# Defensive Security Project
# by: Melai, Charity, Nabta, Lauren, Myia

# Table of Contents

This document contains the following resources:

# Monitoring Environment

# Setup and Log Analyzation

- In this project, we were tasked with taking on the role of a mock SOC analyst for a company called “Virtual Space Industries” or VSI.
- We will use Splunk (a software platform used to  search, monitor, and analyze machine-generated data in real time) to search VSI’s systems and applications for potential attacks from VSI’s competitor ‘Jobecorp’ attempting to disrupt business.

## The VSI products that we will be monitoring include:

### Windows Server Monitoring Logs

- We uploaded and analyzed Windows security logs that represented regular security activity for the company and analyzed the signature_id, signature, user, status, and severity fields
- We then created reports with a table of signatures and associated signature ID’s, a report displaying severity levels (and the count/percentage of each), as well as a report that compares the success and failure of Windows activities
- We also created alerts that will be triggered to inform us when the threshold for failed login attempts and when user accounts have been deleted.
- lastly we created lie charts to help us visualize the different signature field values, user field values, count of different users, and a single value visualization that analyzes a single data point

### Apache Server Monitoring Logs

- We uploaded and analyzed Apache web server logs that represented regular activity for the company, and analyzed the method, referer_domain, status, clientip, and useragent fields.
- We then created reports which were designed to monitor suspicious activity against the Apache web server such as the top 10 domains that refer to VSI’s website, a report that shows the count of each HTTP response code, and a report that shows a table of the different HTTP methods (GET, POST, HEAD etc.)
- We also created alerts that will be triggered to inform us hourly if our threshold has been reached regarding all activity from any country outside of the U.S., and when our threshold has been reached for the hourly count of the HTTP POST method
- Lastly we created a line chart to display the different HTTP methods over time, a geographical map showing location based on clientip fields

# [“Add-On” App]

# Splunk Security Essentials Add On Application

Splunk offers a variety of add on applications to their clients which help to gather, normalize, and enrich data sources

**The add on app that we decided to use is the Splunk Security Essentials (SSE)**

The basic principal function of this app is to make security easy, weather you're a novice, or an advanced splunk user.

**The four main functions of this app are to:**

1. **Find Content** - helps security detection basics, offers advanced detection content, and offers prescriptive content recommendations

1. **Learn** - helps you get comfortable using splunk and learn proper security techniques

1. **Help Deploy** - deploys content into your environment, automatically generate dashboards, and monitors data ingest

1. **Measure** - justifies new data sources via MITRE ATT&CK and documents deployed content

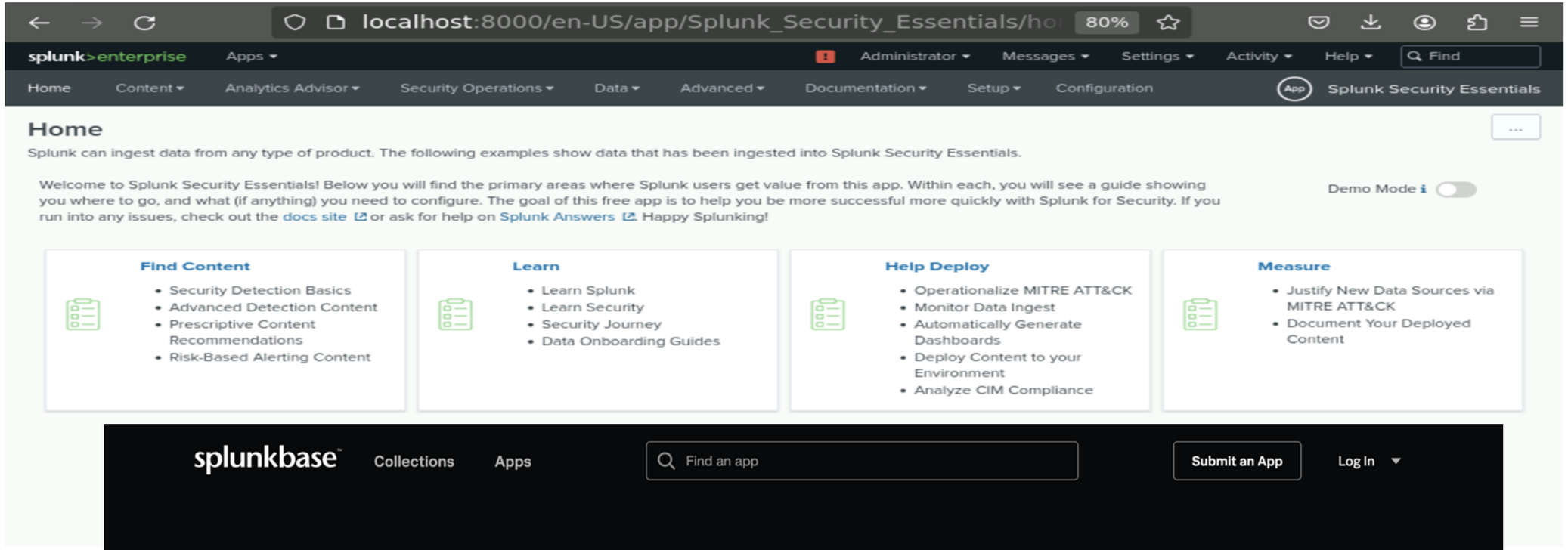
# Splunk Security Essentials Add On Application

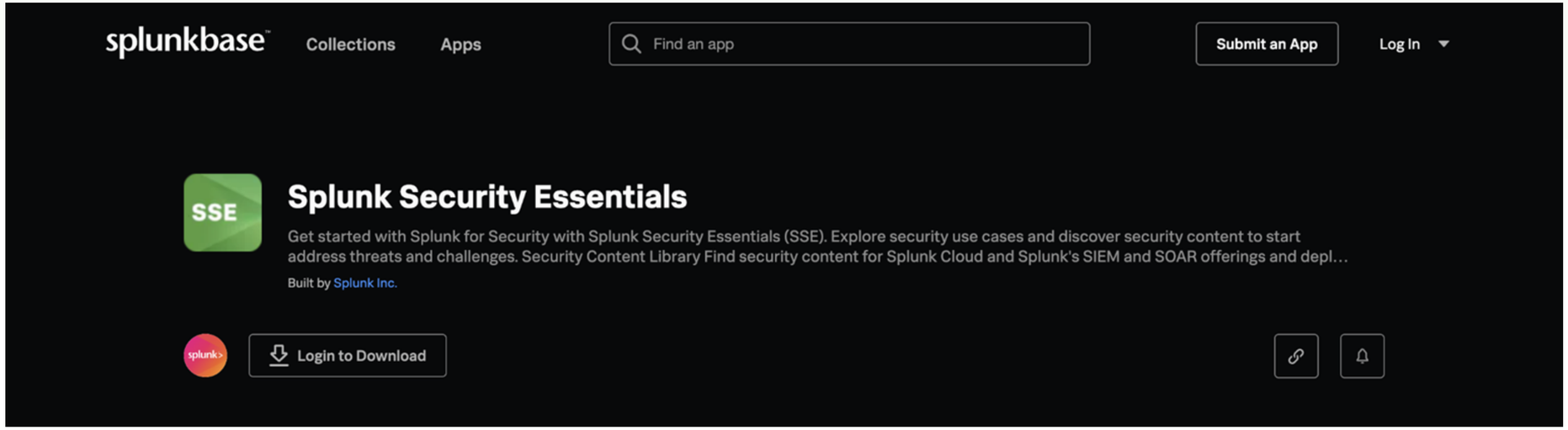
A good situation to use the Splunk SSE add on would be when trying to analyze larger amounts of data over a longer period of time and keep it organized

The splunk security essentials allows users to create a content library using the bookmark features and export the content in a variety of methods to easily integrate it into another splunk environment.

this is very beneficial because it will allow users to hold data in an organized way and easily transfer it when needed

