# Defensive Security Project
# by: [only by Rahibullah]

# Table of Contents

This document contains the following resources:

# Monitoring Environment

# Scenario

- VSI has been suffering from attacks , and now they want someone to monitor their windows server and apache server so the attack dosnt happen again

- i have been hired to create dashboards , alerts and reports to find out how the attack happens and what happened during the attack and if the attack happens again by using these dashboards, alerts stop it before it do bad things again.

# [ Splunk App for Windows Infrastructure ]

# [ Splunk App for Windows Infrastructure ]

**The Splunk App for Windows Infrastructure provides examples of pre-built data inputs, searches, reports, and dashboards for Windows server and desktop management. You can monitor, manage, and troubleshoot Windows operating systems, including Active Directory elements, all from one place.**

**Included are inputs for performance metrics, event logs, user and audit data. The app makes getting started with Splunk a breeze. The App also contains dashboards needed to monitor your Active Directory environment and allows for correlation opportunities from the Active Directory data back to the Operating System.**

**A unique first-time run experience detects data you might already have to highlight areas for your specific environment. Host Monitoring, Print Monitoring, and Network Monitoring also light up new possibilities.**

# Logs Analyzed

1

## Windows Logs

failed activities , successful logins, deleted accounts ,  attempts made to

2

## Apache Logs

HTTP methods ,  refere domains , most traffic is coming from ukraine

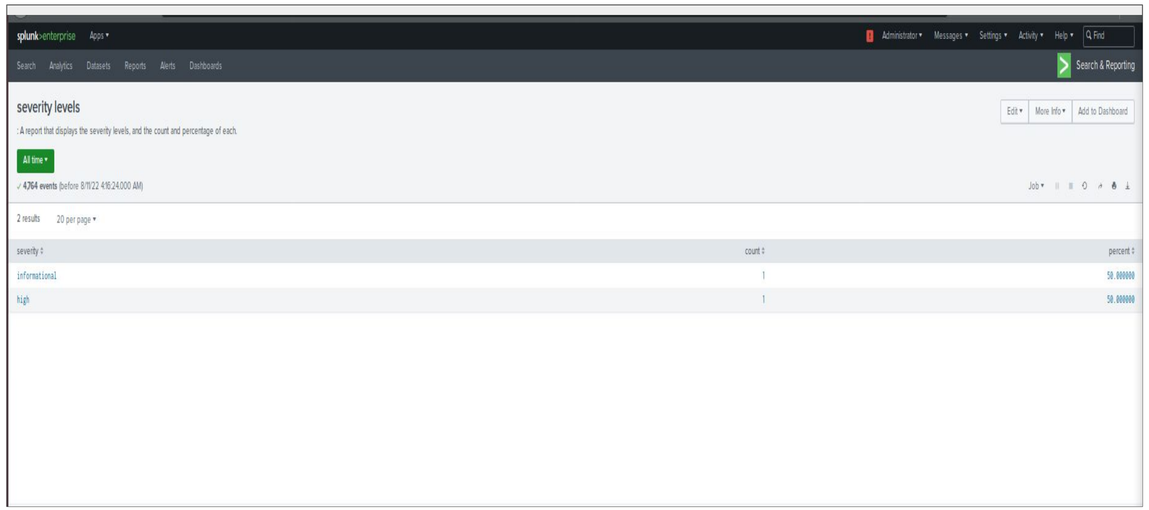
# Windows Logs

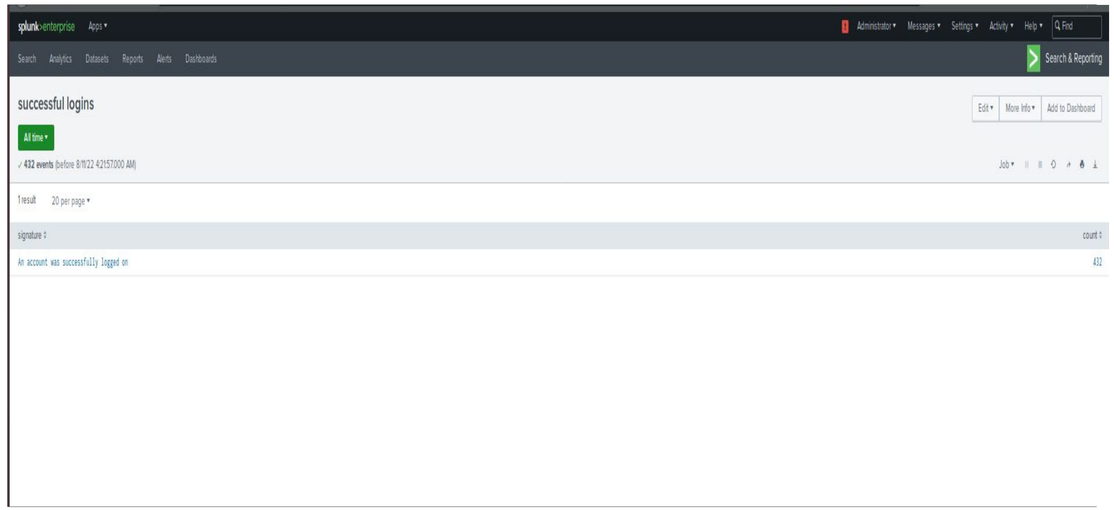
# Reports—Windows

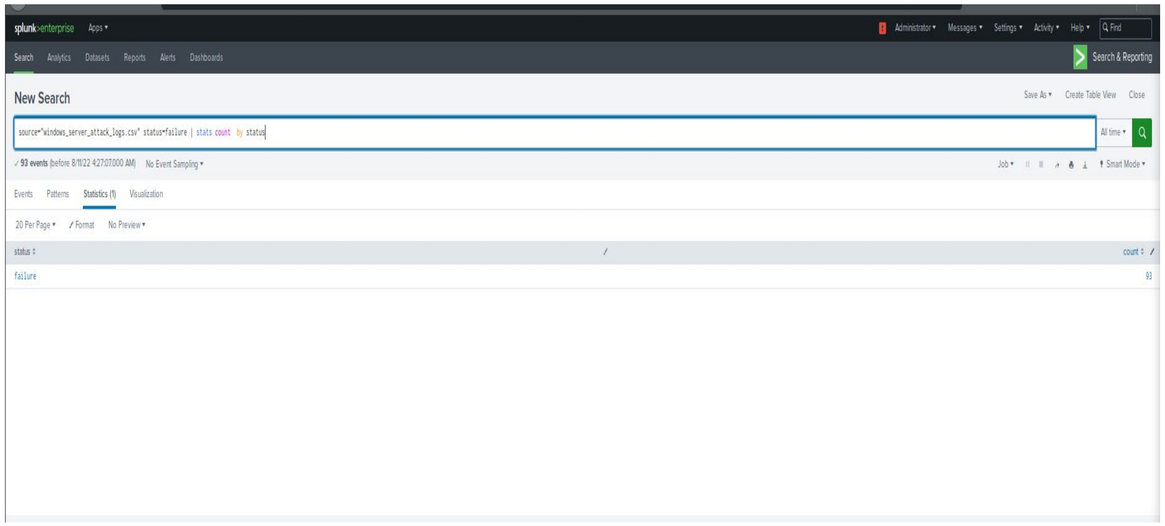
Designed the following Reports:

