# Defensive Security Project by: Marty, Nick & Ben

@Ben

# Table of Contents

This document contains the following resources:

# Monitoring Environment

@Ben

# Scenario

- SOC Analyst working for a small company called Virtual Space Industries (VSI)
- Using the Splunk SIEM platform to monitor against cyberattacks on VSI Windows Machines and Apache Web Server infrastructure
- Review of normal business activity and using this to create baselines for Alerts
- Creation of Dashboards to assist in identifying malicious activity
- Ingest of attack logs
- Analysis of the attack logs using pre-compiled Reports, Alerts and Dashboards to identify what resources were attacked
- Determine the efficacy of the Reports, Alerts and Dashboards

# Splunk Security Essentials

@Marty

# Splunk Security Essentials

Splunk Security Essentials (SSE) builds on Splunk's SIEM offerings by adding enhanced security detection and analytic solutions, such as:

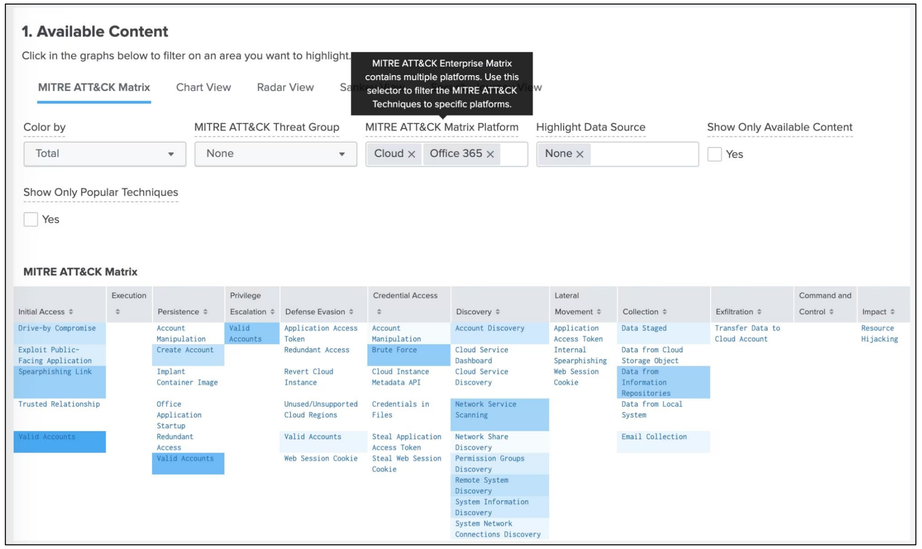
- **Cyber Security Frameworks:**
  Automatic mapping of data and security detections to MITRE ATT&CK and Cyber Kill Chain frameworks.
- **Security Content Library:**
  Pre-built security detections and analytics are stored in the Security Content Library, which can be used to enhance searches in the Splunk environment.

- Benefits of SSE:
  - Improves detections and helps you find content that is most relevant to your environment
  - Content documentation that is easy to use and learn from
  - Improved efficiency and accuracy on deployments
  - Operationalized frameworks, such as MITRE ATT&CK and Cyber Kill chain

https://www.splunk.com/pdfs/product-briefs/splunk-security-essentials.pdf

# Splunk Security Essentials

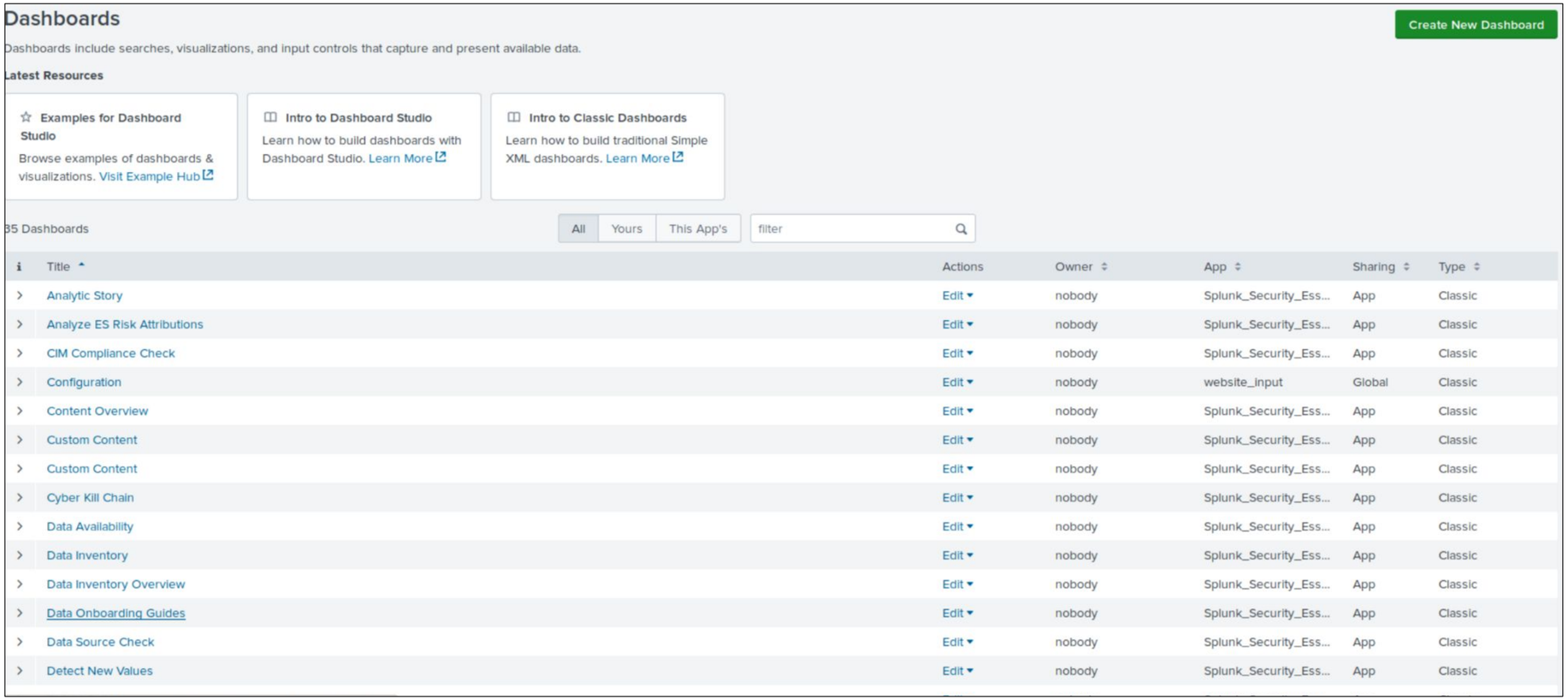
**Scenario:**
As a newly implemented SOC analyst tasked with understanding and interpreting the logs of a company, in this case VSI, I have to quickly ascertain what kind of data is important and how to search for it. Being that I want to I want to enhance my security detections but am not sure where to start I decide to use Splunk Security Essentials to get a jump on it and use industry based search libraries and alerts.



