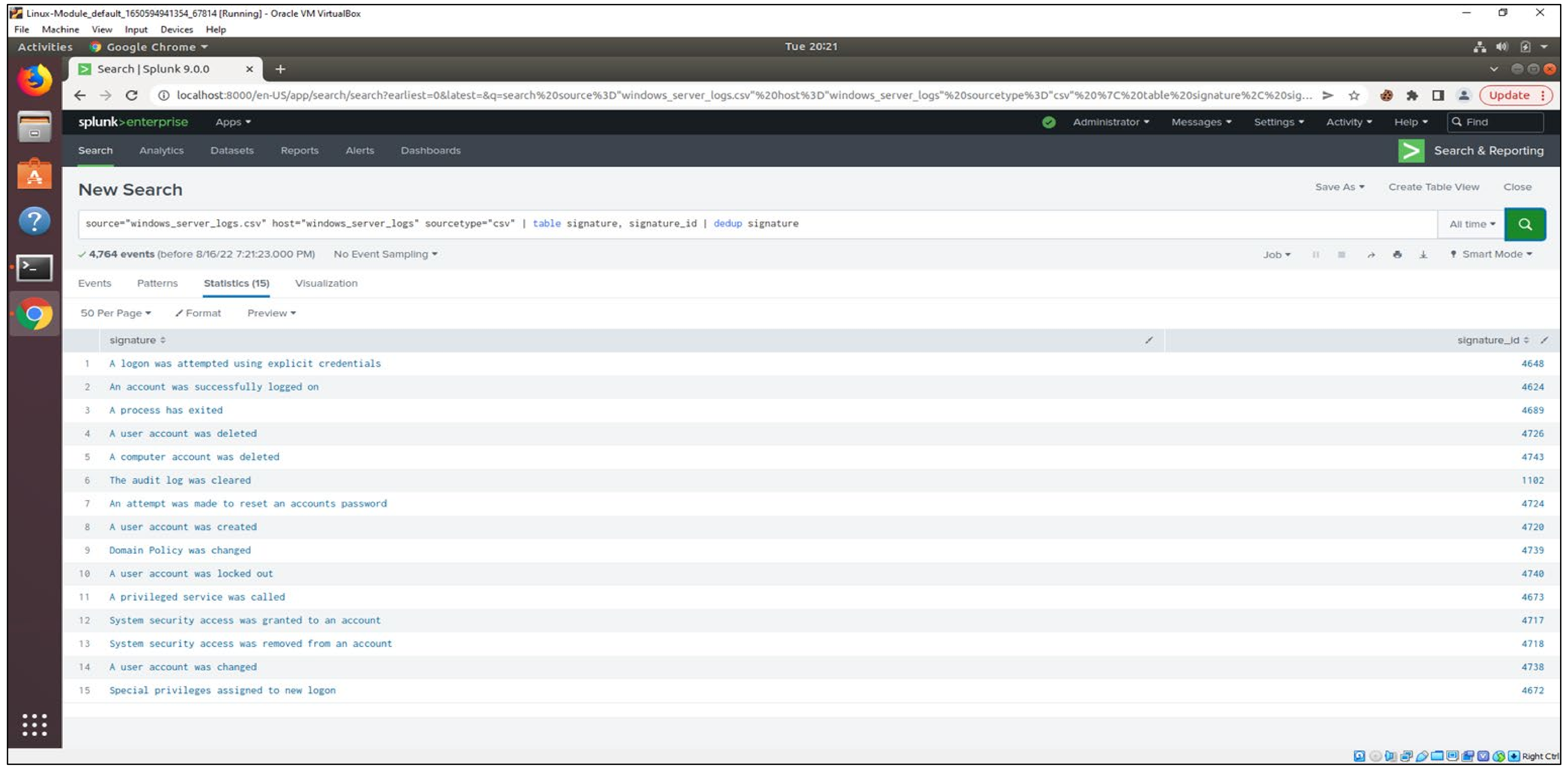
Two sets of Windows logs were analyzed during this exercise, the pre-attack logs and the post attack logs. Special attention would be placed on reviewing the HTTP methods (GET, POST, HEAD, etc..). Focus will be placed on determining the origins of the attack and the overall impact to the environment.

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



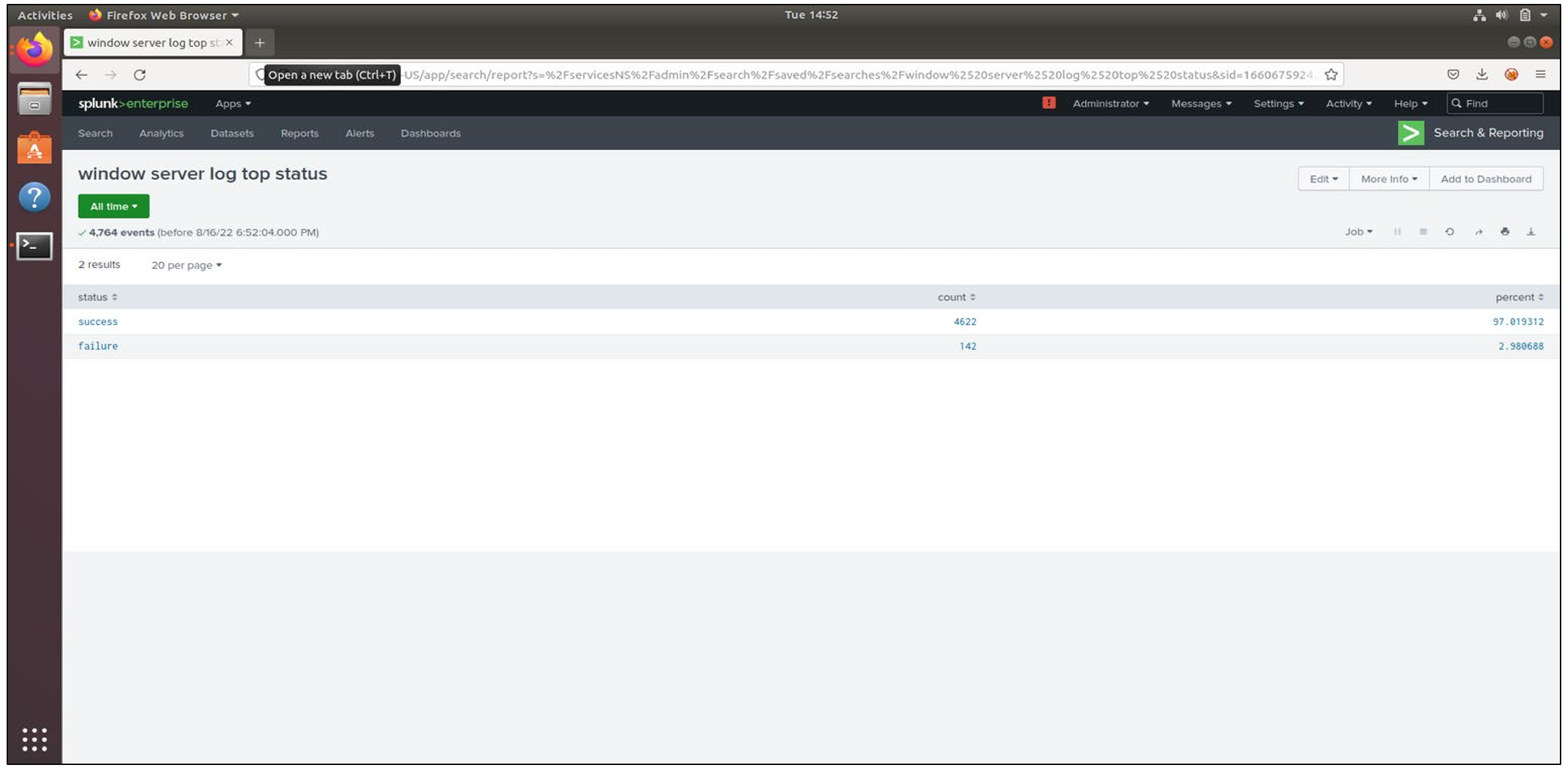
New Search

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" | table signature, signature_id | dedup signature
```

✓ 4,764 events (before 8/16/22 7:21:23.000 PM) No Event Sampling ▾

	signature	signature_id
1	A logon was attempted using explicit credentials	4648
2	An account was successfully logged on	4624
3	A process has exited	4689
4	A user account was deleted	4726
5	A computer account was deleted	4743
6	The audit log was cleared	1102
7	An attempt was made to reset an accounts password	4724
8	A user account was created	4720
9	Domain Policy was changed	4739
10	A user account was locked out	4740
11	A privileged service was called	4673
12	System security access was granted to an account	4717
13	System security access was removed from an account	4718
14	A user account was changed	4738
15	Special privileges assigned to new logon	4672

Fig.2 – Dataset: Signature



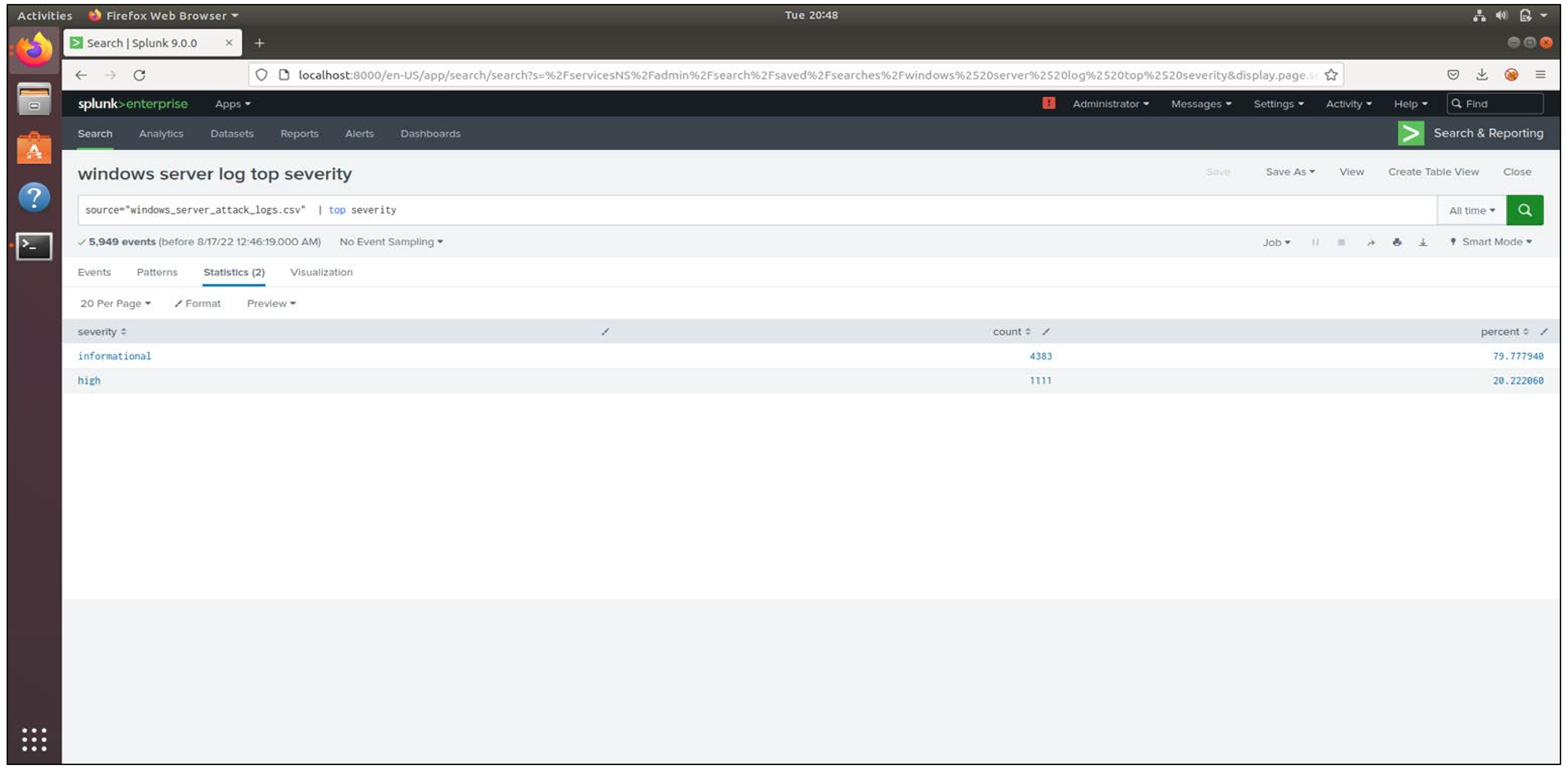
window server log top status

✓ 4,764 events (before 8/16/22 6:52:04.000 PM)

2 results

status	count	percent
success	4622	97.019312
failure	142	2.980688

Fig.3 – Dataset: Status



windows server log top severity

```
source="windows_server_attack_logs.csv" | top severity
```

✓ 5,949 events (before 8/17/22 12:46:19.000 AM) No Event Sampling ▾

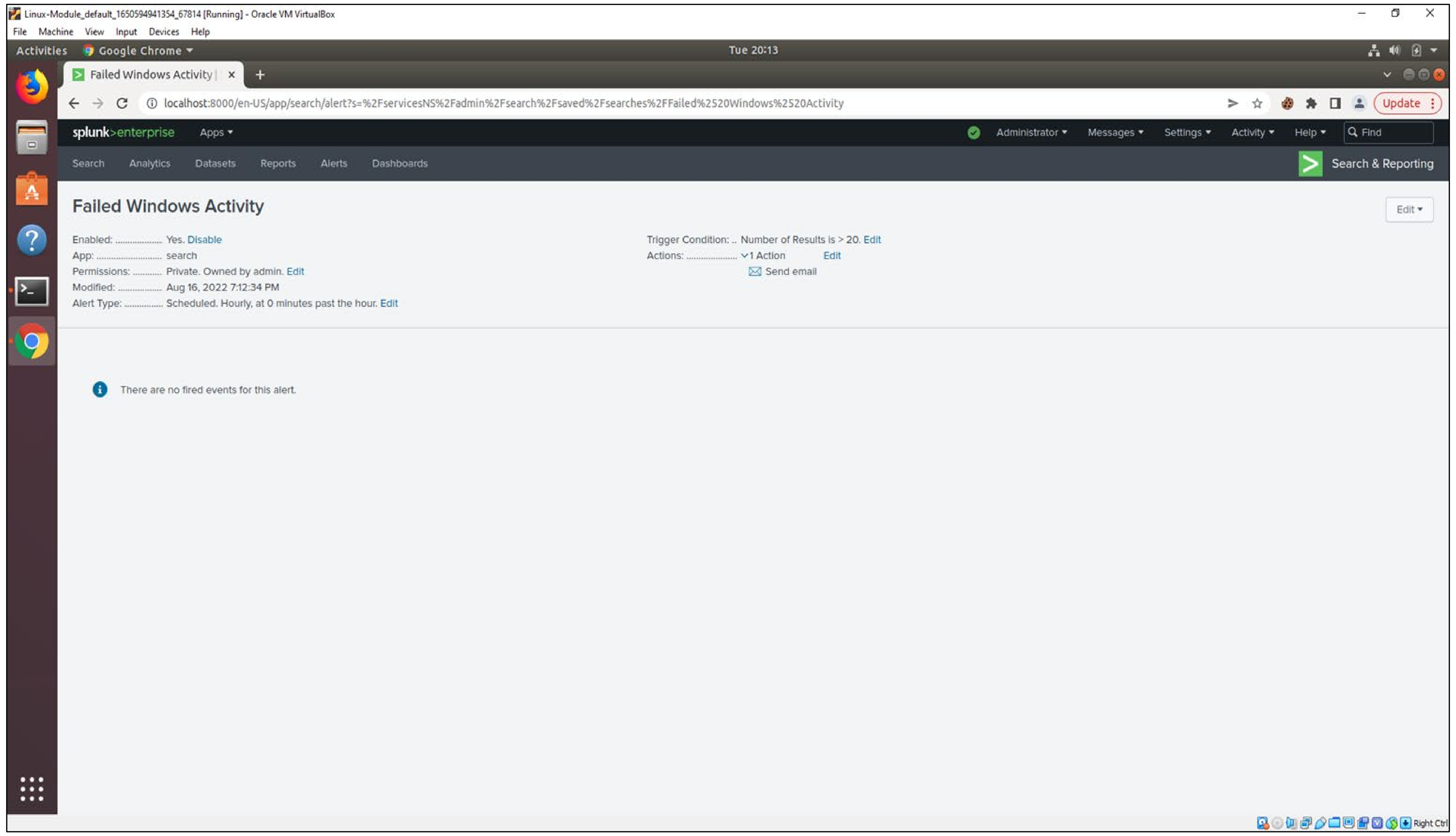
severity	count	percent
informational	4383	79.777940
high	1111	20.222060

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”.


