Defensive Security Project
by: Jennifer, Cesar, Kristina and Ivan

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- In this project we use Splunk to monitor and analyze logs of VSI by:

a. Loading and analyzing logs
b. Creating Alerts, Reports and Dashboards
c. Installing Splunk add-on app

Splunk McAfee epo Add-On App

Splunk McAfee epo Add-On App

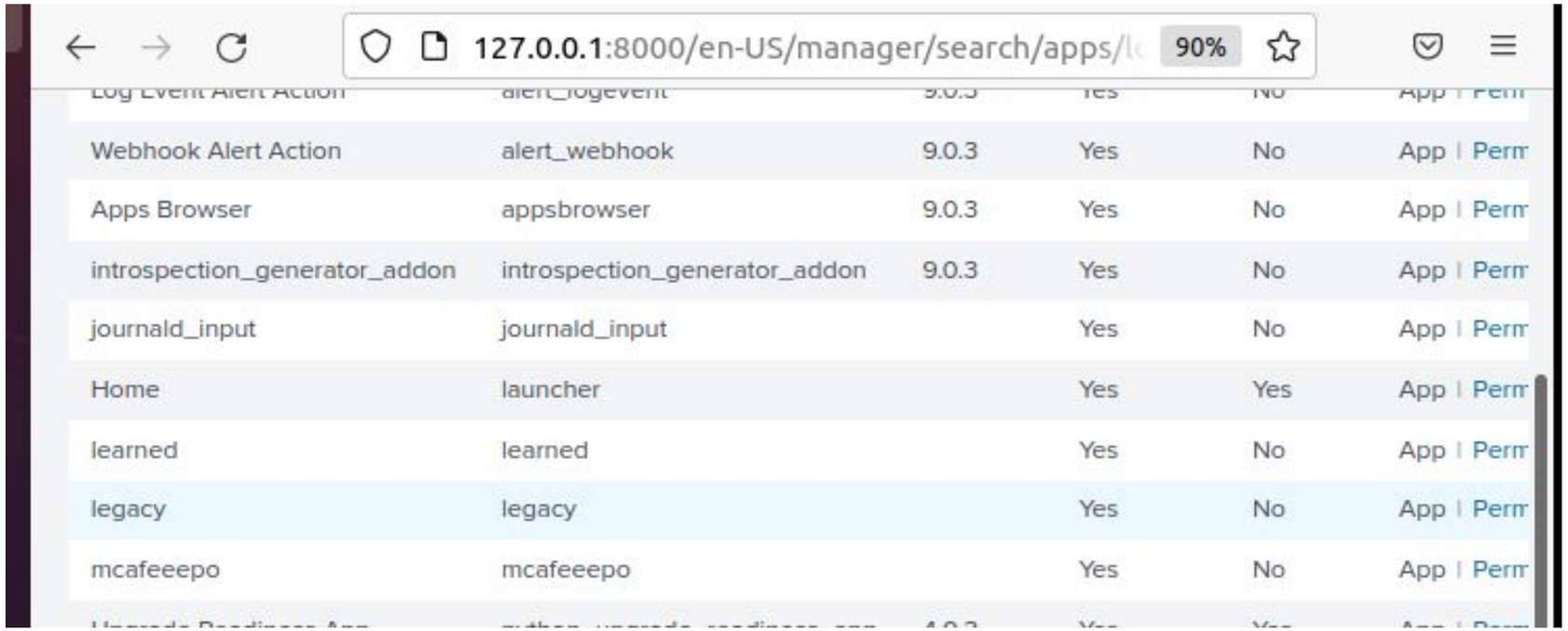
The Splunk McAfee ePO Add-On App is an add-on app for the Splunk platform that provides integration with the McAfee ePolicy Orchestrator (ePO) security management platform. The add-on app enables organizations to collect and analyze security-related data from McAfee ePO and to use that data to gain insights into the security of their systems and networks.