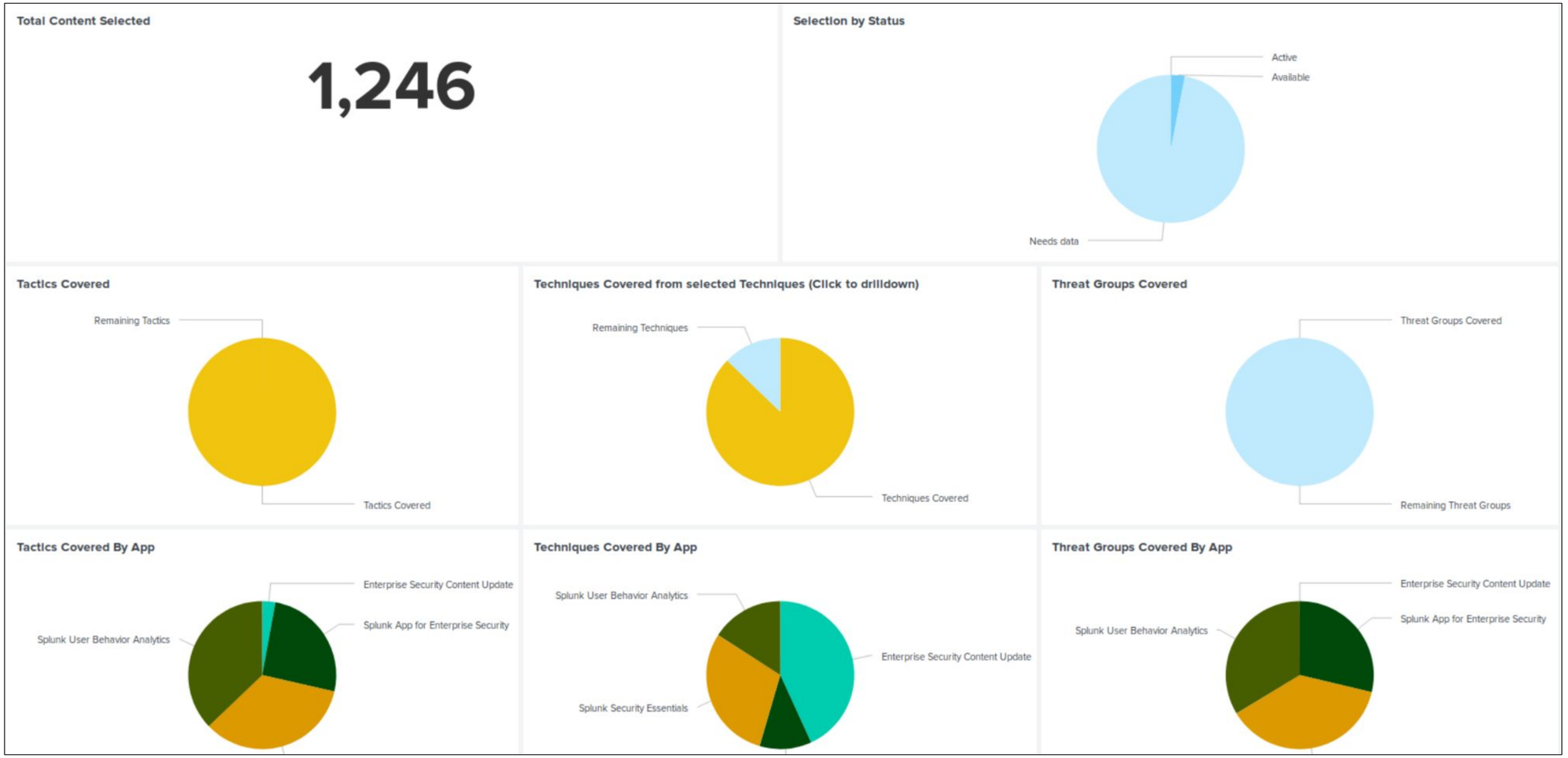

**SSE Use Case:**
By using SSE Cyber Security Frameworks, I am able to identify new detection methods based on industry data (e.g. threat groups that are targeting my industry) rather than relying solely on my company logs. Based on this information, I can ascertain common Techniques, Tactics and Procedures of these threat groups and further utilise SSE to highlight which techniques are covered by my configured detections.

https://www.splunk.com/en_us/blog/security/splunk-security-essentials-3-1-with-enhanced-mitre-att-ck-matrix-find-the-content-that-masters-most-to-you-faster.html

# Splunk Security Essentials



# Splunk Security Essentials



# Log Analysis

@Ben

# Logs Analyzed

## 1 Windows Logs

The Windows Server Logs contain information pertaining to user accounts and the events performed by those user accounts which have occurred on the Windows Operating System. These events include but are not limited to:

- Allocation of user privileges
- Changes to Domain Policies
- Creation and deletion of accounts

## 2 Apache Logs

The Apache Logs contain information relating to network traffic on the VSI Web Server, which primarily consists of resource (GET) requests. The Apache Logs contain information such as:

- Source IP Address
- Source User Agent
- Requested Resource

# Windows Logs

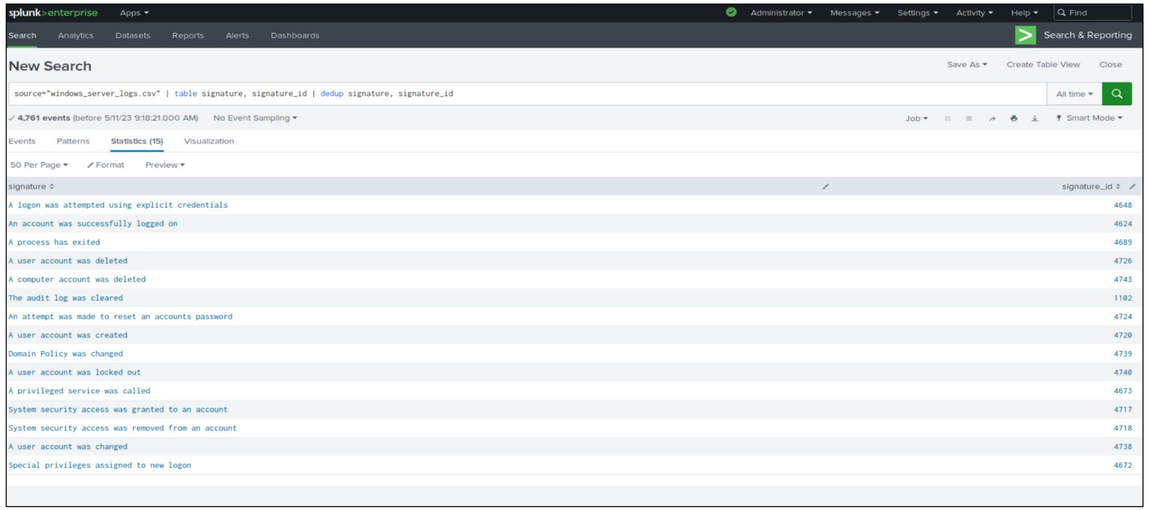
@Ben

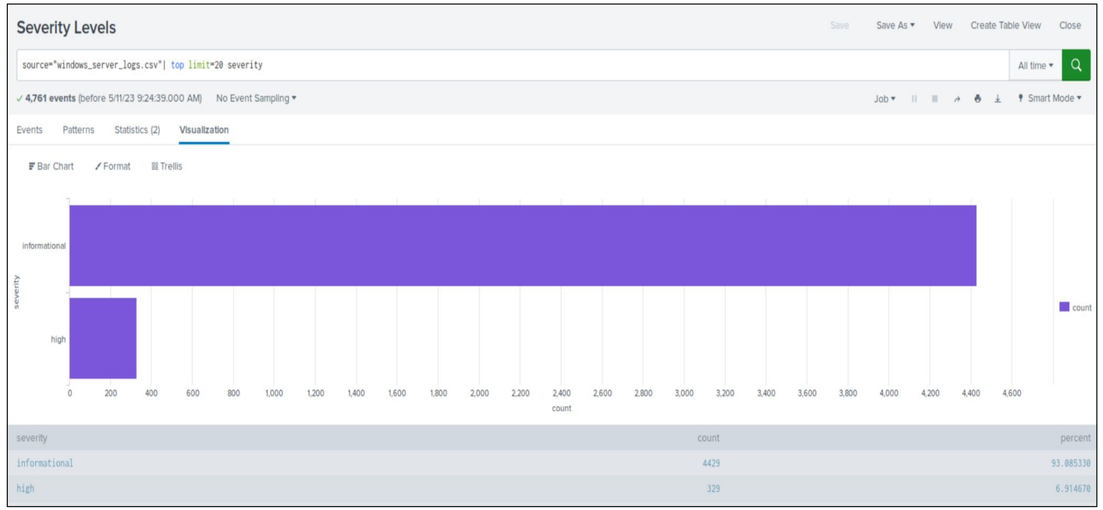
# Reports—Windows

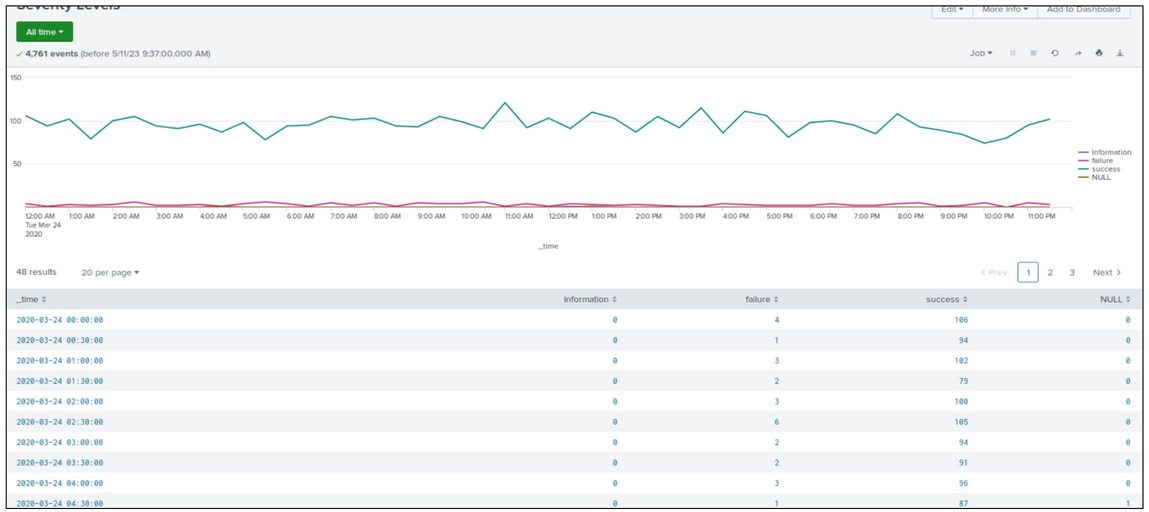
Designed the following reports:

| Report Name | Report Description |
|---|---|
| Windows Security Events | Contains the number of Windows Security Events (Signatures) by Event Type and includes the associated identification numbers. |
| Event Severity | Displays the number of events, categorised by ‘Informational’ or ‘High’ and displays the respective percentage value as a comparison of total events. |
| Event Outcome | Provides a comparison between the success and failure of Windows events. |

# Images of Reports—Windows



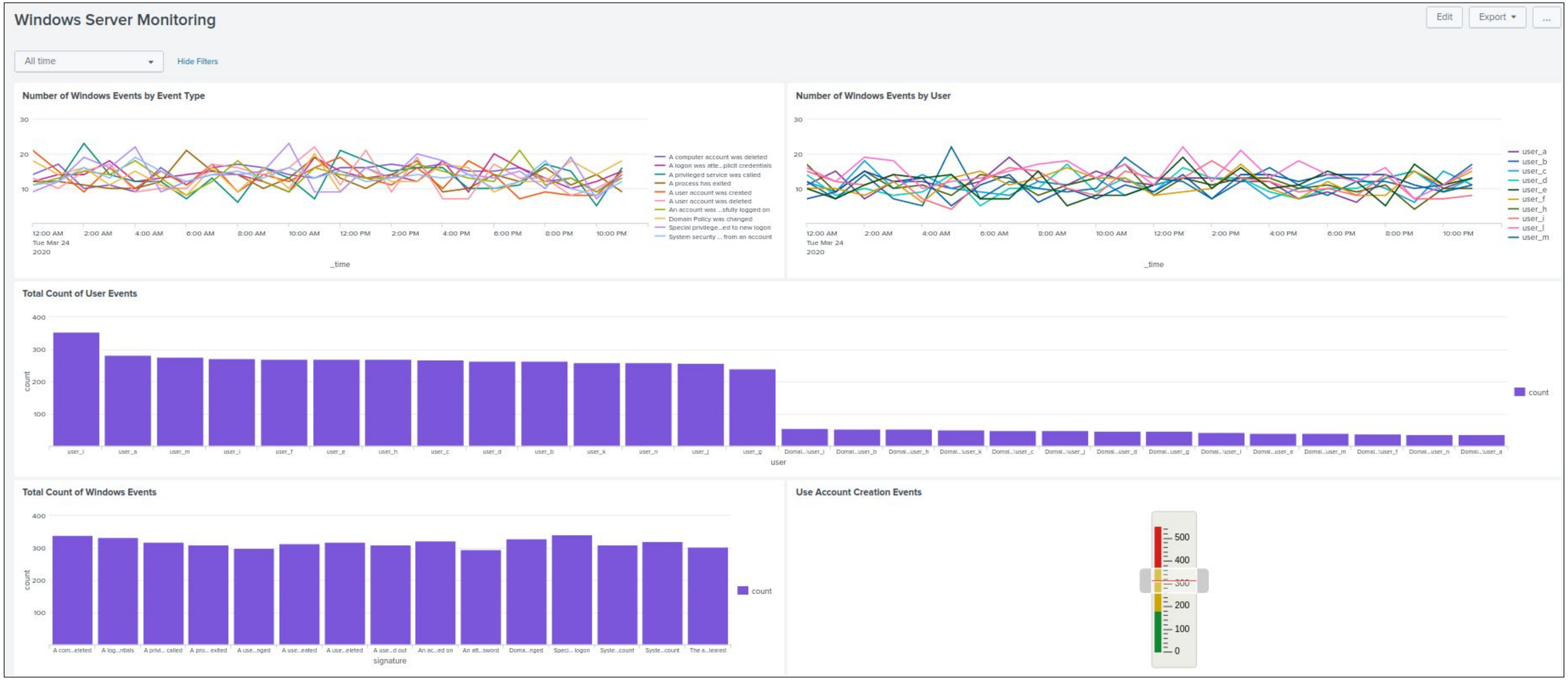
# Alerts—Windows

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Failed Windows Activity | Hourly level of failed Windows activity | 10 | 12 |
| Abnormal Login Attempts | Hourly count of the signature “an account was successfully logged on.” | 20 | 21 |
| Abnormal User Account Deletion Attempts | Hourly count of the signature “a user account was deleted.” | 22 | 23 |

**JUSTIFICATION:** given that VSI is a small company, it has been assumed that the SOC team is limited to one person. To avoid alert fatigue, all alert baselines were determined as 2 standard deviations above the mean, as this accurately captured the outlier data points. A buffer has been applied to the Baseline to determine each Alert Threshold; this ensures that the SOC will be notified of suspicious events.