# Splunk Security Essentials Images



# Logs Analyzed

## 1 Windows Logs

- Signature
- User
- Status
- Signature ID’s
- Status
- Severity

## 2 Apache Logs

- Client IPs
- Method
- Referer Domain
- Status Count
- User Agent

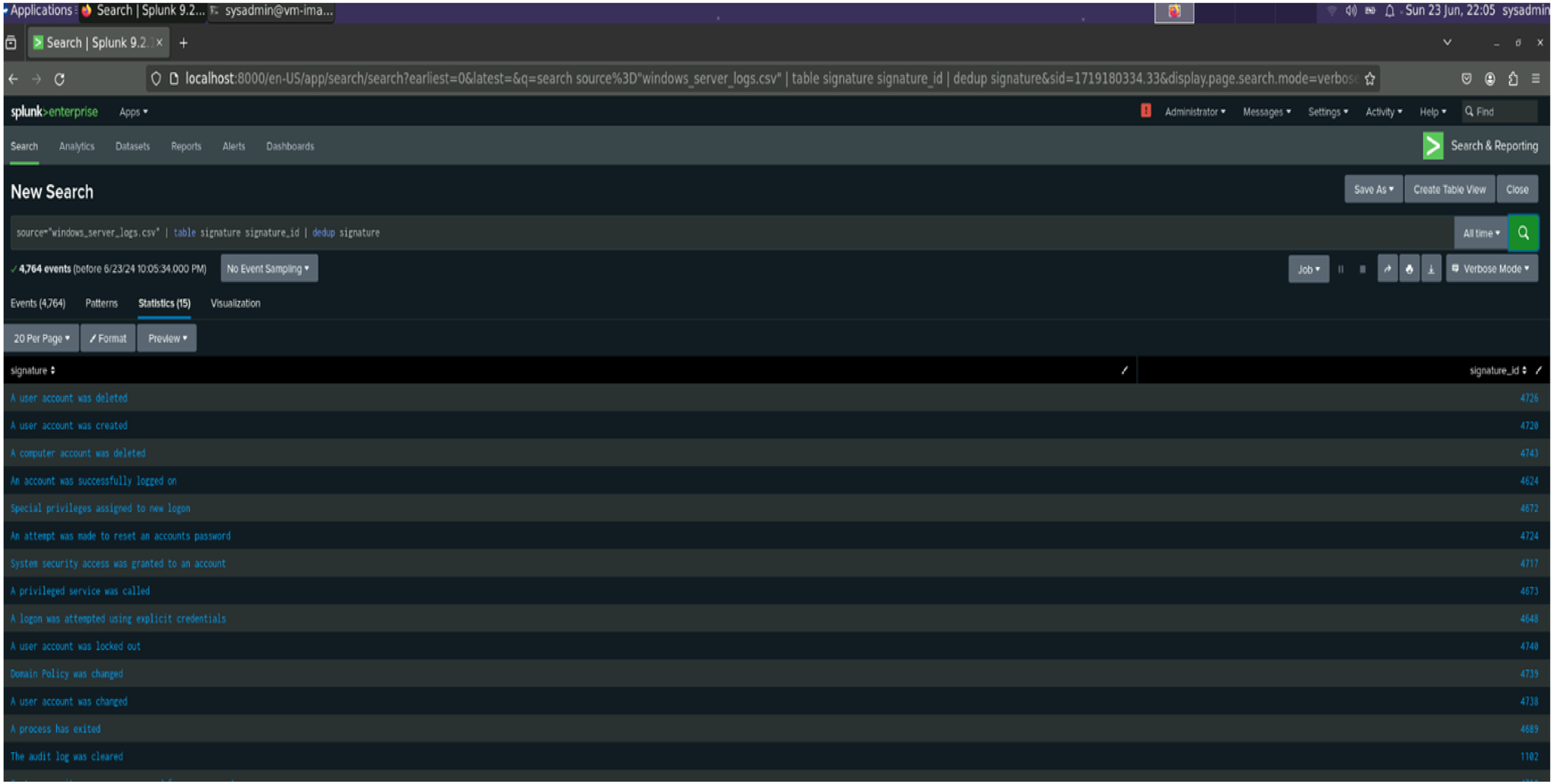
# Windows Logs

# Reports—Windows

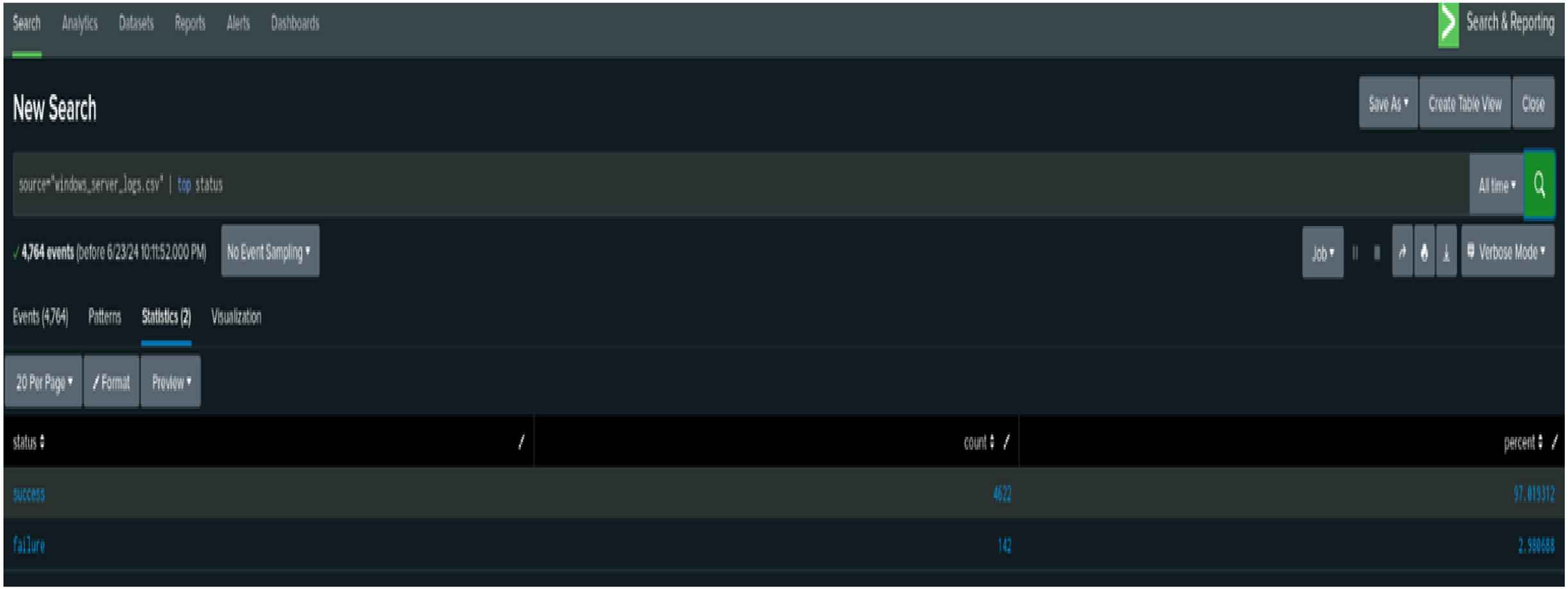
Designed the following reports:

| Report Name | Report Description |
|---|---|
| ID Number Associated w/Signature | Used in security analysis and intrusion detection systems |
| Windows Success/Failure Report | Windows Success and Failure Report refers to a summary of successful and failed login attempts or other security-related events |
| Severity Level | Summary of events categorized by their severity or criticality |
| | |

# Images of Reports—Windows



# Images of Reports—Windows



# Images of Reports—Windows

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Failed Windows Activity | An alert sent when the amount of failed activities has exceeded the threshold | 6 | 10 |

**JUSTIFICATION:** After analyzing the logs and historical data for failed login attempts and other failed activities, we observed that on average, the number of failed activities per hour was consistently around 6. This baseline represents the normal operational level of failed activities, accounting for occasional user errors and expected minor system glitches. Setting the threshold at 10 provides a buffer to account for spikes that may occur due to benign reasons. However, surpassing this threshold is unusual and could indicate a potential security issue, such as a brute force attack or a misconfiguration. Thus, this threshold ensures that we are alerted to abnormal activities without being overwhelmed by false positives, allowing for efficient monitoring and response to genuine security threats.

# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Account Successfully logged in | An alert that is sent whenever the amount of successfully logged accounts has exceeded the threshold | 13 | 21 |

**JUSTIFICATION:** The baseline number of 13 is derived from historical data analysis, reflecting typical user behavior under standard conditions. By setting the threshold at 21, we provide a buffer to accommodate occasional fluctuations and peaks in login activity that may occur during legitimate, high-usage periods. This threshold is strategically chosen to be high enough to minimize false positives, ensuring that alerts are only triggered by significant deviations from the norm, potentially indicating unusual or suspicious activity that warrants further investigation.

# Alerts—Windows

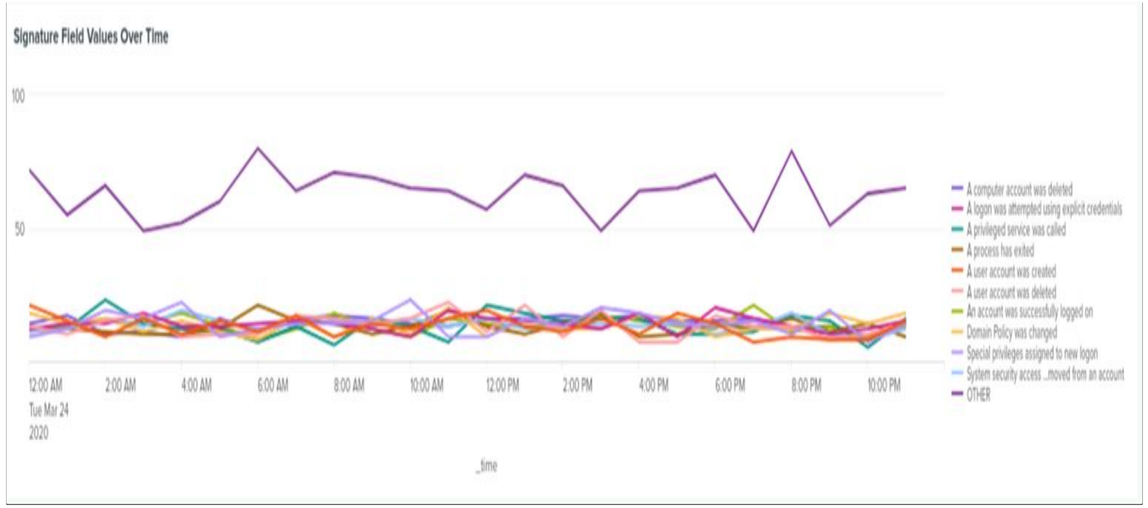
Designed the following alerts:

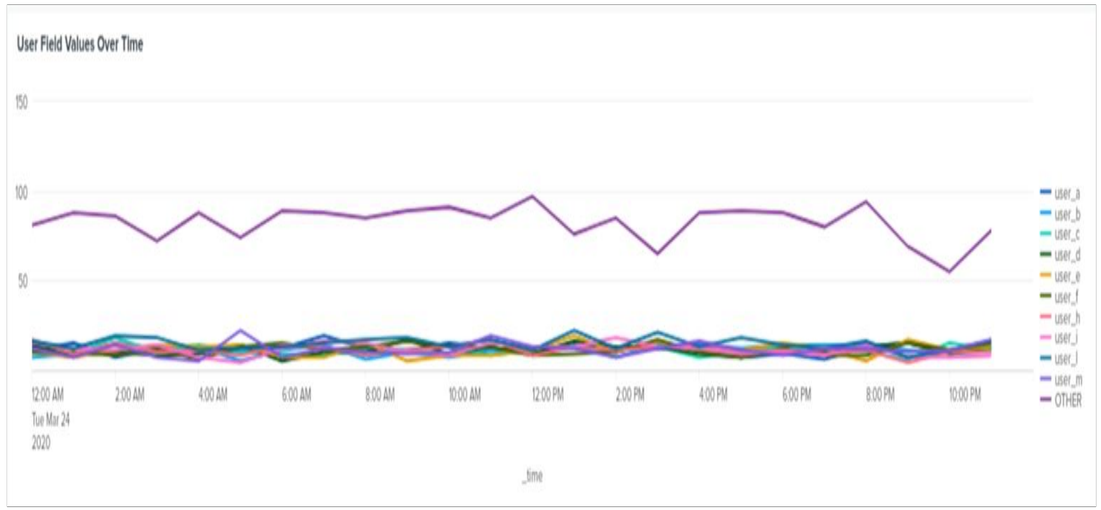
| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| User Account Deleted | An alert that is issued if there are too many deleted user accounts | 13 | 22 |

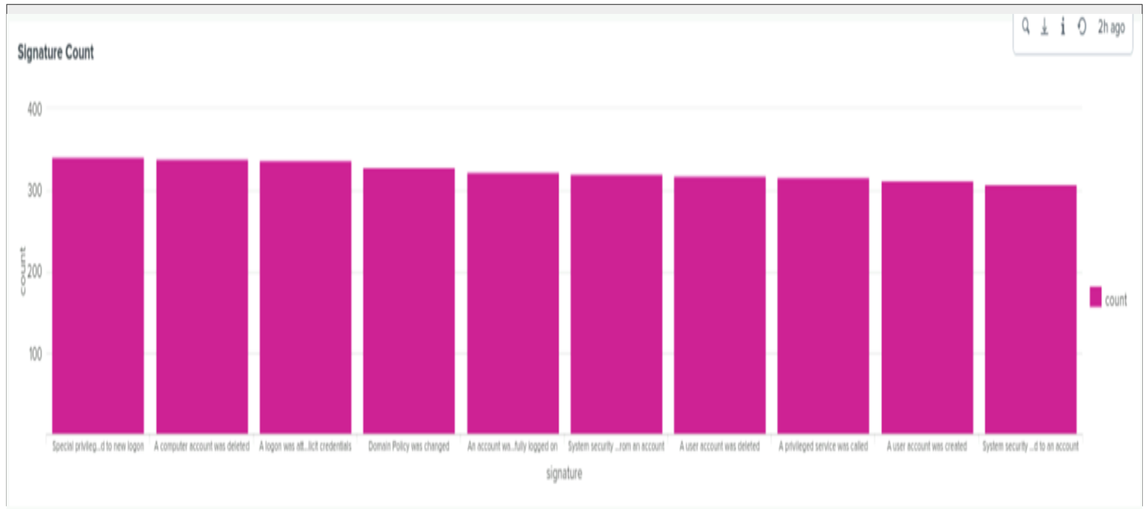
**JUSTIFICATION:** We have established a baseline of 13 user accounts deleted, which represents the typical number of deletions observed over a defined period. This baseline was determined by analyzing historical data to identify the average activity level under normal operational conditions.

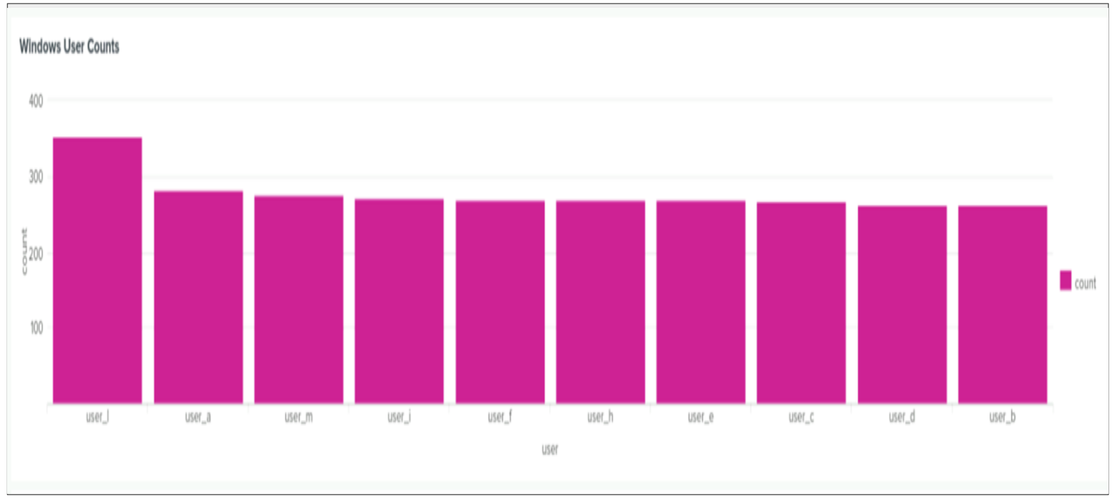
We set the threshold for user account deletions at 22, significantly higher than the baseline. This threshold accounts for natural variations in account management activities while ensuring that any substantial increase, which might indicate potential security issues or unauthorized activities, triggers an alert.