Linux-Module_default_1650594941354_67814 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Google Chrome
Tue 20:13
Failed Windows Activity |
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FFailed%2520Windows%2520Activity
Update
splunk>enterprise Apps
Administrator Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
Edit

Failed Windows Activity

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Aug 16, 2022 7:12:34 PM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: Number of Results is > 20. Edit
Actions: 1 Action Edit
Send email

There are no fired events for this alert.

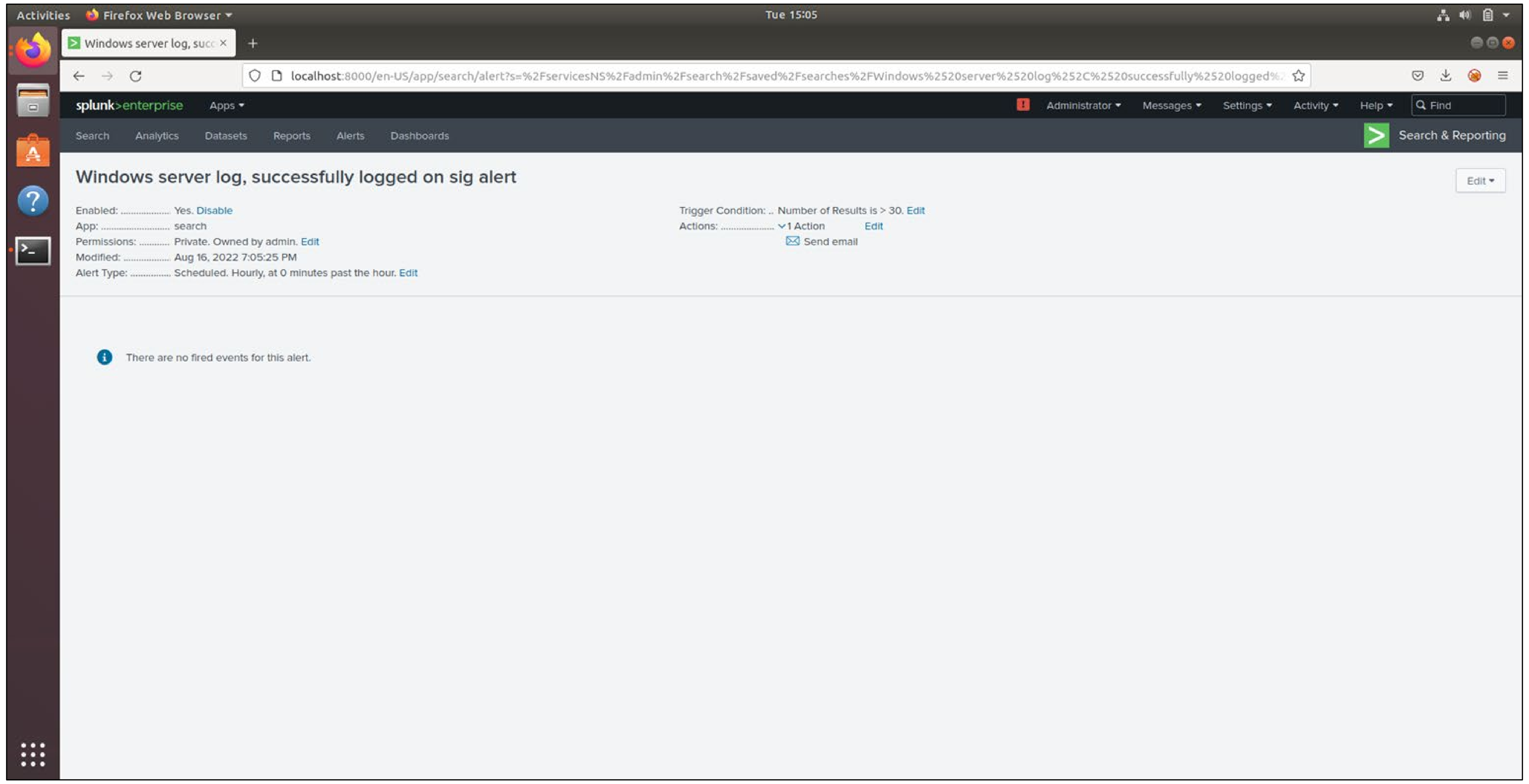
Fig.5 – Failed Windows Activity

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”.



Windows server log, successfully logged on sig alert

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 16, 2022 7:05:25 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 30. Edit
Actions: .... 1 Action Edit
Send email

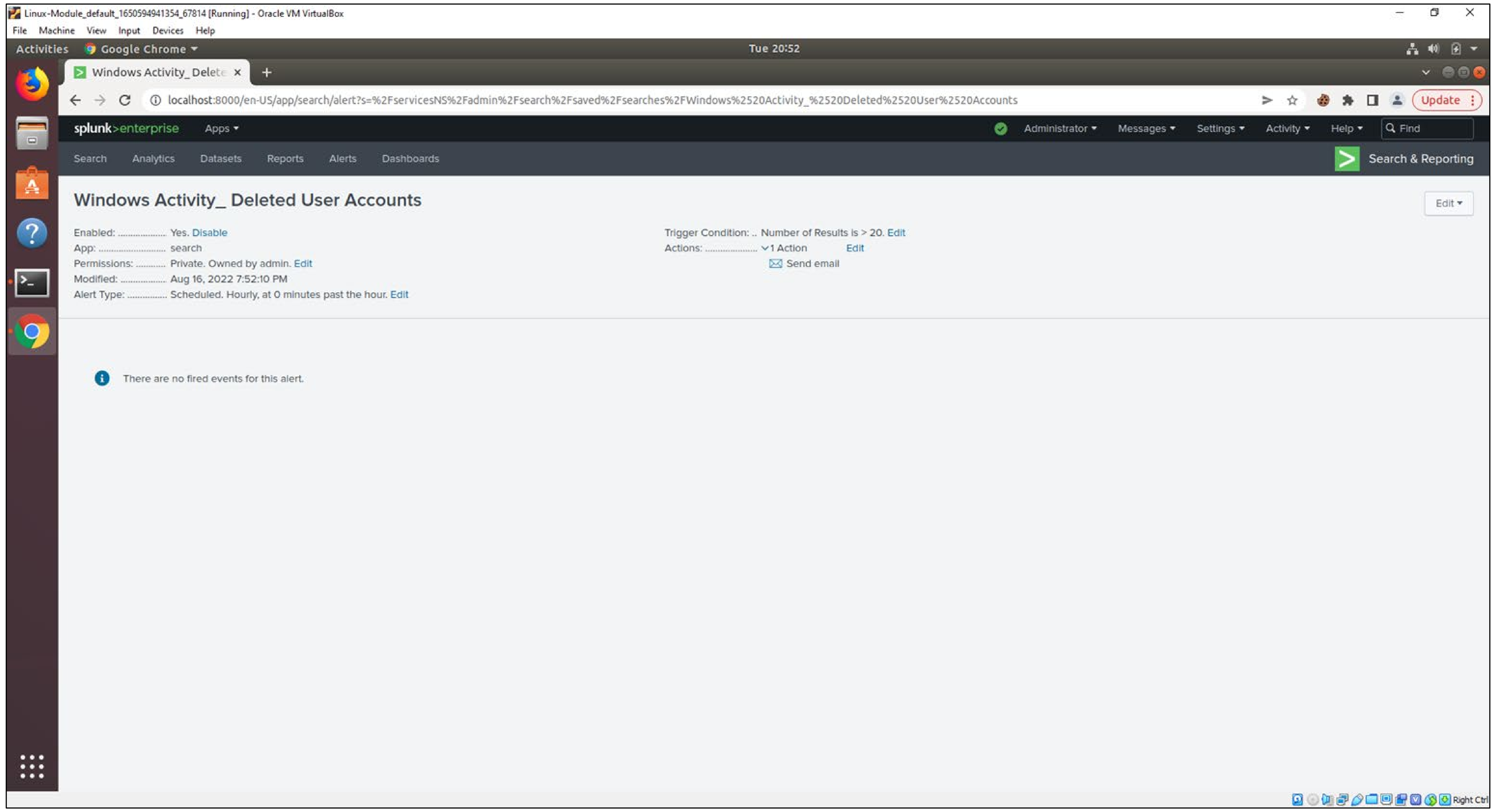
There are no fired events for this alert.

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”.