# Dashboards—Windows



# Apache Logs

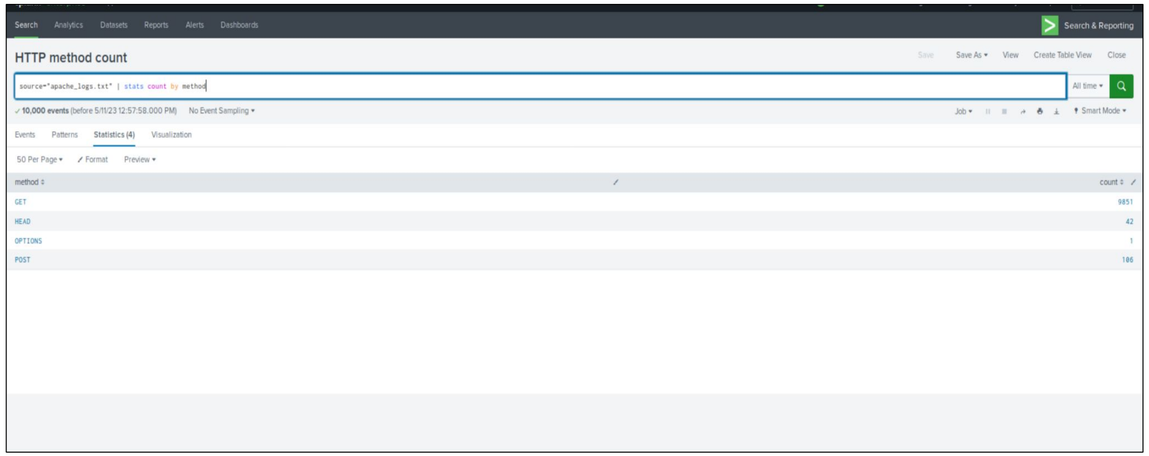
@Marty

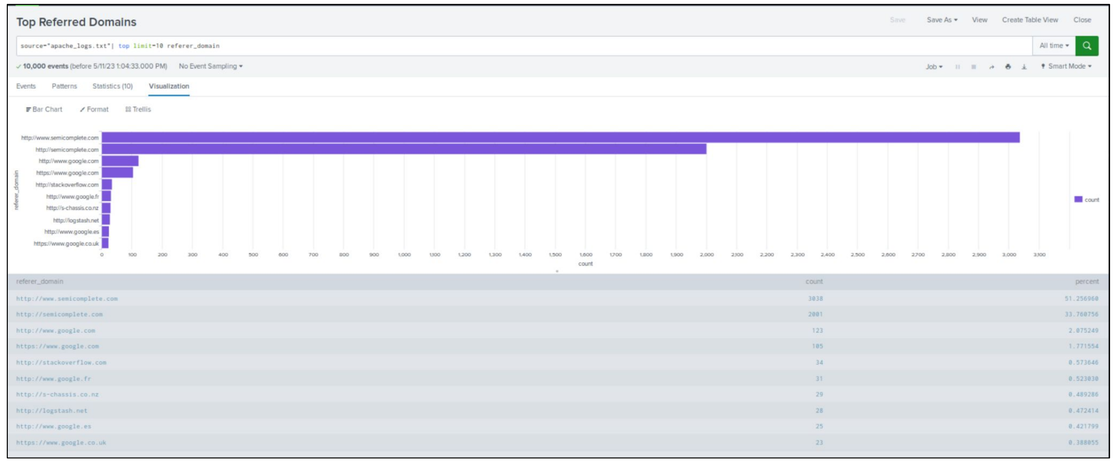
# Reports—Apache

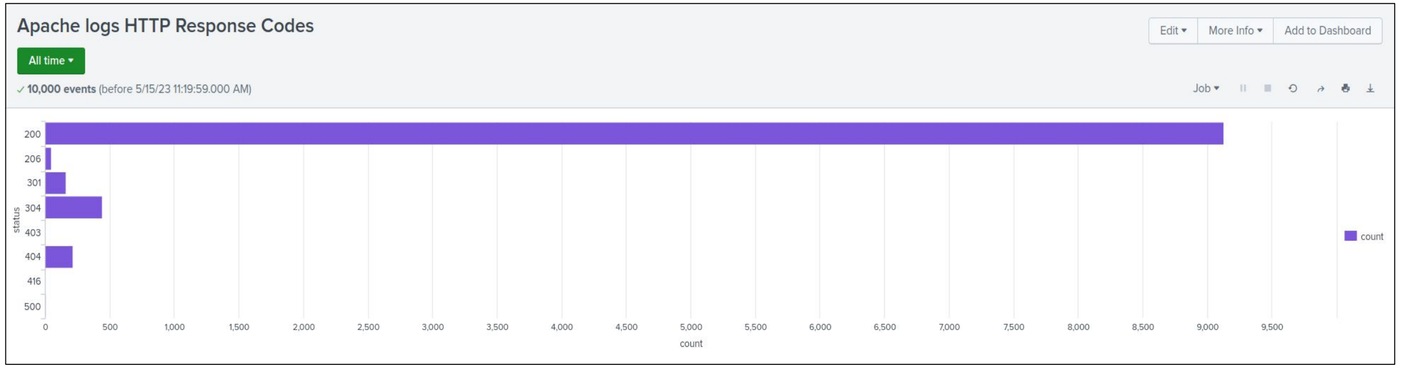
Designed the following reports:

| Report Name | Report Description |
|---|---|
| HTTP Method Count | Report of the type of HTTP activity being requested against VSI's web server. |
| Top Referrer Domains | Report on the top 10 domains that refer to VSI’s website. |
| HTTP Response Code Count | Report on the count of each HTTP response code. |