Splunk McAfee epo Add-On App

1. The add-on app collects data from the McAfee ePO database, including information on threats, vulnerabilities, security incidents, and policy compliance.
2. The collected data is indexed and made searchable in Splunk, allowing users to quickly find and analyze relevant data.
3. The add-on app provides a range of visualizations, including graphs, tables, and charts, to help users understand and explore the security-related data.
4. The Splunk McAfee ePO Add-On App can be integrated with other security tools, such as firewalls, intrusion detection systems, and endpoint security solutions, to provide a comprehensive view of the security of an organization's systems and networks.

Splunk McAfee epo Add-On App

Installed and setup



Webhook Alert Action	alert_webhook	9.0.3	Yes	No	App | Perm
Apps Browser	appsbrowser	9.0.3	Yes	No	App | Perm
introspection_generator_addon	introspection_generator_addon	9.0.3	Yes	No	App | Perm
journald_input	journald_input		Yes	No	App | Perm
Home	launcher		Yes	Yes	App | Perm
learned	learned		Yes	No	App | Perm
legacy	legacy		Yes	No	App | Perm
mcafeeepo	mcafeeepo		Yes	No	App | Perm

Logs Analyzed

1 Windows Logs

This data contains activity to the Windows server that has Intellectual property for VSI. All the user activities based time, login, and their activity is captured in this data including timeframe of their activity.

2 Apache Logs

This has the information about activities on the public facing website of VSI vsi-company.com. This activities entail GET, POST, DELETE, PUT methods of HTTP request communications with the Apache Server.

Windows Logs

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signatures and Signature ID	Contained windows activity signatures and their ID
Severity levels	It has severity levels, count and percentage
Status	Has success and failures of activities

Images of Reports—Windows

signatures and signature ids for windows activity

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **4,764 events** (before 2/14/23 2:15:32.000 AM)

Job ▾

15 results 20 per page ▾

signature	signature_id	count	percent
The audit log was cleared	1102	303	6.360202
An account was successfully logged on	4624	323	6.780017
A logon was attempted using explicit credentials	4648	337	7.073887
Special privileges assigned to new logon	4672	342	7.178841
A privileged service was called	4673	317	6.654072
A process has exited	4689	309	6.486146
System security access was granted to an account	4717	309	6.486146
System security access was removed from an account	4718	321	6.738035
A user account was created	4720	313	6.570109
An attempt was made to reset an accounts password	4724	295	6.192275
A user account was deleted	4726	318	6.675063
A user account was changed	4738	299	6.276238
Domain Policy was changed	4739	329	6.905961
A user account was locked out	4740	309	6.486146
A computer account was deleted	4743	340	7.136860

status of Windows activities

Edit ▾ | More Info ▾ | Add to Dashboard

All time ▾

✓ **5,949 events** (before 2/14/23 2:16:59.000 AM)

Job ▾

2 results 20 per page ▾

status	count	percent
success	5856	98.436712
failure	93	1.563288

Severity levels

Edit ▾ | More Info ▾ | Add to Dashboar

All time ▾

✓ **5,949 events** (before 2/14/23 2:16:20.000 AM)

Job ▾

2 results 20 per page ▾

severity	count	perce
informational	4383	79.77
high	1111	20.22

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed status alert	Triggered when threshold for hourly level of failed Windows activity is reached. Mail is triggered to SOC@VSI-company.com	20	High

When an alert is triggered, it can notify an operator or take automated action, such as sending an email or triggering a remediation script.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Log-on alert	Triggered when threshold is reached. Mail is triggered to SOC@VSI-company.com	47	High

When an alert is triggered, it can notify an operator or take automated action, such as sending an email or triggering a remediation script.

