Defensive Security Project
by: Group 4

David Markey, Brian Zelig, Hector Nunez, Bianca Polanco, Susan Cupito, Alex Ramirez

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- We developed a comprehensive baseline for monitoring network activity within a company using Splunk, focusing on two key areas:
  - Apache web server logs and activity within a Windows environment.

By analyzing log data, including login failures, suspicious activity, and signature-based patterns, we were able to establish an effective baseline for creating alerts and generating reports.

This baseline was then used to assess attack logs and gain insights into ongoing network activity, helping to identify and investigate potential security incidents.

Logs Analyzed

1 Windows Logs

Event Severity and Failures:

- Logs track the severity of events and failed login attempts, helping identify issues like brute force attacks or misconfigurations.

Successful Logins:

- Records successful logins, user IDs, and timestamps, highlighting unusual login patterns that could indicate suspicious behavior.

User Account Changes:

- Tracks account lockouts, password resets, and deletions, which can point to malicious activity or system mismanagement.

Logon Attempts:

- Captures failed logins, signaling potential brute force attacks or unauthorized access attempts.

Signature and User Activity:

- Logs user activities (e.g., password resets), allowing you to detect suspicious behavior and correlate events with specific users.

2 Apache Logs

HTTP Methods:

- Logs HTTP request methods (e.g., **GET**, **POST**) and their counts, helping identify potential attacks like DDoS or brute force.

Referrer Data:

- Tracks where requests are coming from, helping spot suspicious or unexpected traffic sources.

HTTP Response Codes:

- Records server response codes (e.g., 404, 500), with high 404 counts possibly indicating probing or reconnaissance.

International Traffic:

- Tracks the geographical origin of traffic, highlighting suspicious activity from unusual locations.

URI Data:

- Logs the exact endpoints being accessed, helping identify targeted resources or exploited vulnerabilities.

Windows Logs

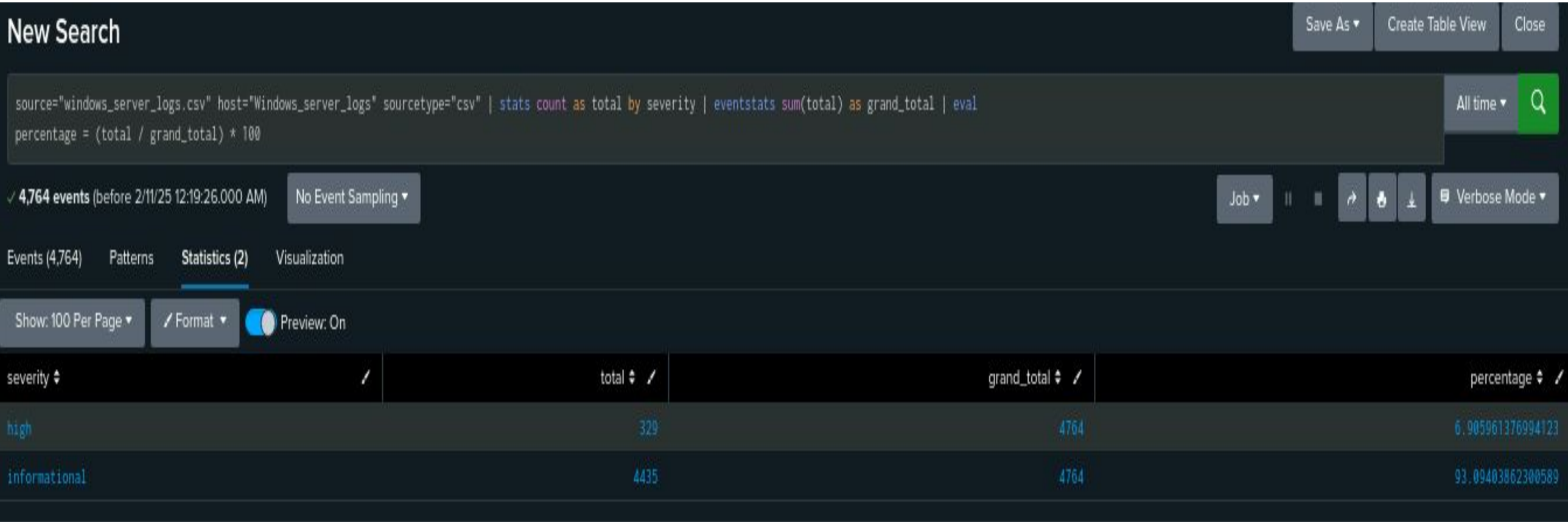
Reports—Windows

Designed the following reports:

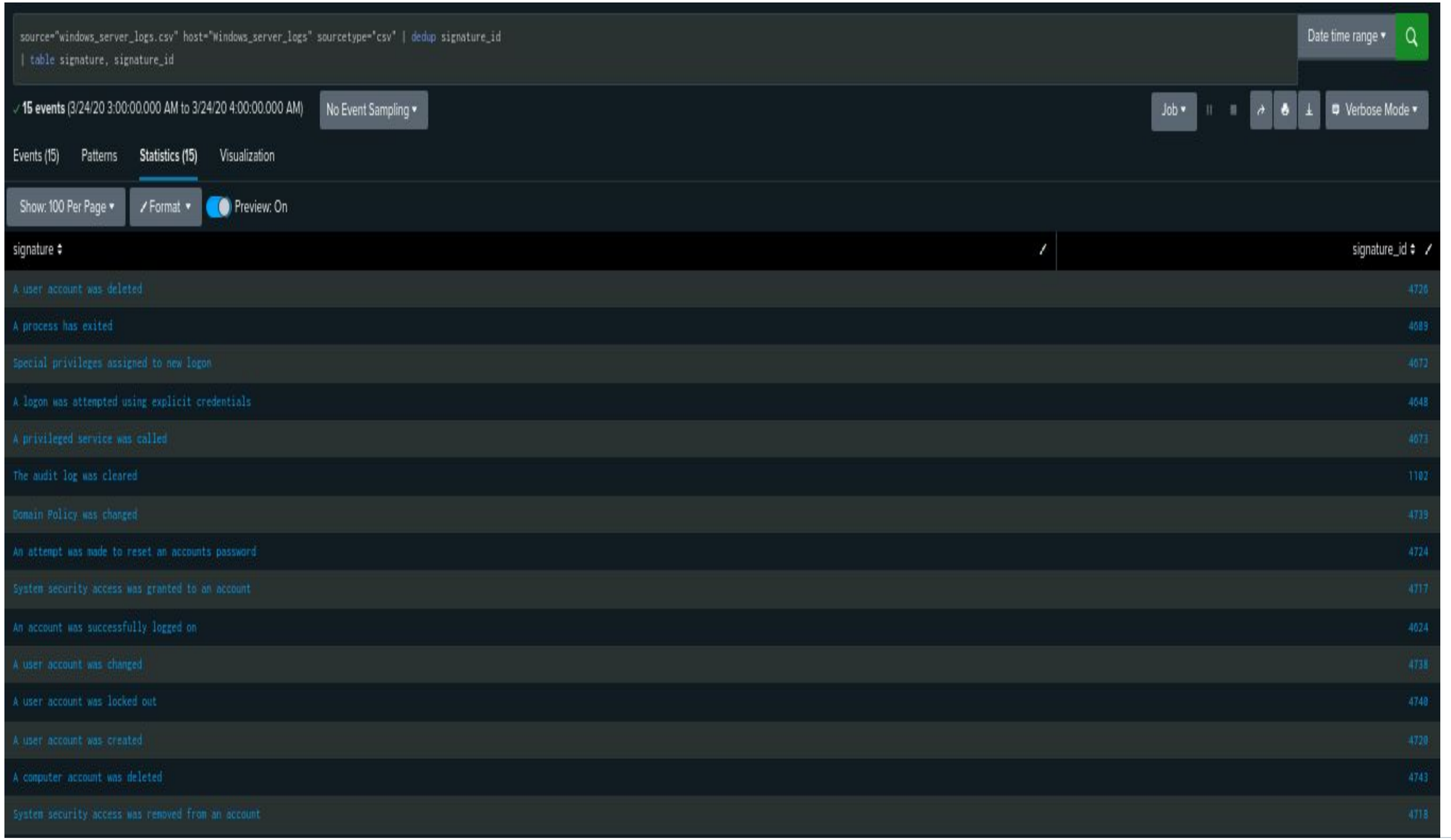
Report Name	Report Description
Report Analysis for Severity	● Logs track the severity of events (High or Informationional)
Report Analysis for Failed Activities	● Logs failed login attempts, helping identify issues like brute force attacks or misconfigurations.
Report for Signature analysis	● Logs user activities (e.g., password resets), allowing you to detect suspicious behavior and correlate events with specific users.