# Dashboards—Windows



# Dashboards—Windows

# Apache Logs

# Reports—Apache

Designed the following reports:

| Report Name | Report Description |
|---|---|
| Different HTTP Methods | Table that shows the count of GET, POST, HEAD and OPTIONS |
| Top 10 Domains | Top 10 domains that refer to VSI’s web server |
| Count of HTTP Response Codes | Displays the count of HTTP response code |

# Images of Reports—Apache

## Different HT...

Save | Save As | View | Create Table View | Close

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

All time

✓ **10,000 events** (before 6/21/24 12:15:09.000 AM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (4)** | Visualization

20 Per Page | Format | Preview

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

## VSI HTTP Response Co...

Save As | Create Table View | Close

```
source="apache_logs.txt" | top status
```

All time

✓ **10,000 events** (before 6/21/24 12:19:35.000 AM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (8)** | Visualization

20 Per Page | Format | Preview

| 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 |

## Top 10 Doma...

Save | Save As | View | Create Table View | Close

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

All time

✓ **10,000 events** (before 6/21/24 12:16:19.000 AM) | No Event Sampling | Job | Smart Mode

Events | Patterns | **Statistics (10)** | Visualization

20 Per Page | Format | Preview

| 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 |

# Alerts—Apache

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Non-USA Activity | Alert if the hourly activity from any country besides the United States exceeds the threshold. | 73 | 120 |

**JUSTIFICATION:** 73 events in a hour seemed standard in the logs, yet exceeding 120 seemed unlikely on a normal day. Seeing any number of events greater than the threshold would indicate issues

# Alerts—Apache

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| HTTP Post Count | Alert if the hourly count of the HTTP POST method exceeds the threshold. | 1 | 7 |

**JUSTIFICATION: : Most events per hour hovered between 1 and 4. A threshold of 7 seemed like a number that would be out of reach of “normal” hourly events but small enough to catch malicious activity.**

# Attack Analysis

# Attack Summary—Windows

The Windows attack system exhibited 13 % decrease in informational events and a 13 % increase in high-severity events . Additionally, there were more successful actions than failures post-attack. Alert analysis revealed a suspicious volume of failed activities:

- Failed logins: 35 events occurred at 8 AM, exceeding the threshold. No changes are recommended.
- Successful logins: An unusual number of successful logins were detected, with 196 events and 77 events occurring within one hour. The primary user was "user_J," logging between 11 AM - 12 PM.

# Attack Summary—Windows

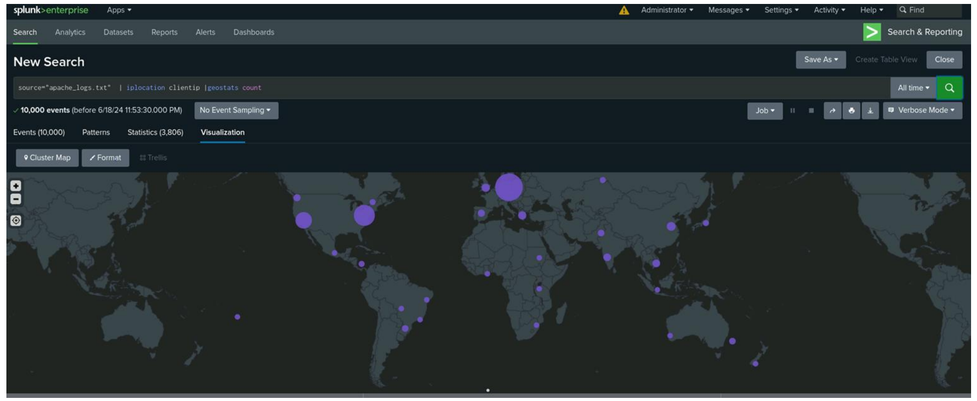
Alert Analysis  didn’t indicated suspicious volume of failed activity or any suspicious volume of deleted accounts.

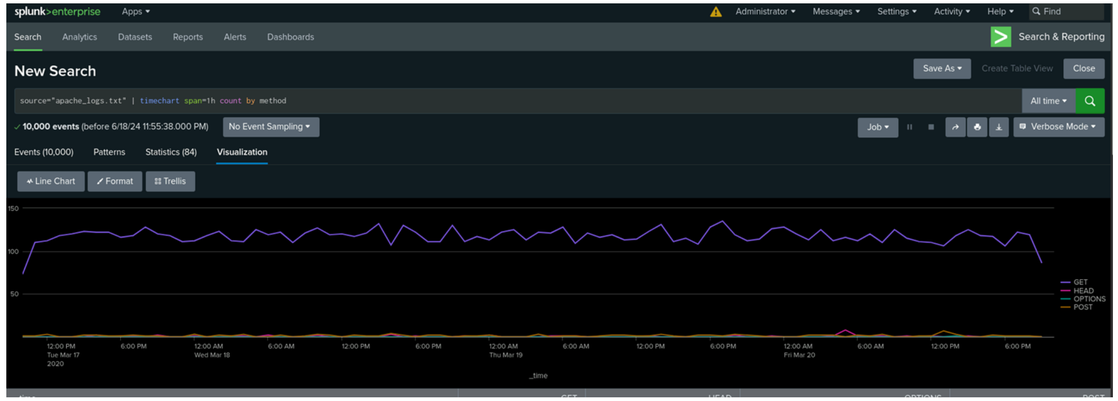
Our Dashboard Analysis showed suspicious activity with the accounts that were locked out (between hours 12 AM - 3 AM) and attempts made to reset the password (between hours 8 AM - 11 AM). The peak for the locked outs was 896, while the attempts to reset the password peaked at 1,258

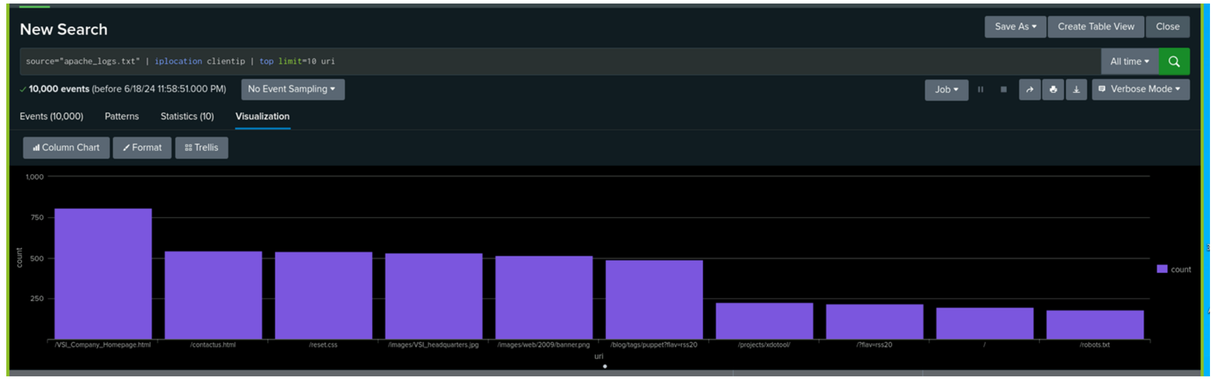
As for Users, there was suspicious activity between User_a (between 12 AM - 3 AM) and User_k (between 8 AM - 11 AM). User_a peaked at 984 , while User_k peaked at 1,256.