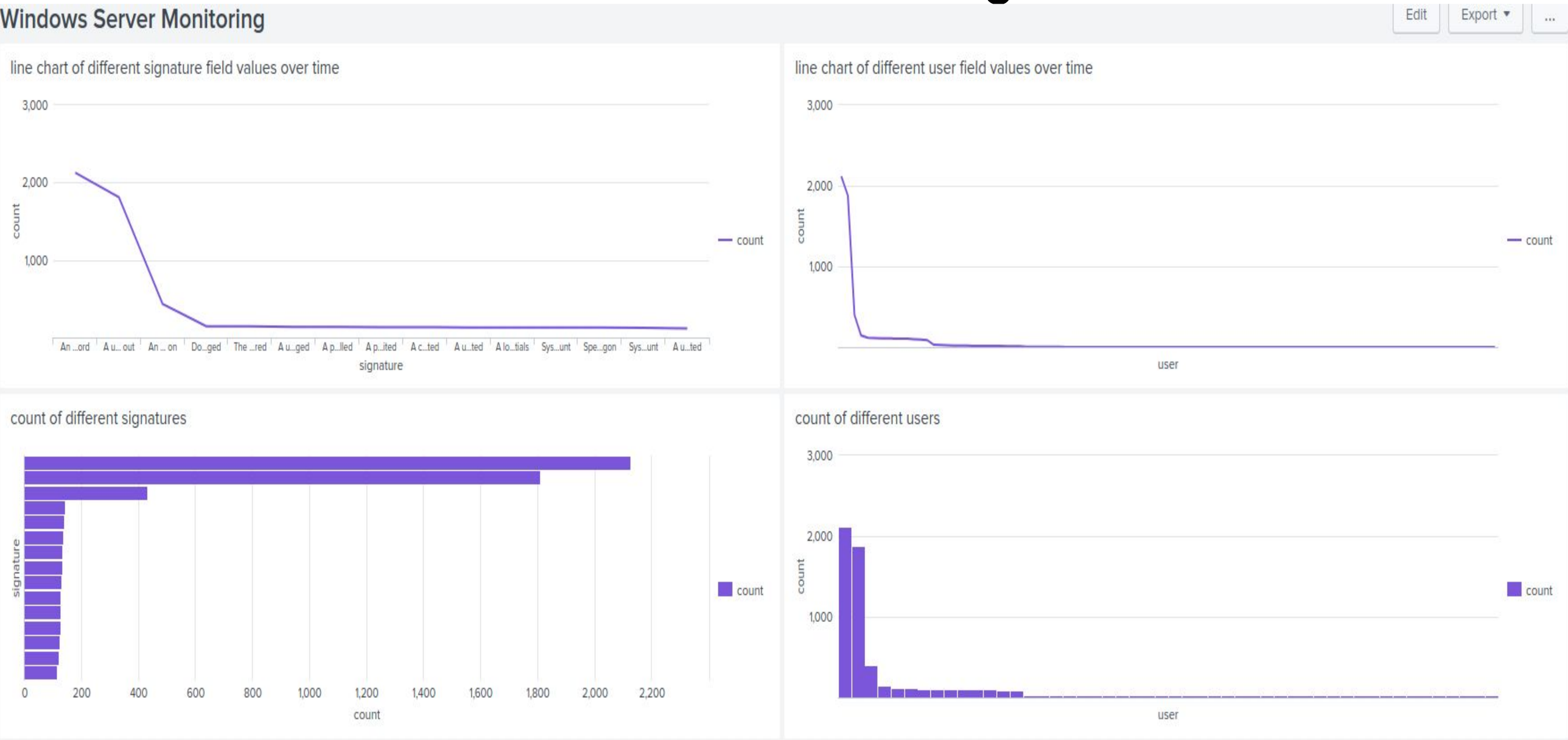
Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Signature ID	When a user account is deleted, its triggered.	30	High

When the signature “a user account was deleted”, an alert will be set off and an email notification will be sent.