Severity

Level of high severity events during normal operations



Signature ID’s



Logs in Windows previews to the attack gives us the main ID’s of activities in the logs

Baseline Success and Failures

Successful vs. failed activities during normal operations

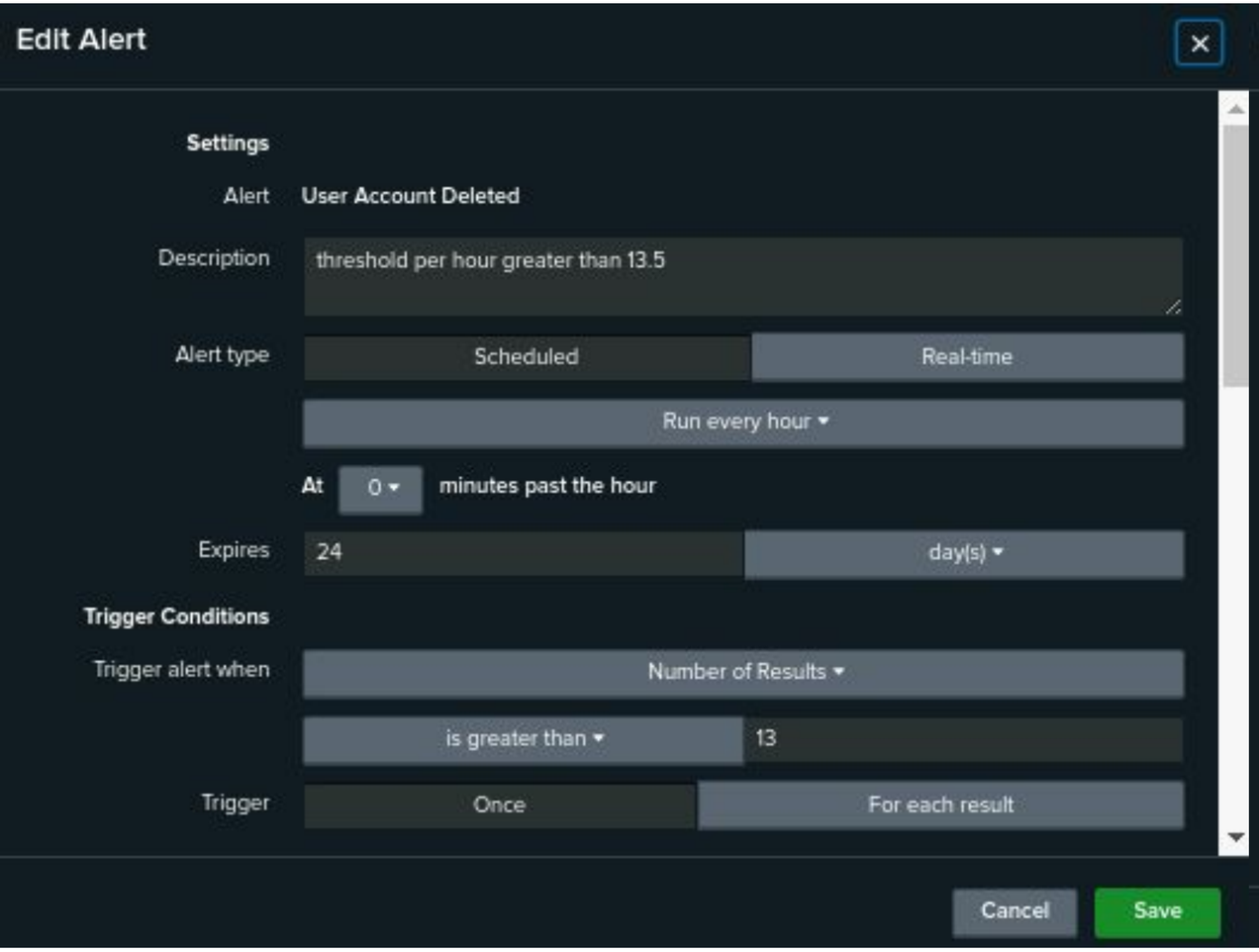
Alerts—Windows

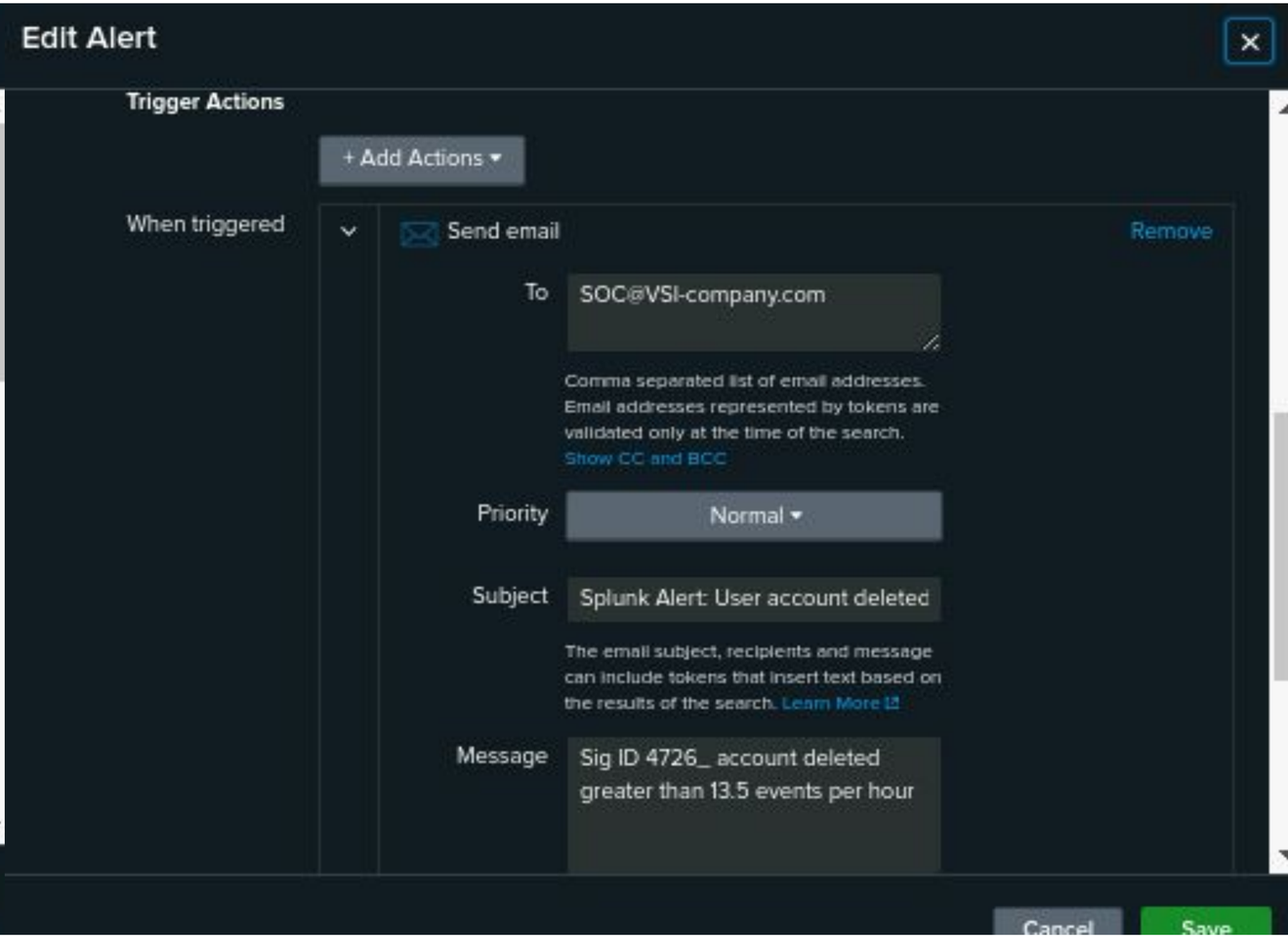
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deleted	Looks for user account deleted events	threshold set to greater than 13.5	13 >
Failed Windows Activity	Checks for failures in Windows logs	baseline average showed greater than 5.9	Alert was set to greater than 6
Successful Logins	Checks for too many successful logins	determined average was 14	Alert was set to greater than 14