Linux-Module_default_1650594941354_67814 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Google Chrome
Tue 20:52
Windows Activity_ Delete
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FWindows%2520Activity_%2520Deleted%2520User%2520Accounts
Update
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit
Right Ctrl

Windows Activity_ Deleted User Accounts

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 16, 2022 7:52:10 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 20. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

Fig.7 – Dataset: Successfully Logged On

Dashboards—Windows

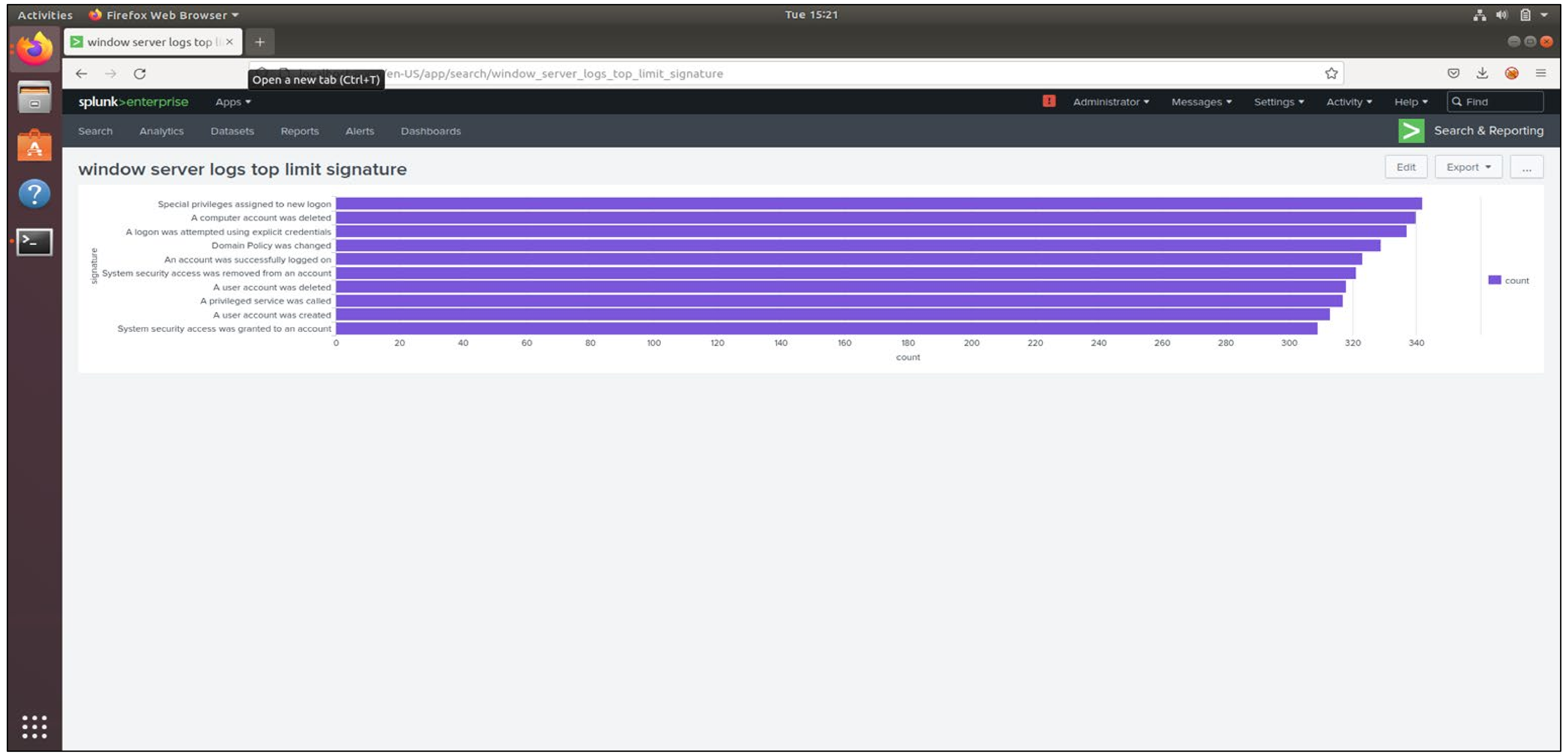
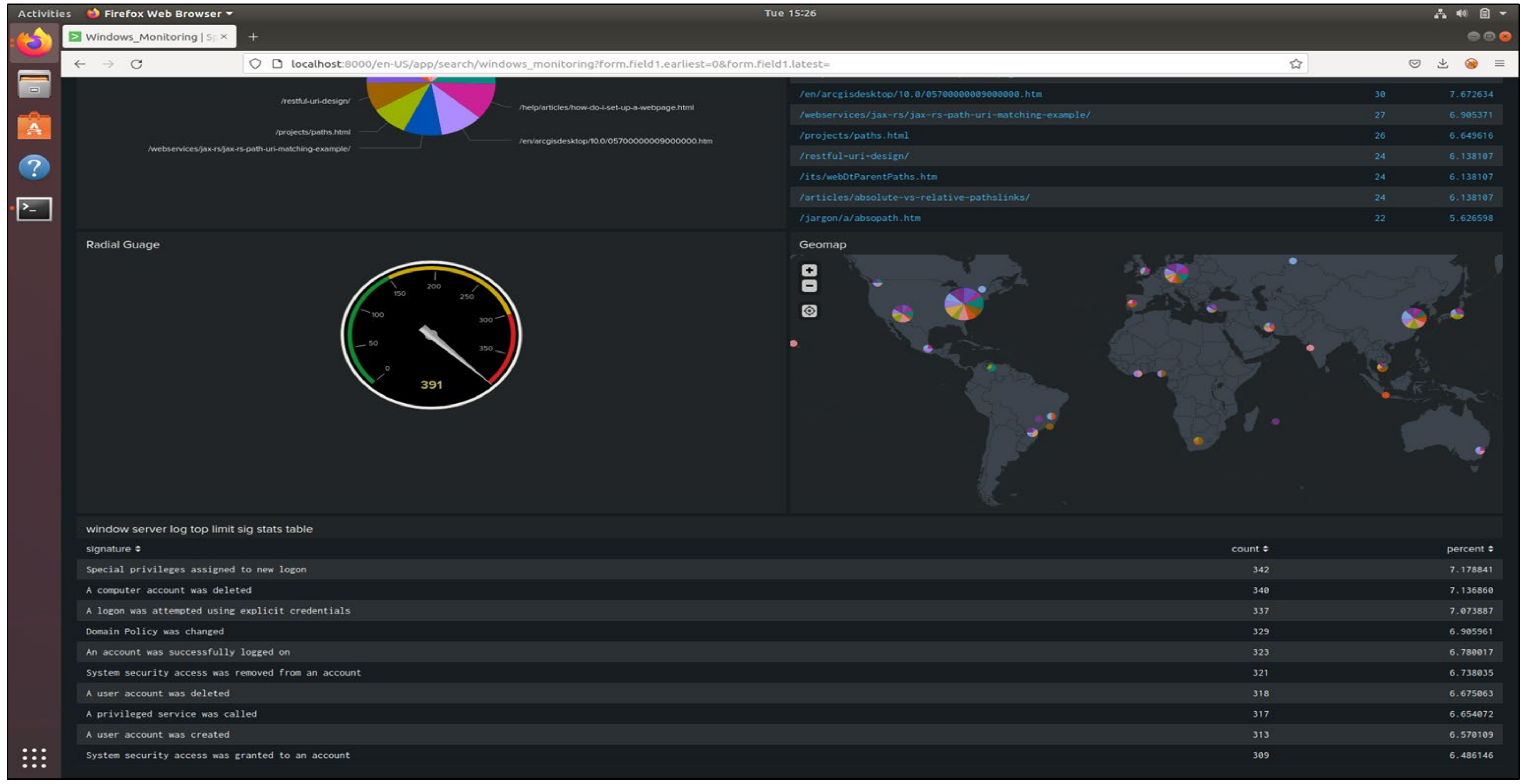

Activities
Firefox Web Browser
Tue 15:21
window server logs top li
Open a new tab (Ctrl+T)
en-US/app/search/window_server_logs_top_limit_signature
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
window server logs top limit signature
Edit
Export
...
Special privileges assigned to new logon
A computer account was deleted
A logon was attempted using explicit credentials
Domain Policy was changed
An account was successfully logged on
System security access was removed from an account
A user account was deleted
A privileged service was called
A user account was created
System security access was granted to an account
signature
0
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
320
340
count
count

Fig.8 – Bar Chart


Activities
Firefox Web Browser
Tue 15:26
Windows_Monitoring | Sp
localhost:8000/en-US/app/search/windows_monitoring?form.field1.earliest=0&form.field1.latest=
/restful-uri-design/
/projects/paths.html
/webservices/jax-rs/jax-rs-path-uri-matching-example/
/help/articles/how-do-i-set-up-a-webpage.html
/en/arcgisdesktop/10.0/05700000009000000.htm
Radial Guage
150
200
250
100
300
50
350
0
391
Geomap

/en/arcgisdesktop/10.0/05700000009000000.htm	30	7.672634