Dashboard—Windows Server Monitoring



Dashboard—Windows Server Monitoring

radial gauge of total stats count

stats count of different users

user	count	percent
user_l	708	7.430730
user_a	564	5.919395
user_m	550	5.772460
user_i	542	5.688497
user_f	540	5.667506
user_h	538	5.646516
user_e	538	5.646516
user_c	534	5.604534
user_d	528	5.541562
user_b	526	5.520571

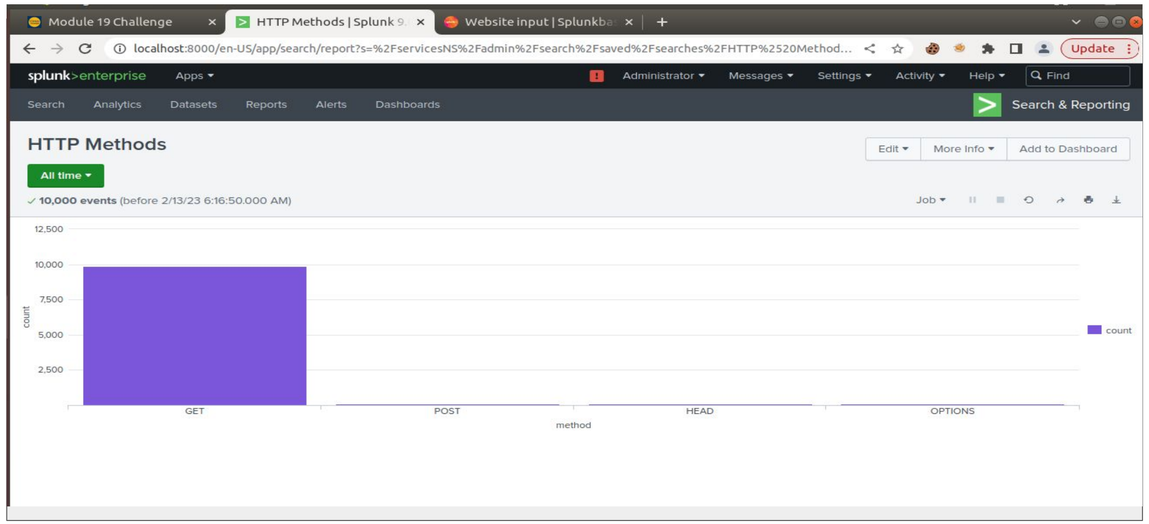
Apache Logs

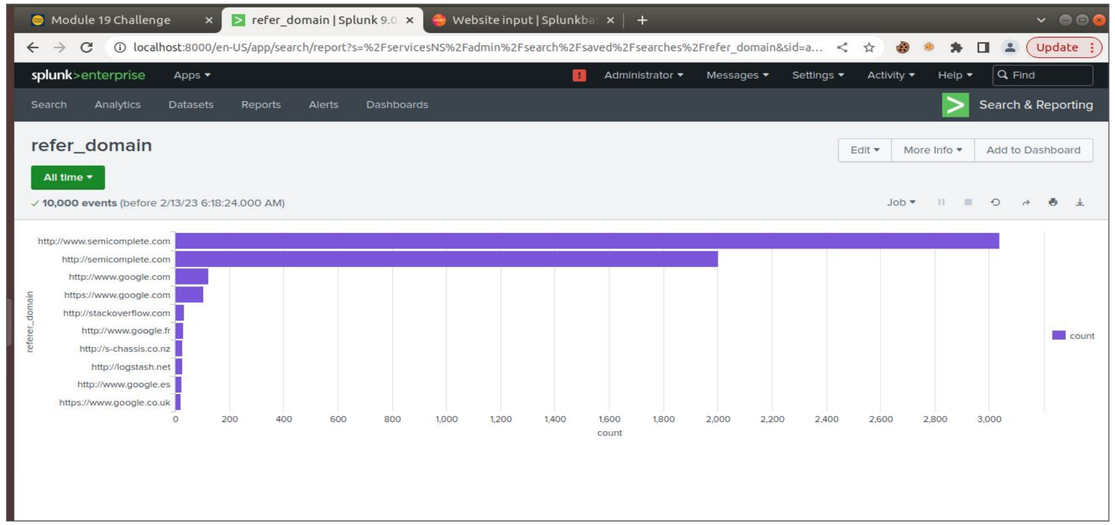
Reports—Apache