User Account Deleted

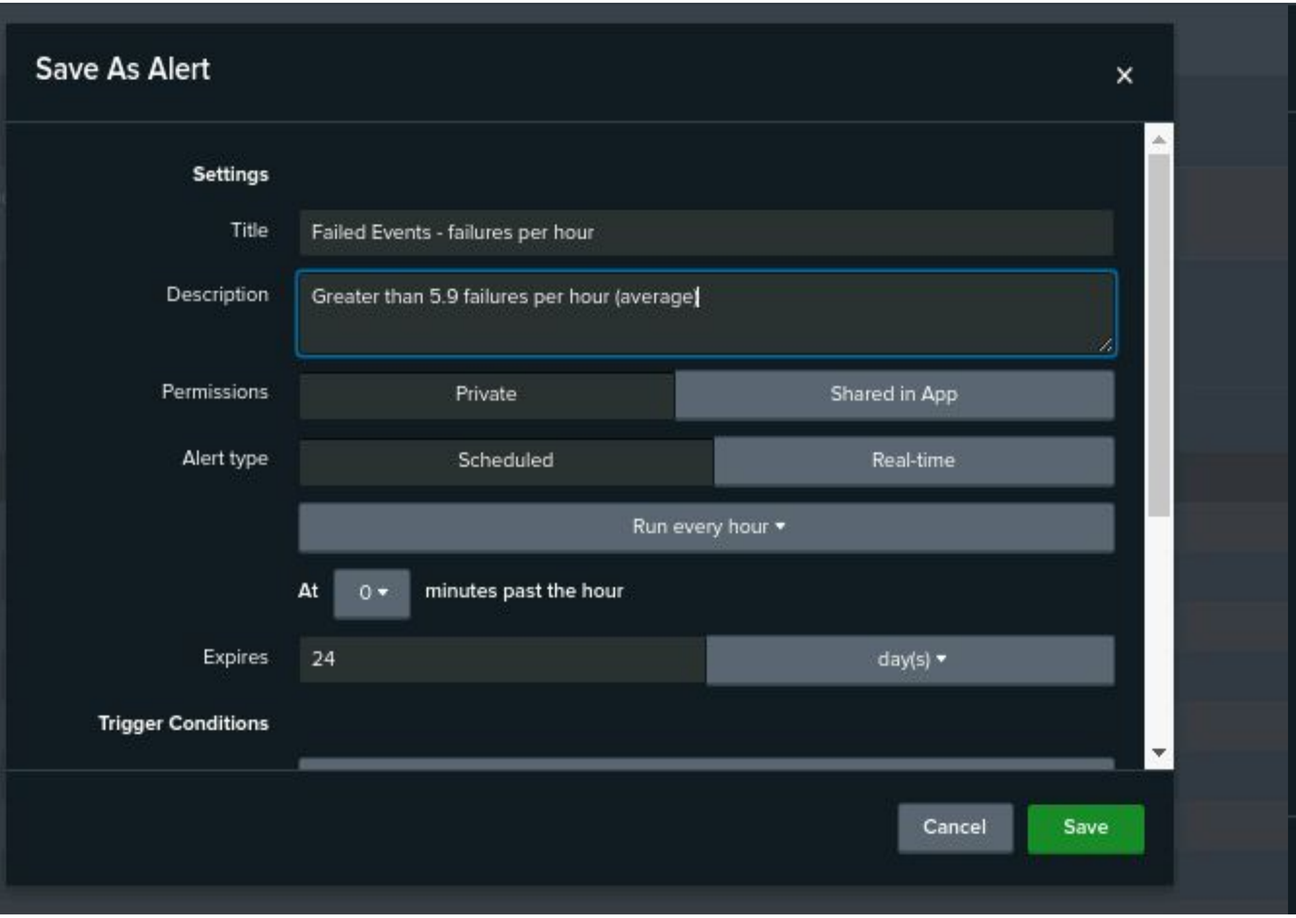
Alert to notify SOC of abnormal user account deletions

