Defensive Security Project
by: Elisabeth Alfaro and Ralph Brecio

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- VSI has obtained reliable information suggesting that JobeCorp, a competitor, might be preparing to carry out a cyber assault that could adversely affect VSI’s daily operations. In response, the SOC management team diligently evaluated several SIEM tools and ultimately chose Splunk as their preferred solution based on its functionalities.
- To prepare for the suspected attack, the selected tool, Splunk, was utilized to establish a baseline of the existing environment. This involved generating reports and configuring alerts that would promptly notify the SOC team of any breaches surpassing predefined thresholds.
- The baselines created for the current environment will serve as benchmarks for evaluating the efficacy of the alerts and identifying the specific type of attack that triggers the notifications.

Number Display

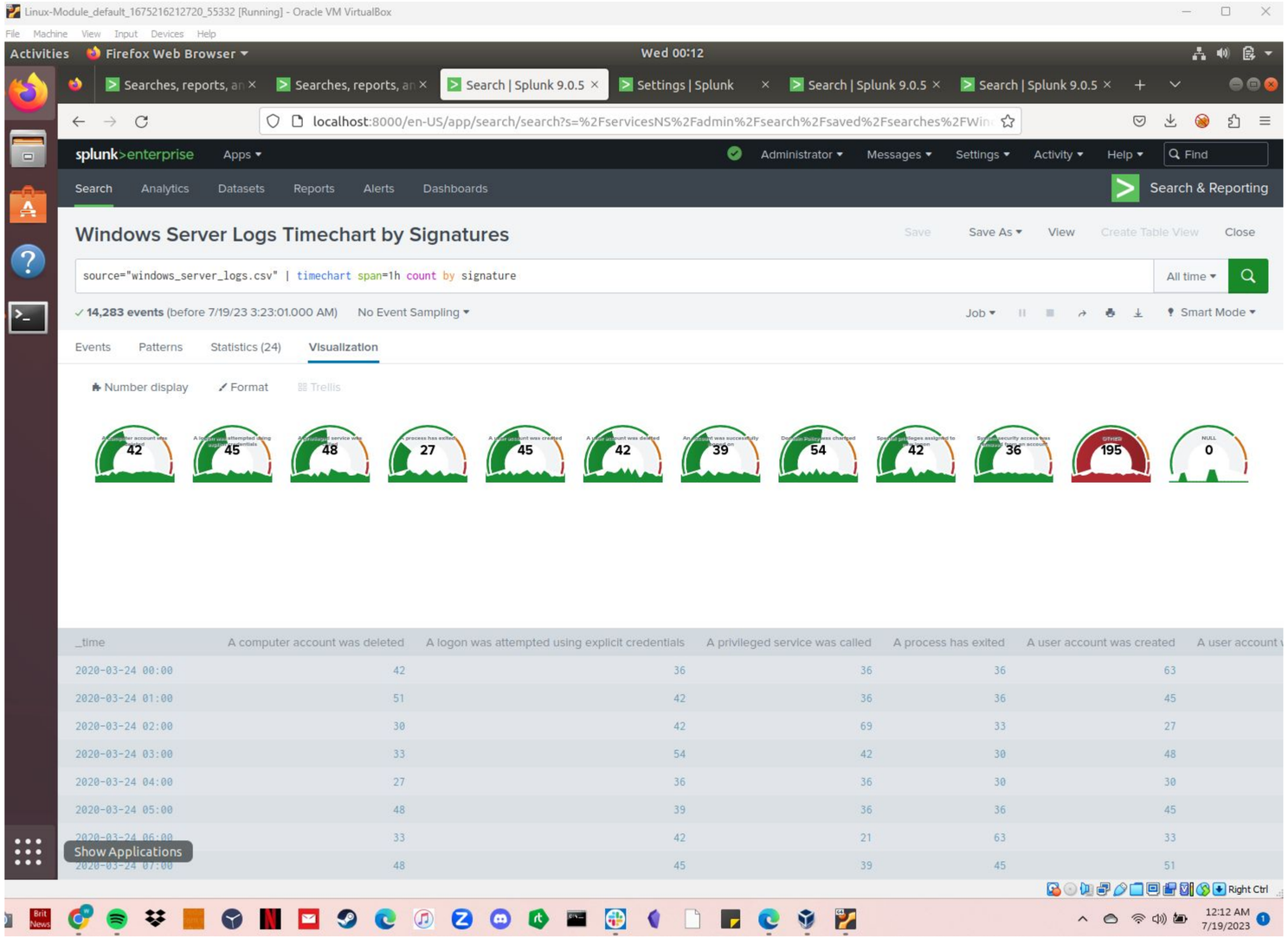
Number Display Viz

A number display add-on in Splunk can be useful for visualizing and presenting numerical data in a clear and concise manner. Number displays allow for the aggregation and summarization of numeric data, making it easier to understand key metrics at a glance. It can provide a quick snapshot of important figures such as total sales, revenue, or customer counts.

Number Display Viz

Number displays provide a visually appealing way to present numeric data, enhancing the overall reporting experience. Users can customize the display format, colors, and styles to suit their preferences or match their organization's branding.

Number Display Viz



Logs Analyzed

1 Windows Logs

Windows_server_logs and windows_server_attack_logs were analyzed thoroughly to identify suspicious activities such as successful and failed logins, suspicious user accounts, deleted user accounts and to check the effectiveness of setting up an alert.

2 Apache Logs

Apache_logs and apache_attack_logs were analyzed and really focused on reviewing HTTP methods to try to determine the origins of the attacks and their overall impact.

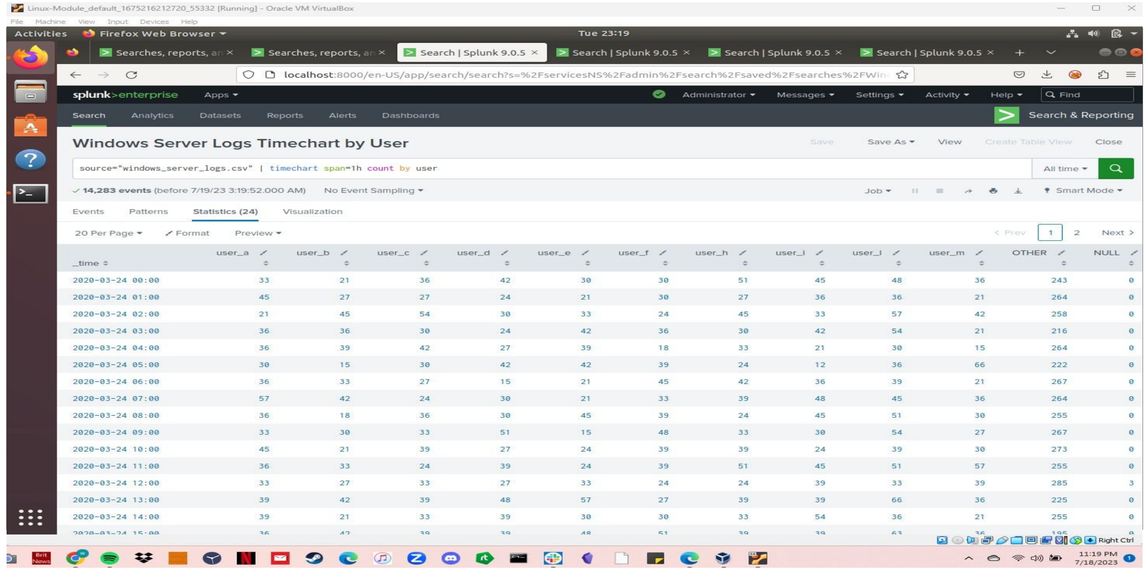
Windows Logs

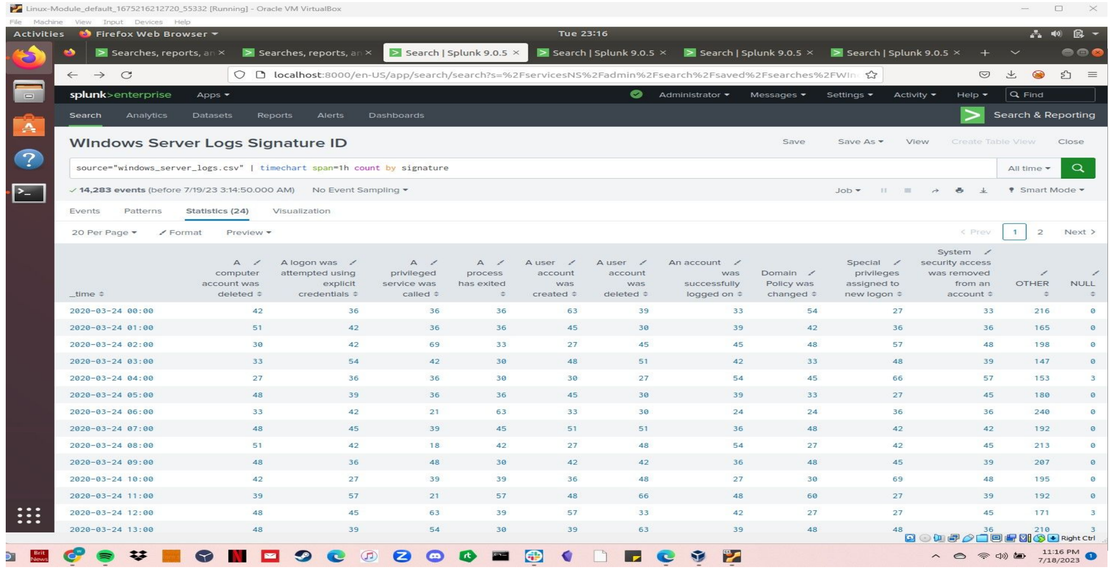
Reports—Windows

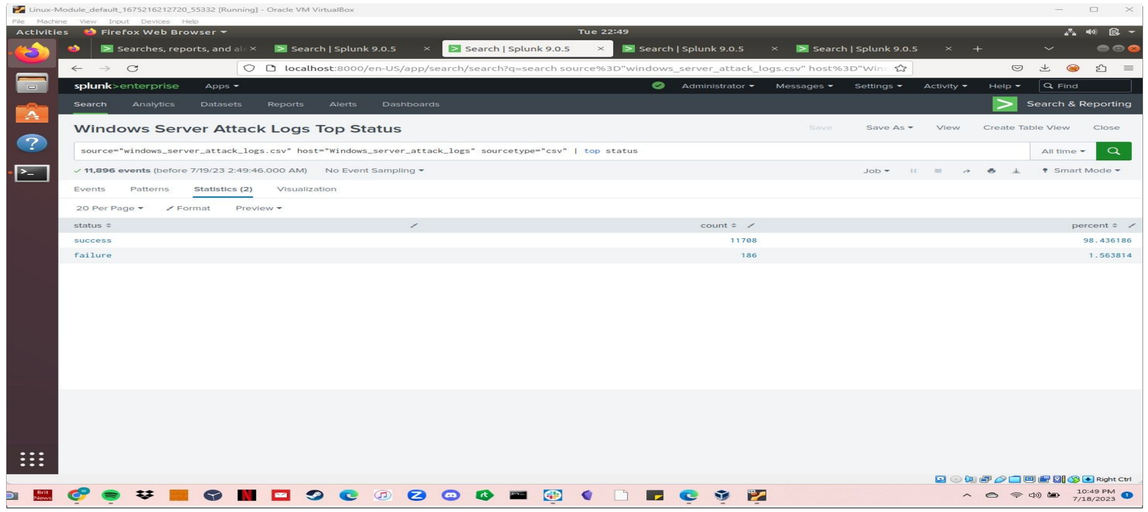
Designed the following reports:

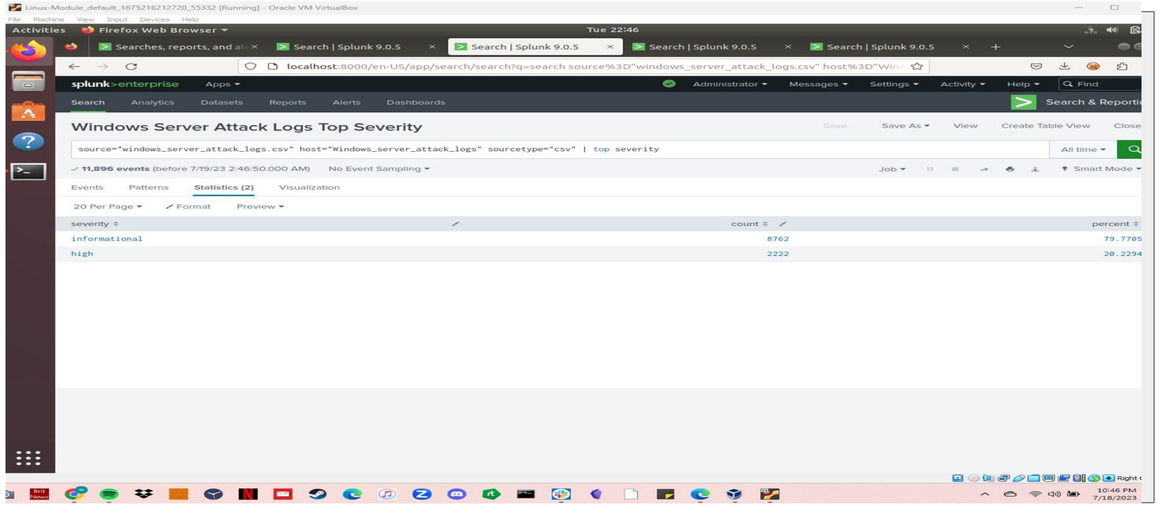
Report Name	Report Description
Windows Server Logs Top Severity	Shows the count and percent of the severity
Windows Server Logs Signature ID	Shows signatures with associated Signature ID
Windows Server Logs Top Status	Shows the count and percent of the successful and failed windows activities
Windows Server Logs Timechart by User	Shows the number of events of each user that occurred per hour in windows