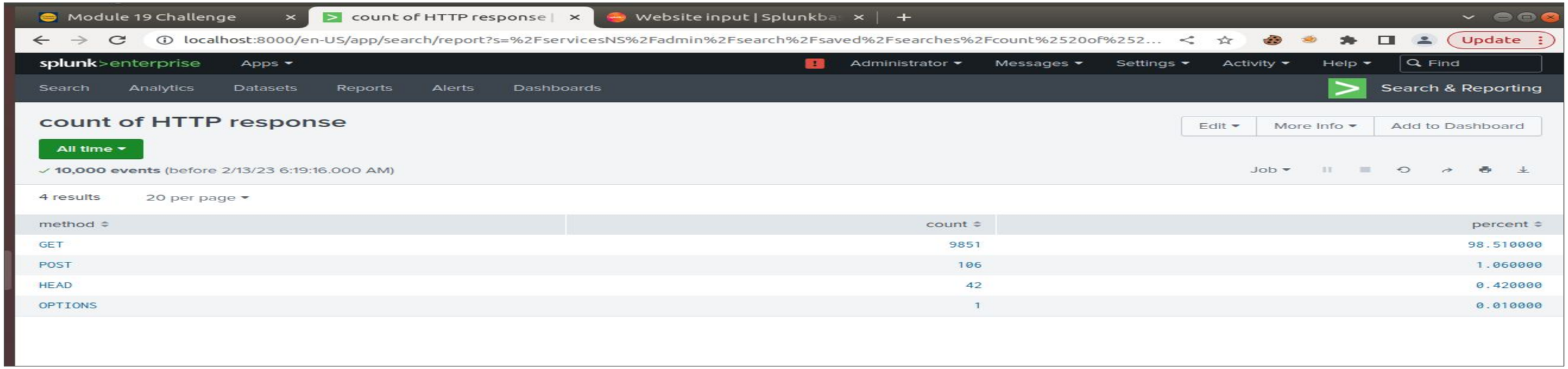
Designed the following reports:

Report Name	Report Description
http	Has http table of get, post, head methods
domains	Has top 10 domains activities
http count	Has http-count of response code

Images of Reports—Apache







method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Out of US activity	monitor activity from outside of US	80	180

Once the threshold is reached an email is triggered when the area triggering and activity to VSI is outside United States.