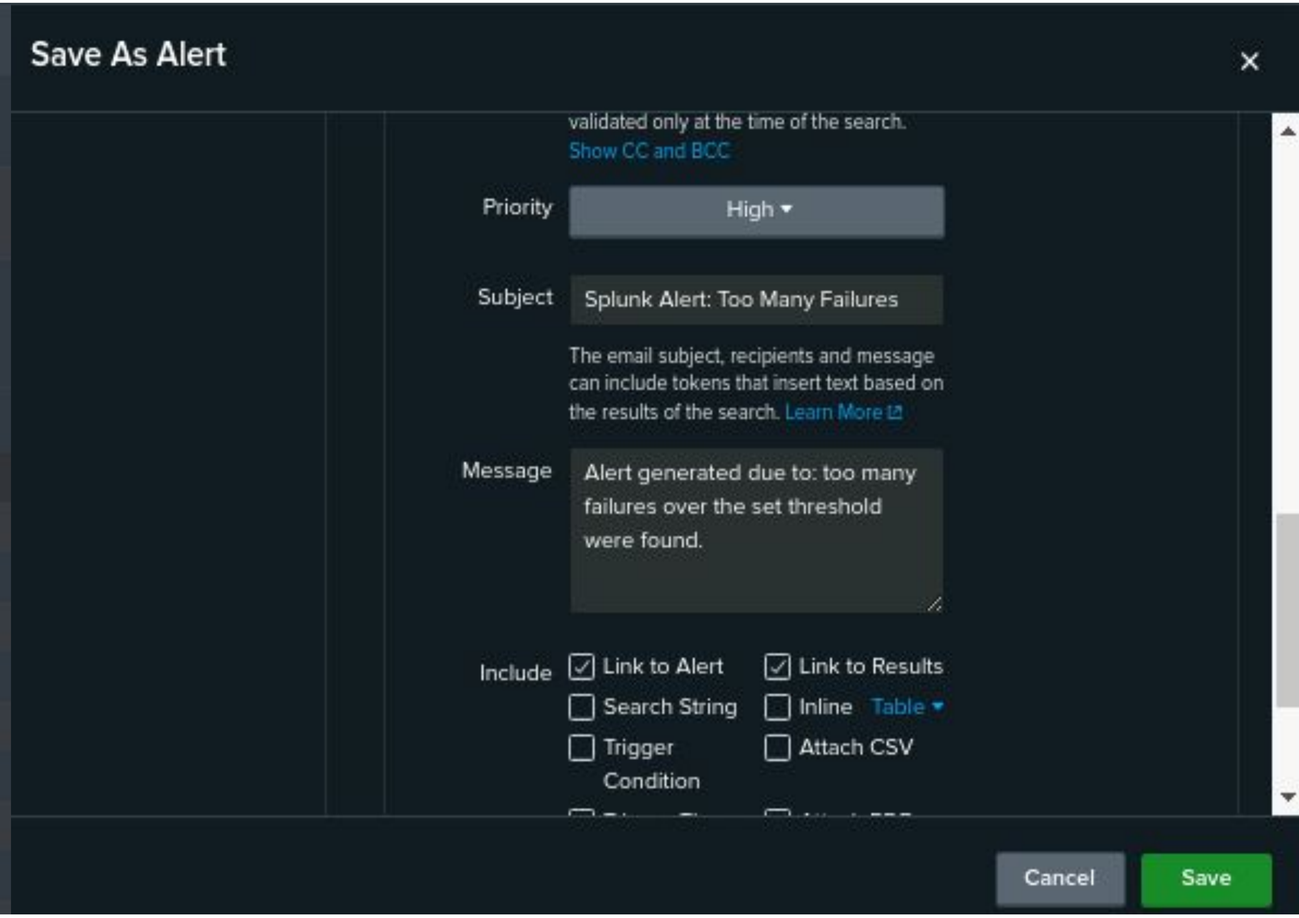




Failed Windows activity

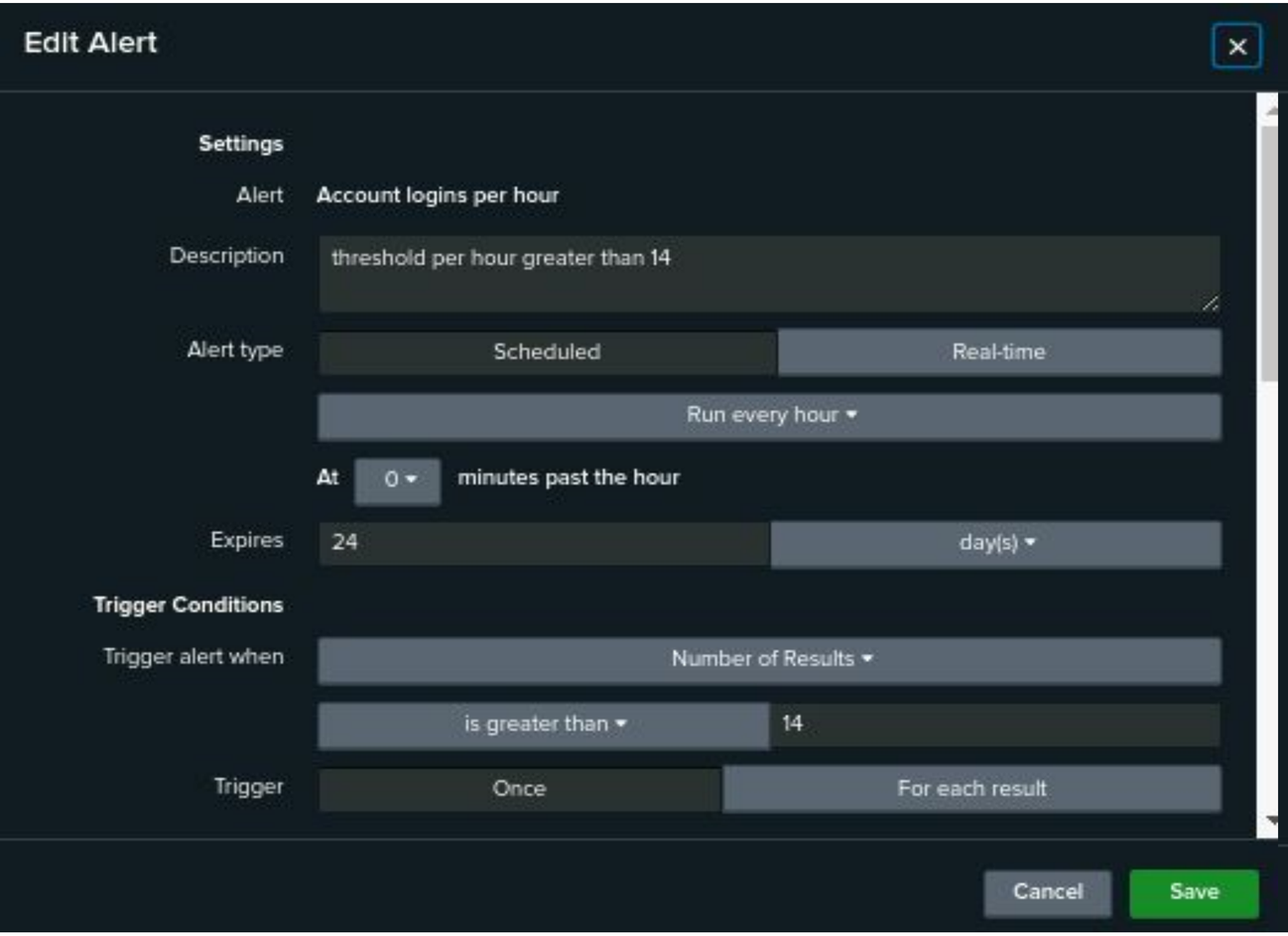
Alert to notify SOC of abnormal failed Windows activity