Images of Reports—Windows





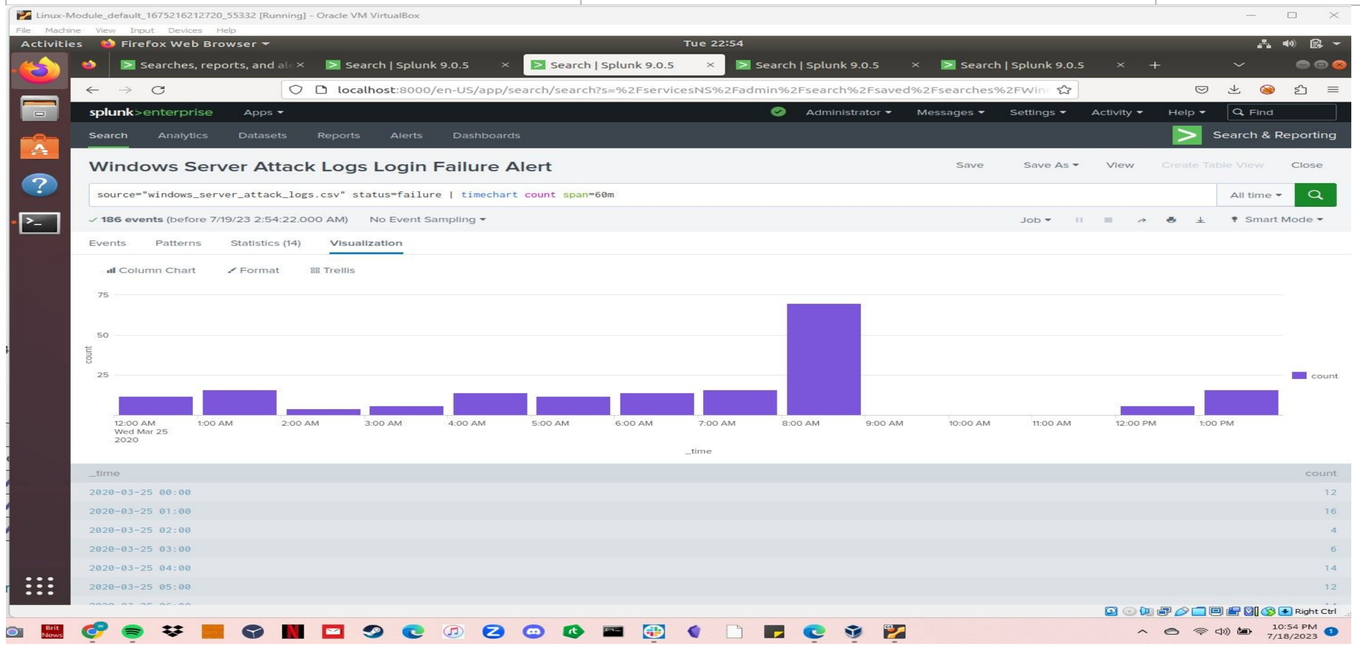




Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Server Attack Logs Login Failure Alert	Triggered by failed windows activity and reported hourly	5	>20

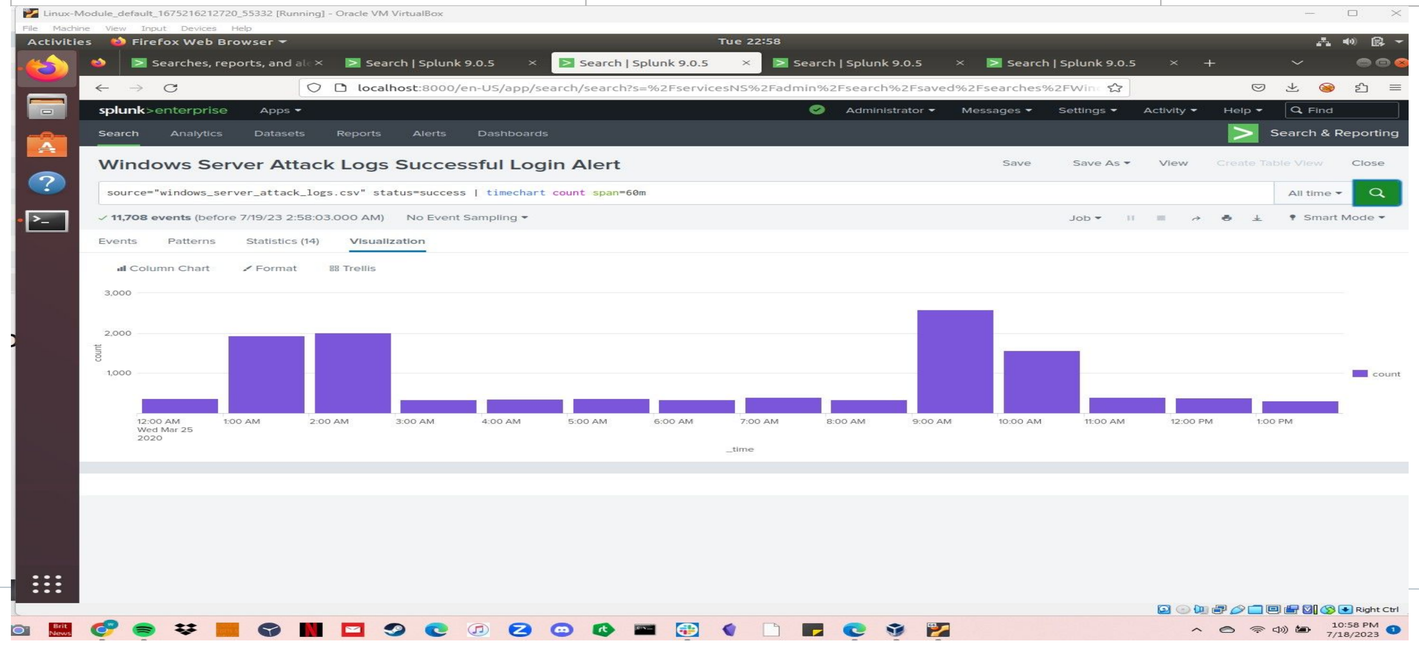


After reviewing the alerts I was able to come up with a baseline of 5 alerts per hour and a threshold of 20 alerts per hour that would make this alert effective while not spamming the SOC team

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Server Attack Logs Successful Login Alert	Triggered when there is a successful log in on an account when the threshold in met.	10	>30

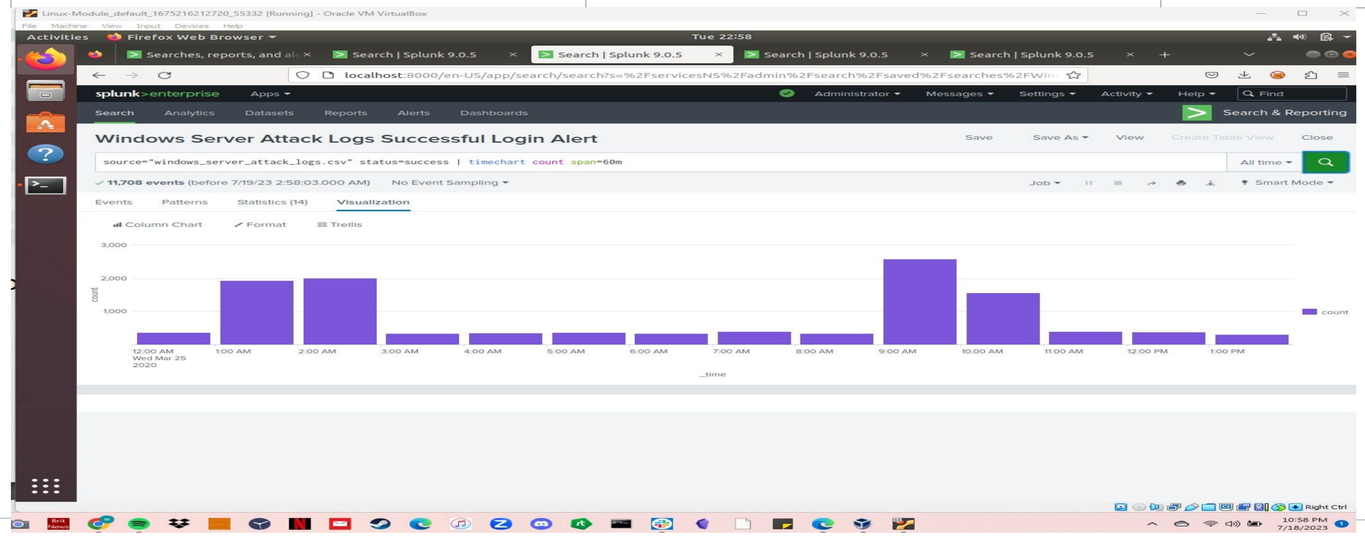


After reviewing the alerts I was able to come up with a baseline of 10 alerts per hour which looked very consistent and a threshold of 30 alerts per hour so it wouldn't spam the SOC team and would only go off when there is a suspicious activity.

Alerts—Windows

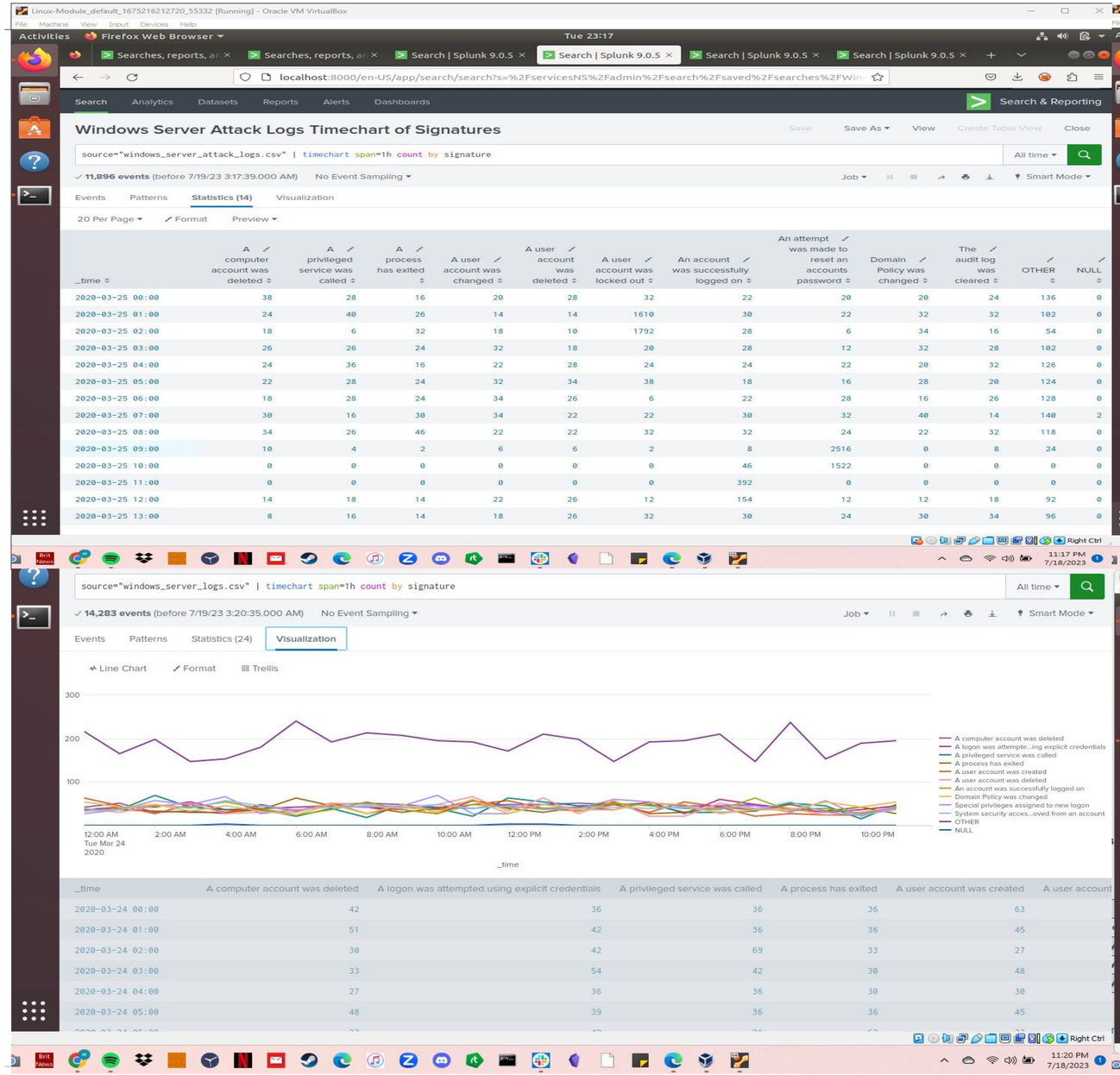
Designed the following alerts:

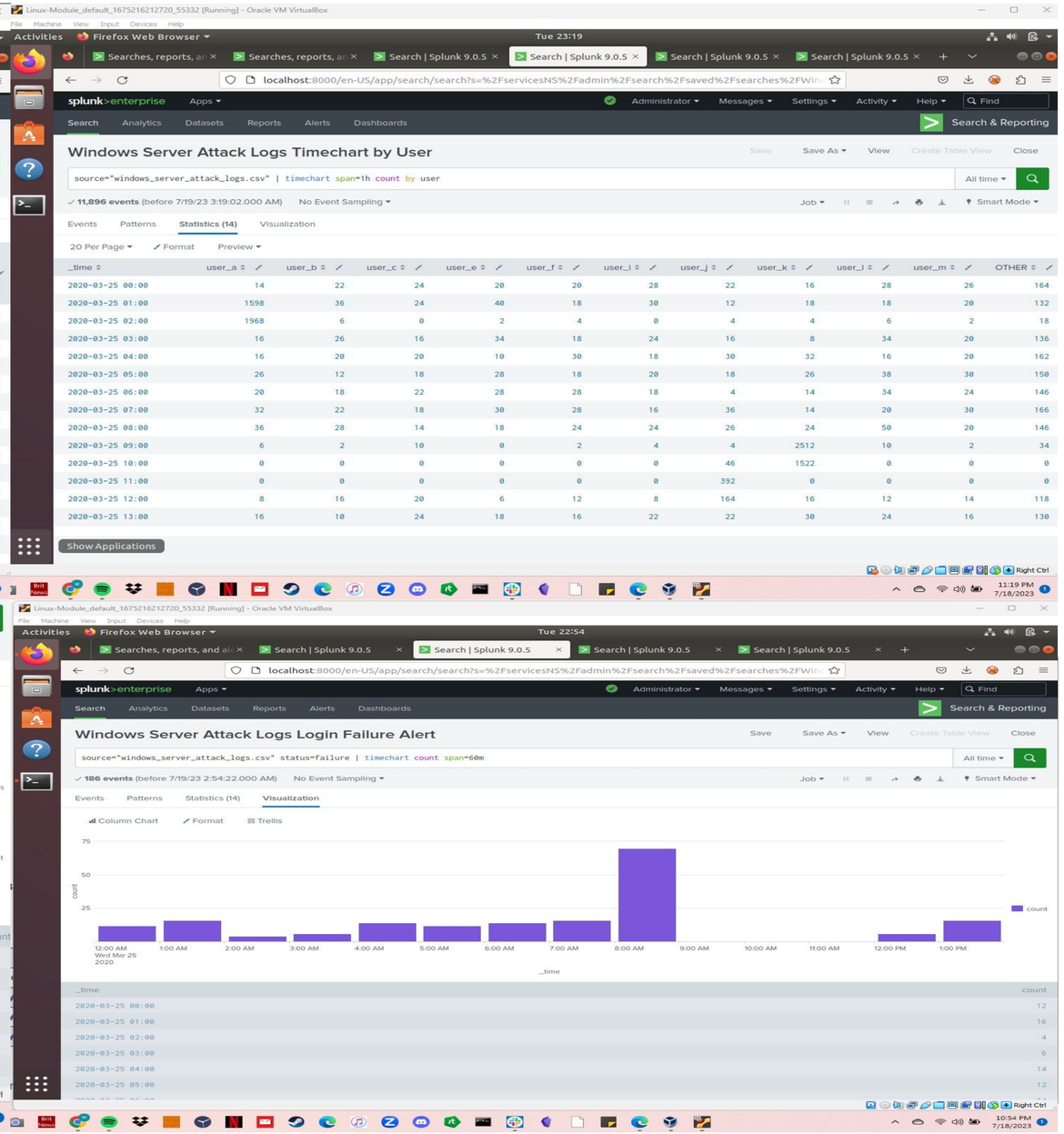
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Windows Server Logs Successful Login Alert	Triggered when there is a successful log in when the threshold is met and is reported hourly	10	>30



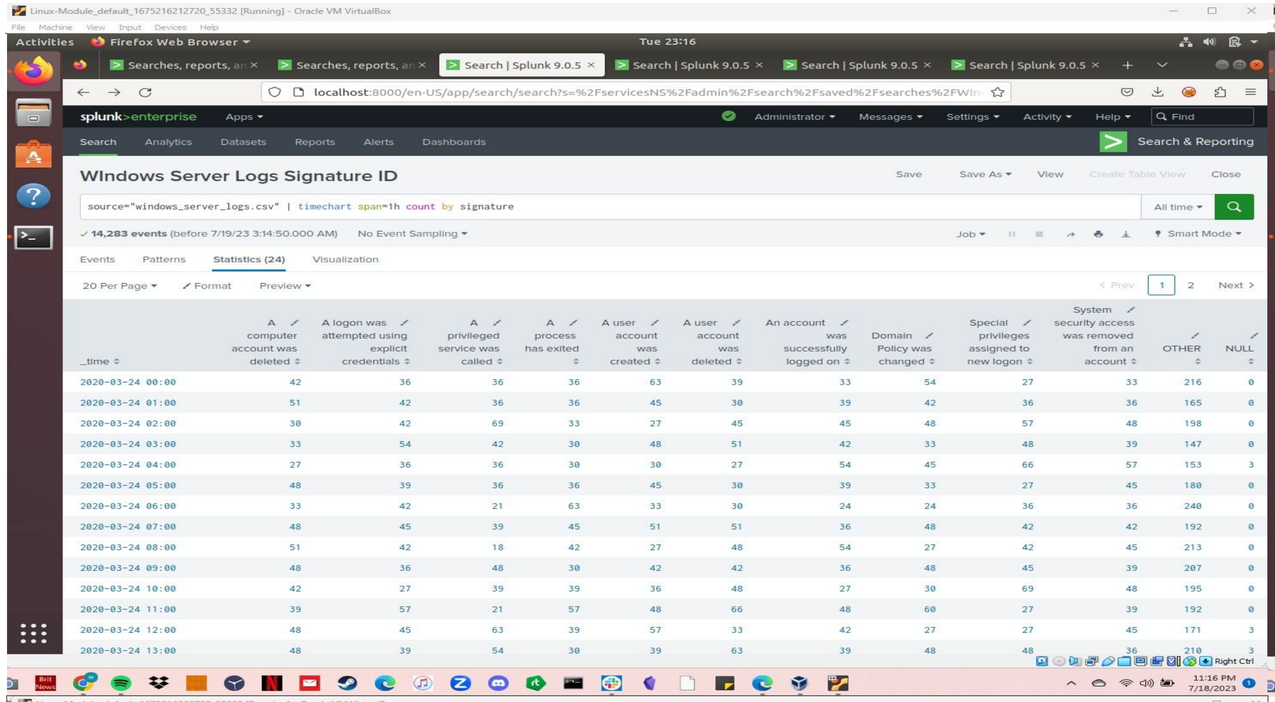
After reviewing the alerts I came up with a consistent baseline of 10 alert and a threshold of 30 successful logins per hour