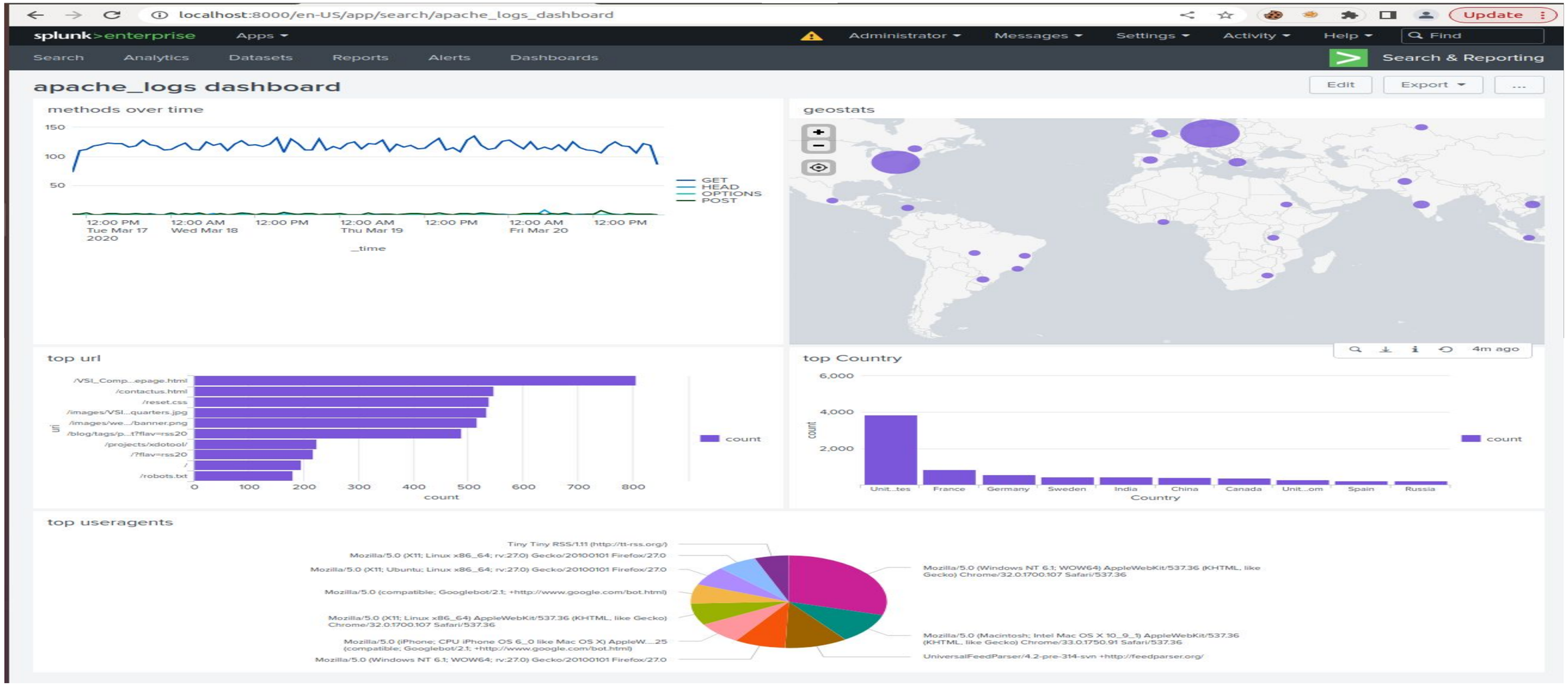
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
http post alert	An alert is triggered when hourly HTTP POSTS exceeds.	2	15

The baseline for hourly HTTP post method count is 2. when it exceeds an alert is triggered.

Dashboards—Apache



Attack Analysis

Attack Summary—Windows

There were changes in severity from the previously analyzed to the current that can be termed as suspicious.
The dashboard, alerts, charts depict changes in the windows activity. Some have not changed some show a significant change for malicious activities