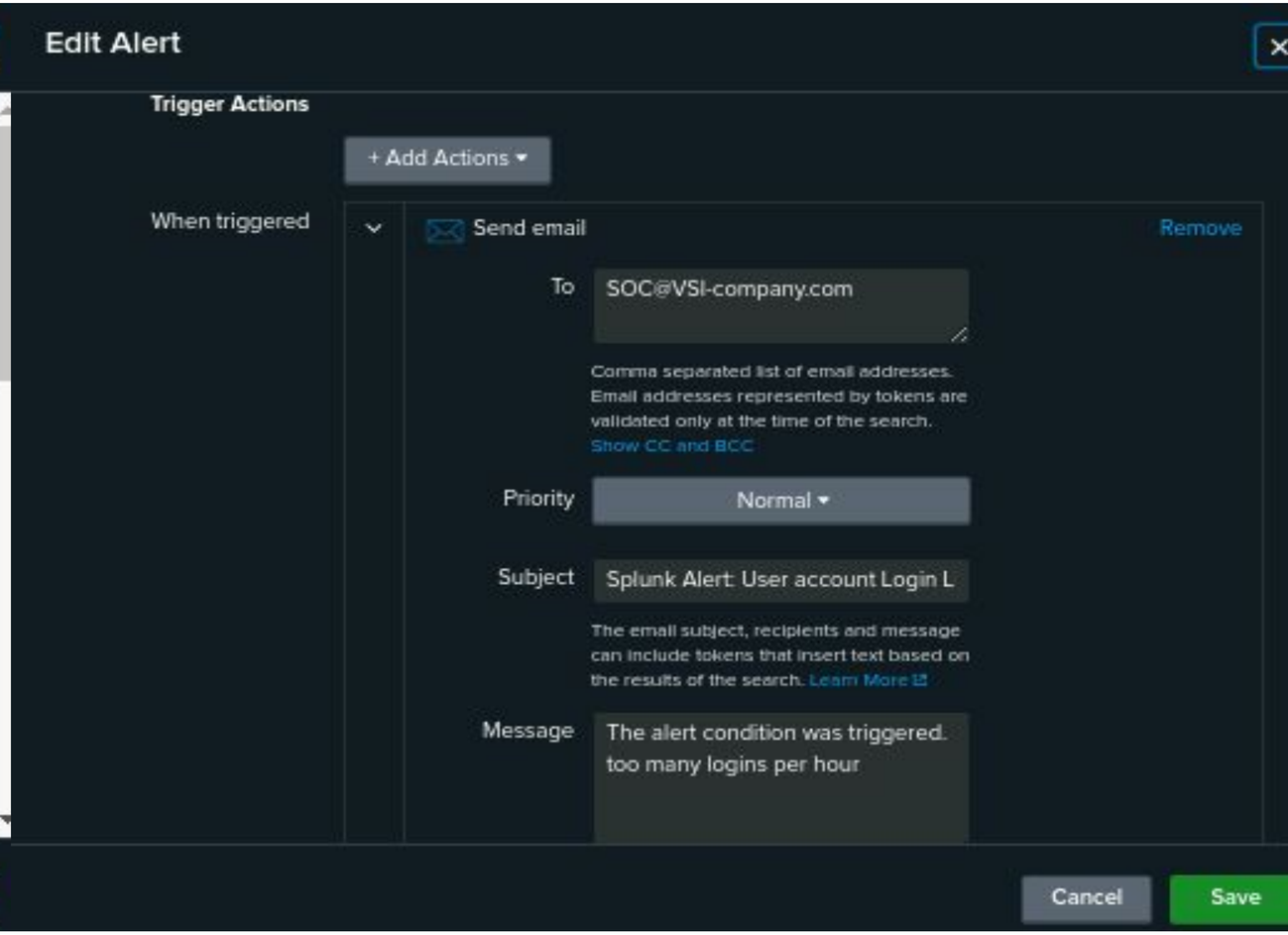




Successful Logins

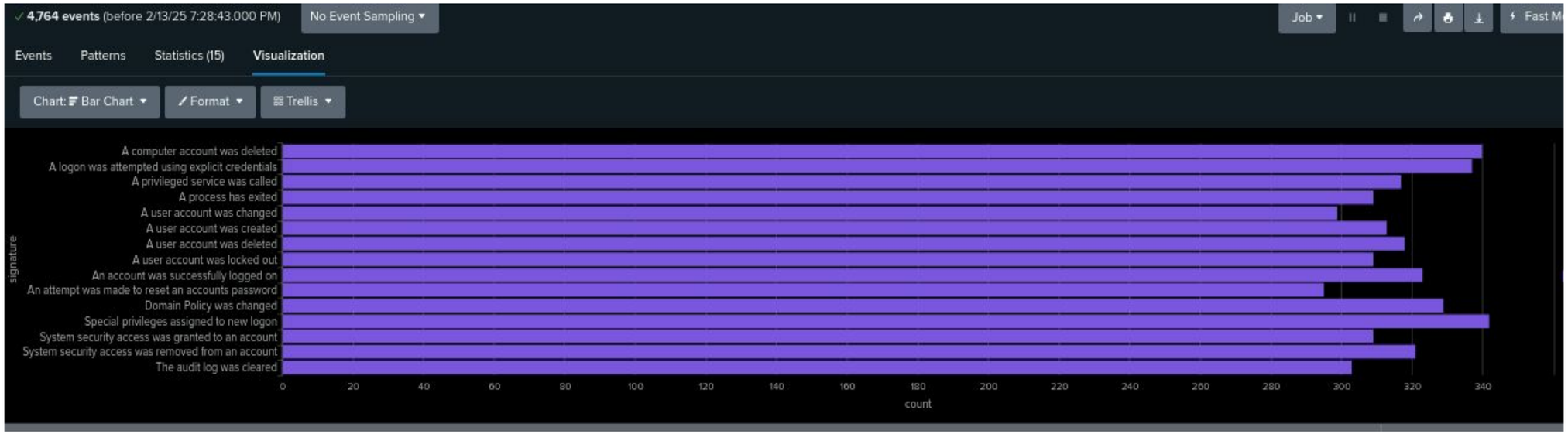
Alert to notify SOC of abnormal successful logins

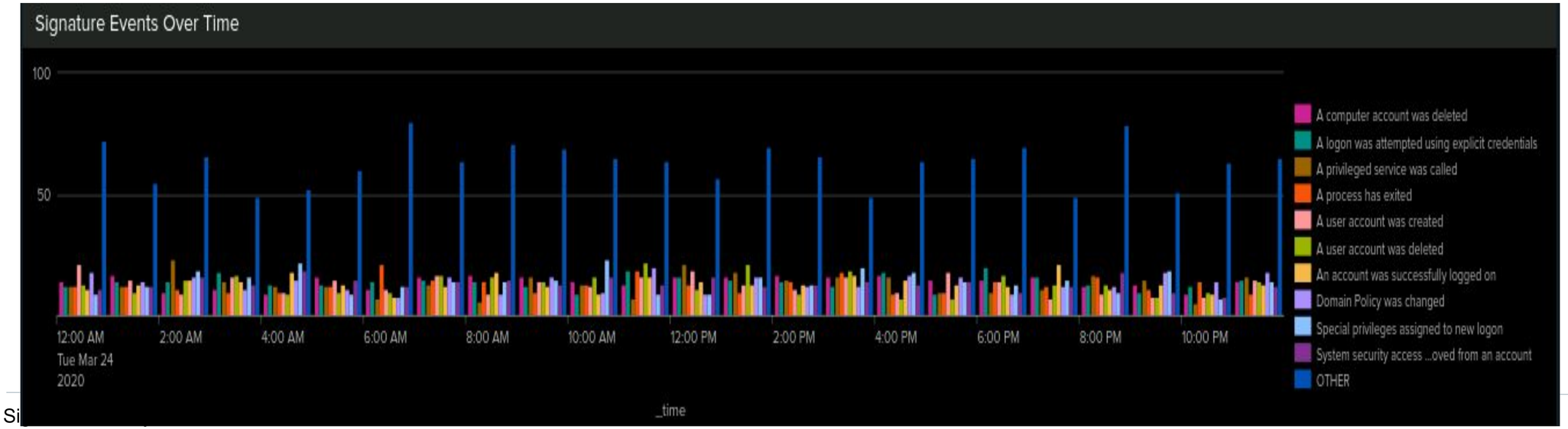




Dashboards—Windows

Signature Activity





Based on the signature's activities we can see their total frequency and the hourly frequency of such activities before the attack

Dashboards—Windows

User Activity

These graphs gives us an insight on the total activity per user before the attack and the hourly activity per hour