/webservices/jax-rs/jax-rs-path-uri-matching-example/	27	6.905371
/projects/paths.html	26	6.649616
/restful-uri-design/	24	6.138107
/its/webDtParentPaths.htm	24	6.138107
/articles/absolute-vs-relative-pathslinks/	24	6.138107
/jargon/a/absopath.htm	22	5.626598

window server log top limit sig stats table

signature ⇕	count ⇕	percent ⇕
Special privileges assigned to new logon	342	7.178841
A computer account was deleted	340	7.136860
A logon was attempted using explicit credentials	337	7.073887
Domain Policy was changed	329	6.905961
An account was successfully logged on	323	6.780017
System security access was removed from an account	321	6.738035
A user account was deleted	318	6.675063
A privileged service was called	317	6.654072
A user account was created	313	6.570109
System security access was granted to an account	309	6.486146

Fig.9 – Complied Dashboard

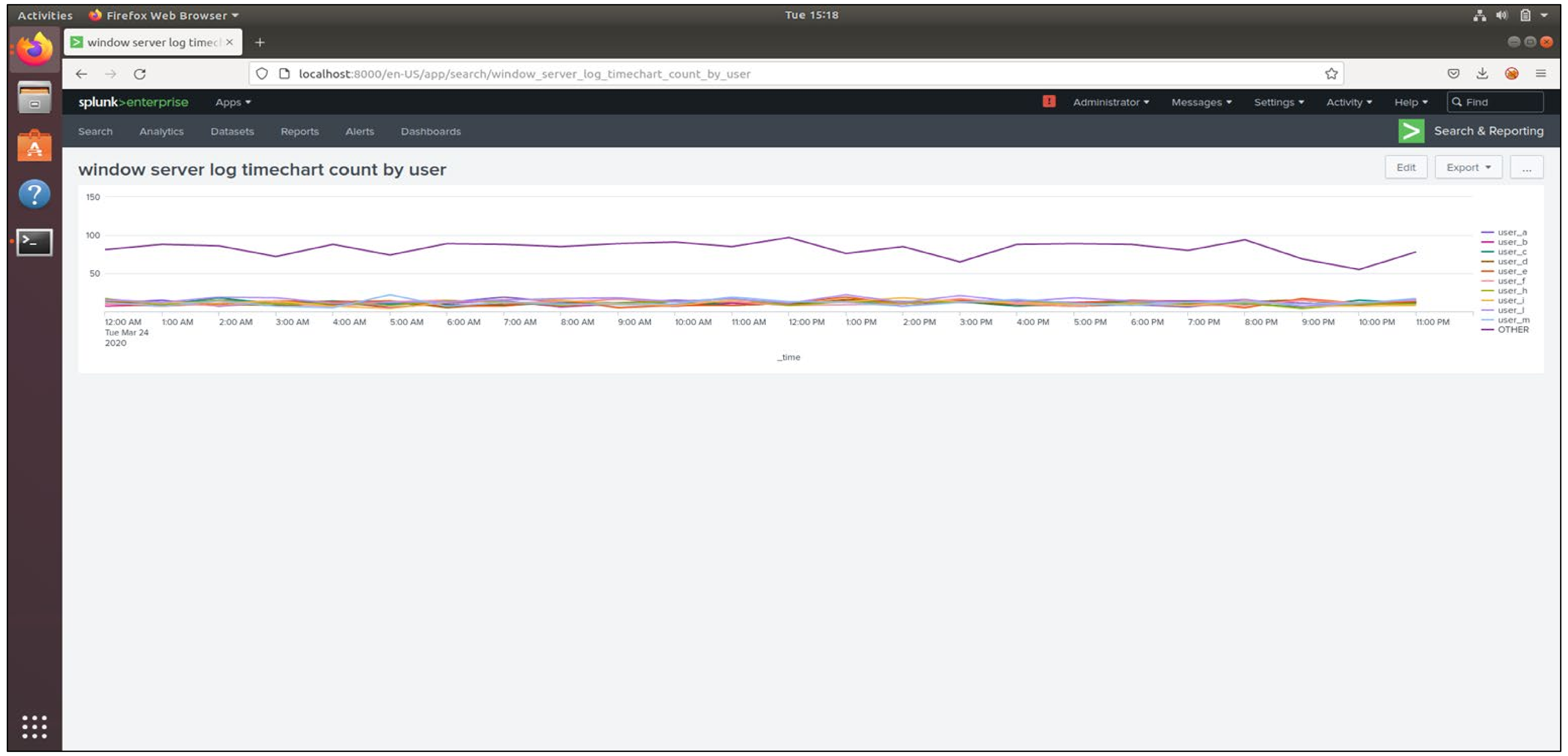


Fig.10 – Count by User Line Chart

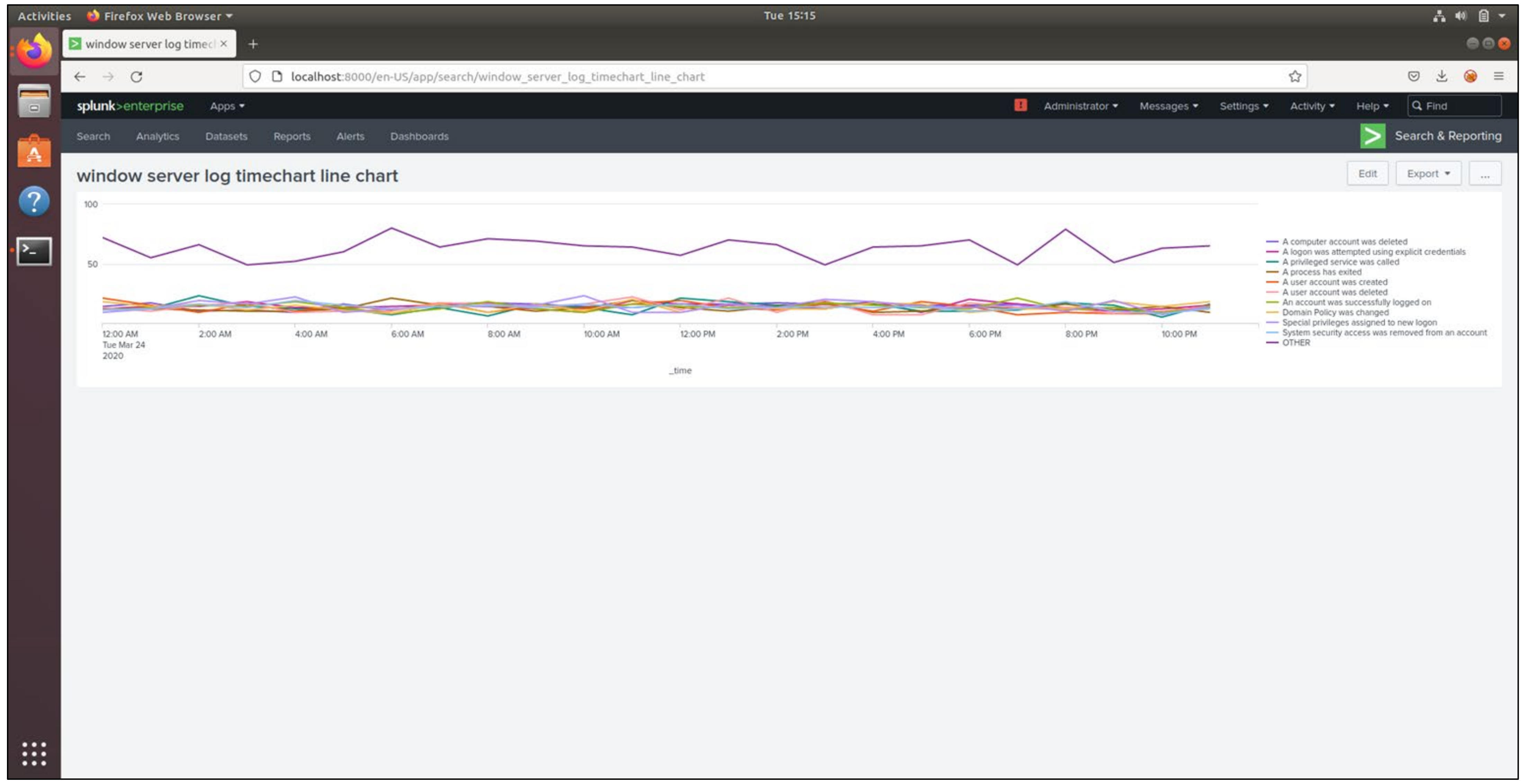
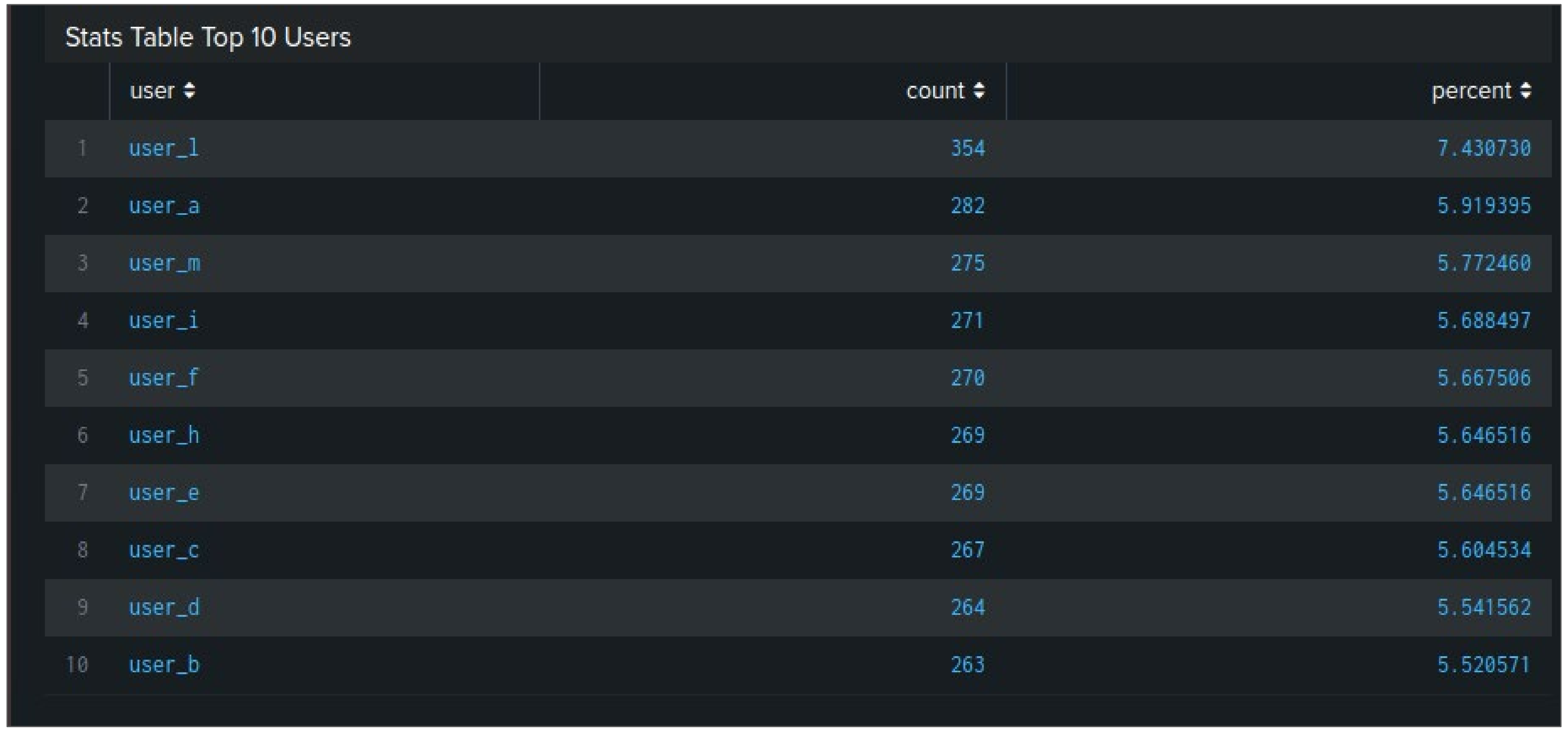

Activities
Firefox Web Browser
Tue 15:15
window server log timec
localhost:8000/en-US/app/search/window_server_log_timechart_line_chart
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
window server log timechart line chart
Edit
Export
...
100
50
12:00 AM
Tue Mar 24
2020
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
_time
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was created
A user account was deleted
An account was successfully logged on
Domain Policy was changed
Special privileges assigned to new logon
System security access was removed from an account
OTHER

Fig.11 – Time Interval Line Chart

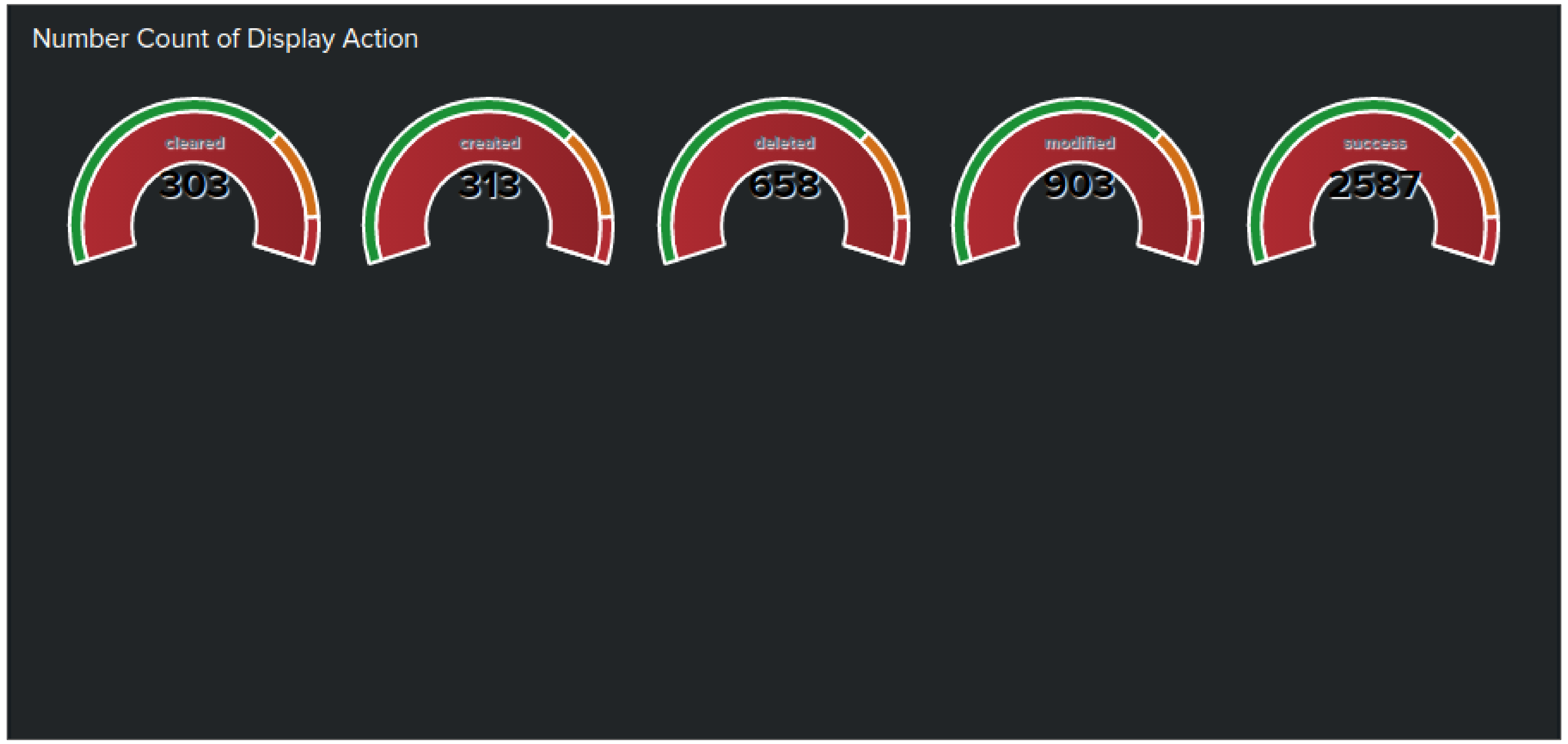
Dashboards—Windows



Stats Table Top 10 Users

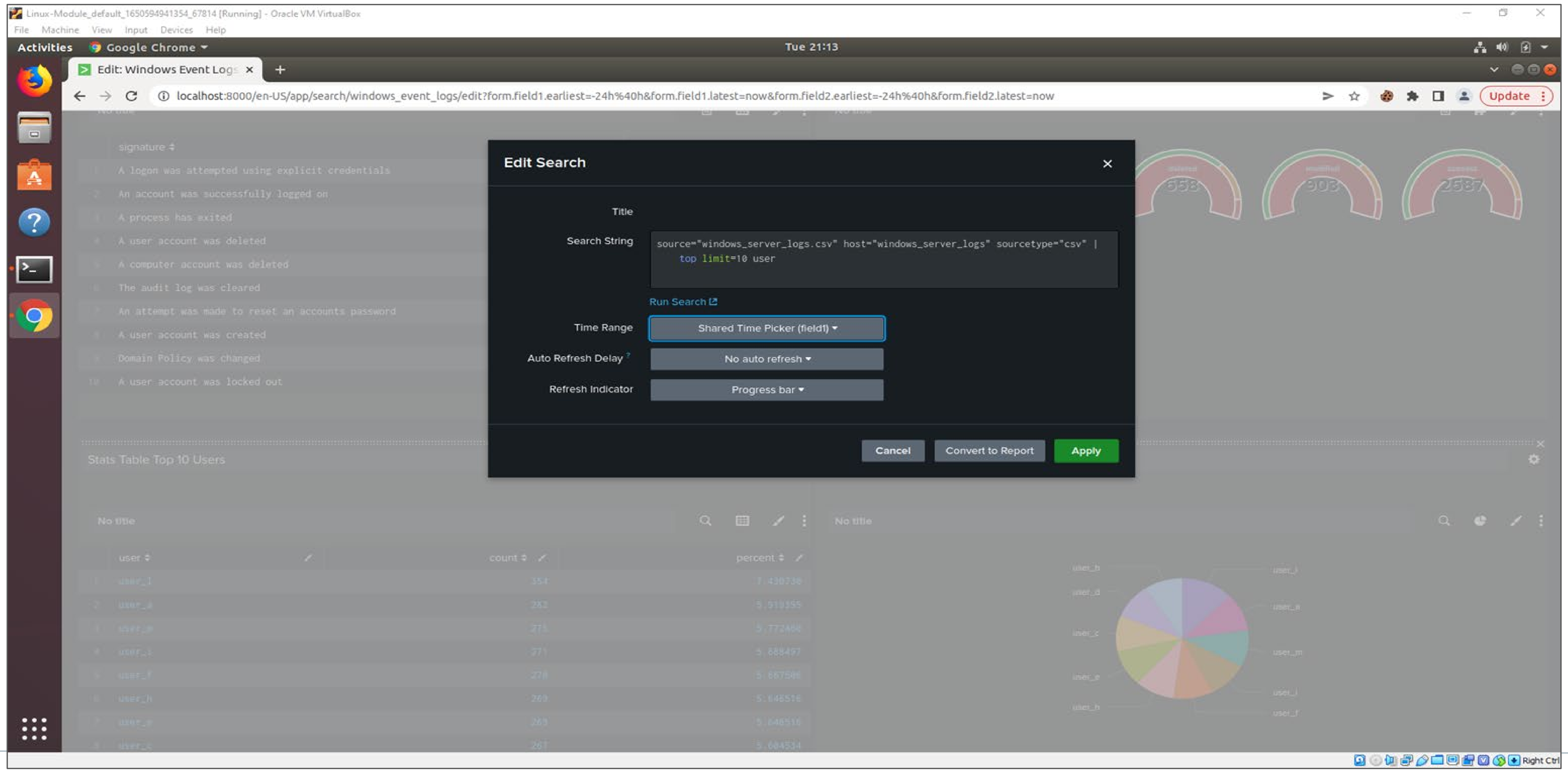
	user	count	percent
1	user_l	354	7.430730
2	user_a	282	5.919395