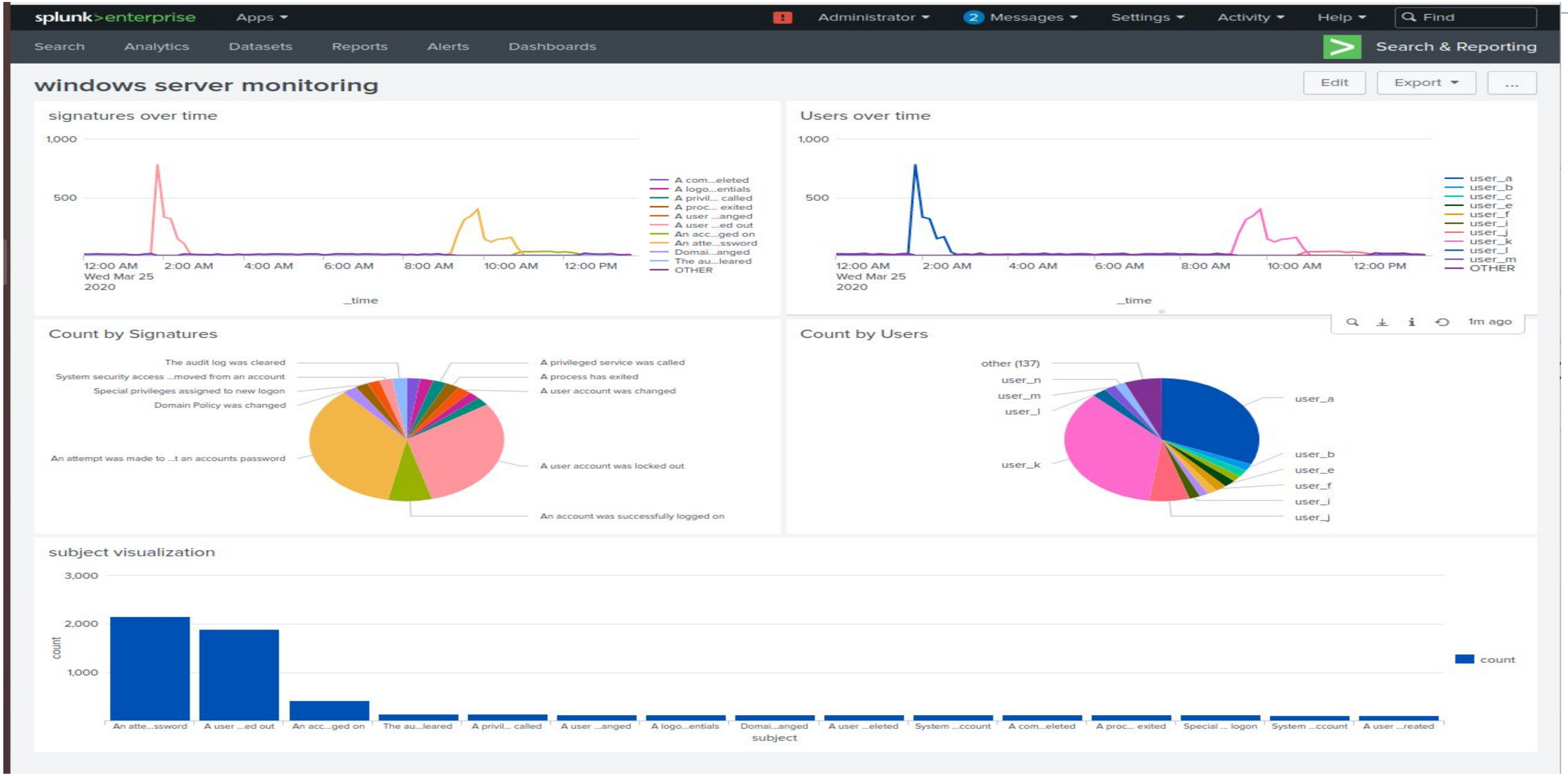
Attack Summary—Windows

Security administrators may immediately discover possible security issues and quickly respond to them thanks to alerts, which are essential for security log analysis.
From the designed alerts. Several alerts have been triggered and notify the VSI team by sending an email to SOC@VSI-company.com

Attack Summary—Windows

Dashboards analysis of the attack logs helps visualize and show trends in the windows logs. This is used to detect the changes and act accordingly to any suspicious malicious activity against VSI.

Screenshots of Attack Logs



Attack Summary—Apache

The attack logs finding depended on the reports, alerts and dashboard created earlier for day 1 activity. The Apache logs analysis depicted some malicious activities like account deletion, injection through http methods and many more. With dashboard and visualization it was easy to easy certain changes in trends of the logs activity. Alerts was one way to see and gauge the changes with reports having an upper hand of help over the same detection and finding of suspicious activities.