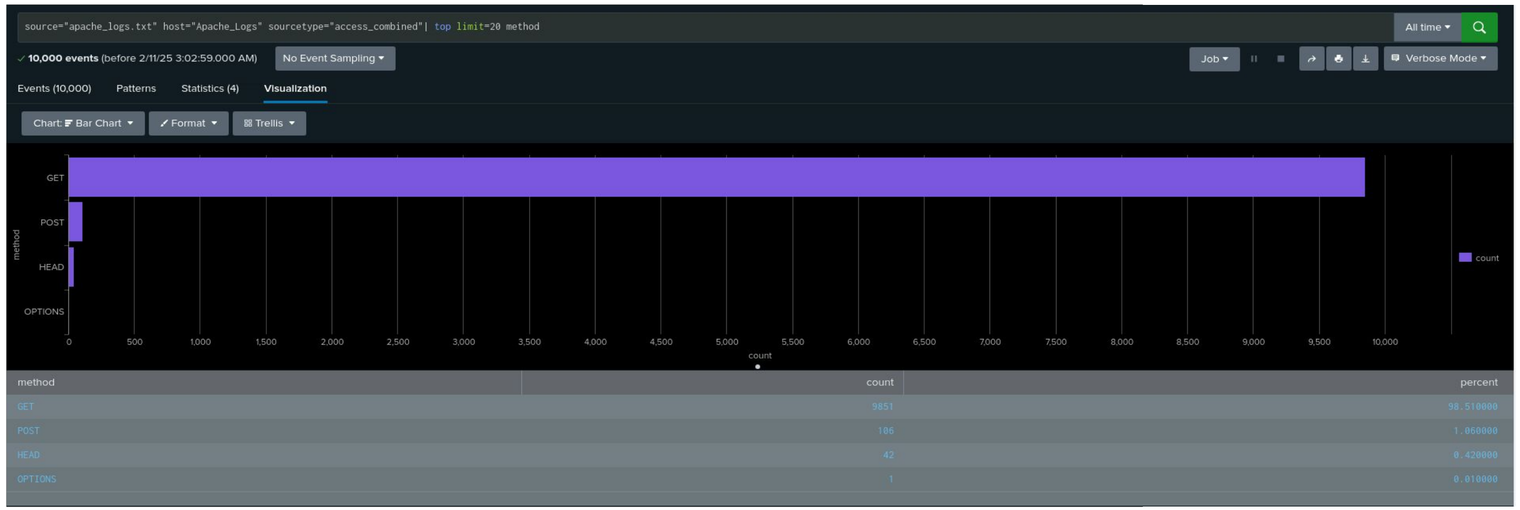
Apache Logs

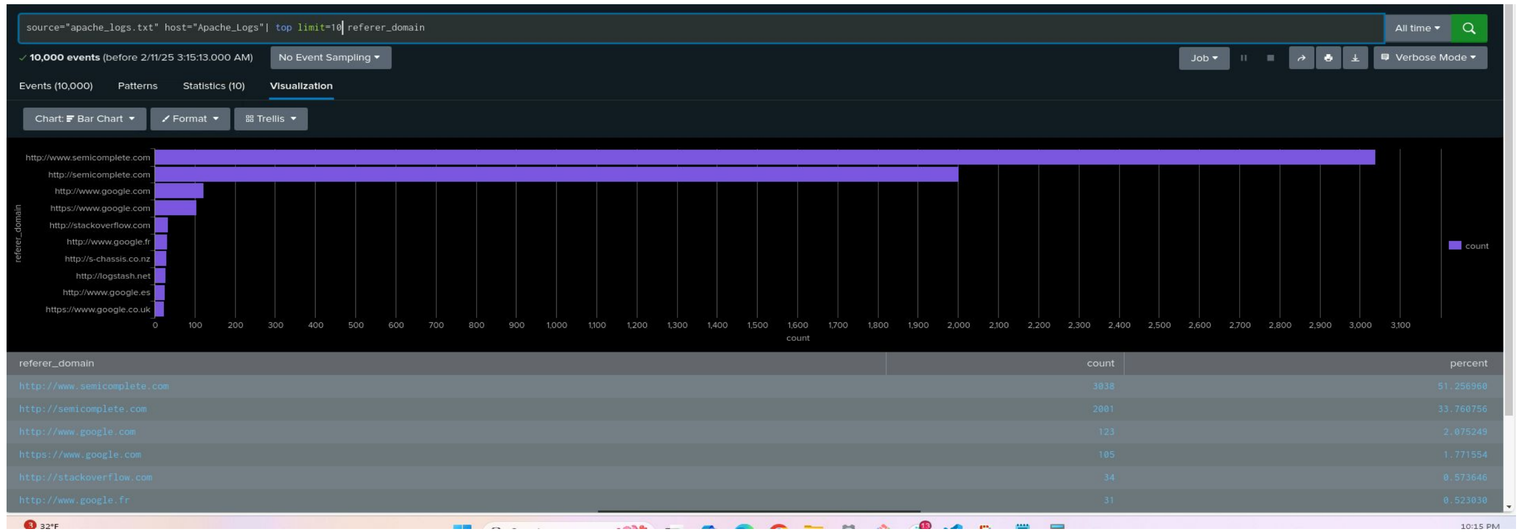
Reports—Apache

Designed the following reports:

Report Name	Report Description
Different HTTP Methods Report	• This report shows a table of different HTTP methods that gives a better look at the type of HTTP activity that is being requested against the VSI web server.
Top 10 Referred Domains Report	• This report generates the top 10 domains can be identified as suspicious referrers that may be used for malicious purposes.
HTTP Response Code Report	• This report shows suspicious levels of HTTP responses.

Images of Reports—Apache





To see the activities of the Apache's server before the attack we made graphs that measures the HTTP requests and top domains

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity Based on Countries	Showcase the activity in the server relative to the country	73.095	74

JUSTIFICATION: We took the average alerts per hour and used that as the baseline. We raised it to create the threshold.

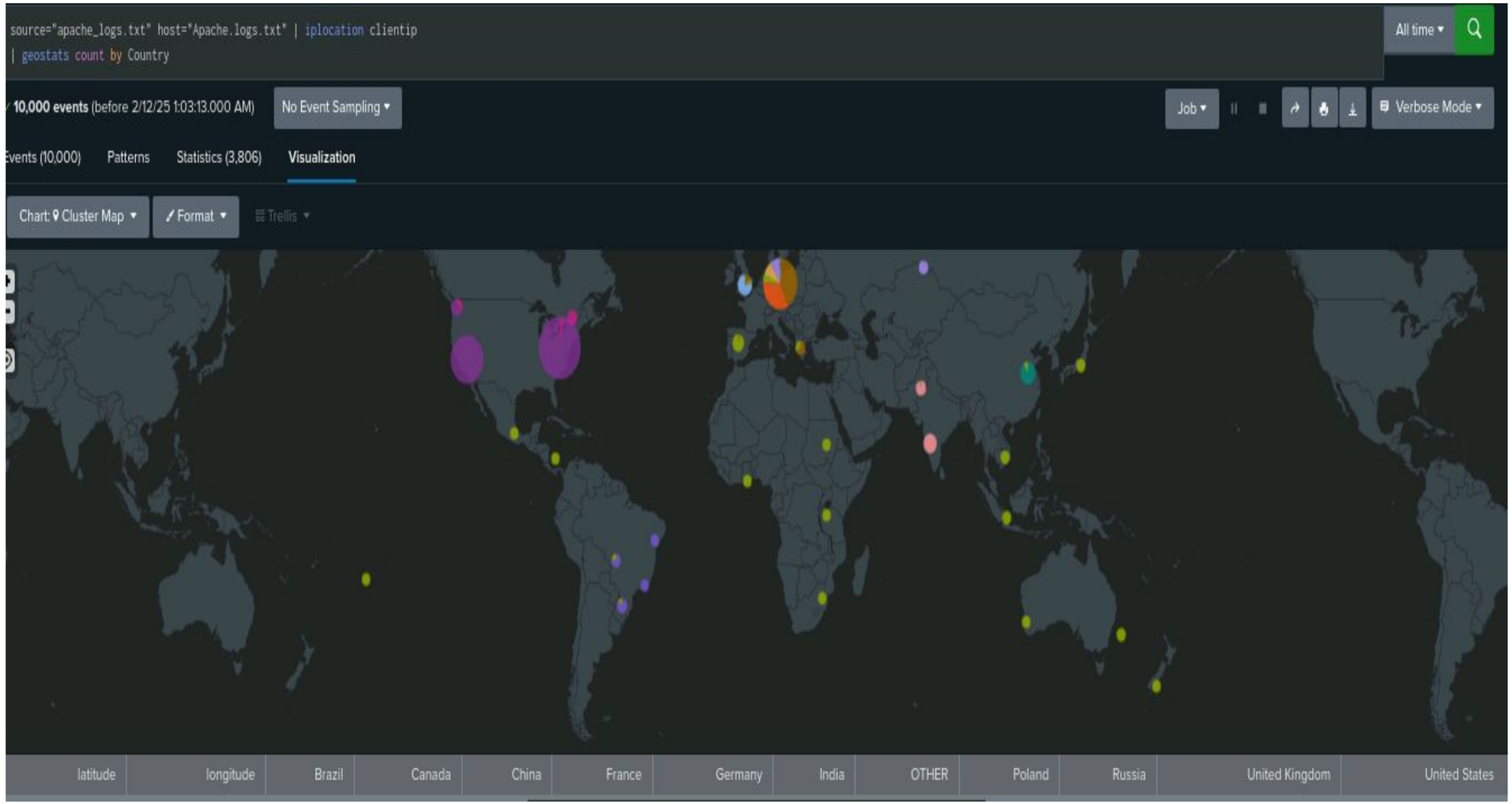
Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Alert for HTTP POST activity	The activity will showcase POST request activities in the server	100	150