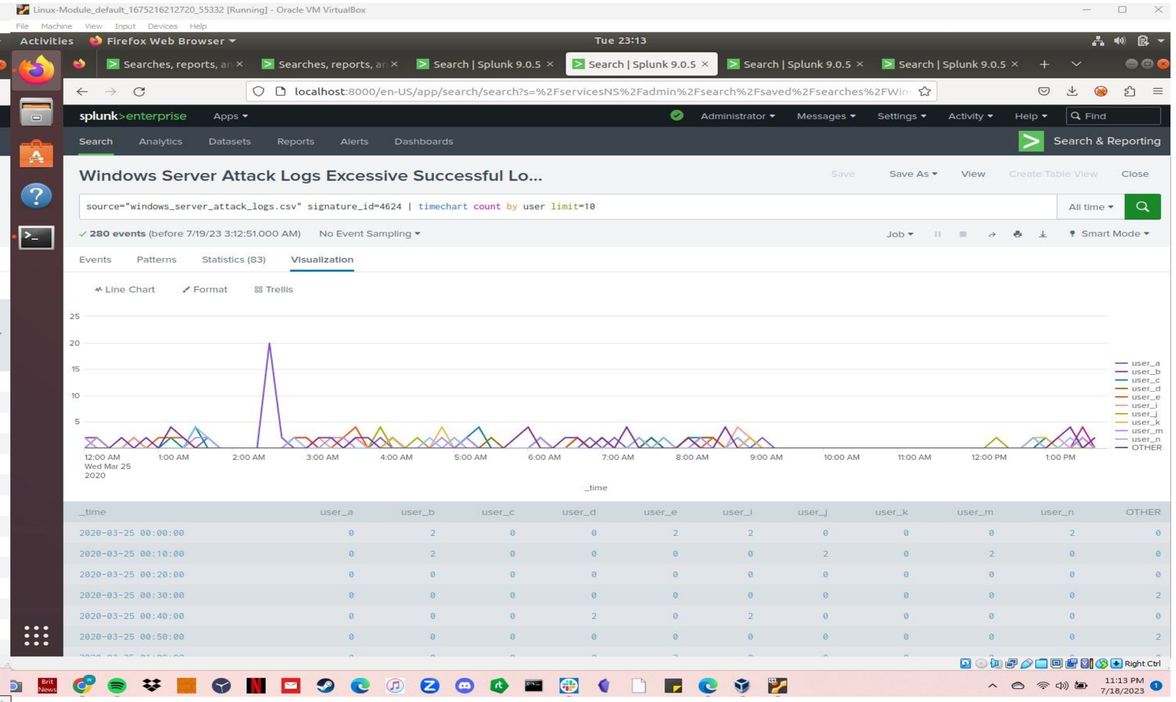
Dashboards—Windows

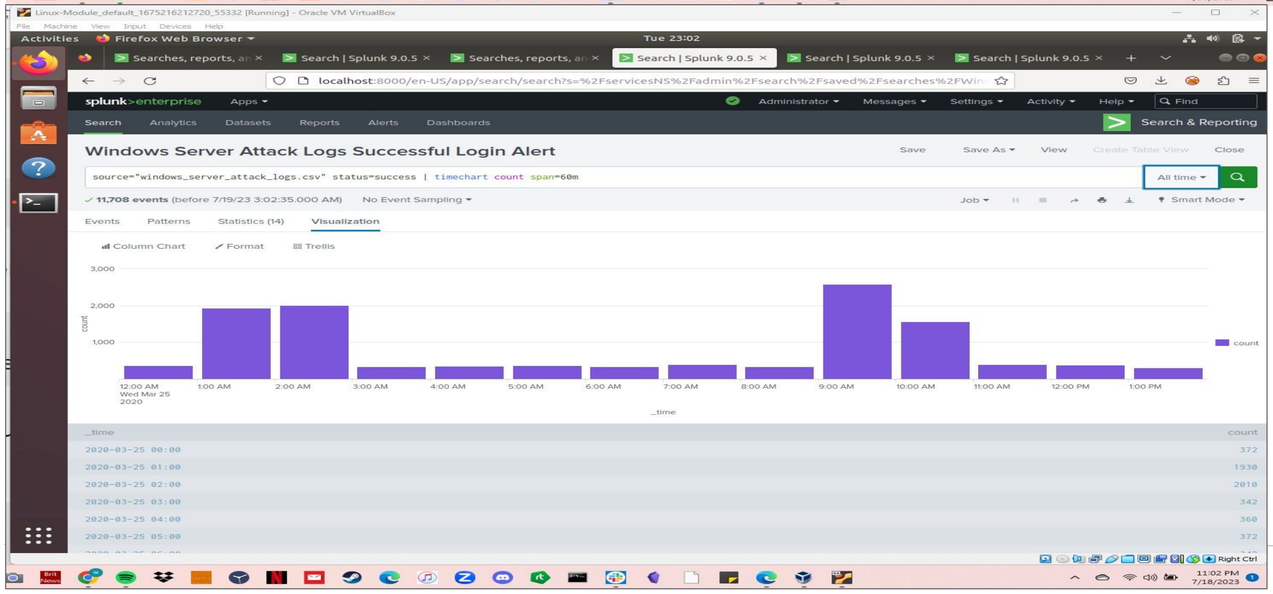


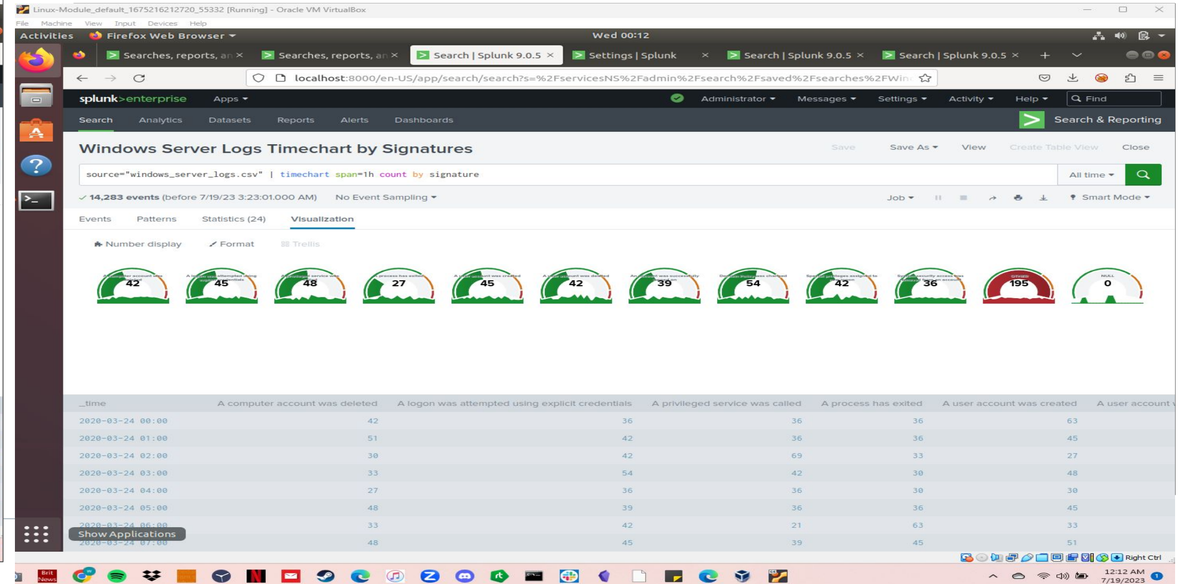


Dashboards—Windows









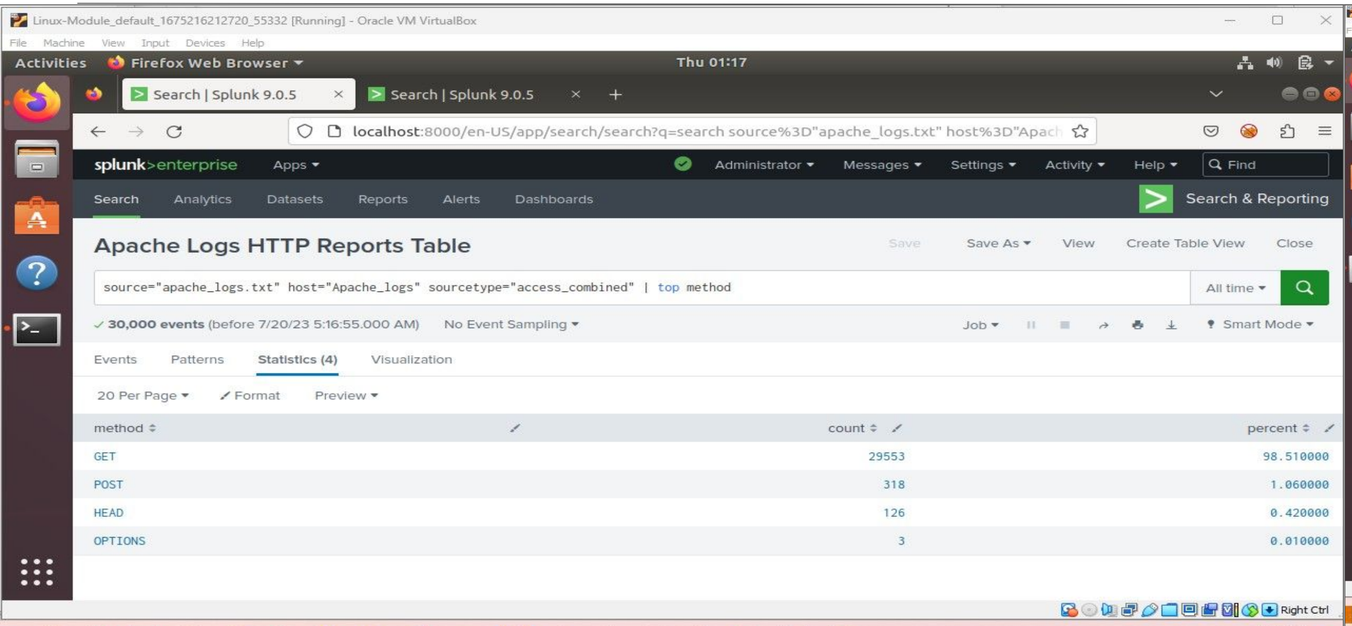
Apache Logs

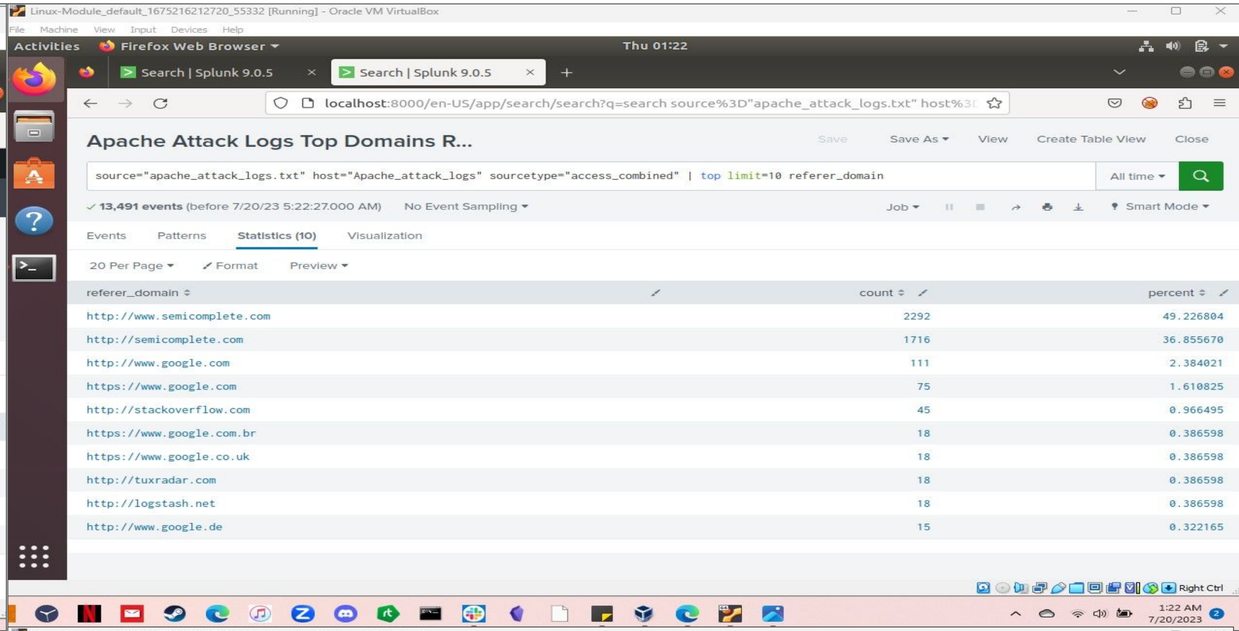
Reports—Apache

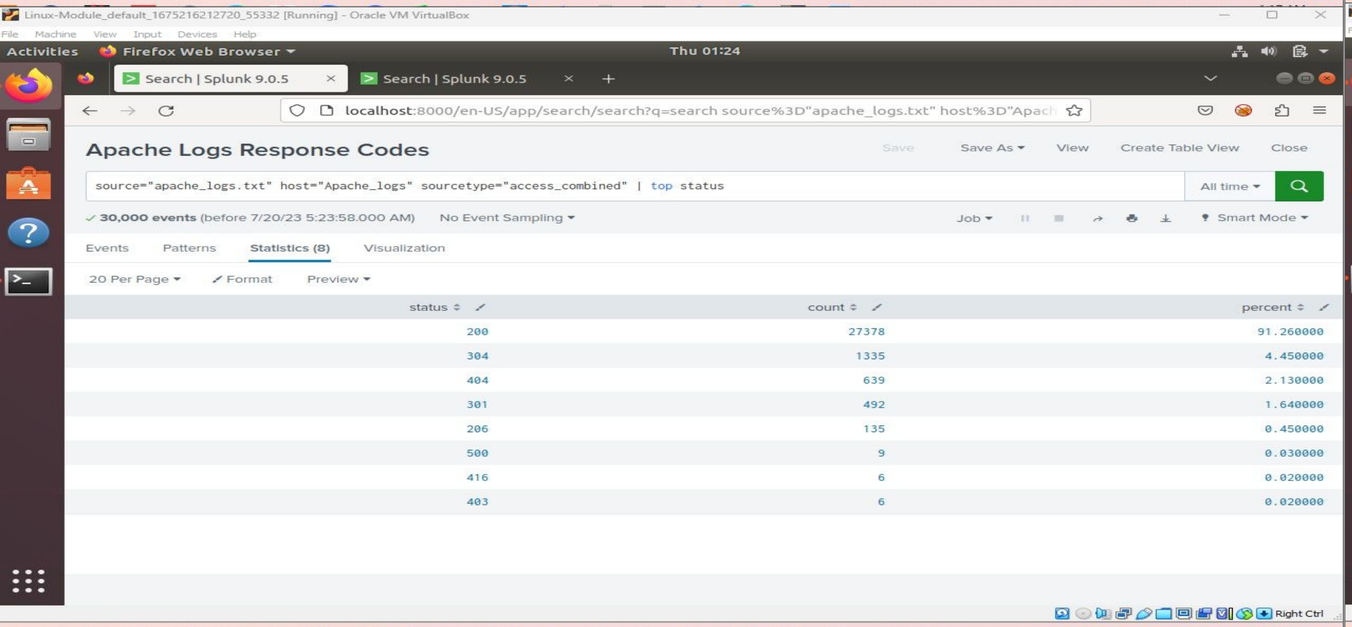
Designed the following reports:

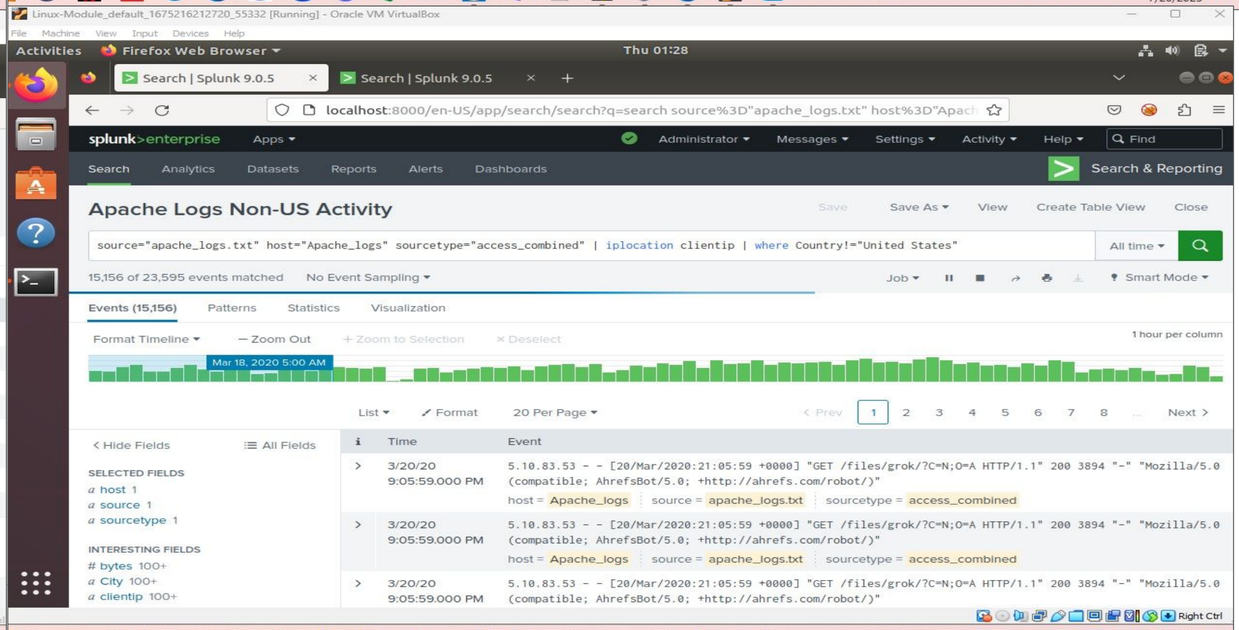
Report Name	Report Description
Apache Logs HTTP Reports Table	Shows reports for methods
Apache Logs Top Domains Referred	Shows reports for referred domains
Apache Logs Response Codes	Shows reports for response codes
Apache Logs Non-US Activity	Shows reports for activities outside of US

Images of Reports—Apache





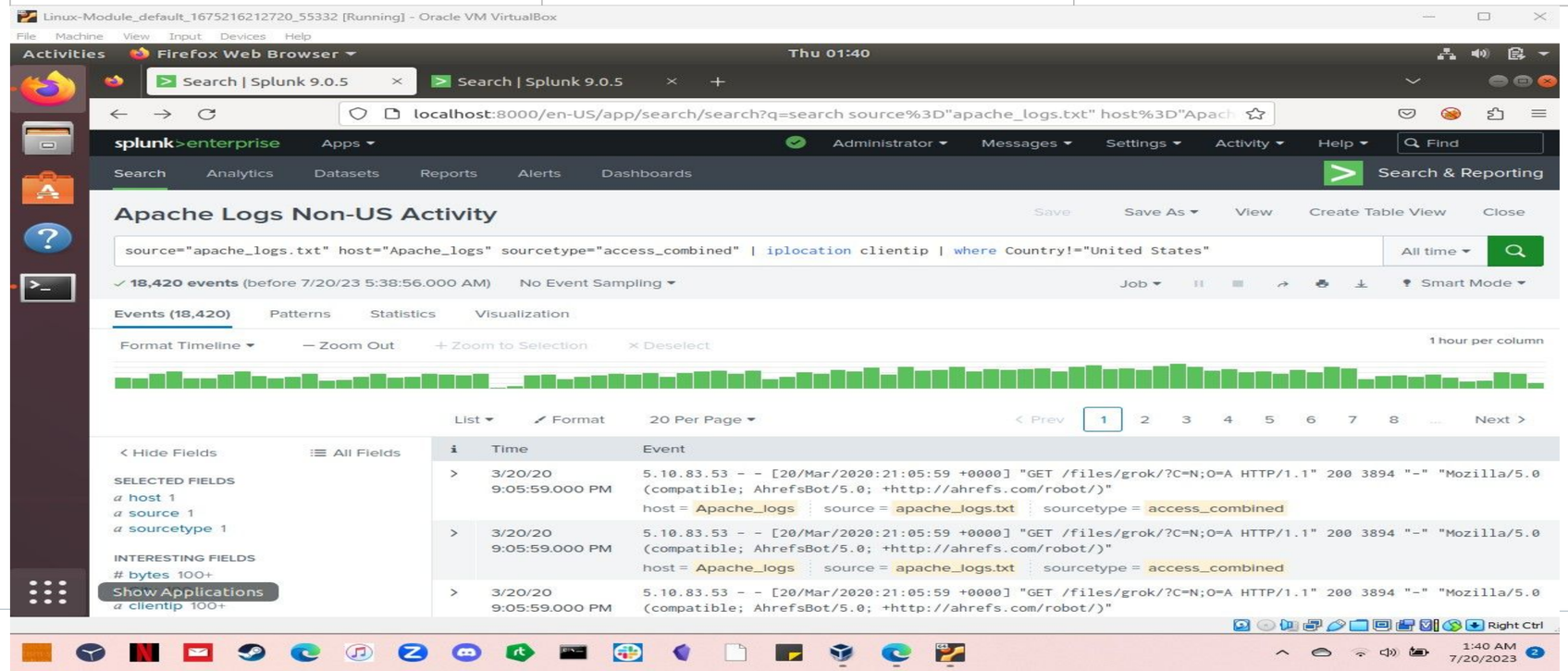




Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Logs Non-Us Activity	Alert for suspicious activities outside of US	150	215

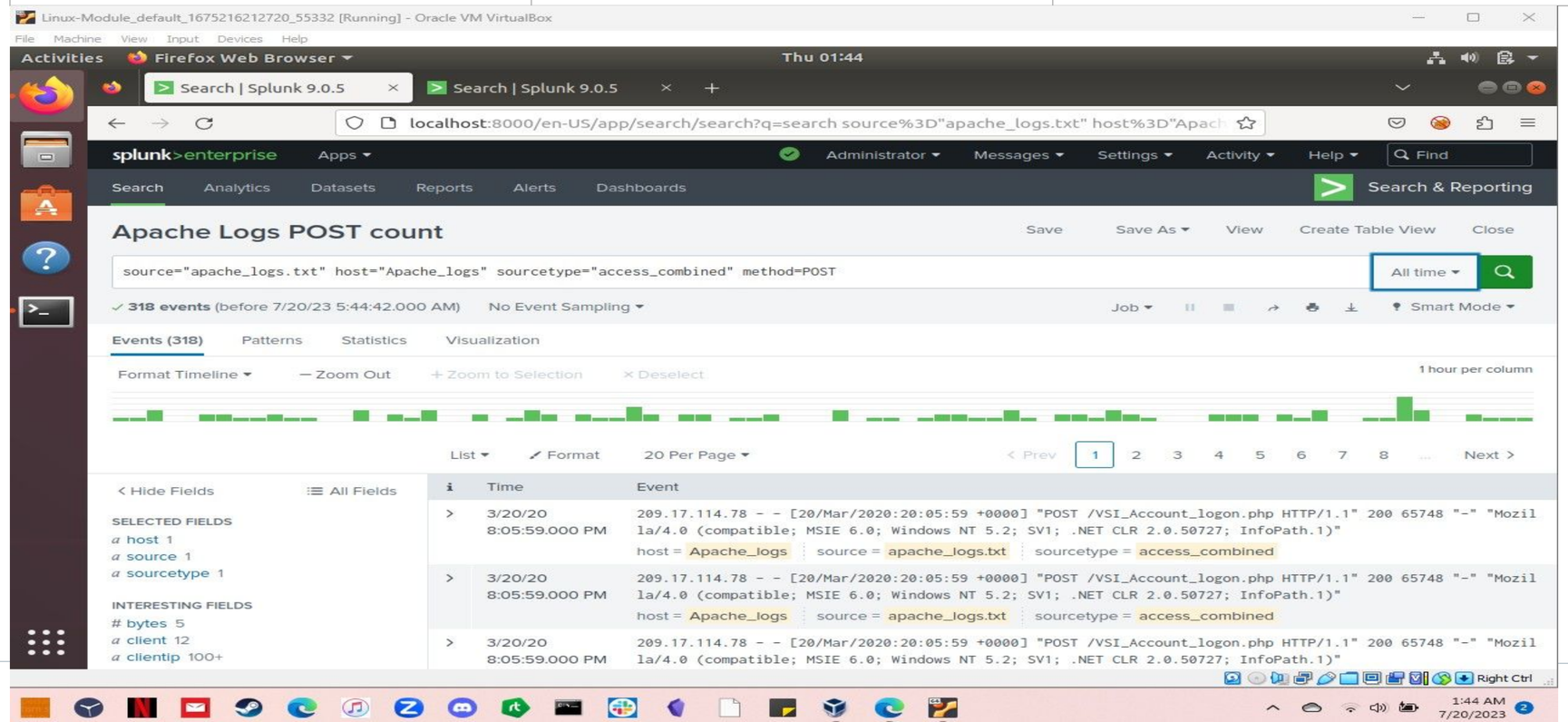


After reviewing the alerts I came up with a baseline of 150 alerts and a threshold of 215 alerts which will notify the SOC team.