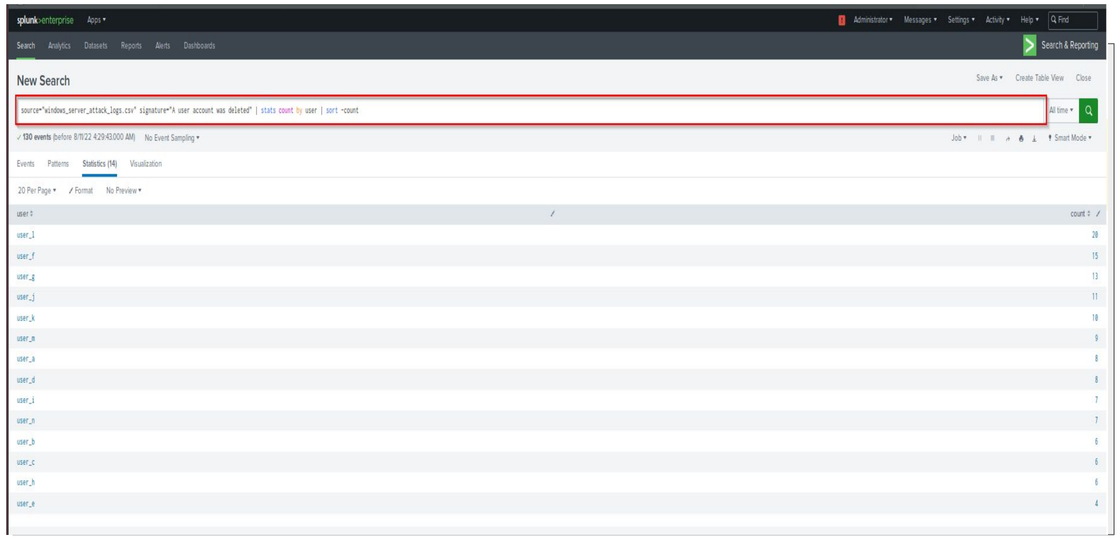
| Report Name | Report Description |
|---|---|
| [failed activities ] | [Report Analysis for Failed Activities] |
| [ severity levels ] | [A report that shows the severity levels with in the windows server] |
| [successful logins ] | [report for successful logins ] |
| [ deleted accounts ] | [report for deleted accounts] |

# Images of Reports—Windows



# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| [successful logins ] | [there has been more successful logins then normal ] | [14] | [15] |

**JUSTIFICATION: the normal logins are 15 max events in an hr , so if there is moer then 15 events happened