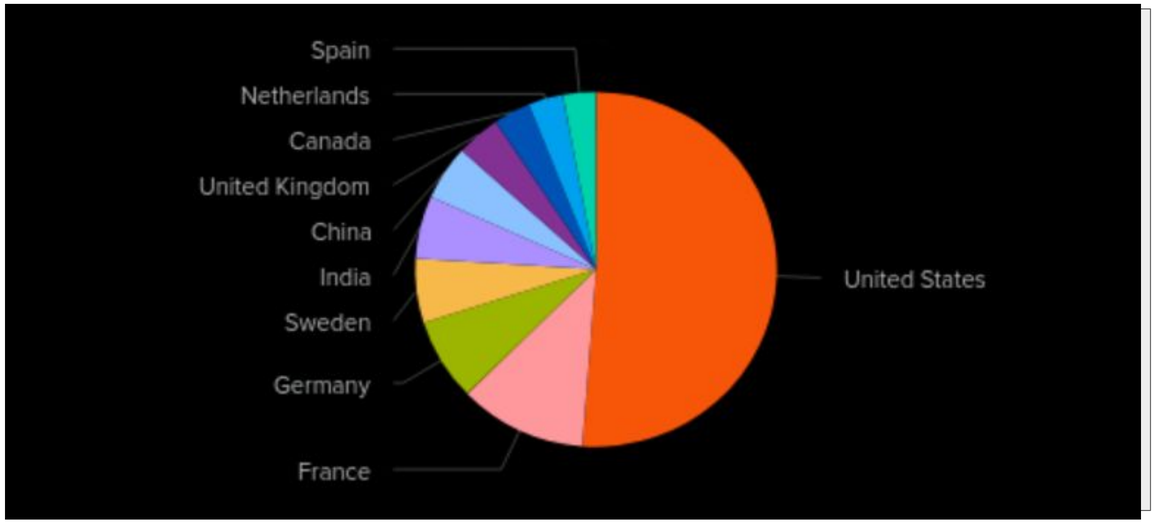
JUSTIFICATION: The average POST request went from 75 to a 100