3	user_m	275	5.772460
4	user_i	271	5.688497
5	user_f	270	5.667506
6	user_h	269	5.646516
7	user_e	269	5.646516
8	user_c	267	5.604534
9	user_d	264	5.541562
10	user_b	263	5.520571

Fig.12 – Top 10 Users



Number Count of Display Action

Fig.13 – Number Count of Display Action



Linux-Module_default_1650594941354_67814 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Google Chrome
Tue 21:13
Edit: Windows Event Logs
Update

localhost:8000/en-US/app/search/windows_event_logs/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.field2.earliest=-24h%40h&form.field2.latest=now

	signature
1	A logon was attempted using explicit credentials
2	An account was successfully logged on
3	A process has exited
4	A user account was deleted
5	A computer account was deleted
6	The audit log was cleared
7	An attempt was made to reset an accounts password
8	A user account was created
9	Domain Policy was changed
10	A user account was locked out

Stats Table Top 10 Users

Edit Search

Title

Search String

```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" |
    top limit=10 user
```

Run Search

Time Range: Shared Time Picker (field1)

Auto Refresh Delay: No auto refresh

Refresh Indicator: Progress bar

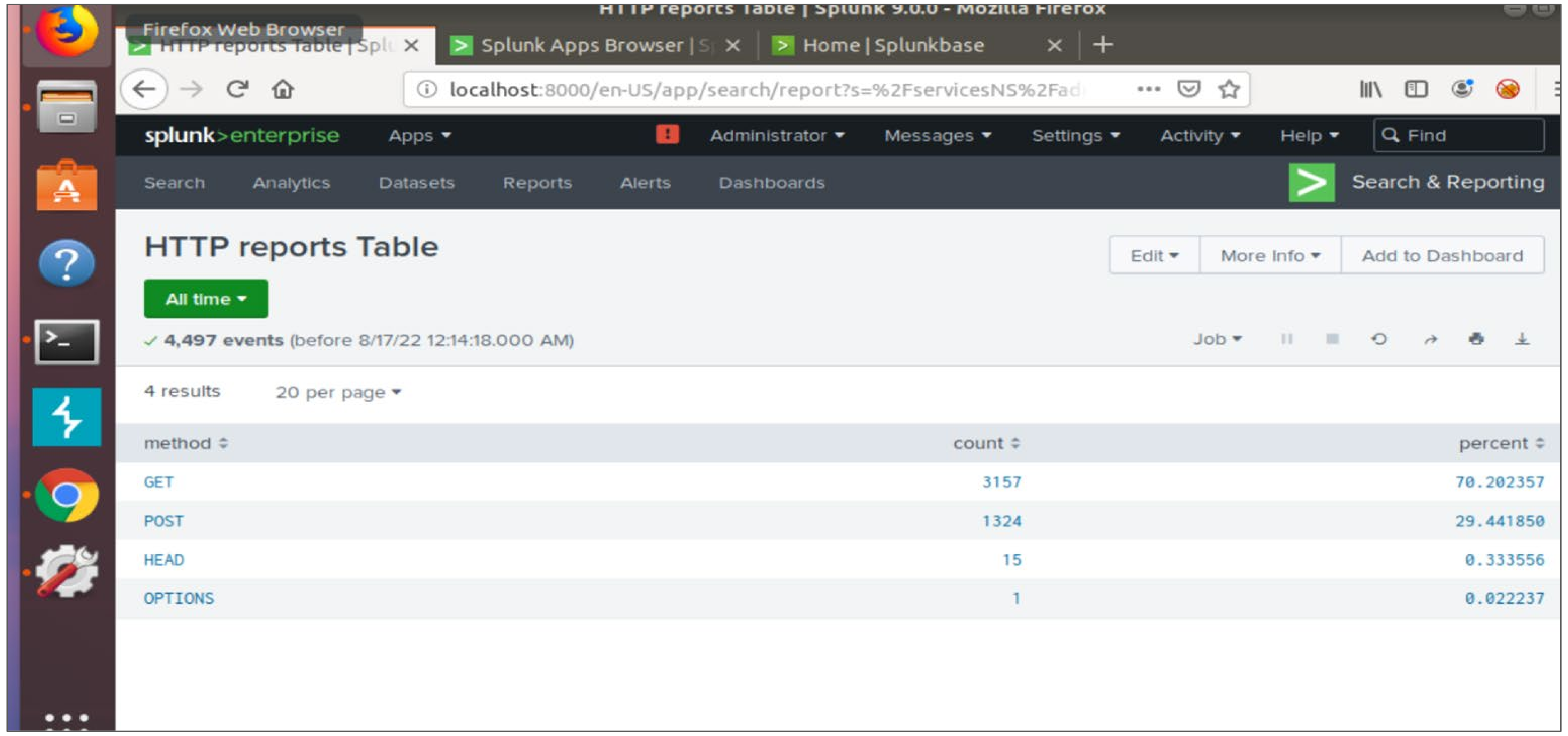
Fig.14 – Dashboard Configuration

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



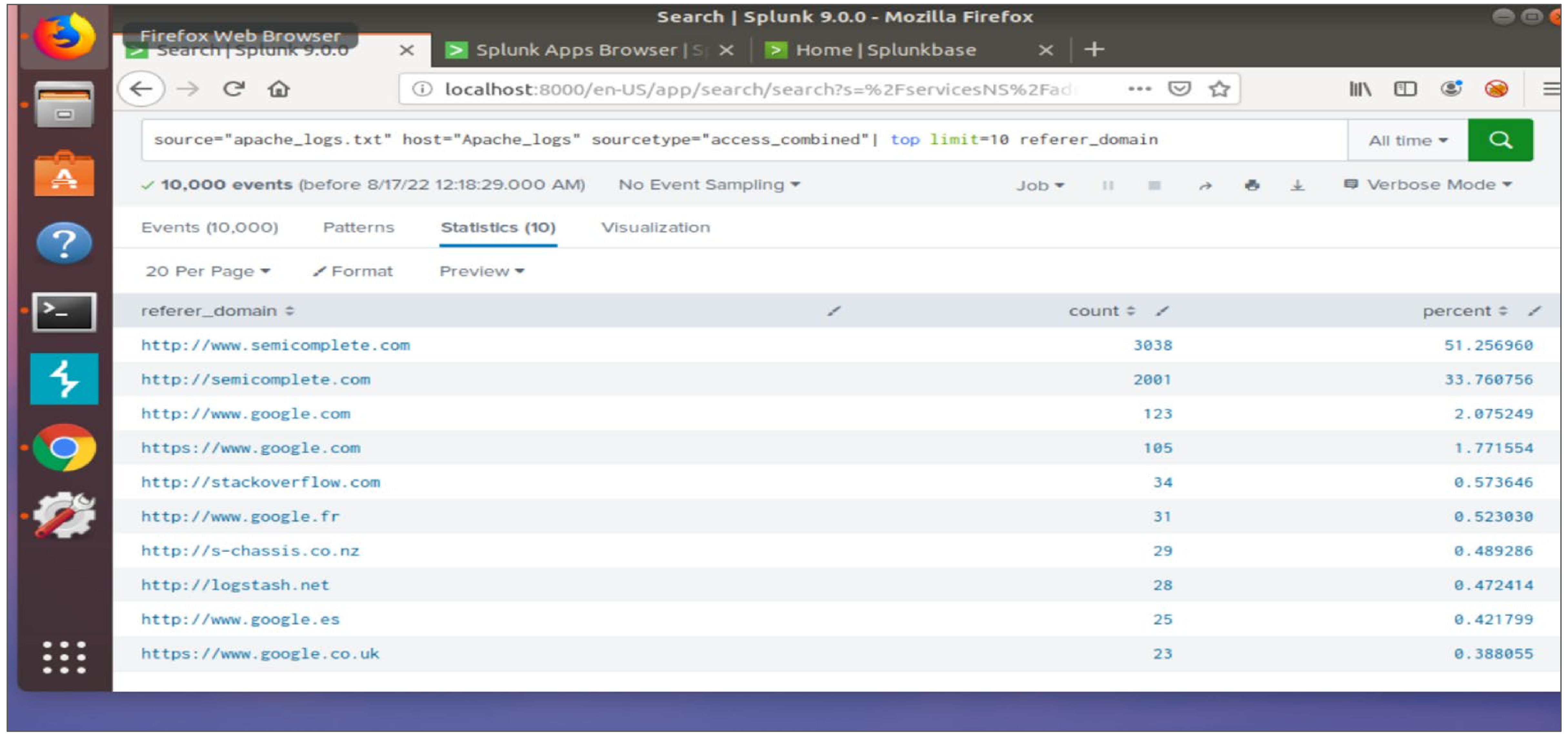
HTTP reports Table

✓ 4,497 events (before 8/17/22 12:14:18.000 AM)

4 results

method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

Fig.15 – HTTP Method Count & Percentages

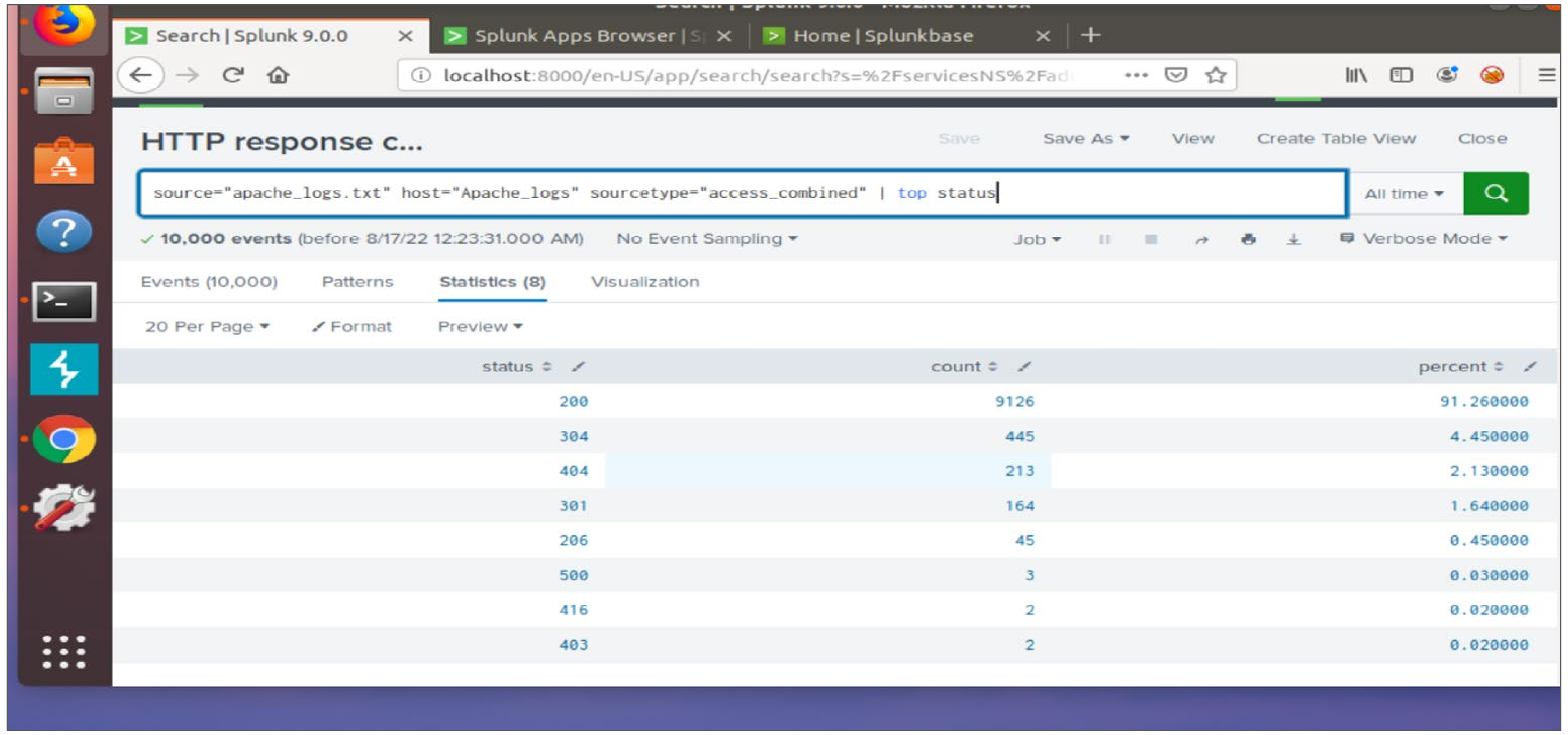


```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined"| top limit=10 referer_domain
```

✓ 10,000 events (before 8/17/22 12:18:29.000 AM)

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

Fig.16 – Top 10 “referer_domain”



HTTP response c...