with successful logins then it will alert**

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| [user account deleted] | [some users created and deleted over and over ] | [4-6] | [ 7 events based on the logs ] |

**JUSTIFICATION: its not normal when a user account is deleted over and over. but based on the logs 7 events for deleted accounts is in between normal, so if there is more then 7 events it should alert**

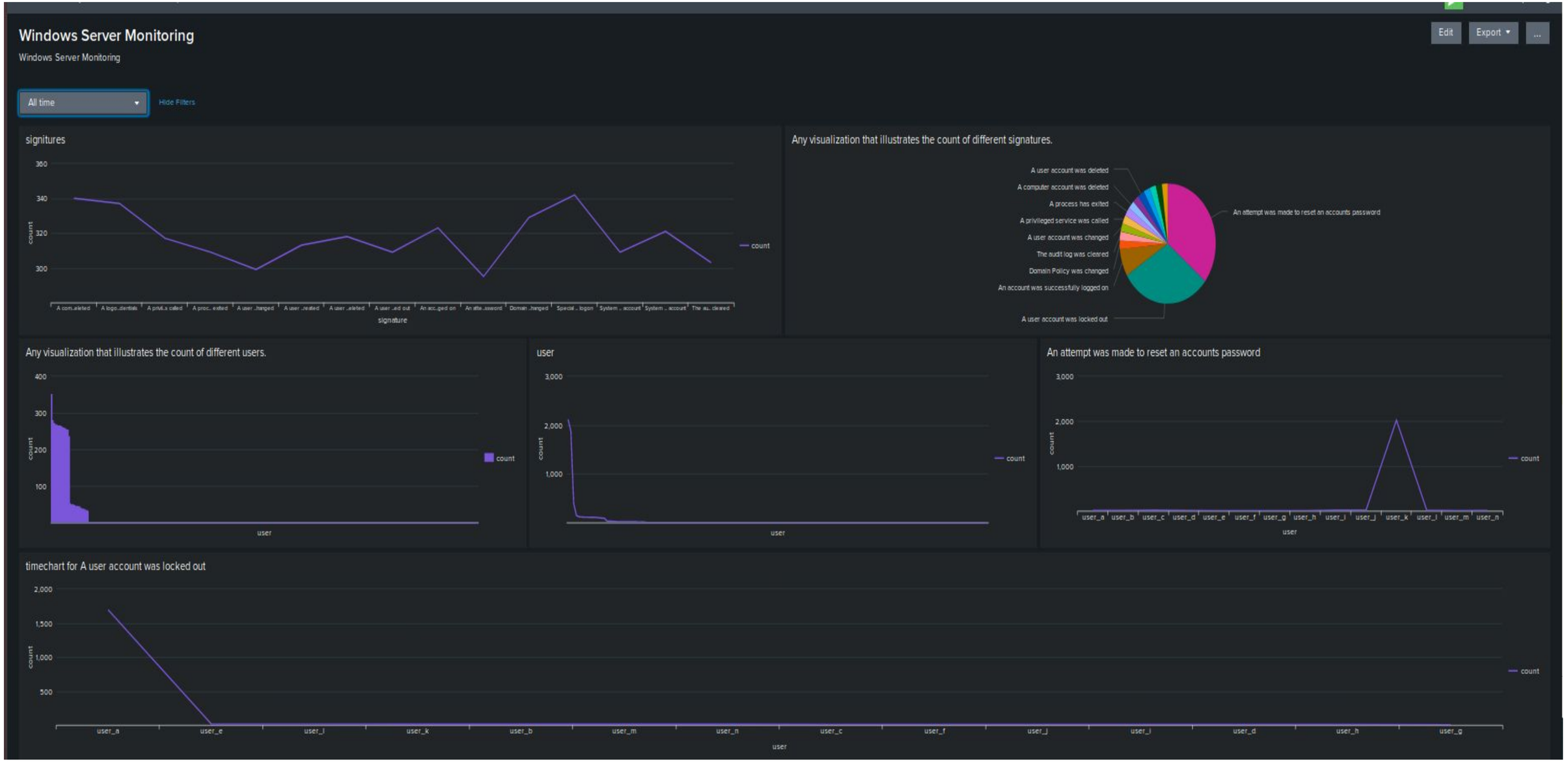
# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| [ attempt to reset password ] | [there has been alot of events where the reset password was attempt which is not normal ] | [9] | [10] |