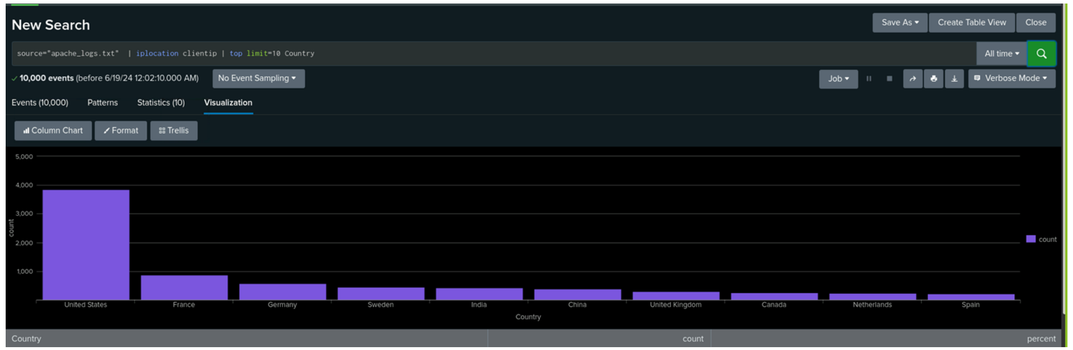
As for the my other findings, the data concluded there was suspicious activity.

# Dashboards—Apache

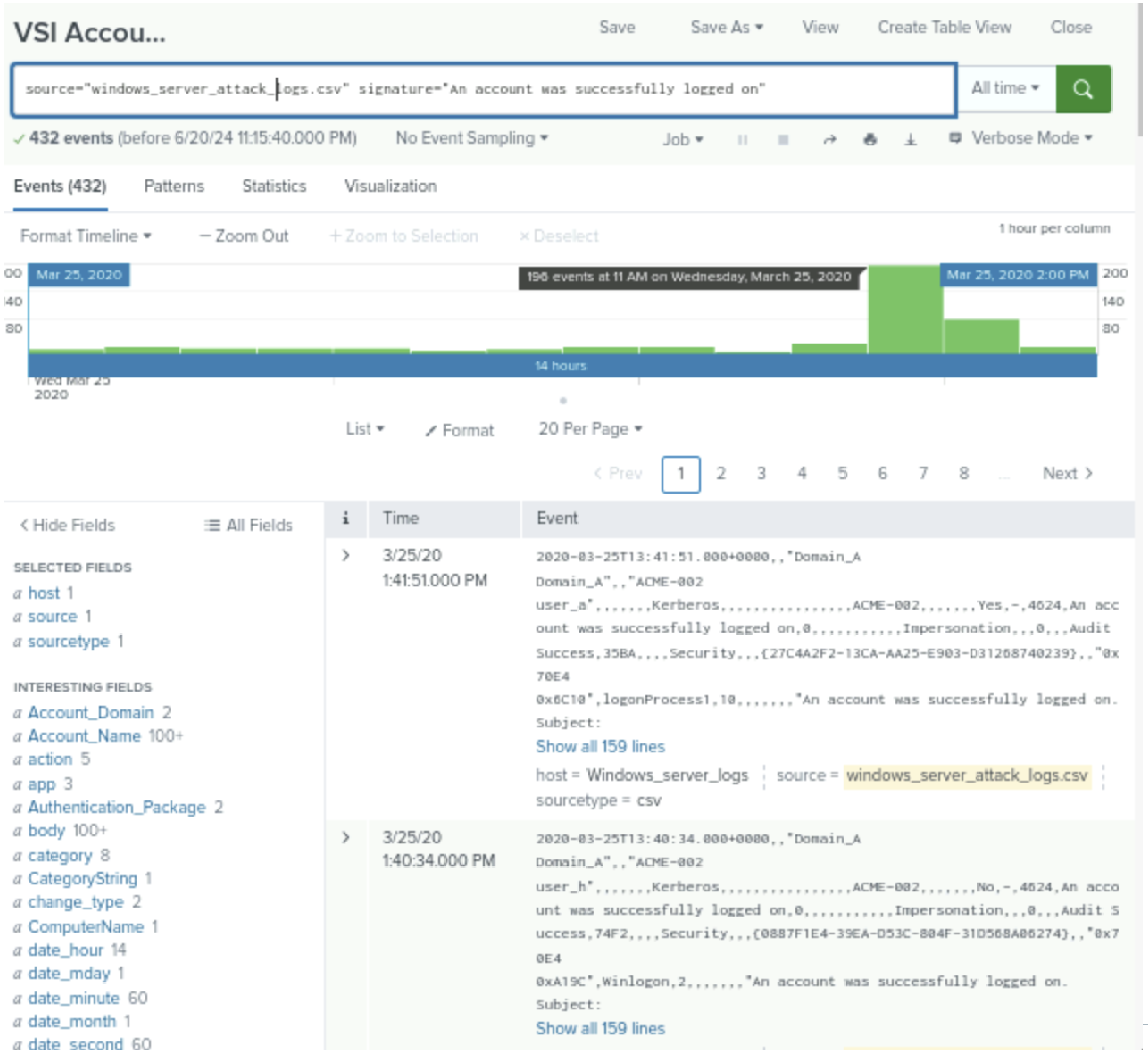



# Screenshots of Windows Attack Logs



```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"
```

3/25/20 1:41:51.000 PM

```
2020-03-25T13:41:51.000+0000,,"Domain_A
Domain_A",,"ACME-002
user_a",,,,,,,Kerberos,,,,,,,,,,,,,,,,ACME-002,,,,,,,Yes,-,4624,An acc
ount was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit
Success,35BA,,,,Security,,,{27C4A2F2-13CA-AA25-E903-D31268740239},,"0x
70E4
0x6C10",logonProcess1,10,,,,,,,"An account was successfully logged on.
Subject:
```