```
source="apache_logs.txt" host="Apache_logs" sourcetype="access_combined" | top status
```

✓ 10,000 events (before 8/17/22 12:23:31.000 AM)

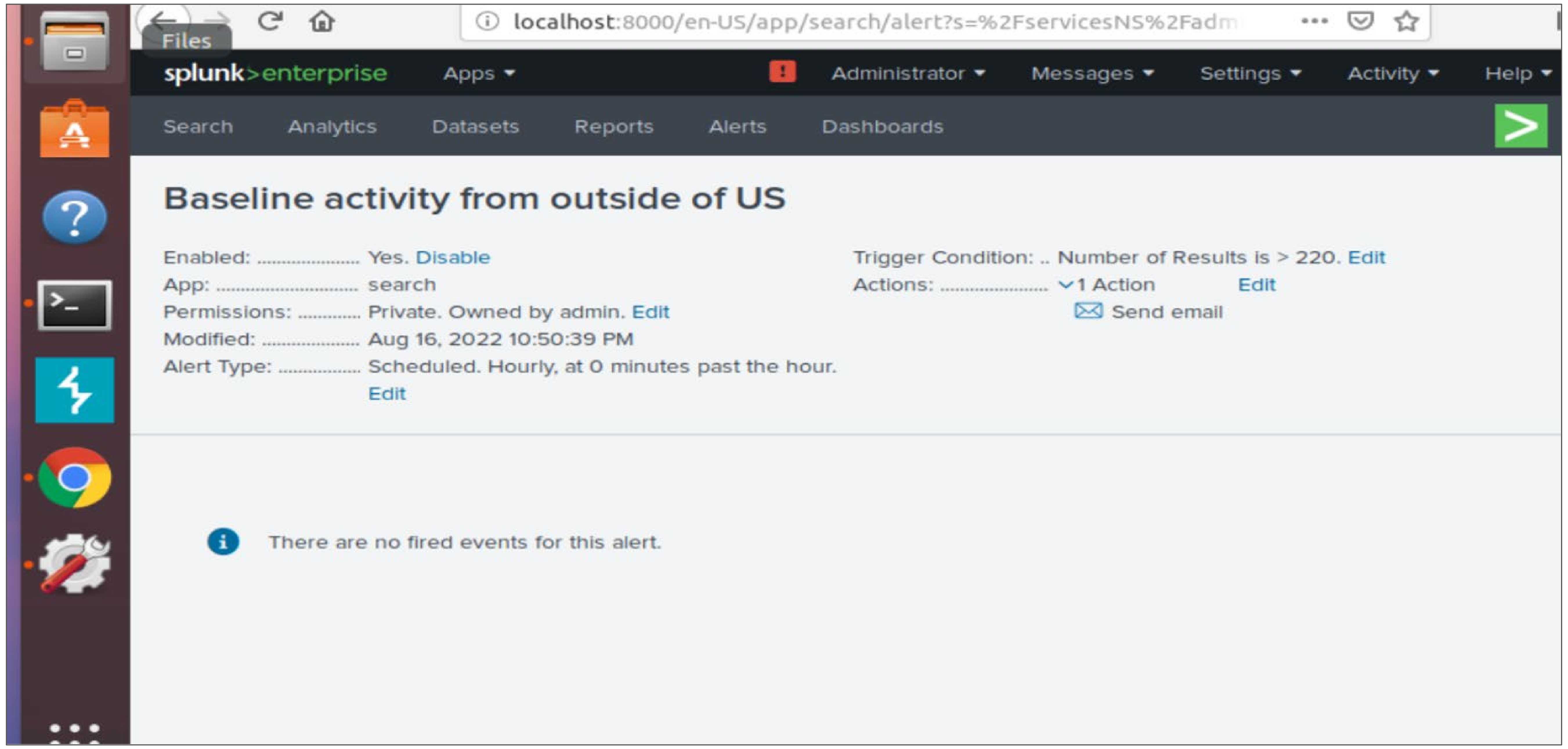
status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

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”.



Baseline activity from outside of US

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 16, 2022 10:50:39 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 220. Edit
Actions: .... 1 Action Edit
Send email

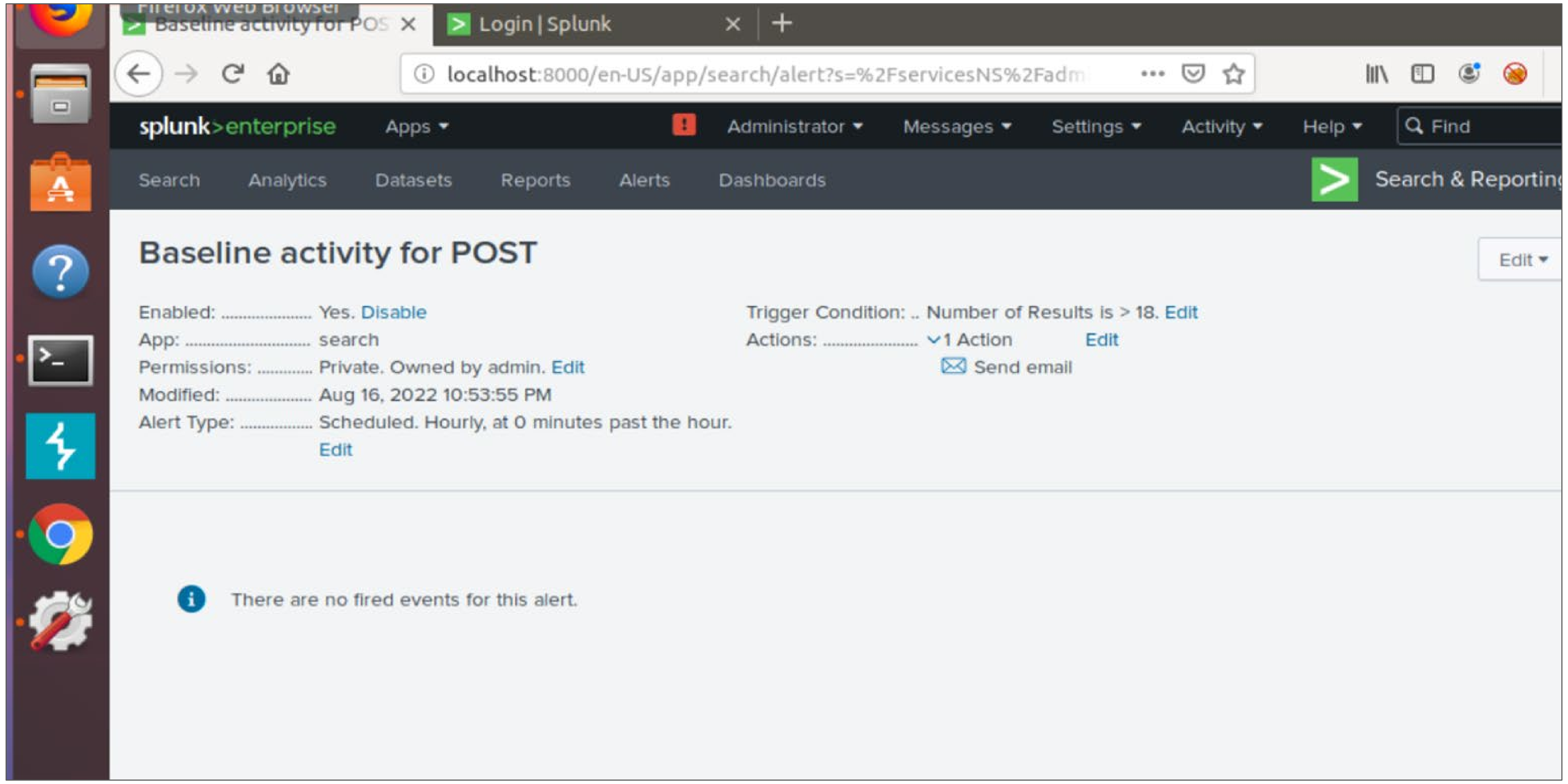
There are no fired events for this alert.

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”.



Baseline activity for POST

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Aug 16, 2022 10:53:55 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 18. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

Fig.19 – Baseline Activity for POST

Dashboards—Apache

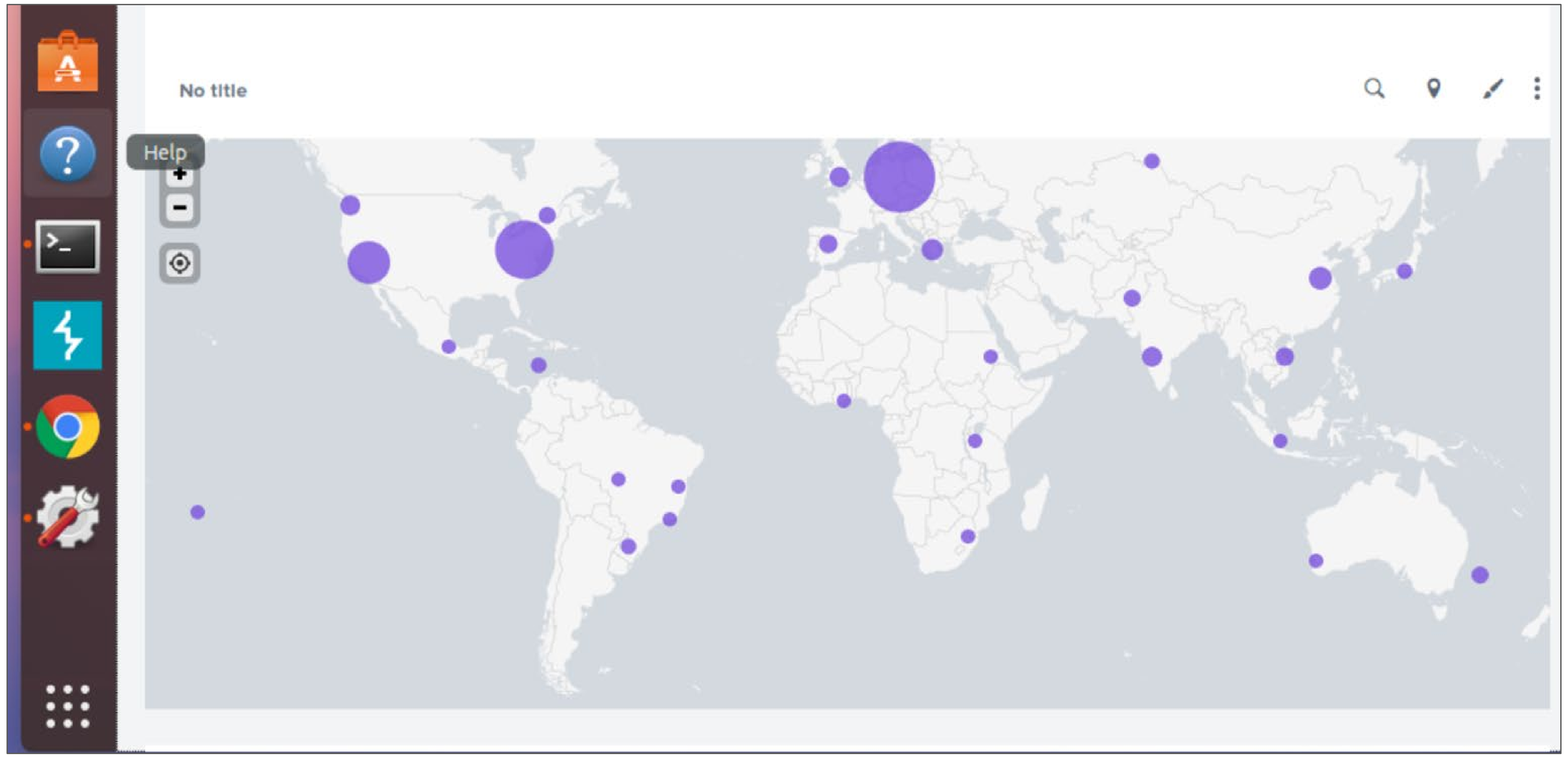


Fig.20 – Internet Connection by Continent

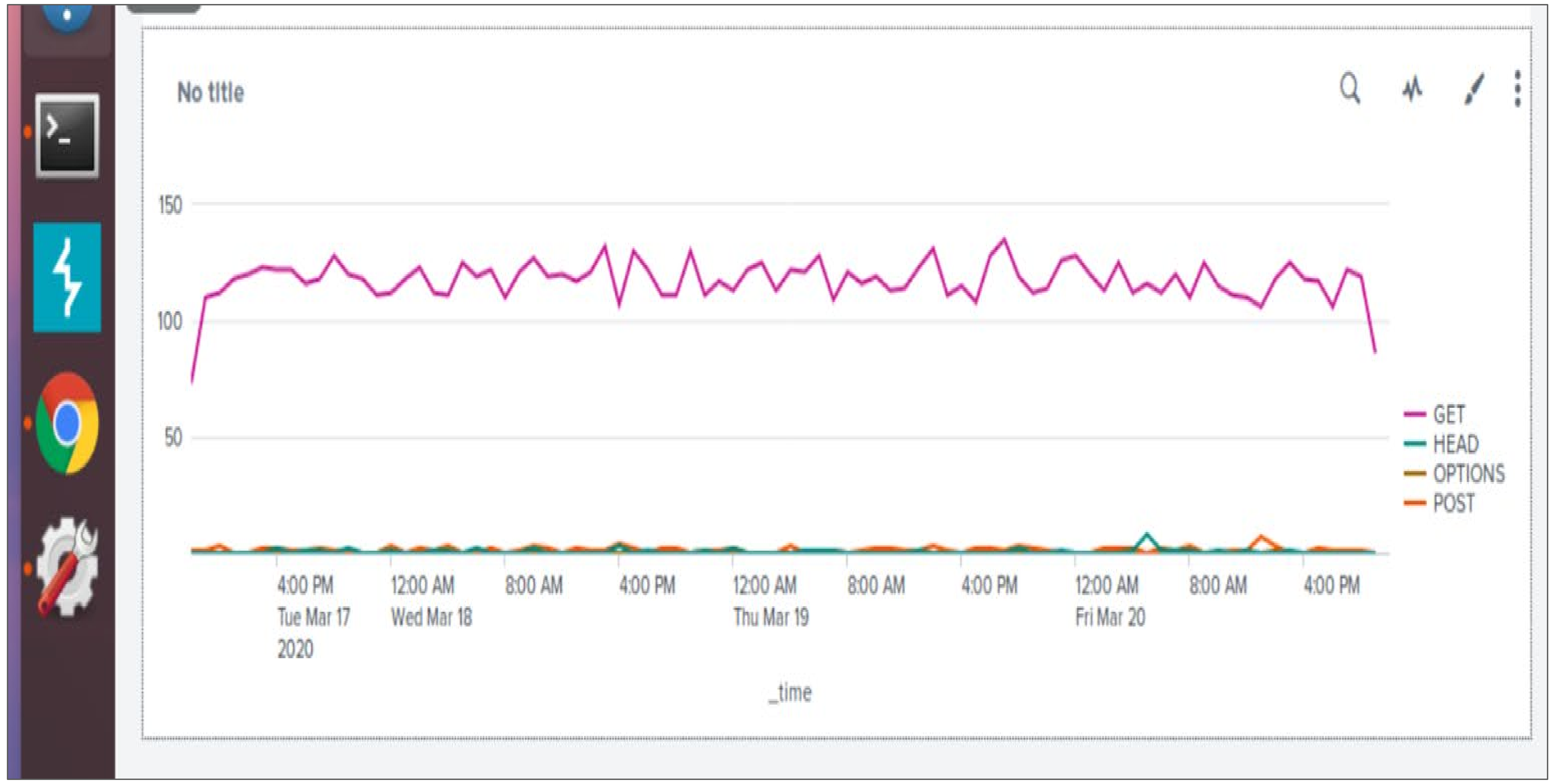


Fig.21 – Line Chart of HTTP Methods based on Type

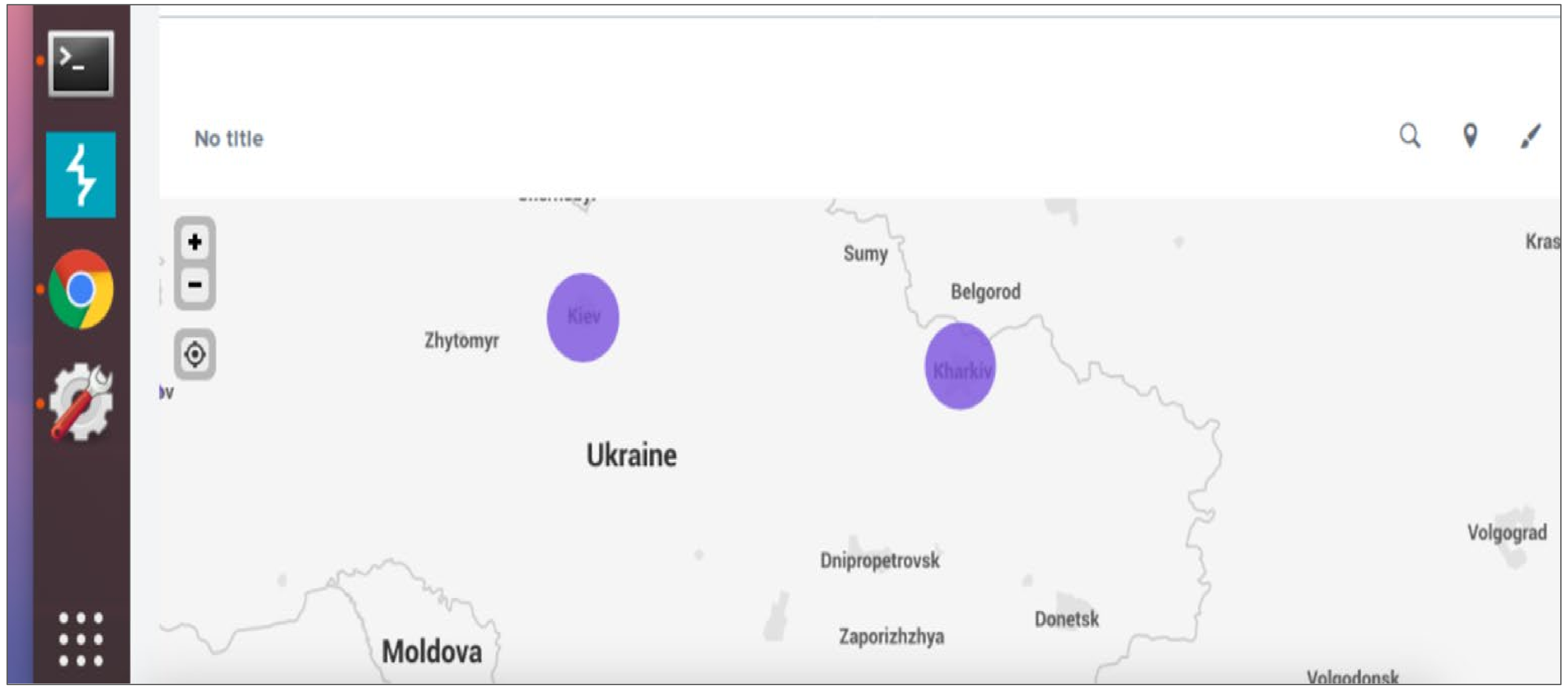