**JUSTIFICATION: based on the logs the 9 event is normal that happens with reset password , so if there is more then 9 events it should alert**

# Dashboards—Windows



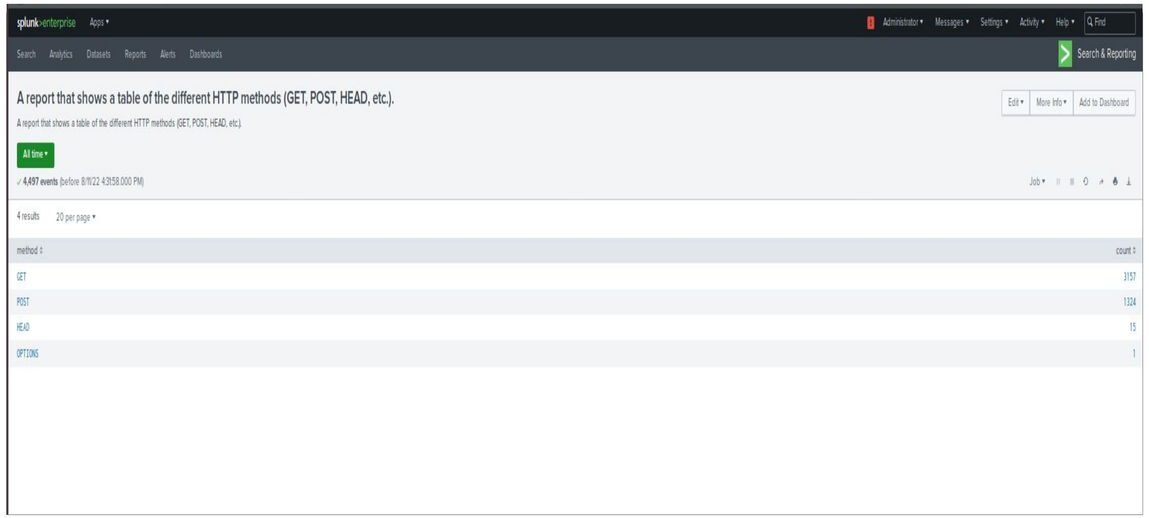
# Apache Logs

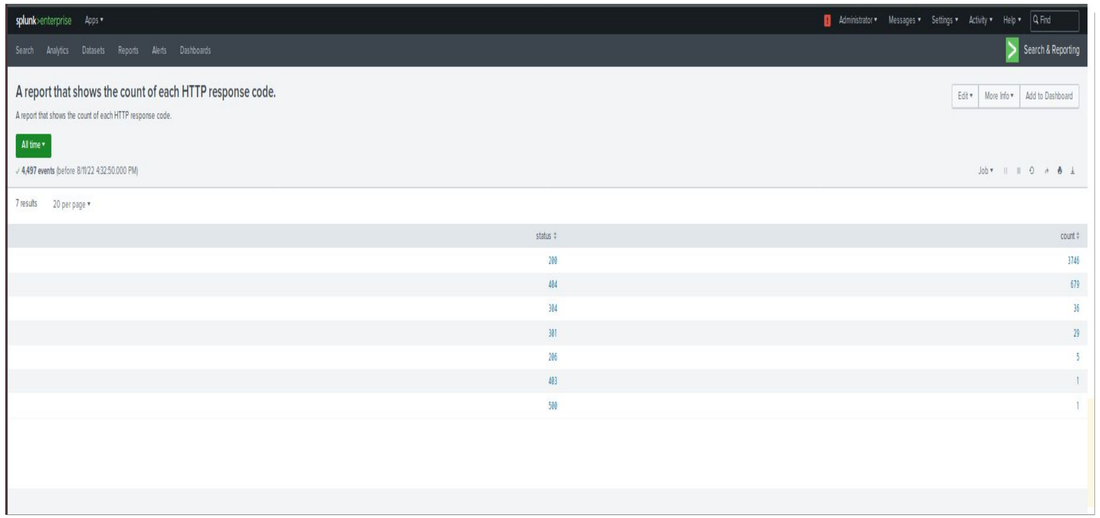
# Reports—Apache

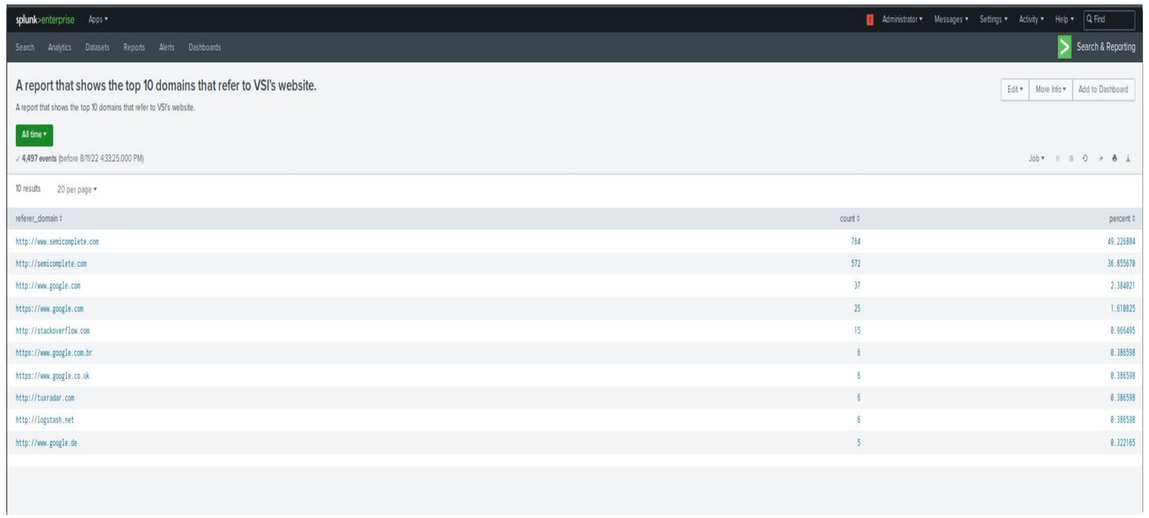
Designed the following reports:

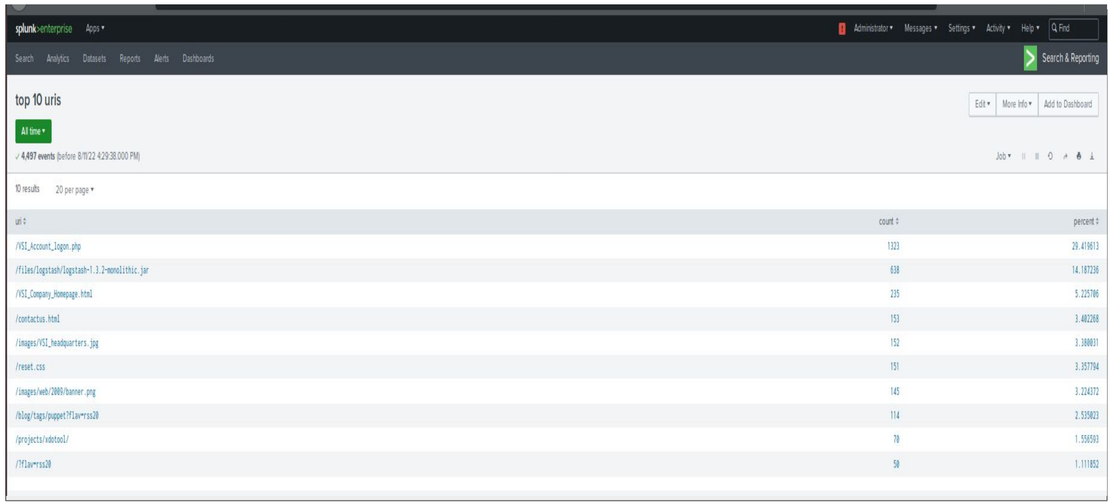
| Report Name | Report Description |
|---|---|
| [HTTP methods] | [A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.).] |
| [HTTP response] | [A report that shows the count of each HTTP response code.] |
| [top 10 domains] | [A report that shows the top 10 domains that refer to VSI’s website.] |
| [top 10 URIs] | [a report about most visited URIs] |

# Images of Reports—Apache



# Alerts—Apache

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| [international actvity] | [this alert is about activity or traffic  that is coming from other countries ] | [50-69] | [70] |

**JUSTIFICATION: [based on the logs if there is more then 70 events that is coming from outside US then it will alert ]**