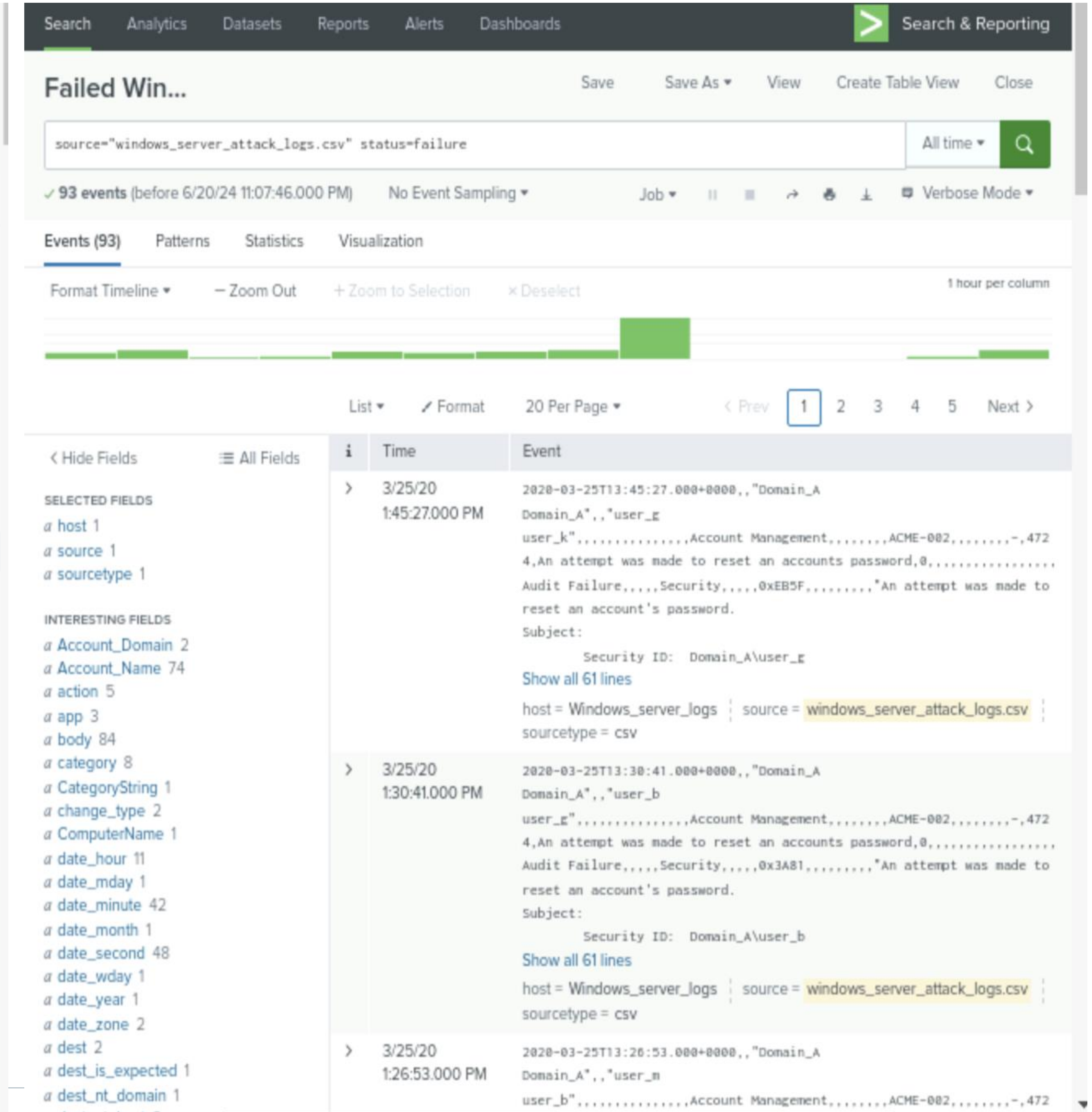
Show all 159 lines

host = Windows_server_logs | source = windows_server_attack_logs.csv | sourcetype = csv

3/25/20 1:40:34.000 PM

```
2020-03-25T13:40:34.000+0000,,"Domain_A
Domain_A",,"ACME-002
user_h",,,,,,,Kerberos,,,,,,,,,,,,,,,,ACME-002,,,,,,,No,-,4624,An acco
unt was successfully logged on,0,,,,,,,,,,,Impersonation,,,0,,,Audit S
uccess,74F2,,,,Security,,,{0887F1E4-39EA-D53C-804F-31D568A06274},,"0x7
0E4
0xA19C",Winlogon,2,,,,,,,"An account was successfully logged on.
Subject:
```

Show all 159 lines



```
source="windows_server_attack_logs.csv" status=failure
```

3/25/20 1:45:27.000 PM

```
2020-03-25T13:45:27.000+0000,,"Domain_A
Domain_A",,"user_g
user_k",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,472
4,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,,
Audit Failure,,,,,Security,,,,,0xEB5F,,,,,,,,,"An attempt was made to
reset an account's password.
Subject:
        Security ID:  Domain_A\user_g
```

Show all 61 lines

host = Windows_server_logs | source = windows_server_attack_logs.csv | sourcetype = csv

3/25/20 1:30:41.000 PM

```
2020-03-25T13:30:41.000+0000,,"Domain_A
Domain_A",,"user_b
user_g",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,472
4,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,,
Audit Failure,,,,,Security,,,,,0x3A81,,,,,,,,,"An attempt was made to
reset an account's password.
Subject:
        Security ID:  Domain_A\user_b
```

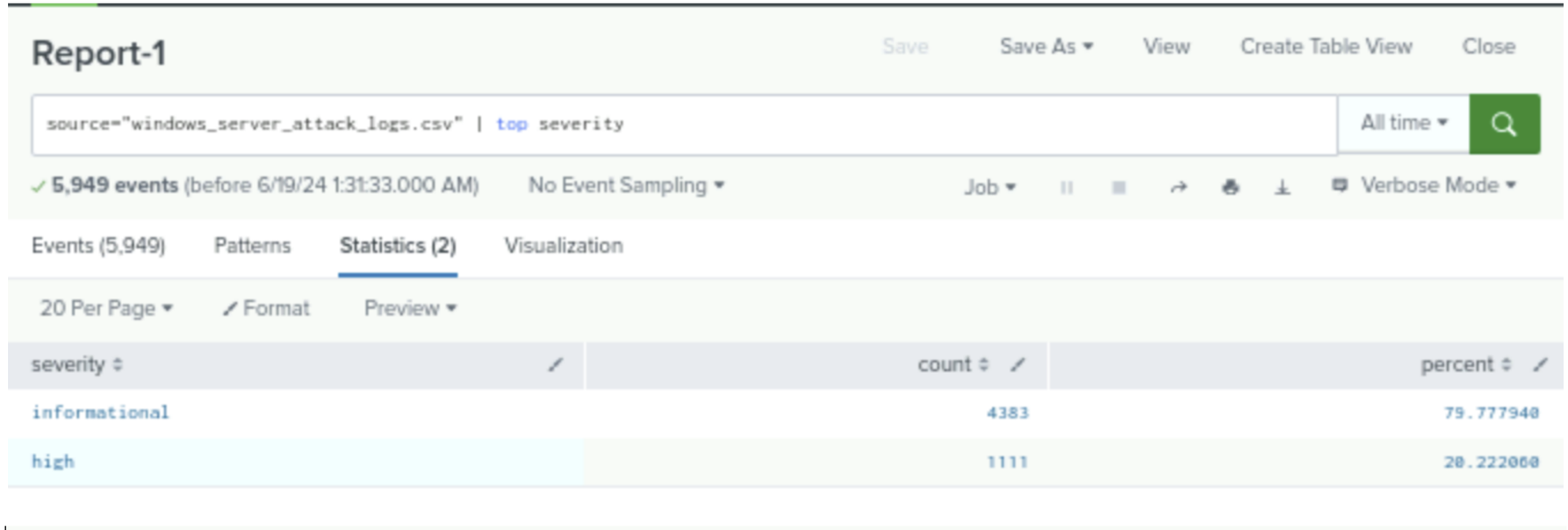
Show all 61 lines

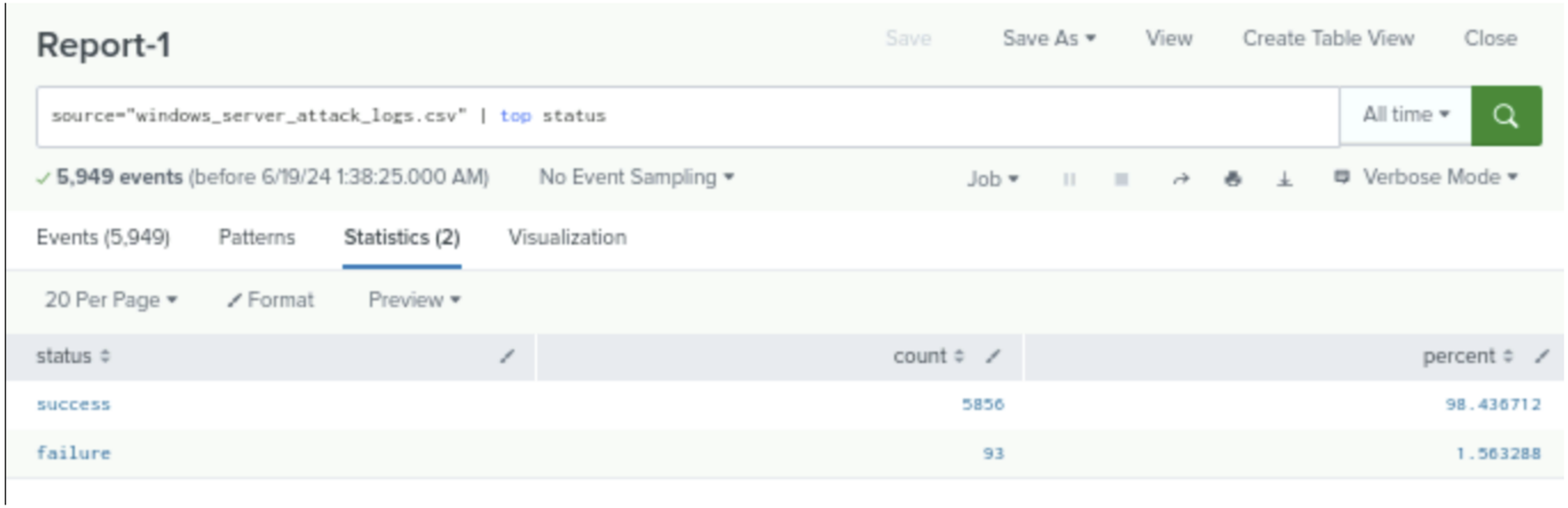
host = Windows_server_logs | source = windows_server_attack_logs.csv | sourcetype = csv