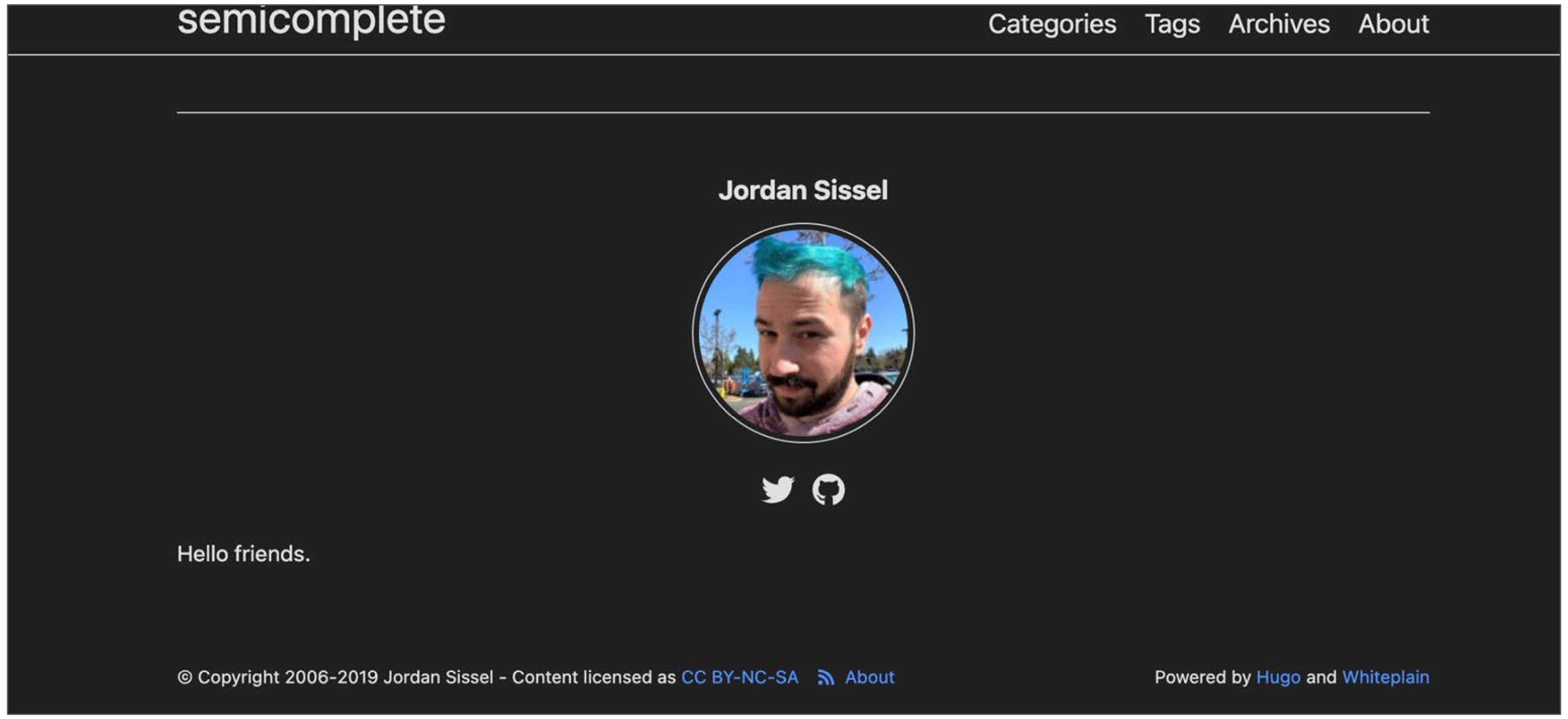


Fig.22 – Origins of Attack


semicomplete

Categories Tags Archives About

Jordan Sissel

Hello friends.

© Copyright 2006-2019 Jordan Sissel - Content licensed as CC BY-NC-SA About

Powered by Hugo and Whiteplain

Fig.23 – Suspicious Site Associated with Attack

Dashboards—Apache

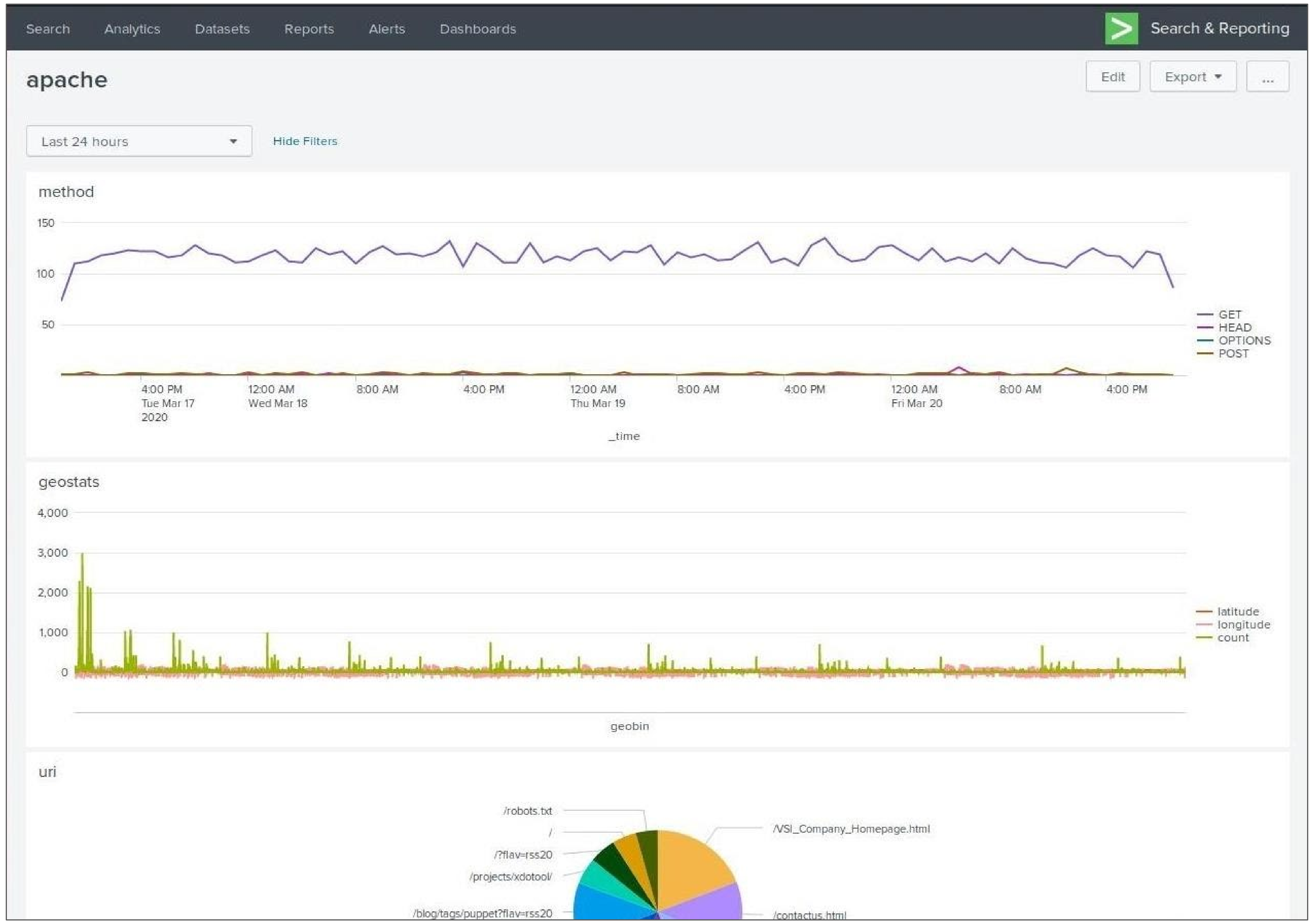
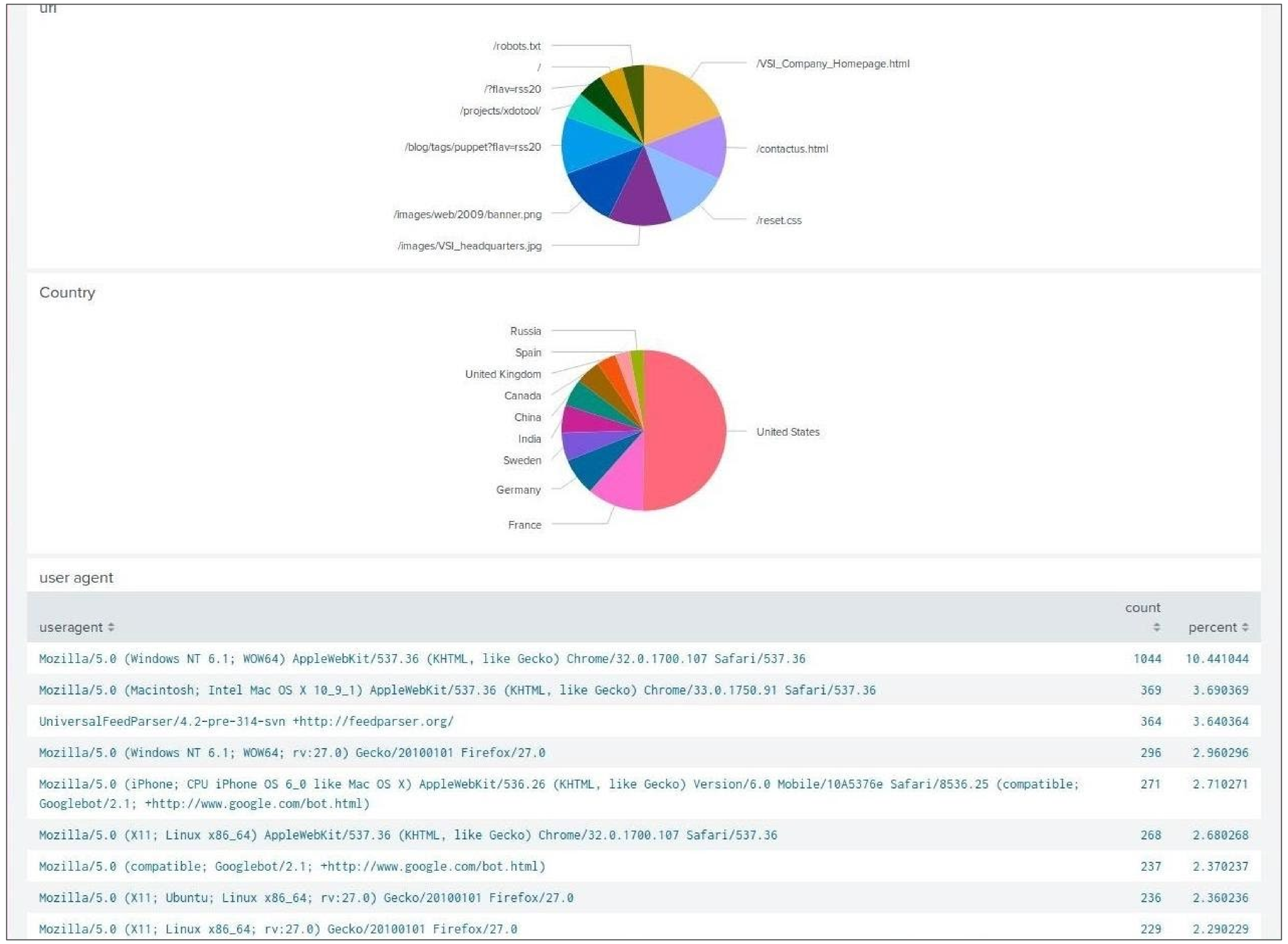


Fig.24 – Dashboard (Method Line Chart & geostats Bar Chart)



user agent

useragent ⇕	count ⇕	percent ⇕
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1044	10.441044
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	369	3.690369
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364	3.640364
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	296	2.960296
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	271	2.710271
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268	2.680268
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237	2.370237
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	236	2.360236
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	229	2.290229

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.