Alerts—Apache

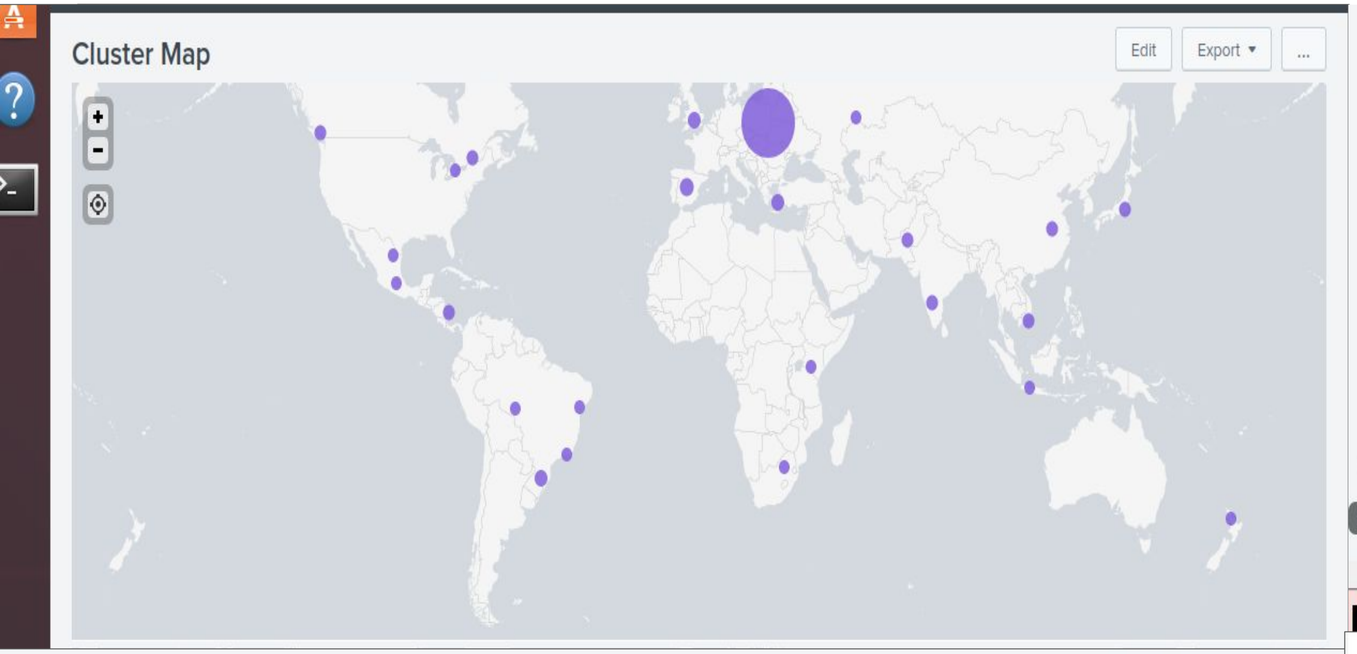
Designed the following alerts:

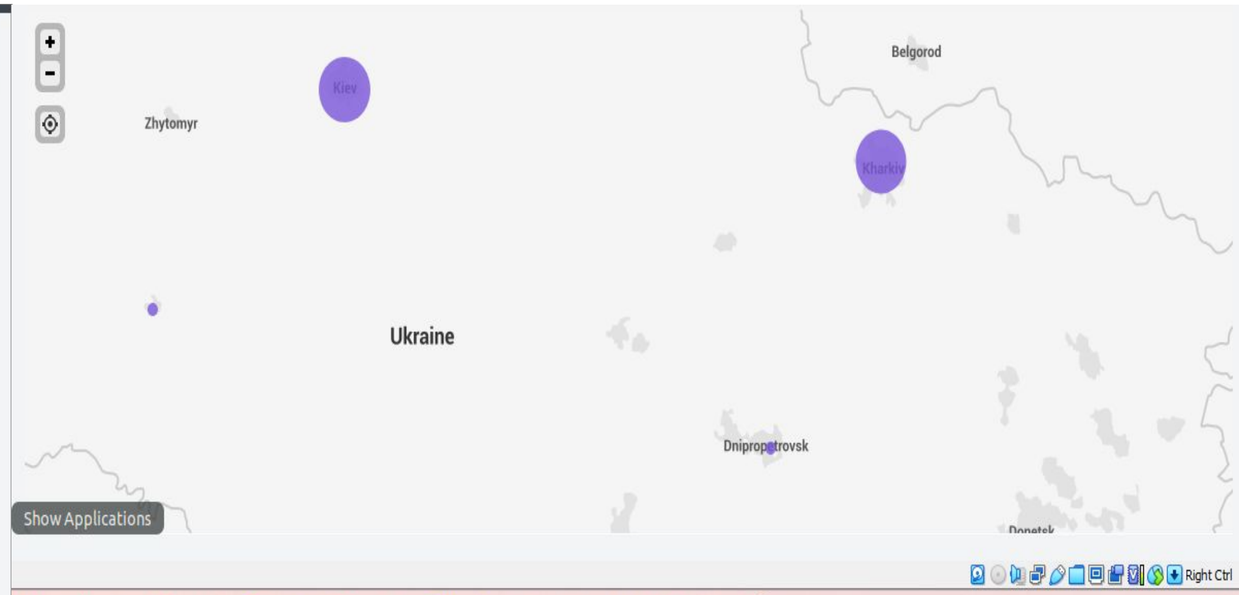
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Apache Logs POST count	Alert of HTTP POST count per hour	11	20

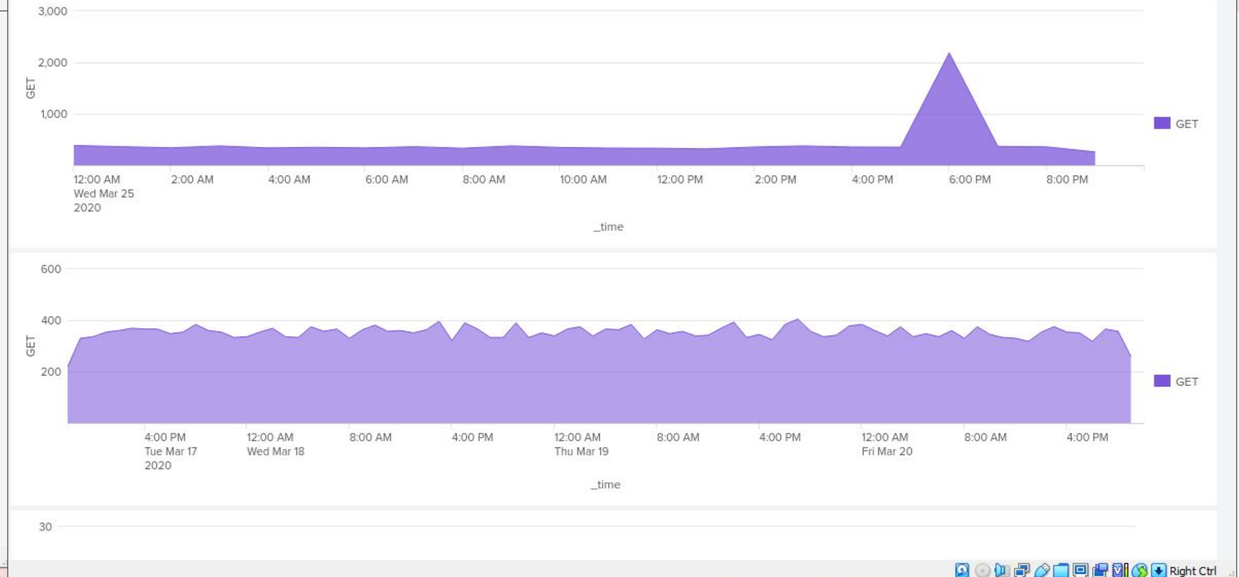


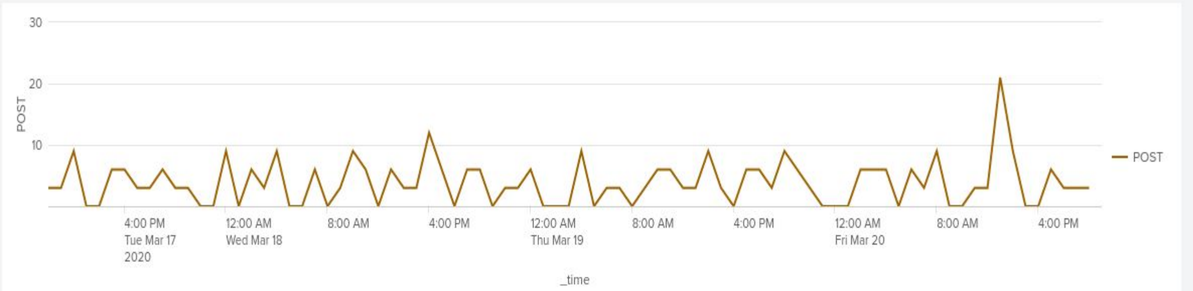
After reviewing the alerts I was able to come up with a baseline of 11 and a threshold of 20 alerts which will notify the SOC team.