# Images of Reports—Apache



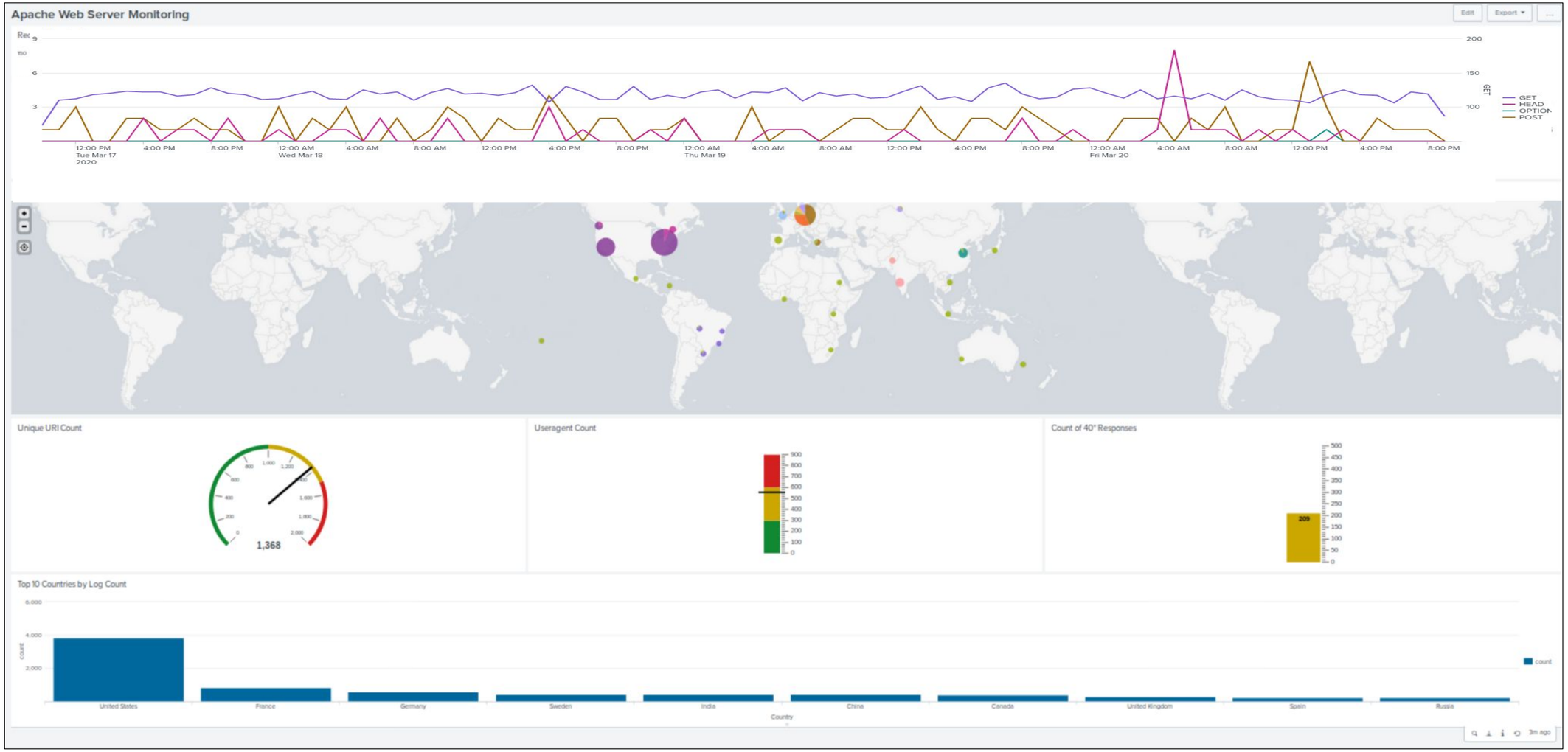
# Alerts—Apache

Designed the following alerts:

| Alert Name | Alert Description | Alert Baseline | Alert Threshold |
|---|---|---|---|
| Abnormal External Traffic Levels | This alert will trigger when the hourly activity from any country besides the United States exceeds the threshold. | 117 | 120 |
| Abnormal HTTP POST Levels | This alert will trigger when the  hourly count of the HTTP POST method exceeds the threshold. | 3 | 5 |

**JUSTIFICATION:** the Windows Log Alerts methodology for Baselines and Thresholds has also been applied to the Apache Logs for the same reasons outlined in the Windows Log justification.

# Dashboards—Apache



# Attack Analysis - Windows

@Nick

# Attack Summary—Windows

Summary of findings from Windows reports after analyzing the attack logs.

**Report Analysis for Severity**

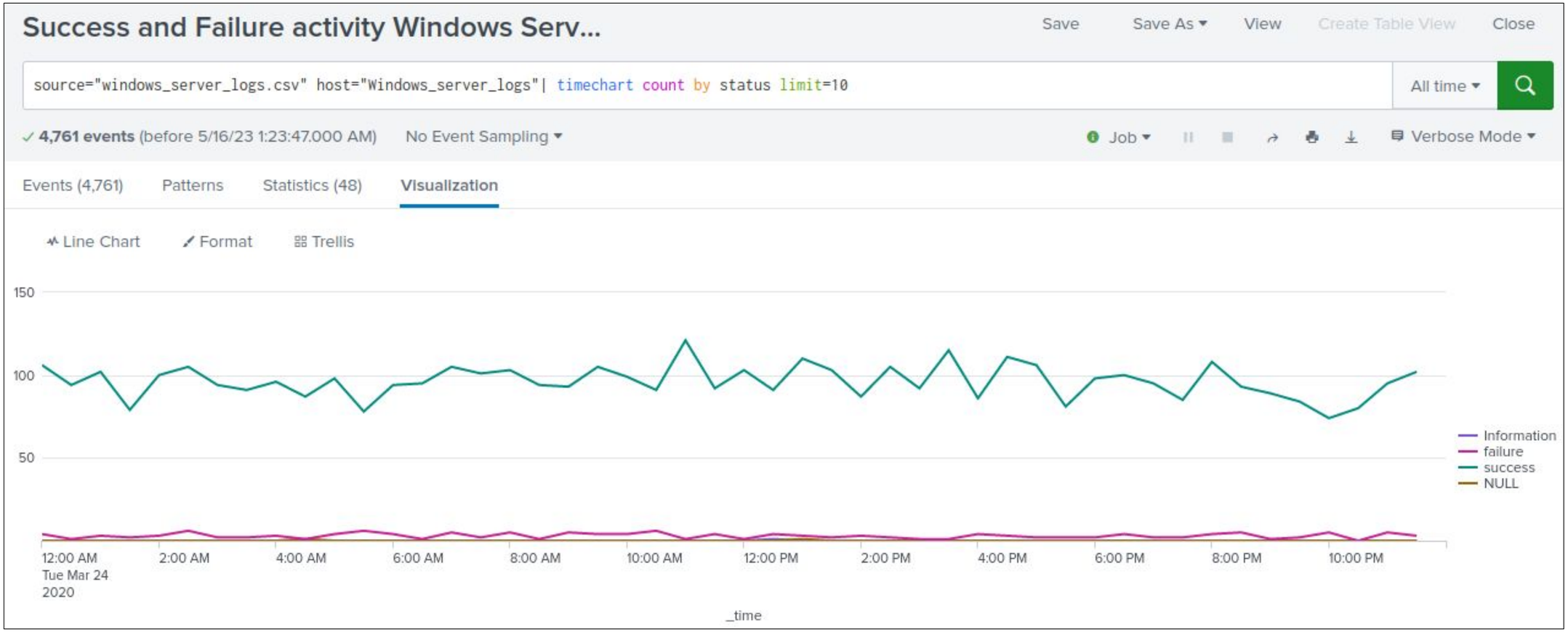
- High ‘severity’ increased to 1,111 from 329

**Report Analysis for Failed Activities**

- Wed March 25th 2020, 8.30 am there was a small spike of failed activity. The rest of the day there were only small incidents.