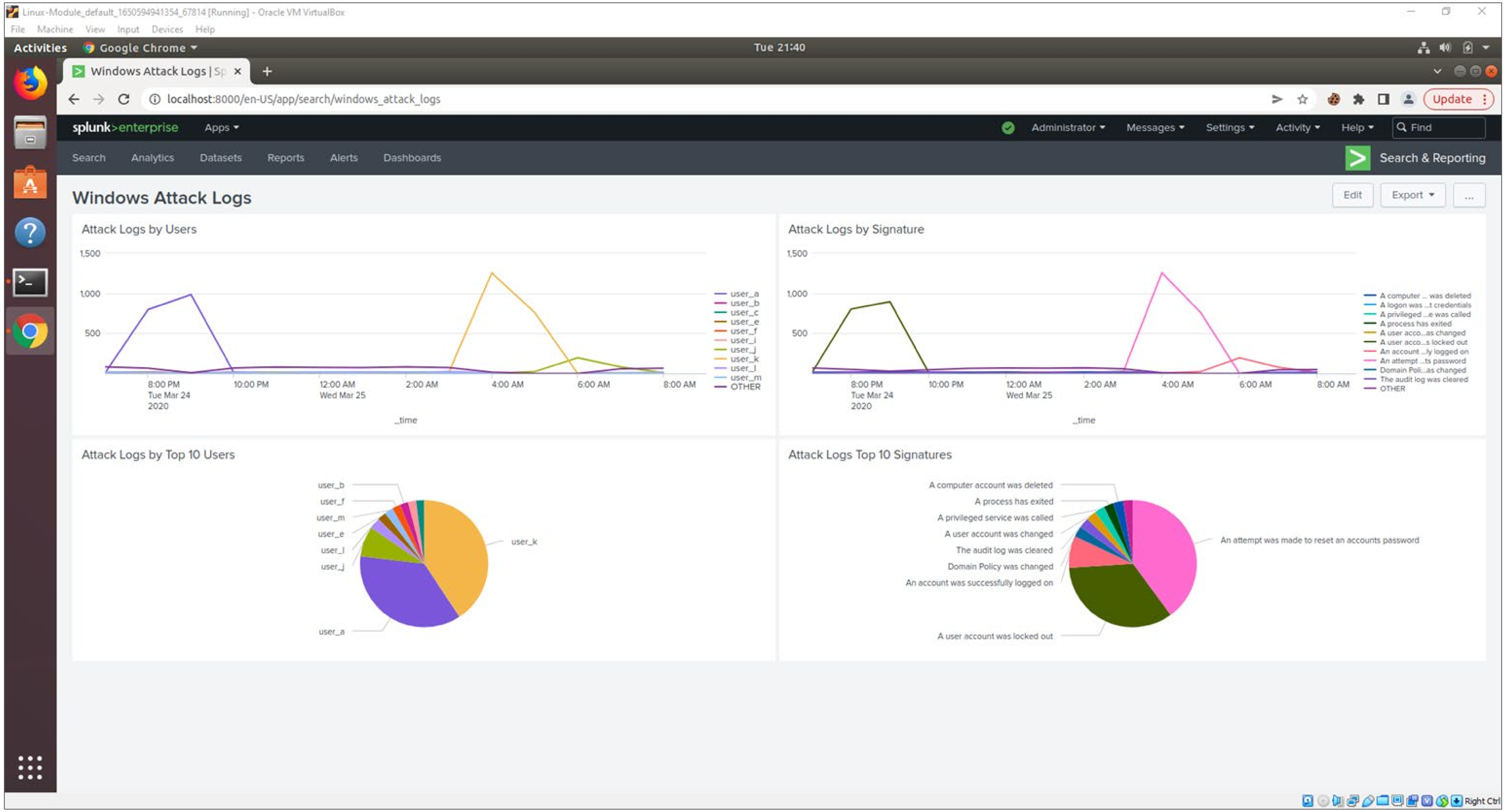


Fig.26 – Windows Attack Logs Users & Signatures

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 even 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.

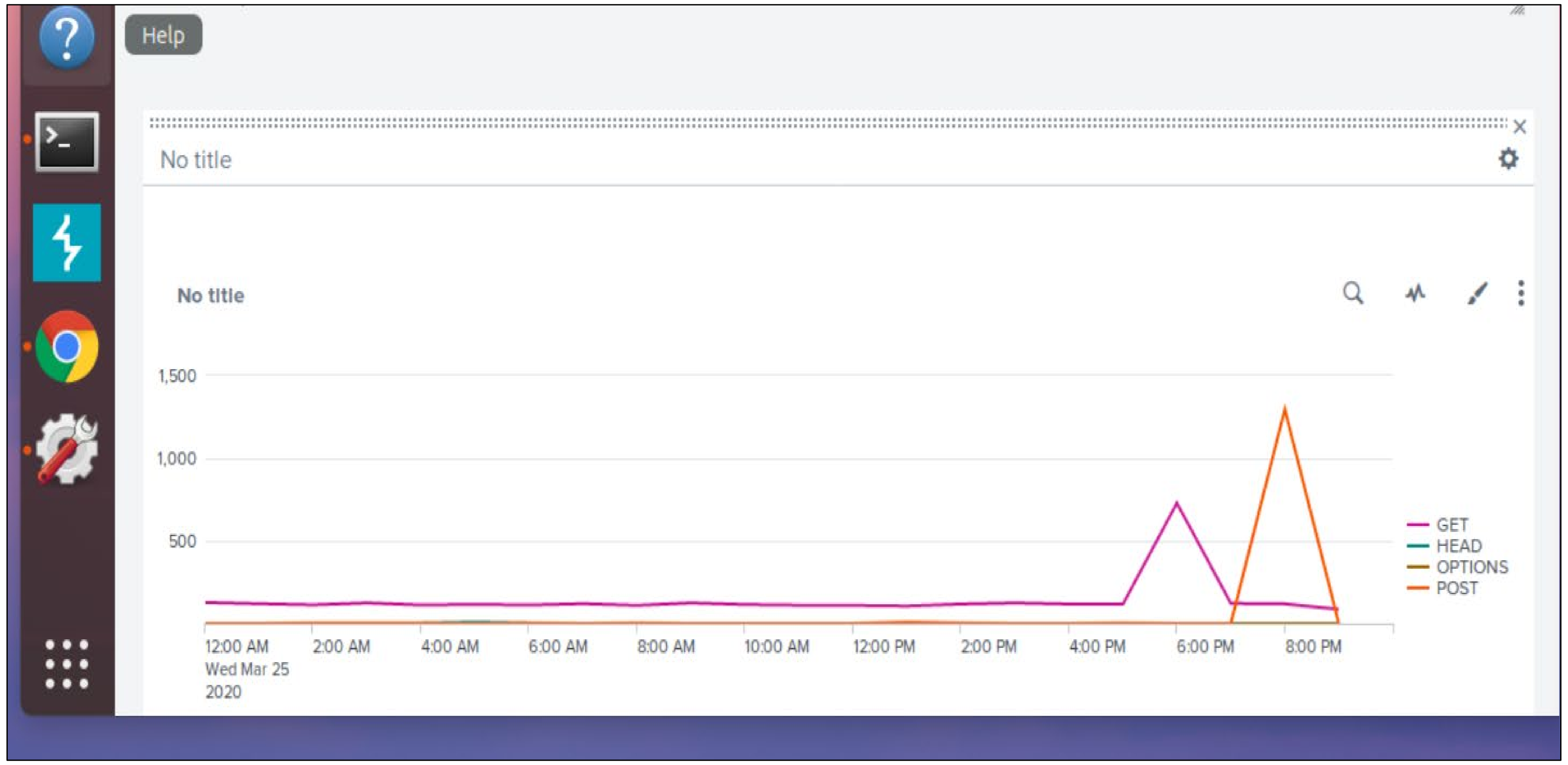


Fig.27 – Apache Attack Logs GET & POST

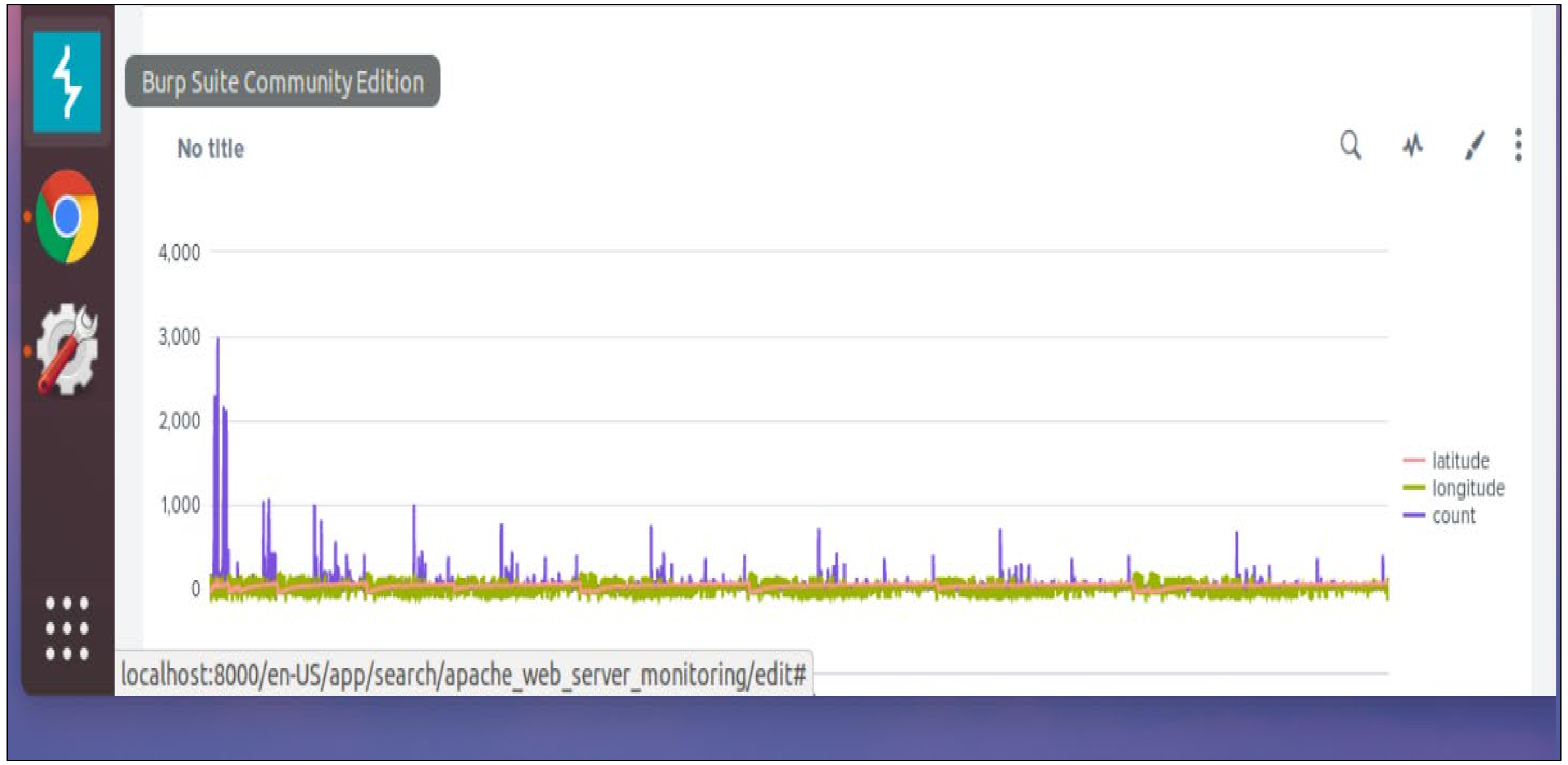

Burp Suite Community Edition
No title
4,000
3,000
2,000
1,000
0
latitude
longitude
count
localhost:8000/en-US/app/search/apache_web_server_monitoring/edit#

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.