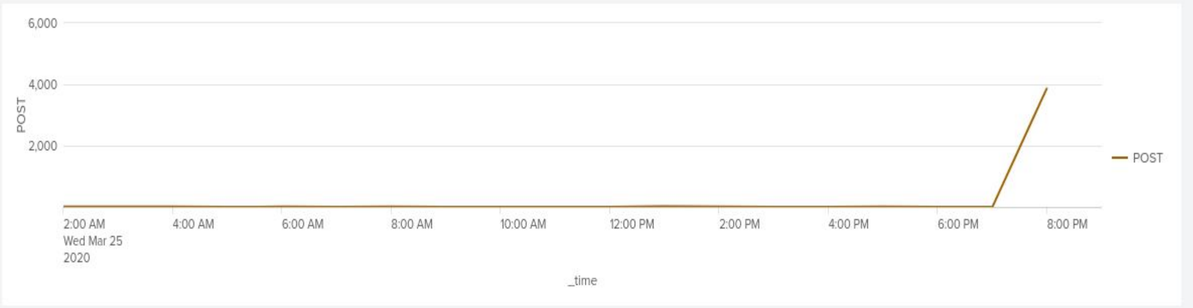
Dashboards—Apache





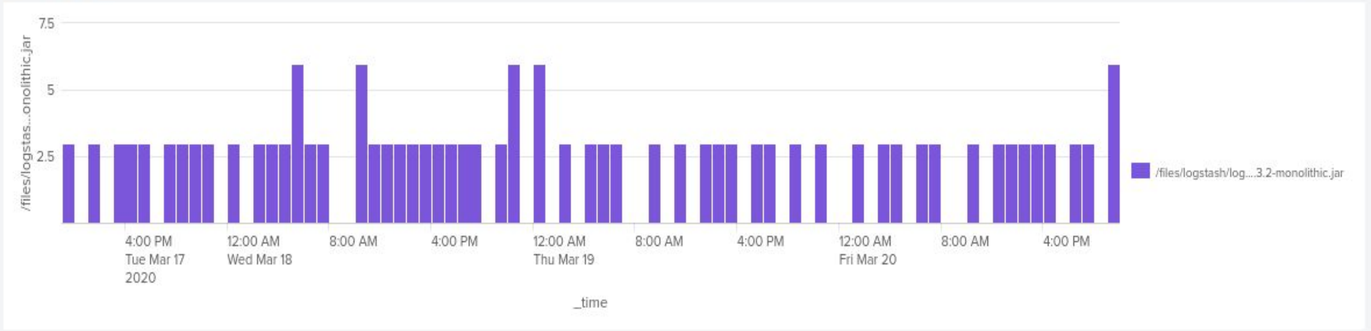


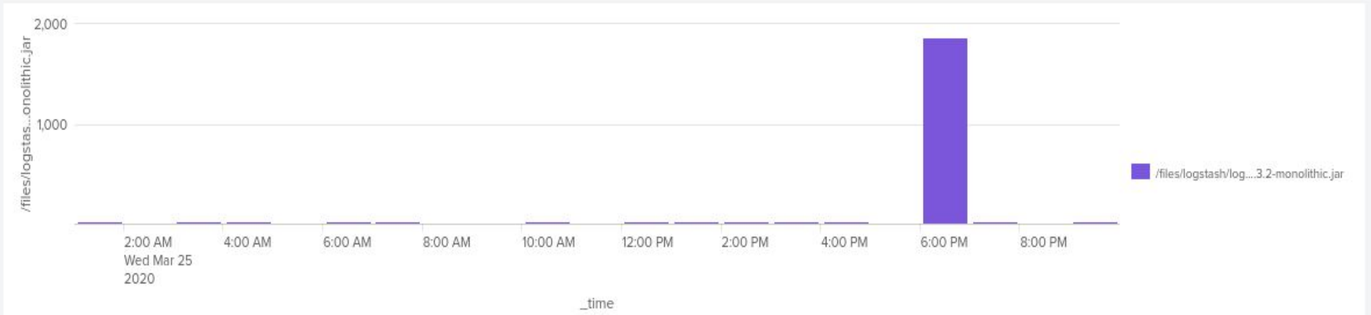


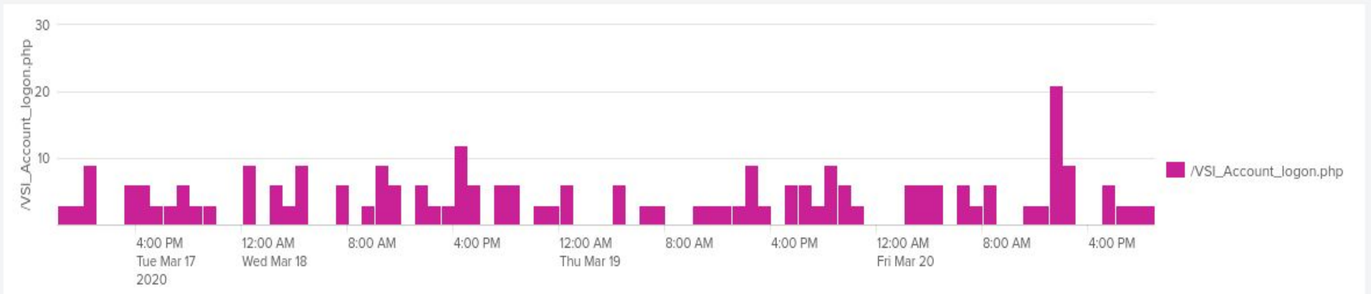


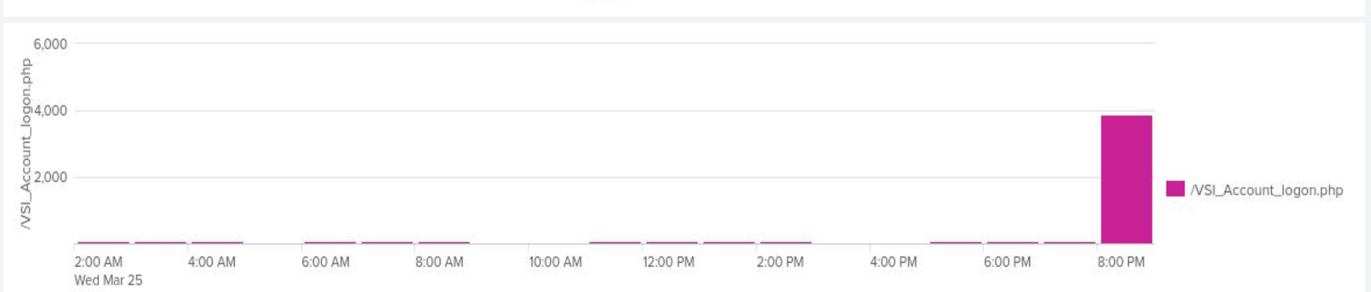
URI Data

Edit | Export | ...









Attack Analysis

Attack Summary—Windows

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

- During the log file analysis, we noticed instances of account deletions and several other activities, such as account creation and modifications with granted access.
- Moreover, some accounts were granted special privileges, and successful logons were recorded. The changes made to account management password policies during the attack raised concerns, warranting further investigation.
- Additionally, we observed excessive user account lockouts and attempted password resets. An alarming discovery was that a user account was deleted during the attack, and the audit logs were cleared. This suggests an attempt by the attacker to cover their tracks. Furthermore, we noticed that special privileges were assigned to a newly created login account after its creation.

Attack Summary—Windows

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

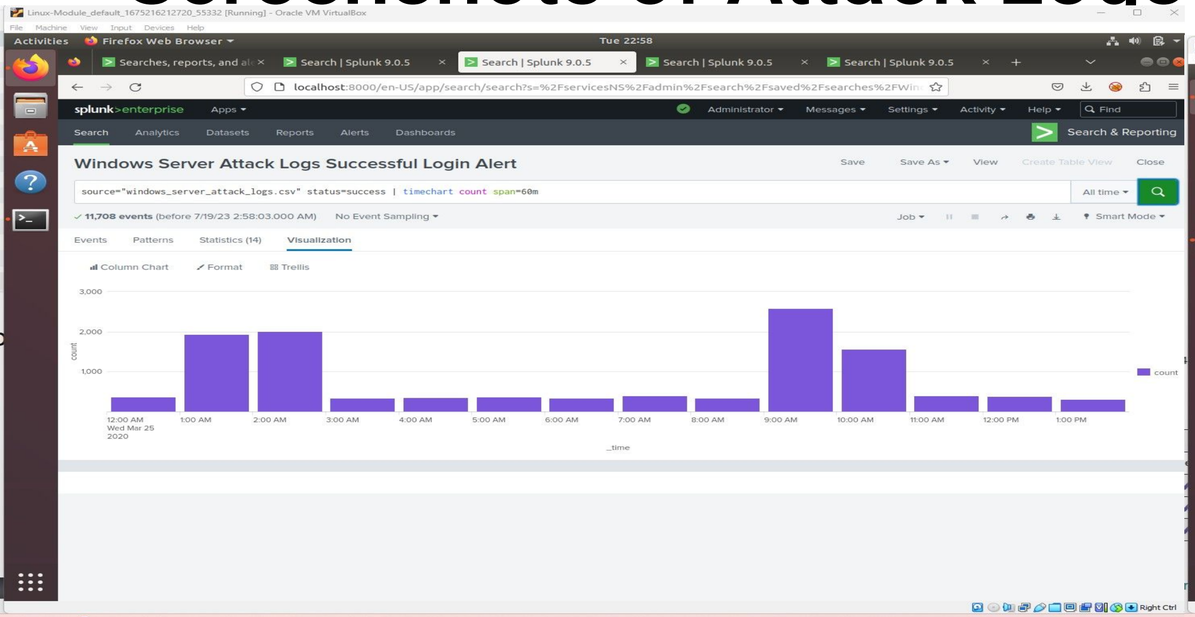
- During the incident, occurring at specific intervals on March 24th and 25th, 2020, the Security Operations Center (SOC) team received notifications about unusual network activities. These activities were identified as multiple failed login attempts, surpassing approximately 35 attempts per hour. The alerts configured in our Security Information and Event Management (SIEM) tool promptly notified the SOC team, as the alert thresholds were set to detect such suspicious behavior. After careful observation, we are confident in the effectiveness of these thresholds and do not intend to make any modifications.

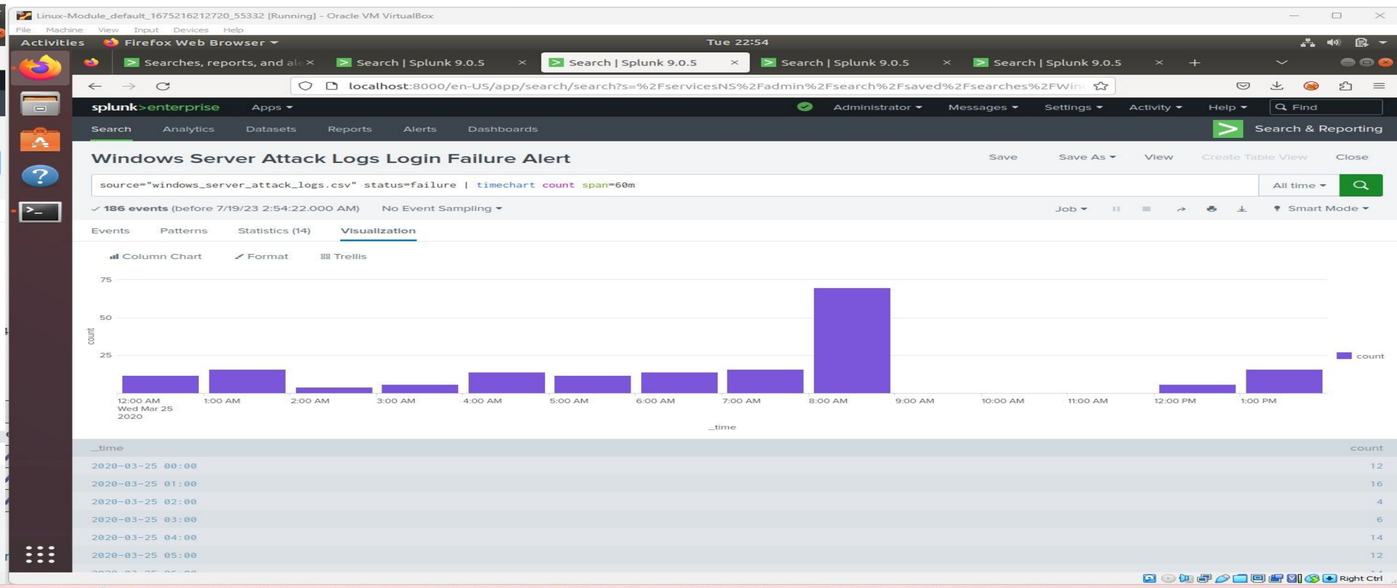
Attack Summary—Windows

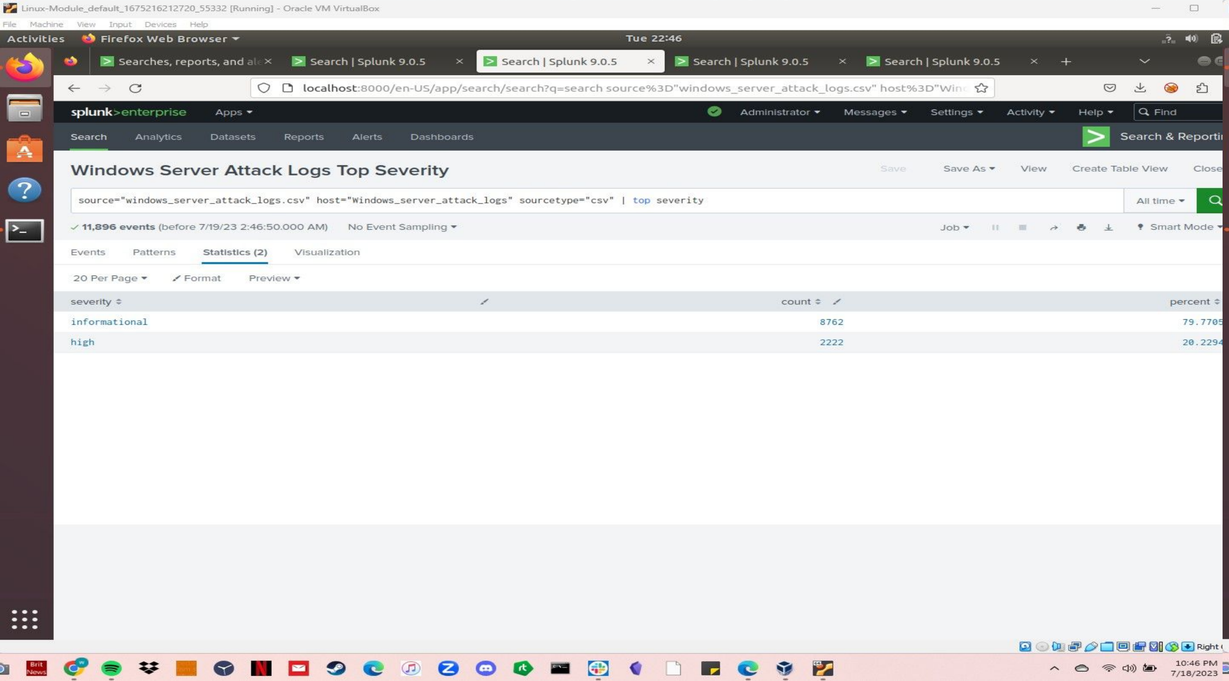
Summarize your findings from your dashboards when analyzing the attack logs.

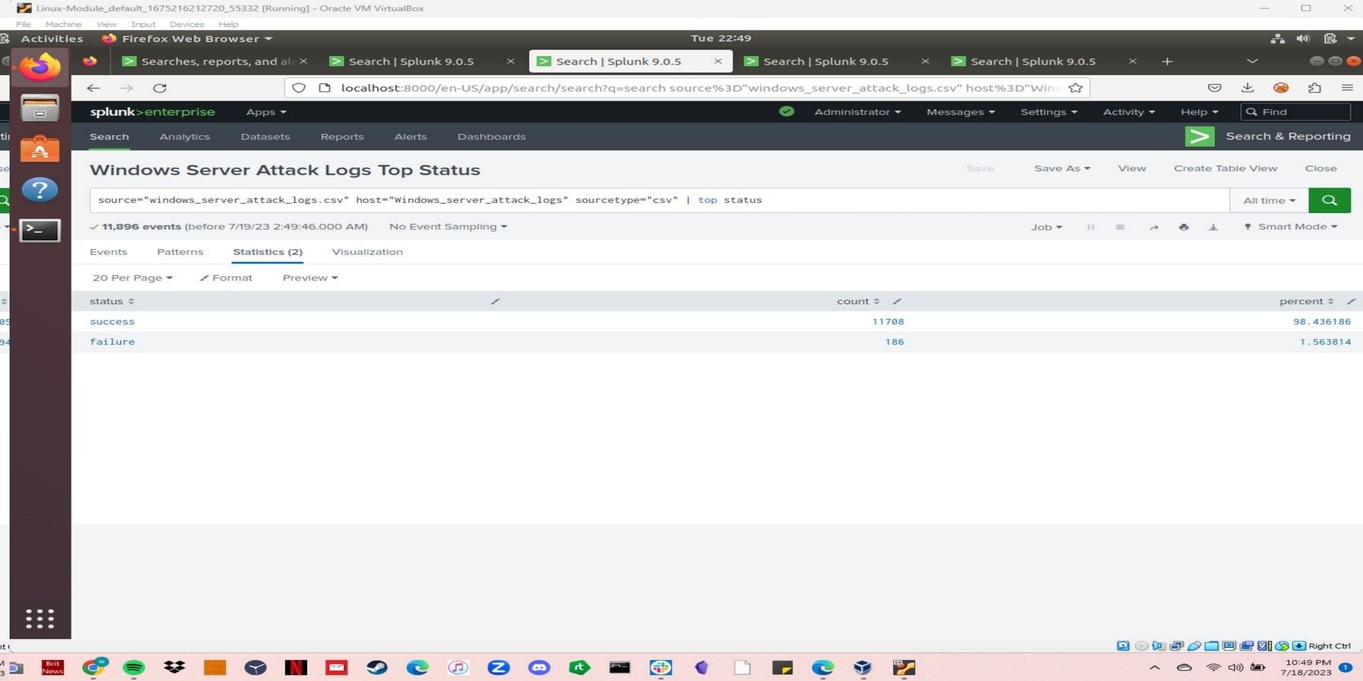
- The comprehensive dashboards provided valuable evidence. Through the reports and alerts, we successfully pinpointed the precise time and date of the attack. Around 8 pm on Tuesday, March 24th, 2020, the attacker exploited the "user_a" account to gain unauthorized access to network resources. The attacker attempted a thousand logins through this specific user, indicating a brute force attack, specifically the credential stuffing technique. The corresponding alert triggered was labeled "A user account was locked out."
- Following the attack, network activity returned to normal until 4 am on Wednesday, March 25th, 2020. During this time, there was a sudden spike in activity under the "user_k" account, with approximately twelve hundred (1200) attempts to change the account password. Such activity at this hour is highly suspicious, as staff members aren't required to be logged in at that time. This evidence strengthens our suspicions that the attacker gained access to the network and was trying to secure a legitimate account that would allow them to later traverse and log in without alerting the SOC team.