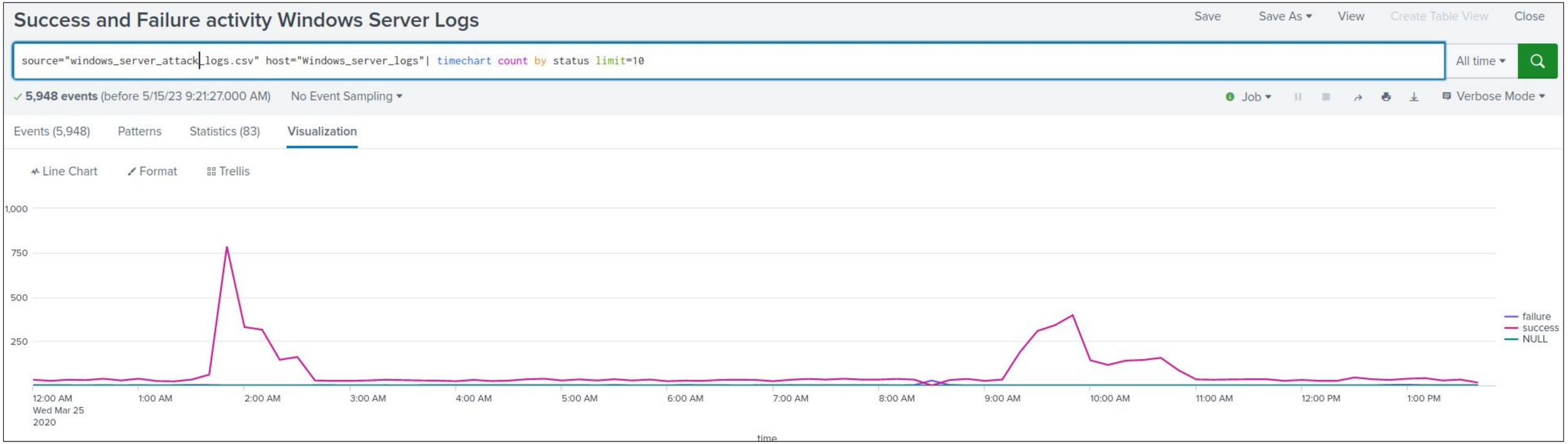
# Attack Summary—Windows

## Baseline



# Attack Summary—Windows

## Attack Data



# Attack Summary—Windows

Summary of findings from Windows alerts after analyzing the attack logs. Were the thresholds correct?

### Alert Analysis for Failed Windows Activity

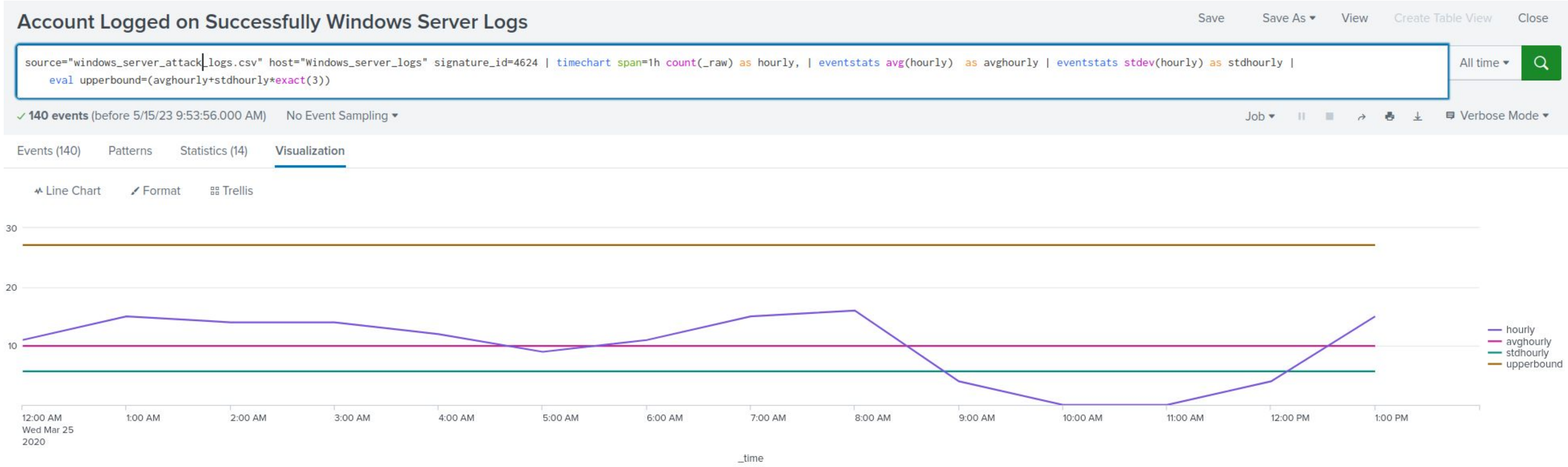
- Failures began on the **evening of March 24th 2020**. The largest spike in failures (35 total) occurred on March 25th at 8:00 am.
- The **alert threshold of 12** would have captured this activity in an alert.

### Alert Analysis for Successful Logins

- Suspicious number of successful logins for ‘user_j’ between 11:00 am and 12:00 pm.
- 196 successful logins in the first hour and and 75 successful logins in the following hour
- Alert threshold of ‘greater than 21’ would have detected this suspicious event if we had used the signature name rather than ID.
- Interestly these login attempts were not captured when using the alert with the signature id as the source. The 196 successful login attempts were only captured when using the signature name.

# Attack Summary—Windows

There appears to be an issue with the ingest of ‘signature_id’; the below visualisation shows 0 successful login attempts, however when viewing the same search with the corresponding signature name, it shows an inverse result.



# Attack Summary—Windows

Summary of findings from Windows dashboards after analyzing the attack logs.