3/25/20 1:26:53.000 PM

```
2020-03-25T13:26:53.000+0000,,"Domain_A
Domain_A",,"user_m
user_b",,,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,472
```

# Screenshots of Windows Attack Logs



# Attack Summary—Apache

In analyzing the attack logs, it was evident the existing thresholds in place were correct; periodic spikes in attack activity were all above the threshold and thus VSI would have been notified during each method of attack. Each of the alert analysis are listed below:

Shift in VSI HTTP Methods; **Threshold: 7 Events**

- there was a suspicious decrease in GET activity by 29%, which conversely increased POST activity by 29% (count: 1,324 events)

Shift in VSI Top 10 Domains Referred

- None

Shift in VSI HTTP Response Codes

- 404 response code increased from 2% to 15%

Shift in Volume of International Activity (Non-U.S.); **Threshold: 120 Events**

- 1,369 events in Kyiv, Ukraine

# Screenshots of Attack Logs

Different HT...

Save | Save As | View | Create Table View | Close

```
source="apache_attack_logs.txt" | top method
```

All time

✓ **4,497 events** (before 6/21/24 12:15:41.000 AM) No Event Sampling Job Smart Mode

Events | Patterns | **Statistics (4)** | Visualization

20 Per Page | Format | Preview

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

# Screenshots of Attack Logs

Top 10 Doma...

Save | Save As | View | Create Table View | Close

```
source="apache_attack_logs.txt" | top limit=10 referer_domain
```

All time

✓ 4,497 events (before 6/21/24 12:16:45.000 AM) No Event Sampling Job Smart Mode

Events | Patterns | Statistics (10) | Visualization

20 Per Page | Format | Preview

| referer_domain | count | percent |
|---|---|---|
| http://www.semicomplete.com | 764 | 49.226804 |
| http://semicomplete.com | 572 | 36.855670 |
| http://www.google.com | 37 | 2.384021 |
| https://www.google.com | 25 | 1.610825 |
| http://stackoverflow.com | 15 | 0.966495 |
| https://www.google.com.br | 6 | 0.386598 |
| https://www.google.co.uk | 6 | 0.386598 |
| http://tuxradar.com | 6 | 0.386598 |
| http://logstash.net | 6 | 0.386598 |
| http://www.google.de | 5 | 0.322165 |

# Screenshots of Attack Logs

## VSI HTTP Response Logs

Save As ▾ Create Table View Close

```
source="apache_attack_logs.txt" | top status
```

All time ▾

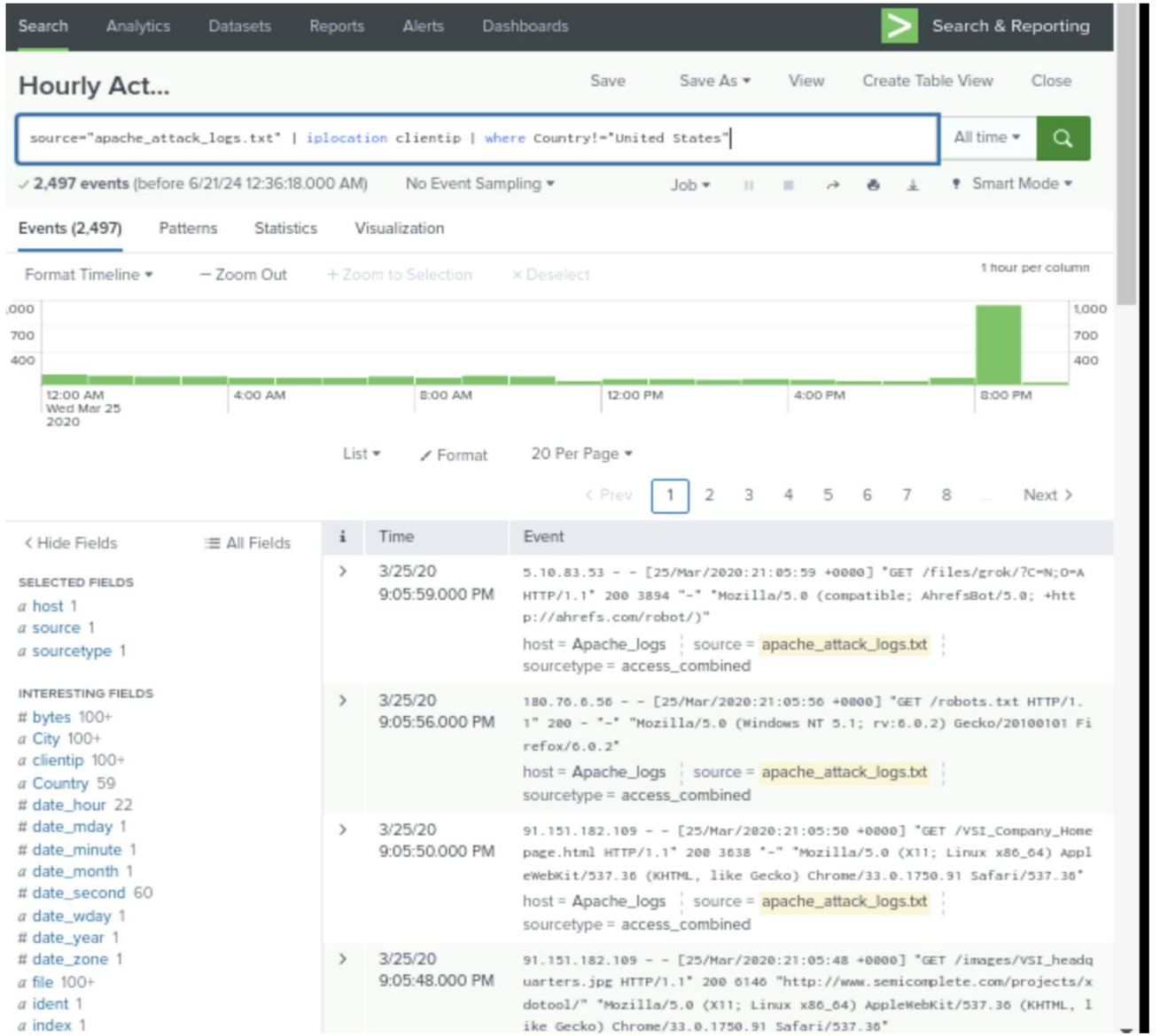
✓ **4,497 events** (before 6/21/24 12:20:12.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