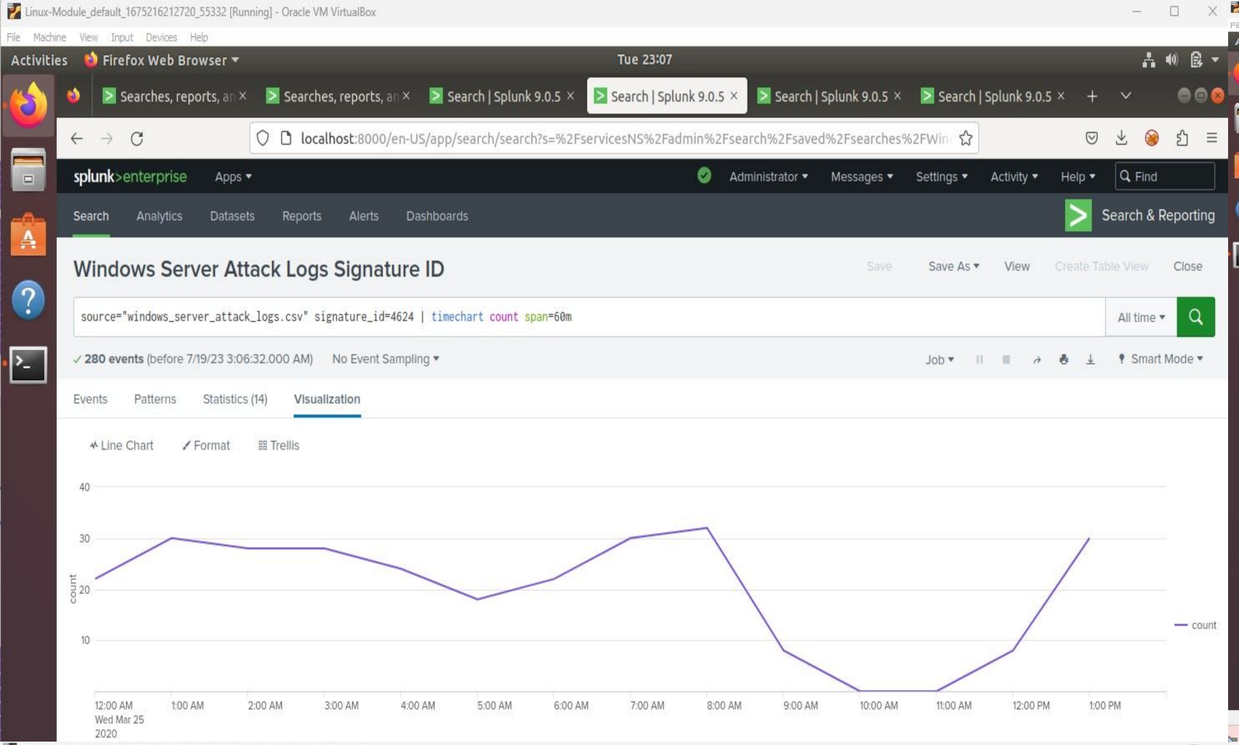
Screenshots of Attack Logs

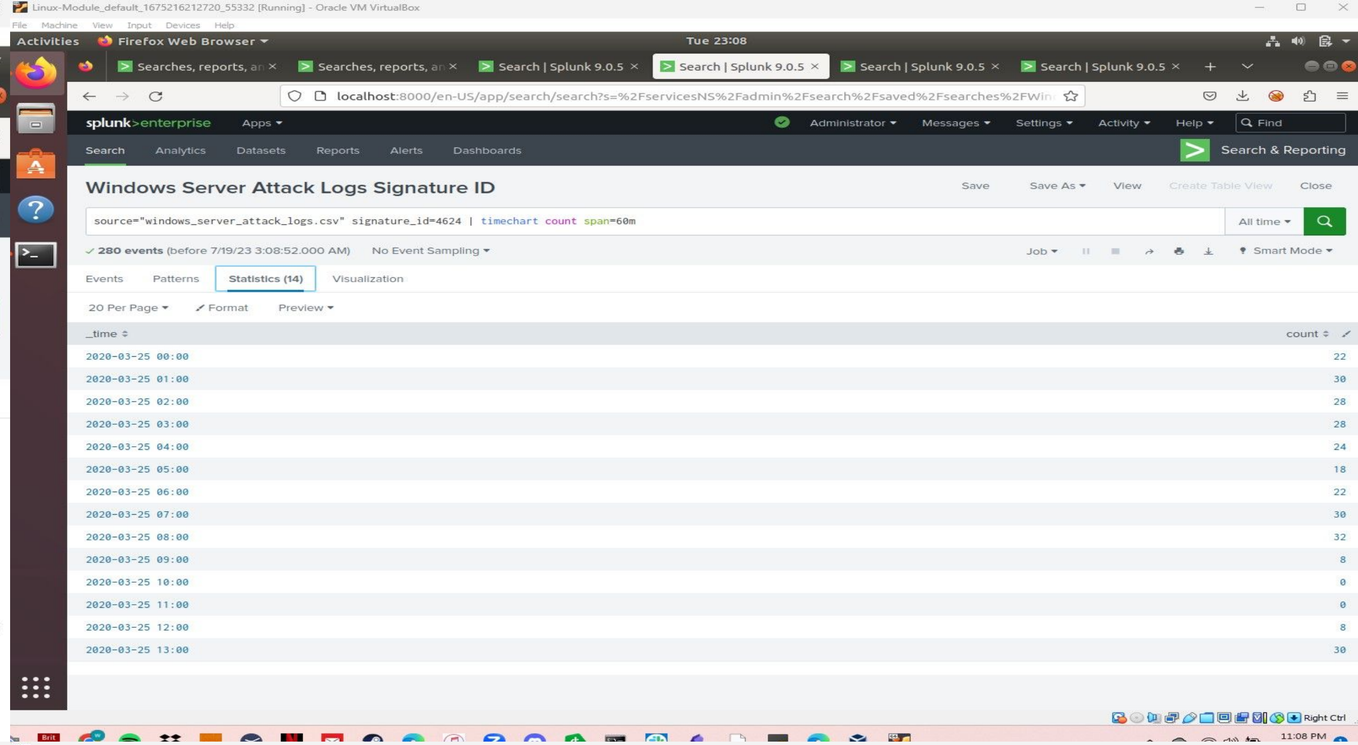


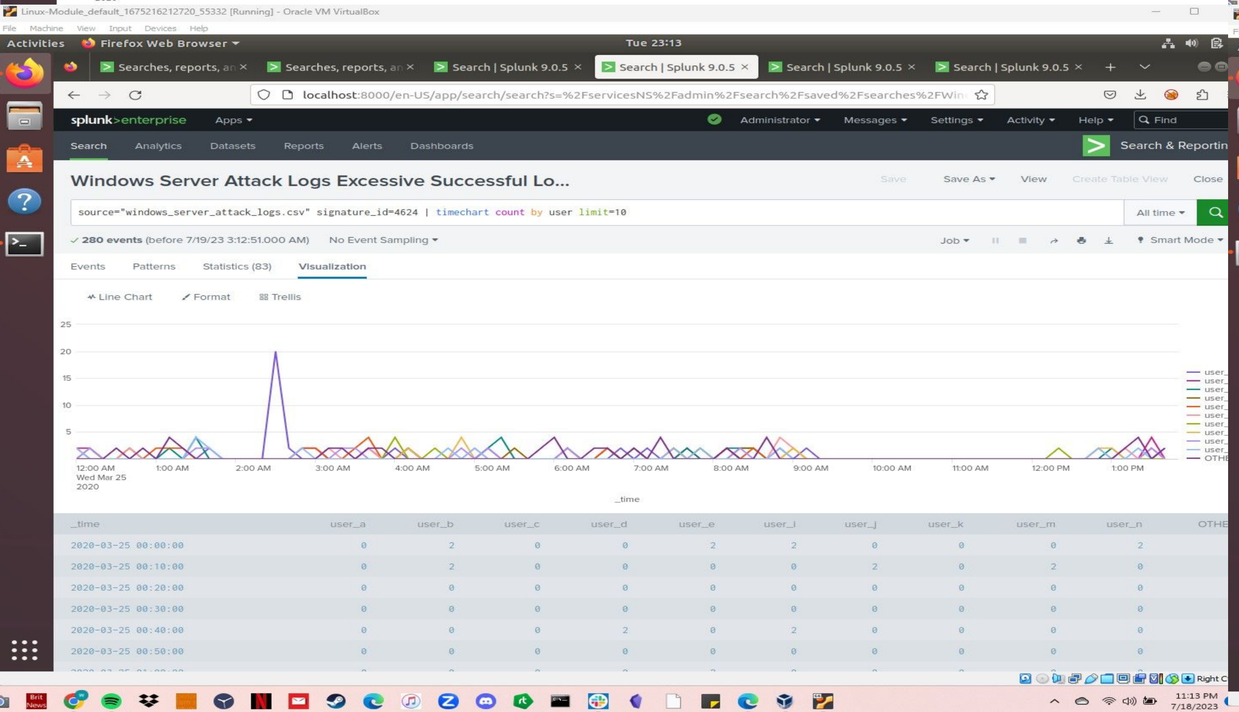


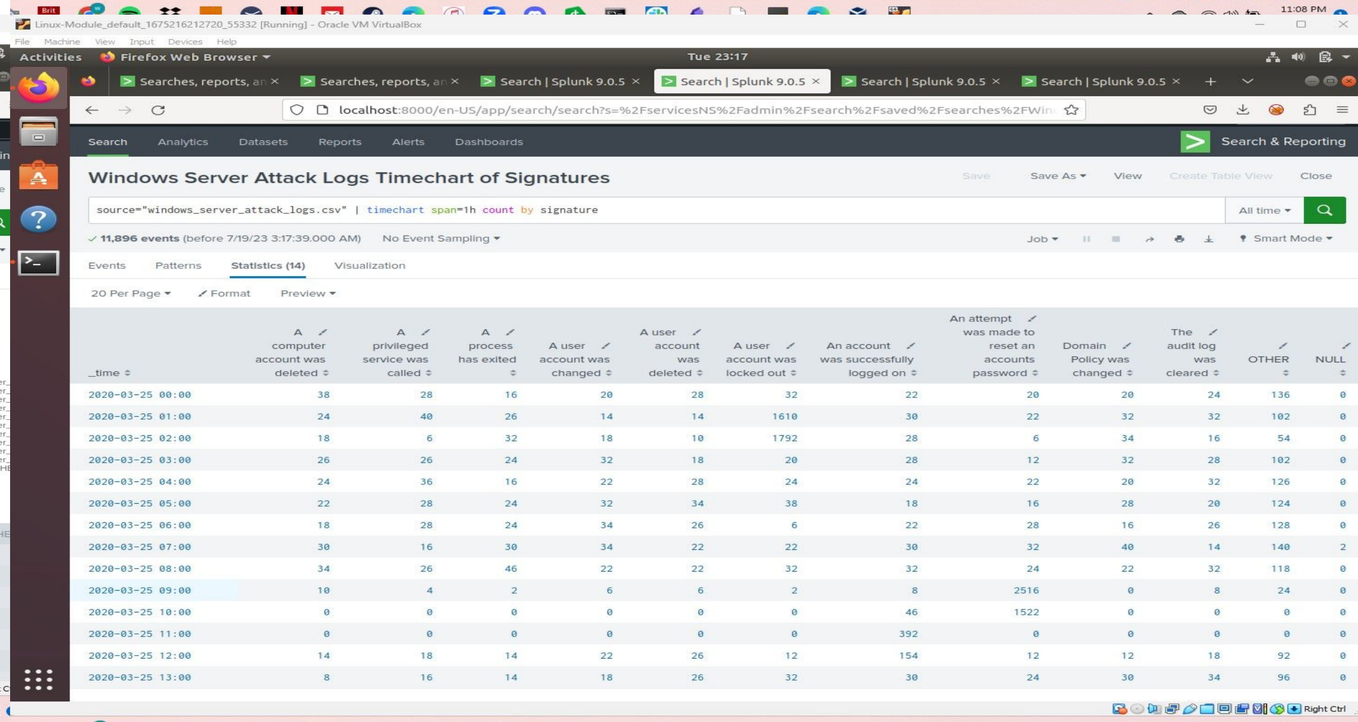





Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Tue 23:07
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Windows Server Attack Logs Signature ID
Save
Save As
View
Create Table View
Close
source="windows_server_attack_logs.csv" signature_id=4624 | timechart count span=60m
All time
280 events (before 7/19/23 3:06:32.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (14)
Visualization
Line Chart
Format
Trellis
count
12:00 AM Wed Mar 25 2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM


Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Tue 23:08
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Windows Server Attack Logs Signature ID
Save
Save As
View
Create Table View
Close
source="windows_server_attack_logs.csv" signature_id=4624 | timechart count span=60m
All time
280 events (before 7/19/23 3:08:52.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (14)
Visualization
20 Per Page
Format
Preview
_time
count
2020-03-25 00:00 22
2020-03-25 01:00 30
2020-03-25 02:00 28
2020-03-25 03:00 28
2020-03-25 04:00 24
2020-03-25 05:00 18
2020-03-25 06:00 22
2020-03-25 07:00 30
2020-03-25 08:00 32
2020-03-25 09:00 8
2020-03-25 10:00 0
2020-03-25 11:00 0
2020-03-25 12:00 8
2020-03-25 13:00 30


Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Tue 23:13
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Windows Server Attack Logs Excessive Successful Lo...
Save
Save As
View
Create Table View
Close
source="windows_server_attack_logs.csv" signature_id=4624 | timechart count by user limit=10
All time
280 events (before 7/19/23 3:12:51.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (83)
Visualization
Line Chart
Format
Trellis
12:00 AM Wed Mar 25 2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
_time
user_a
user_b
user_c
user_d
user_e
user_i
user_j
user_k
user_m
user_n
OTHER
2020-03-25 00:00:00 0 2 0 0 2 2 0 0 0 2
2020-03-25 00:10:00 0 2 0 0 0 0 2 0 2 0
2020-03-25 00:20:00 0 0 0 0 0 0 0 0 0 0
2020-03-25 00:30:00 0 0 0 0 0 0 0 0 0 0
2020-03-25 00:40:00 0 0 0 2 0 2 0 0 0 0
2020-03-25 00:50:00 0 0 0 0 0 0 0 0 0 0


Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Tue 23:17
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Windows Server Attack Logs Timechart of Signatures
Save
Save As
View
Create Table View
Close
source="windows_server_attack_logs.csv" | timechart span=1h count by signature
All time
11,896 events (before 7/19/23 3:17:39.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (14)
Visualization
20 Per Page
Format
Preview
_time
A computer account was deleted
A privileged service was called
A process has exited
A user account was changed
A user account was deleted
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER
NULL
2020-03-25 00:00 38 28 16 20 28 32 22 20 20 24 136 0
2020-03-25 01:00 24 40 26 14 14 1610 30 22 32 32 102 0
2020-03-25 02:00 18 6 32 18 10 1792 28 6 34 16 54 0
2020-03-25 03:00 26 26 24 32 18 20 28 12 32 28 102 0
2020-03-25 04:00 24 36 16 22 28 24 24 22 20 32 126 0
2020-03-25 05:00 22 28 24 32 34 38 18 16 28 20 124 0
2020-03-25 06:00 18 28 24 34 26 6 22 28 16 26 128 0
2020-03-25 07:00 30 16 30 34 22 22 30 32 40 14 140 2
2020-03-25 08:00 34 26 46 22 22 32 32 24 22 32 118 0
2020-03-25 09:00 10 4 2 6 6 2 8 2516 0 8 24 0
2020-03-25 10:00 0 0 0 0 0 0 46 1522 0 0 0 0
2020-03-25 11:00 0 0 0 0 0 0 392 0 0 0 0 0
2020-03-25 12:00 14 18 14 22 26 12 154 12 12 18 92 0
2020-03-25 13:00 8 16 14 18 26 32 30 24 30 34 96 0

Attack Summary—Apache

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

- During the initial attack, we observed notable alterations in the HTTP methods, specifically GET and POST requests. Both types of requests experienced a substantial increase in their counts, as evidenced in the report. This spike in counts showed a strong correlation with another alert we had configured for the "referrer_domain." Notably, a single domain appeared to be the primary source behind the high number of alerts recorded in the report.

Attack Summary—Apache

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

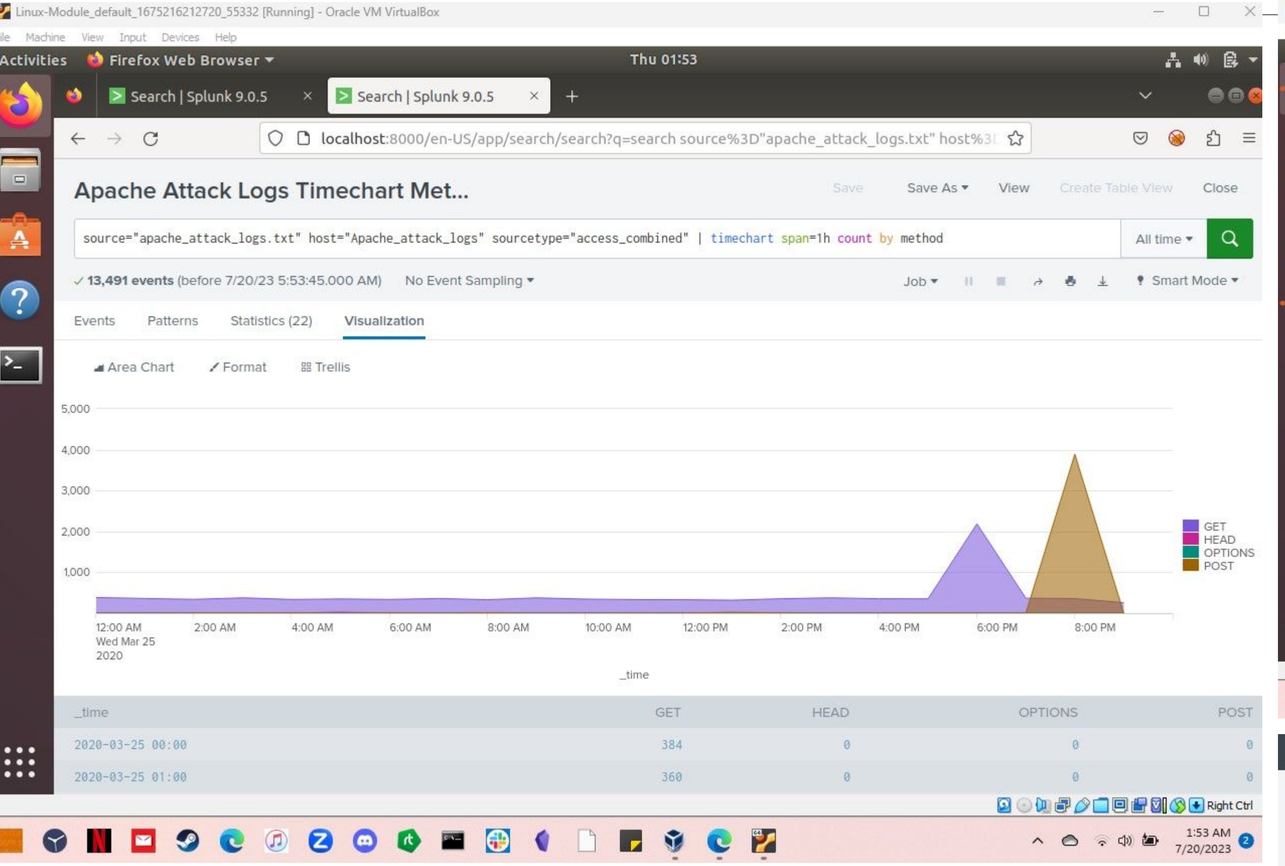
- On Wednesday, March 25th, 2020, between 4:30 pm and 6:30 pm, we observed a significant spike in HTTP method GET events originating from international addresses. The event count reached 939 during this two-hour period, with the peak activity recorded at 6:00 pm, where the event count reached thirty-eight (38). Subsequently, there was a rapid decline back to normal levels by 6:30 pm. Similarly, we detected analogous activities with the HTTP method POST, where the event count surged to 1,296 events on the same day, between 6:30 pm and 8:30 pm. These findings align with our previous analysis of HTTP methods.

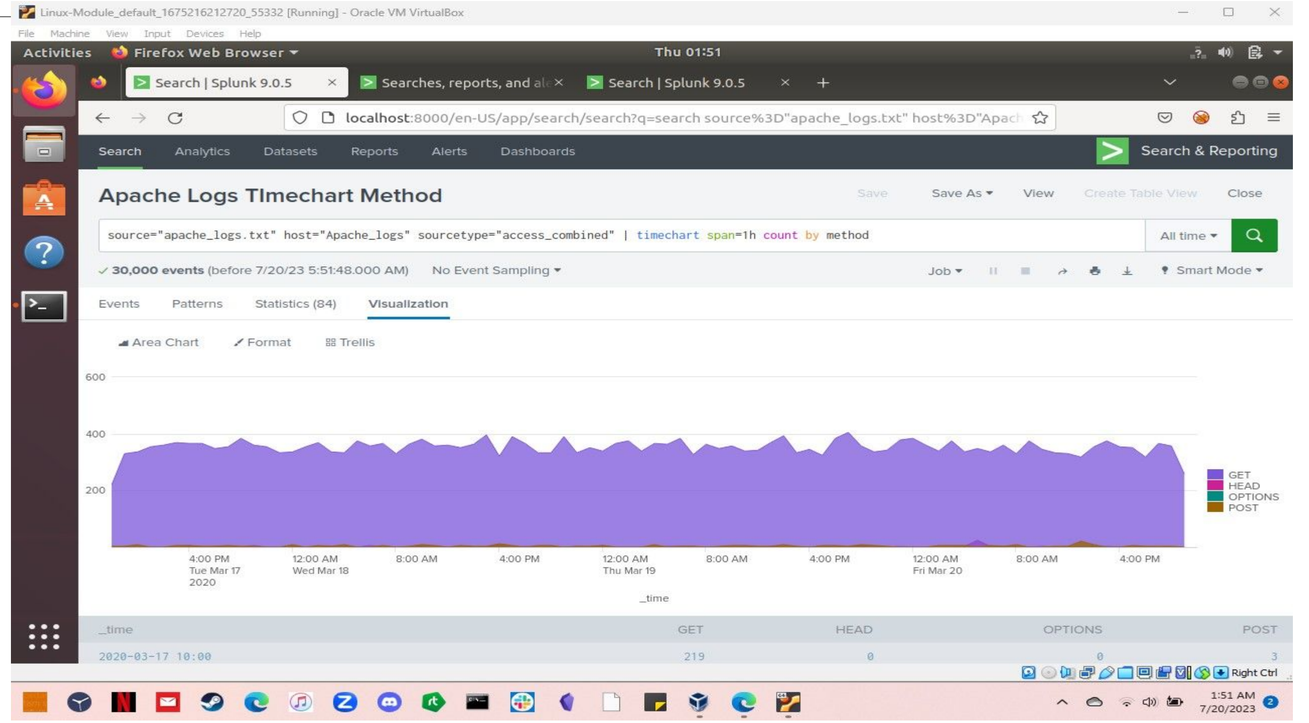
Attack Summary—Apache

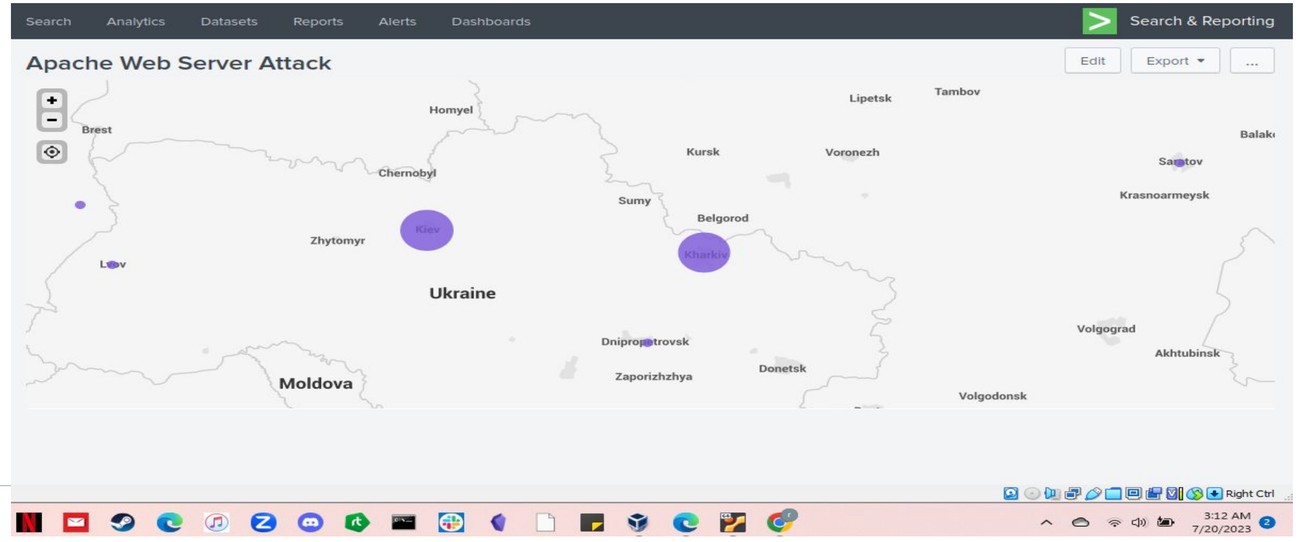
Summarize your findings from your dashboards when analyzing the attack logs.

- From our Time Chart analysis of HTTP methods, we discovered a notable increase in both POST and GET methods. Suspicious POST events were observed between 7:00 pm and 9:00 pm, amounting to a total event count of 1,296. Additionally, suspicious GET events occurred between 5:00 pm and 7:00 pm, totaling 729 events. Utilizing the Cluster Map, we identified that the majority of this activity originated from Ukraine, with Kharkiv registering 433 events and Kyiv reporting 439 events during the attack. Based on the collected information, our analysis led us to conclude that it was a brute force attack targeting the VSI logon page.

Screenshots of Attack Logs







Summary and Future Mitigations

Project 3 Summary

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

  There were brute force and hijack reconnaissance activities going on.

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

  Enhance firewall parameters. Use two-step authentication. Make users change their passwords every couple of months. Set a limit to failed login attempts that will temporarily block out the user until an IT specialist checks and clears the situation.