**Dashboard Analysis for Signatures**

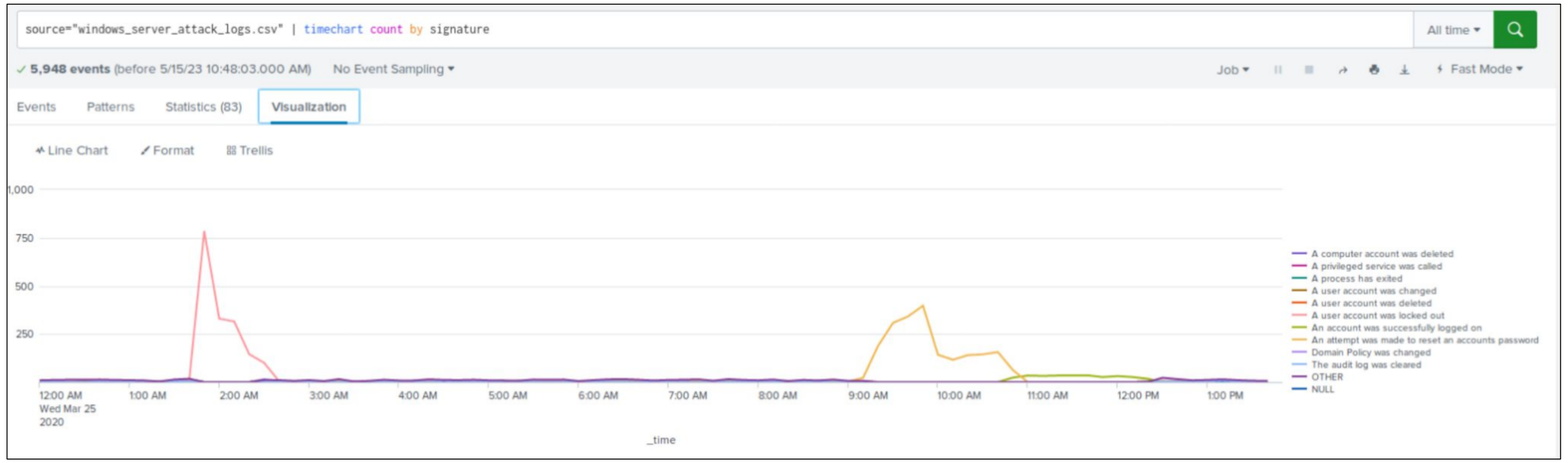
- There is a large volume of activity on Wed the 25th of March 2020 for User_a, User_k and User_j.
- We also see an overall drop in successful account logins.
- Between 1:00 am and 2:00 am we see a peak lockout of 896 and at between 9:00 am and 10:00 am we see a peak of 1,258 password resets.
- Access to user accounts via a password reset method appears to have been successful, with a total of 271 successful login attempts following the spike password reset events.

**Dashboard Analysis for Users**

- **user_a** has activity that correlates with the large amount of **lockout activity**.
- **user_k** has activity correlating with the large amount **password reset activity**.
- **user_j** has activity correlating with the large amount **successful login activity**.

# Screenshots of Attack Logs

## Analysis for Failed Activities




## Updated Windows Web Server Monitoring Dashboard

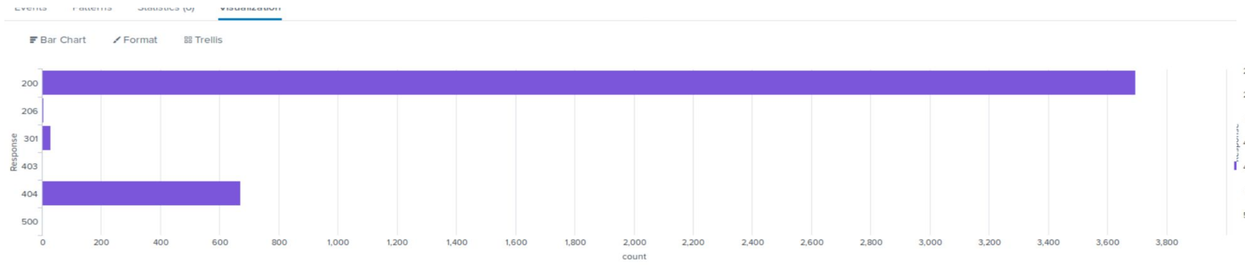
# Attack Analysis - Apache

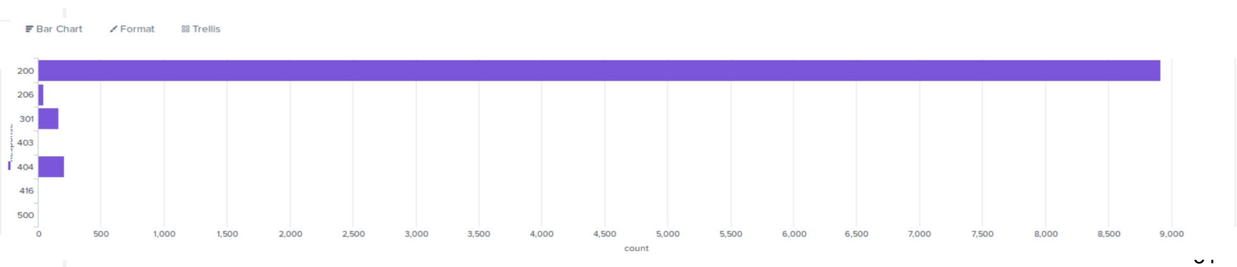
@Nick

# Attack Summary—Apache

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

- **GET and POST requests increased dramatically**. **GET** requests went from an average of roughly **120 per hour to 729** and **POST** requests increased from a rough average of **2 per hour to 1296**
- **GET requests** begin at **5:00 pm**, reaching its apex at **6:00 pm** and returning to normal by **7:00 pm**.
- **POST requests** begin climbing at **7:00 pm**, peaking at **8:00 pm** and returning to normal by **9:00 pm**.
- There was a significant reduction in the count of referrer domains with the results being almost a quarter of when compared with typical results. The actual sources of the domains remained similar if not the same.
- **Significant** relative increase in **404 responses**. (4,497 events with 671 404 responses, 10,000 events with 205 404 responses).



# Attack Summary—Apache

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

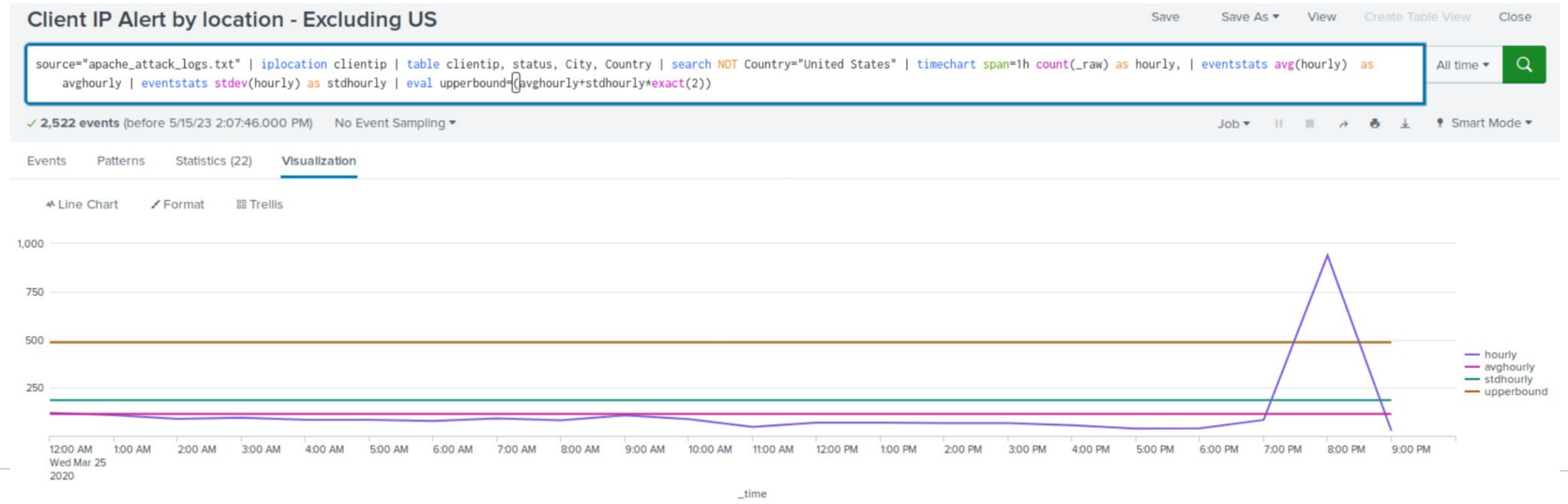
Date of attack- 25th of March 2020

- **GET Alert threshold of 125**

  Attack occurred between **7 to 8pm** - **peaked at 939**.