Attack Summary—Apache

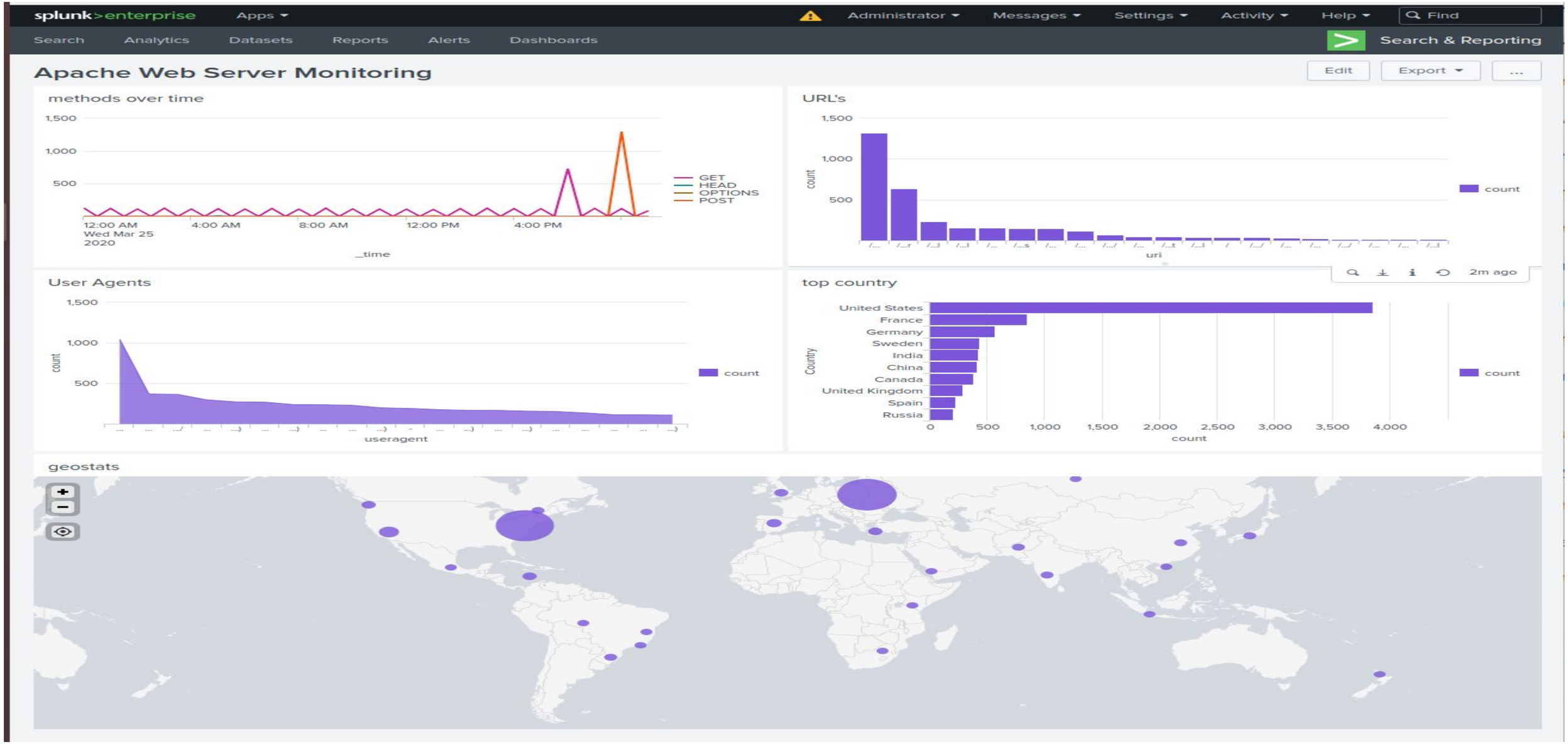
From the findings not all thresholds were correct in this analysis. Those that were corrects should not be changed while those that were incorrect are subject to change as commented earlier.

Attack Summary—Apache

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

The dashboards gave a clear picture on the data log trends. The earlier pre-generated dashboards in day 1 task were a prerequisite in the Apache attack logs analysis. The difference in the two was the bassline for a suspicious activity.

Screenshots of Attack Logs



Summary and Future Mitigations

Project 3 Summary

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

  From the attack that took place. Some user accounts were deleted. This was detected by alerts to email SOC@VSI_company.com. There were other suspicious activities but were not as intense as this account deletion. HTTP get method being the most hit in the scenario of the VSI website was being harnessed by attackers to try and get private information from the website servers.

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

  I would recommend the use of firewalls between the servers of VSI this will help filter traffic to and from the servers.

  I would recommend the use of cloud servers maintained by well established vendors like Amazon who have put in place hybrid security against their servers.