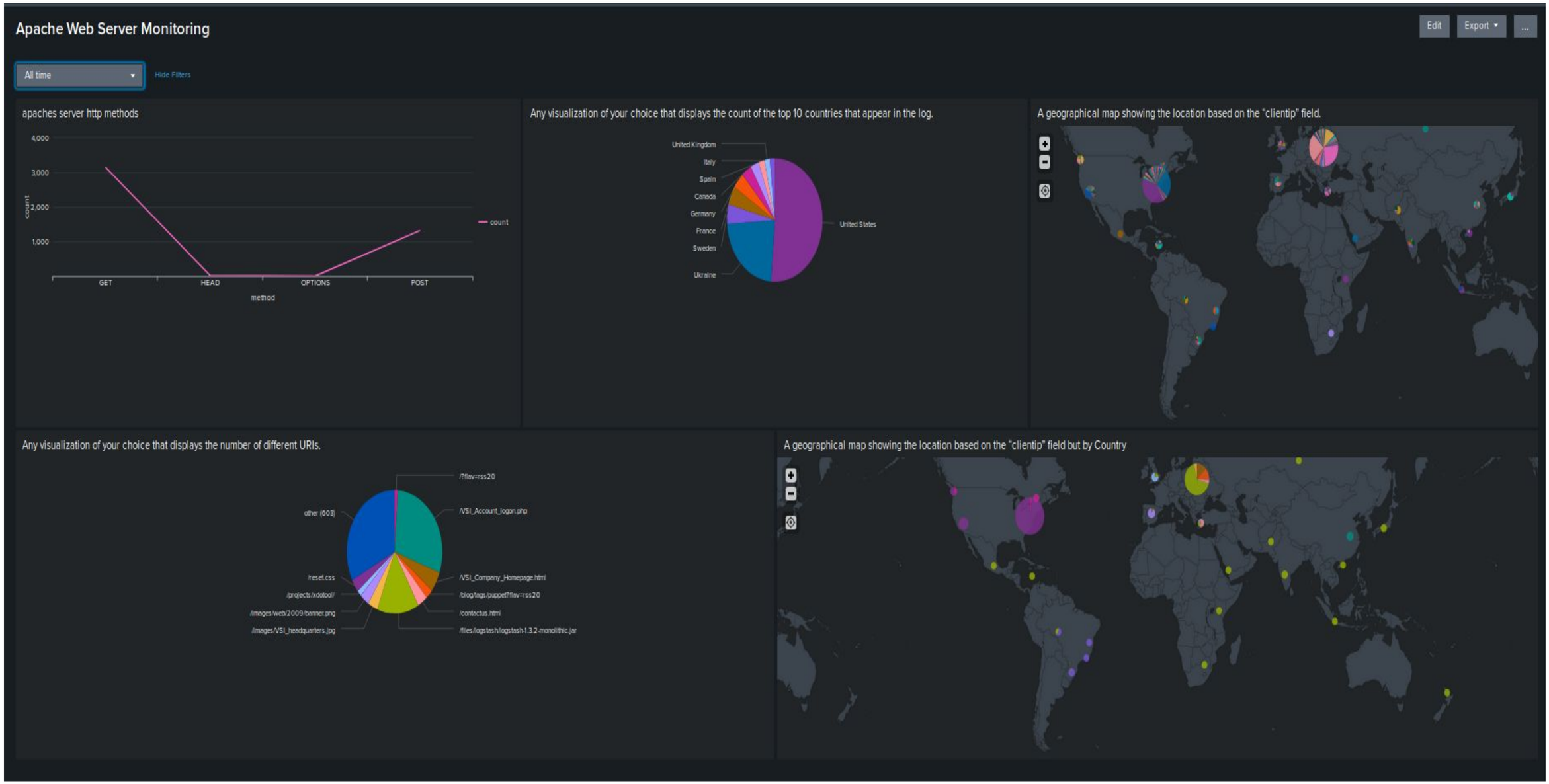
# Alerts—Apache

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| [ post method ] | [its alert about post method ] | [2] | [4] |

**JUSTIFICATION: [ based on the logs if there is more then 4 events it should alert ]**

# Dashboards—Apache



# Attack Analysis

# Attack Summary—Windows

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

- there has been a lot happening , there  was big amount of attempts made to reset passwords, and also successful logins, deleted accounts , new log on assigned special privileges. and the deleted users were recreated and this part kind makes me think there is an insider that is helping the attackers, the first question is that how they knows what are the usernames? then they can attempt to login in to it or reset its password.

# Attack Summary—Windows

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

- the thresholds made arent correct if they were they would alert and those events would be stopped like the big volume of successful logins , deleted accounts…

# Attack Summary—Windows

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

- there is big volume of events happened that dosnt make sense at all. like deleted accounts, which then they recreated. the highest attempt made to reset the password was on user_k, user account that was locked out which user_a was locked the most which create a confusing question who unlocked the account ? means if a an account is locked it should at least stay locked for 1-2 hrs or even until its unlocked by an admin.

# Screenshots of Attack Logs

**[Optional: Place images that illustrate attack findings here.]**

# Attack Summary—Apache

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

- [there was high valume of POST request method  which is used for logging in , that means that there was a big volume of login attempts , a new country has been connecting to the server and its Ukraine  ]