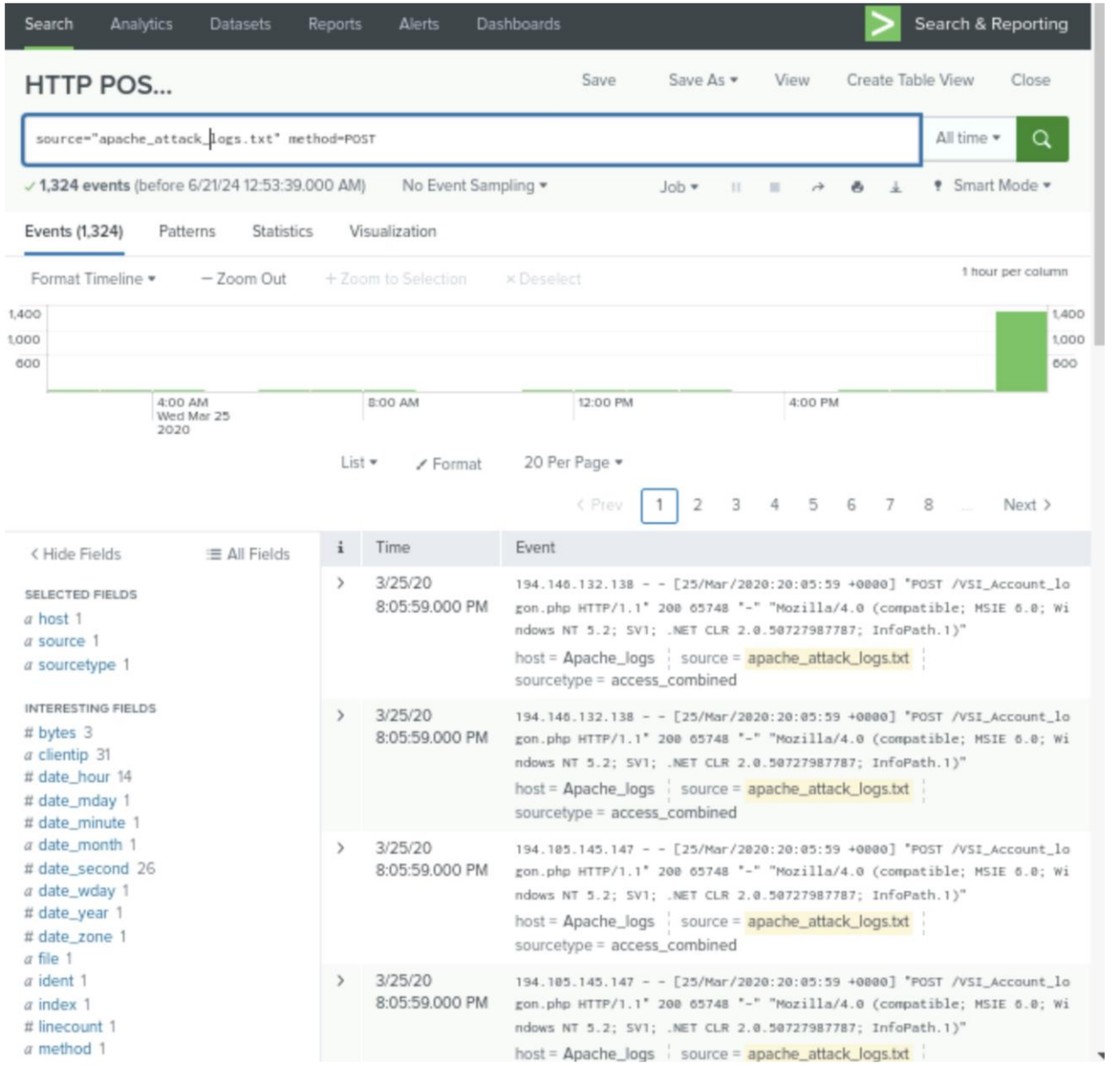
Events Patterns **Statistics (7)** Visualization

20 Per Page ▾ Format Preview ▾

| status | count | percent |
|---|---|---|
| 200 | 3746 | 83.299978 |
| 404 | 679 | 15.098955 |
| 304 | 36 | 0.800534 |
| 301 | 29 | 0.644874 |
| 206 | 5 | 0.111185 |
| 500 | 1 | 0.022237 |
| 403 | 1 | 0.022237 |

# Screenshots of Attack Logs

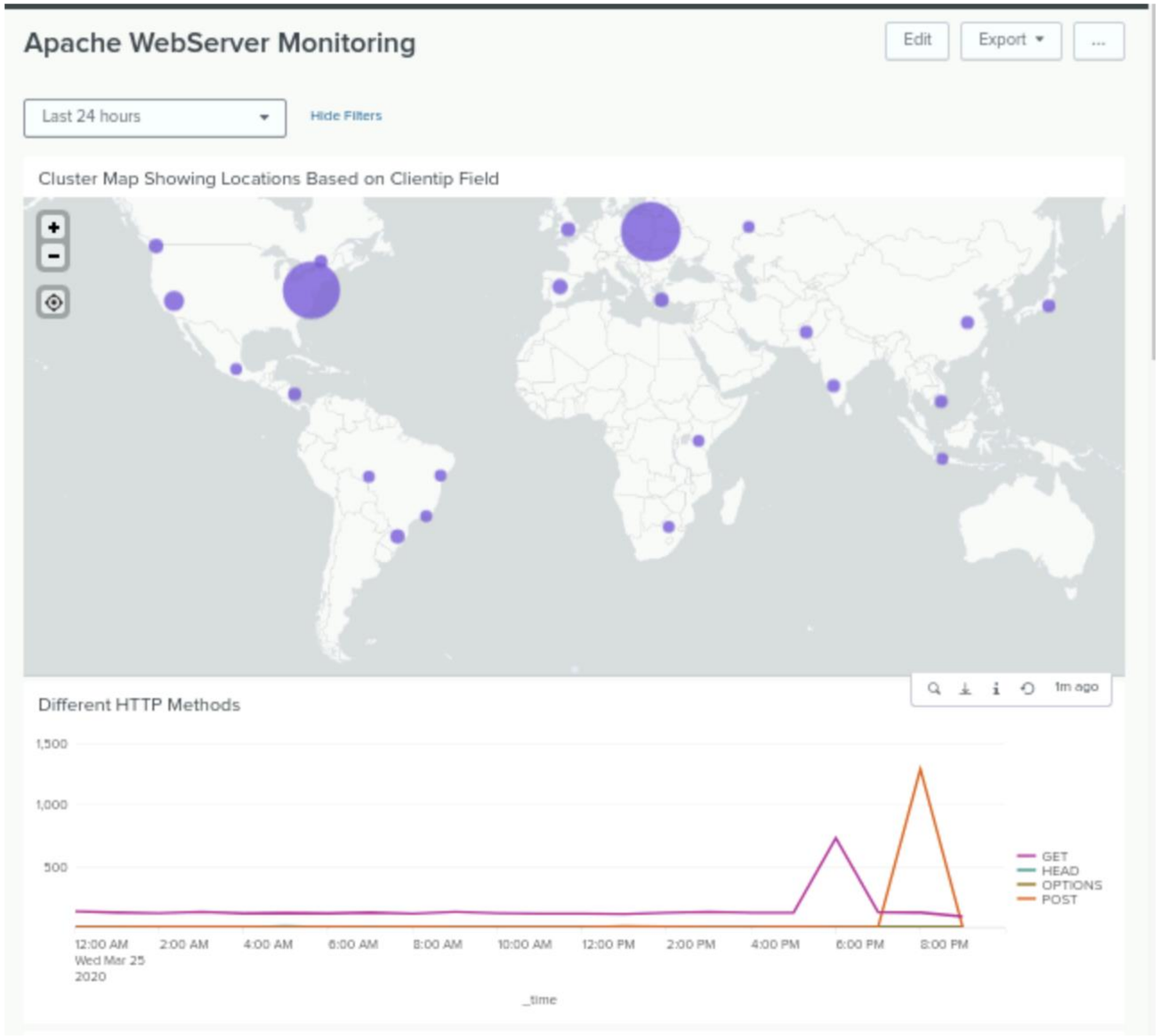


# Attack Summary—Apache

Using the Apache Web Server Dashboard to analyze the attack logs, it was evident that both the “GET” and “POST” methods were used in the attack, with GET starting at 4:00 pm and ending at 6:00 pm, and POST starting at 6:00 pm and ending at 8:00 pm; the peak count during the attack was 1,296 events for GET and 729 for POST.

Additionally, a high volume of activity was seen in Washington, D.C., U.S.A. at 724 events. And further, the URI “/VSI/Account/logon.php” was hit the most, at 1,415 events from 8:00 pm to 9:00 pm.



# Summary and Future Mitigations

# Project 3 Summary

Ultimately, we conclude that a brute force attack occurred throughout March 25th, in which the primary method of exploitation was user account logins.

In order to protect VSI from future attacks, we would recommend the following:

- Install endpoint protection on all machines
- Install a firewall
- Allow whitelisting
  - Create a firewall rule to block HTTP requests from a specified URI (i.e. “/VSI/Account/logon.php”
- Develop a strong password policy that includes two factor authentication
  - Limit account lockouts for individual users (both periodically and numerically)
  - Enforce two-factor authentication