- **Post Alert threshold of 5**

  The peak of POST requests occurred at **8pm with a count of 1296**.

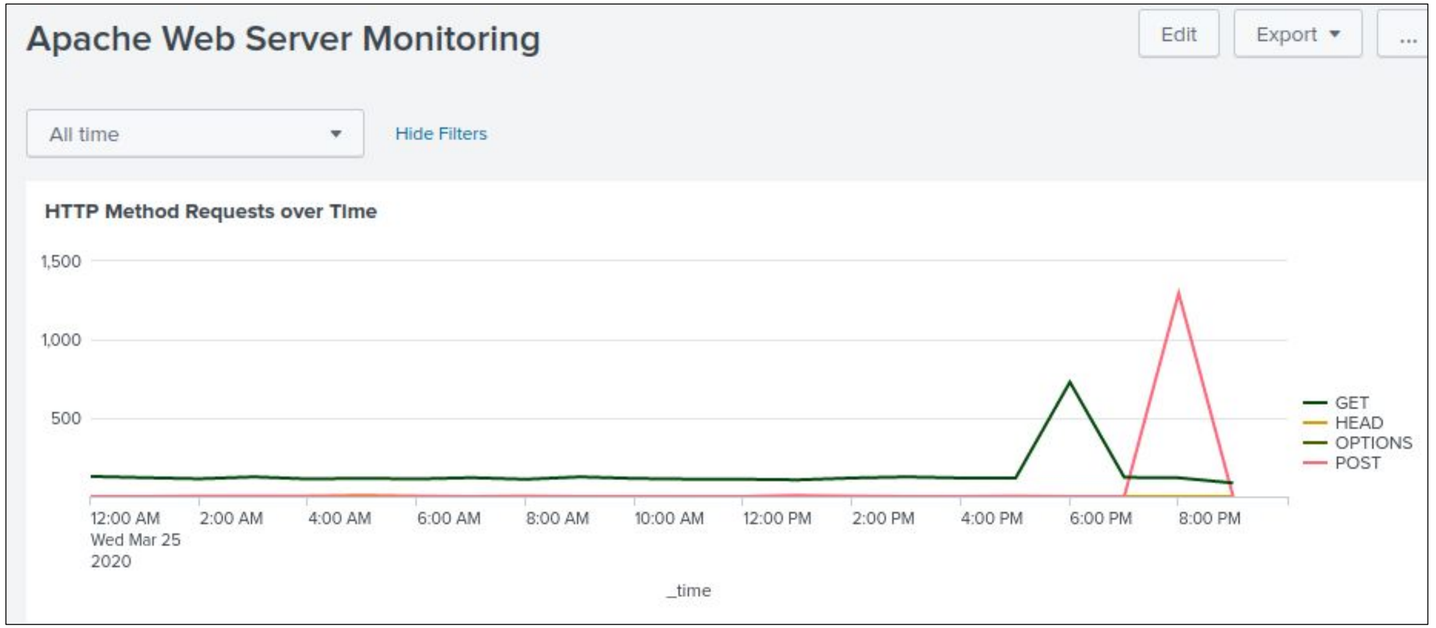


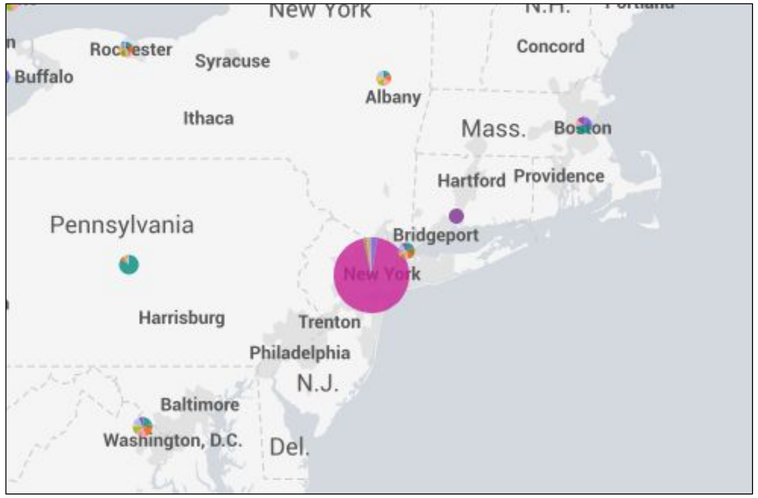
# Attack Summary—Apache

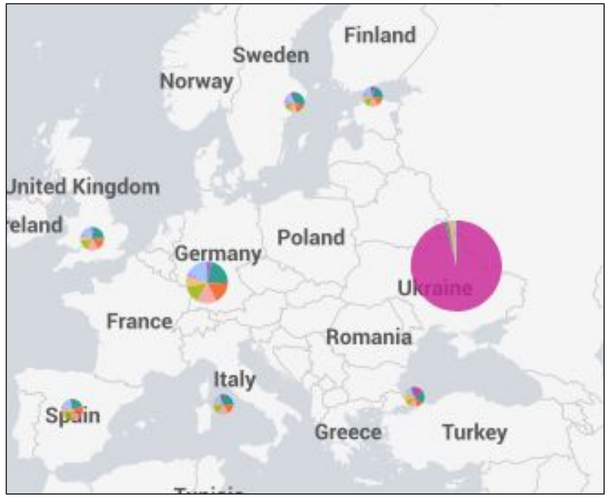
Summarize your findings from your **dashboards** when analyzing the attack logs.

- At **6pm** on Wednesday the 25th of March 2020 **GET requests** spiked to **729**. More concerning was the **POST request** which hit **1296 at 8pm**.
- At this time there was also huge spike in activity from both **New York** and **Kharkiv in Ukraine**.
- The activity from Ukraine matches the **brute force** at the time and numbers.
- Therefore we can surmise that a brute force took place from the Ukraine on the VSI webserver.

# Screenshots of Attack Logs



# Summary and Future Mitigations

@Marty

# Project 3 Summary

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

- A Brute force attack was attempted on the VSI machines on 25th March 2020 as evidenced by an increase in login attempts/POST requests to the web server
- This attack was successful as evidenced by a spike in successful logins
- It is probable that the password reset function on the login page was utilised for the bruteforce attack
- The attack appears to have originated from Ukraine

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

- Enhance log analysis and malicious event detection through the use of the SSE application
- Evaluate if exposed VSI assets are required in order to reduce the attack surface
- Implementation of an IPS to block IP Addresses of suspicious users