# Attack Summary—Apache

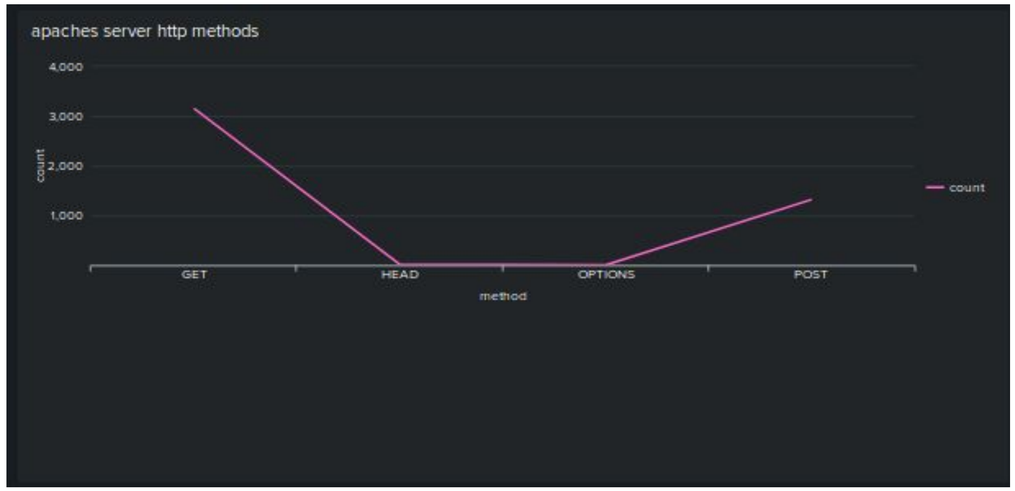
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

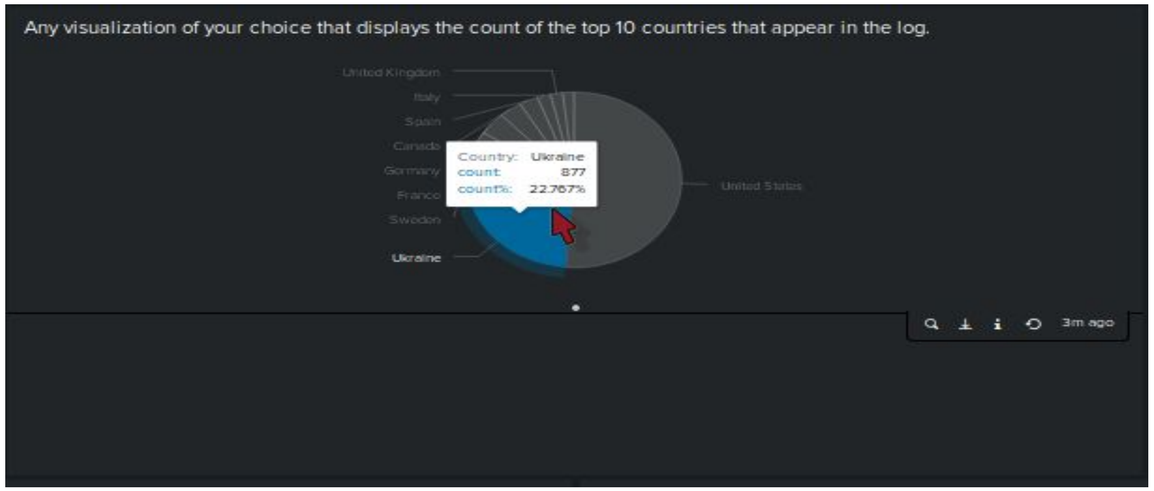
- [ no the threshold were not correct if they were , they would alert and the attack would be stopped  before it happened  ]

# Attack Summary—Apache

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

- [high valume of POST method , most of the traffic is coming from US, and then its UKRAINE which isnt normal  ,most visited URI which /VSI_Account_logon.php  ]



# Project 3 Summary

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

  [ high volume of successful logins , deleted accounts and then they recreated high volume, given special privilege to new logons, high volume of rest password  , alot of traffic coming from UKRAINE ,  potential brute force… ]

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

  [ there should be lockout account mechanism, and also monitoring , if we see there is high volume of attempt to rest a password on a account , we look at that account to see if someone will be able to login with it , if logged in we will disable that account  ]

# Summary and Future Mitigations

# Summary and Future Mitigations

for windows we need a good account lockout mechanism if there is an account tried to reset its password more 3 times , it should lock the account and it should lock until the admin unlock it. and with apache server must be patched and update all the time