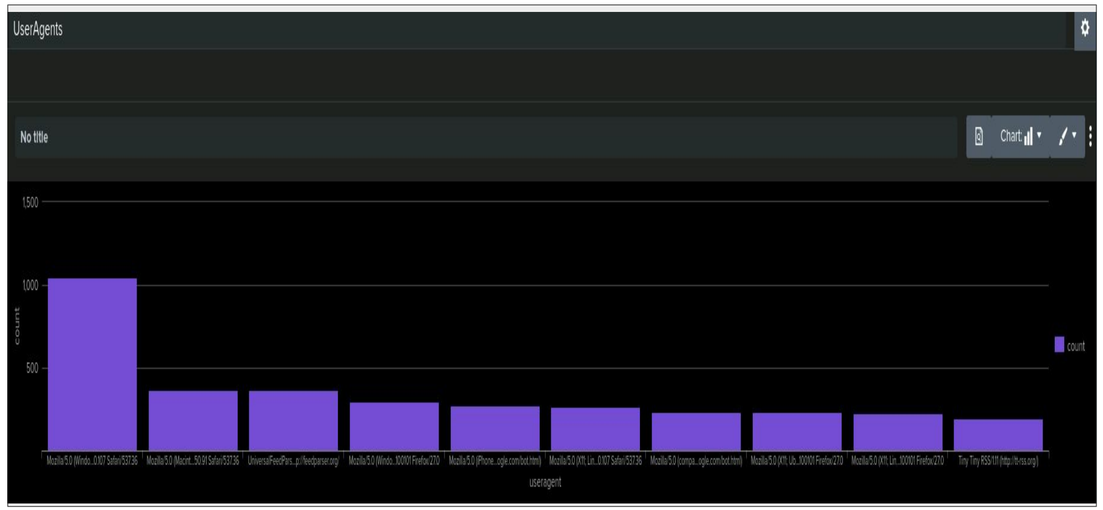
Dashboards-Apache

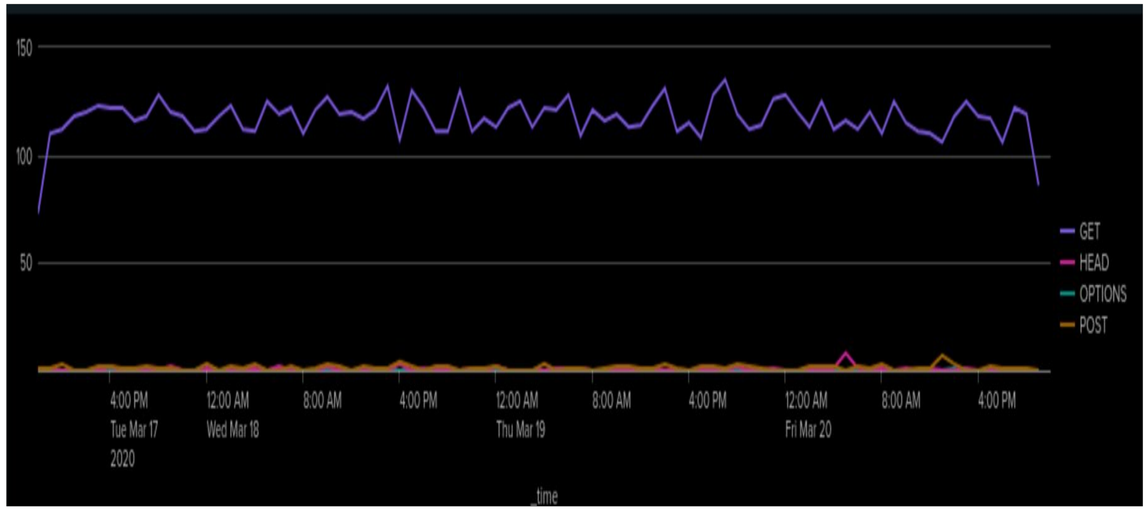


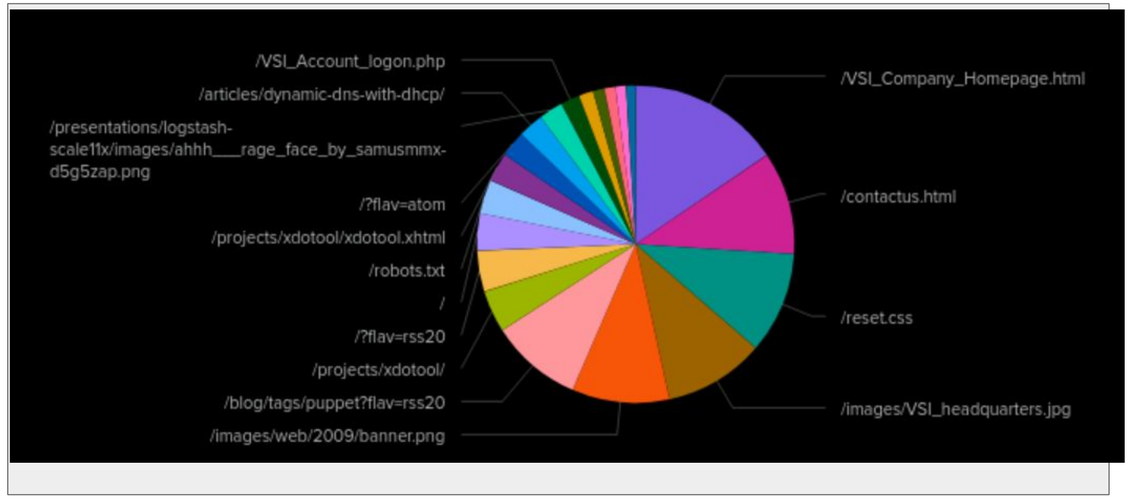
Besides the top domains and the requests, we wanted to have a clear picture from where the traffic was coming from through the following graph

Dashboards—Apache







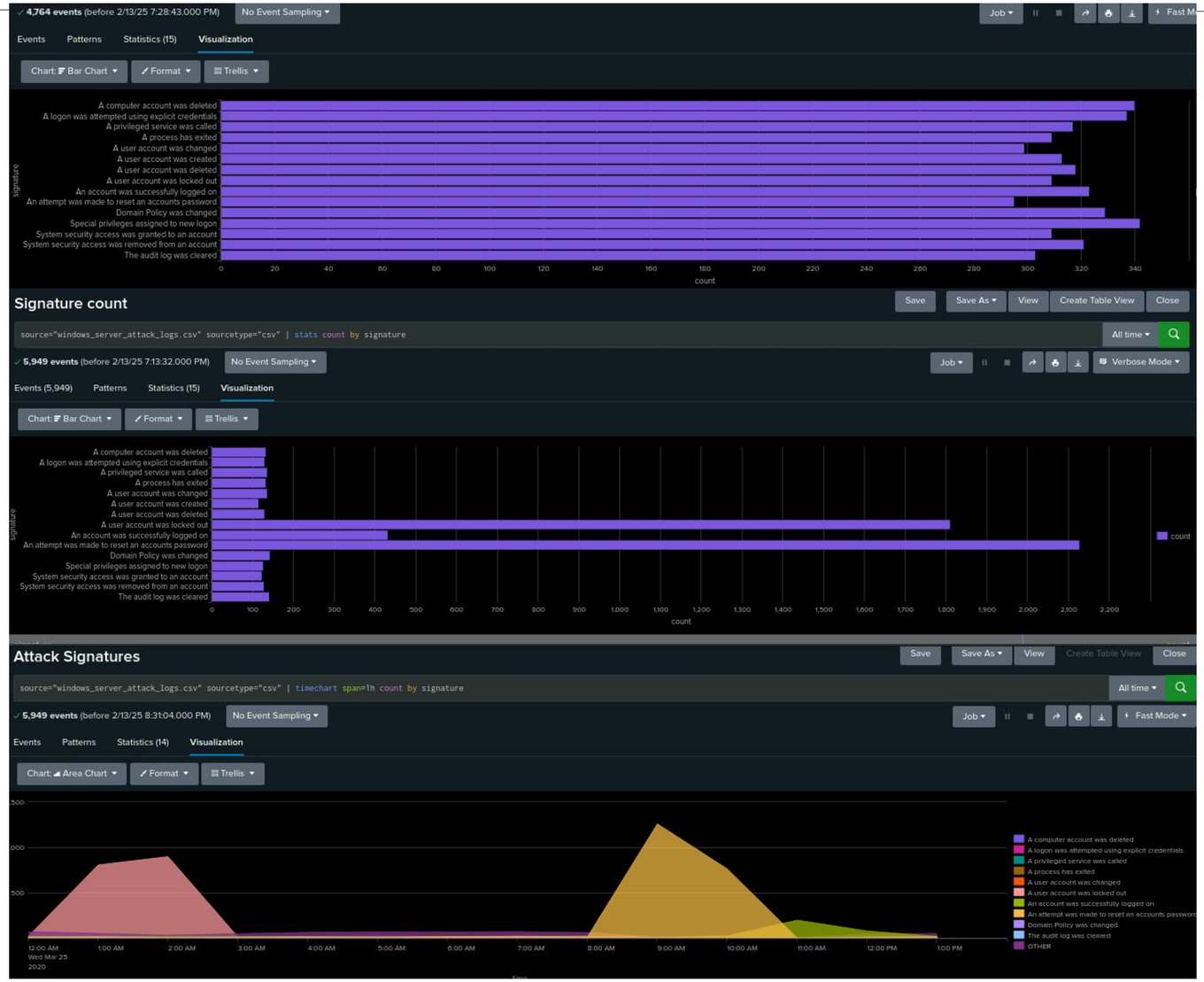


Attack Analysis

Attack Summary—Windows Signature Data

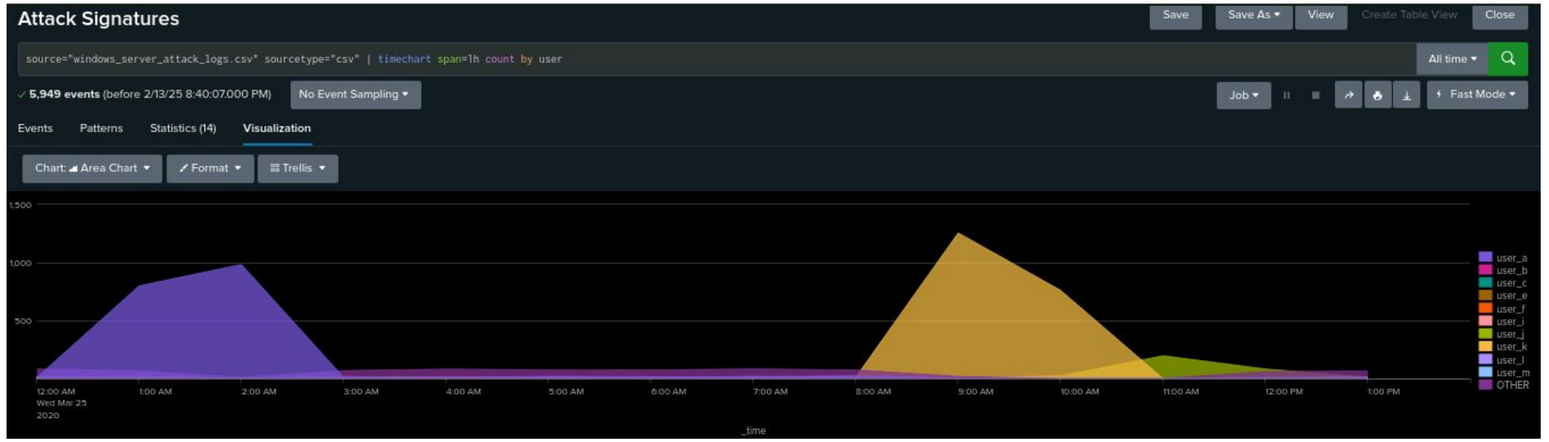
Windows Signature Baseline:

Windows Attack Signature:

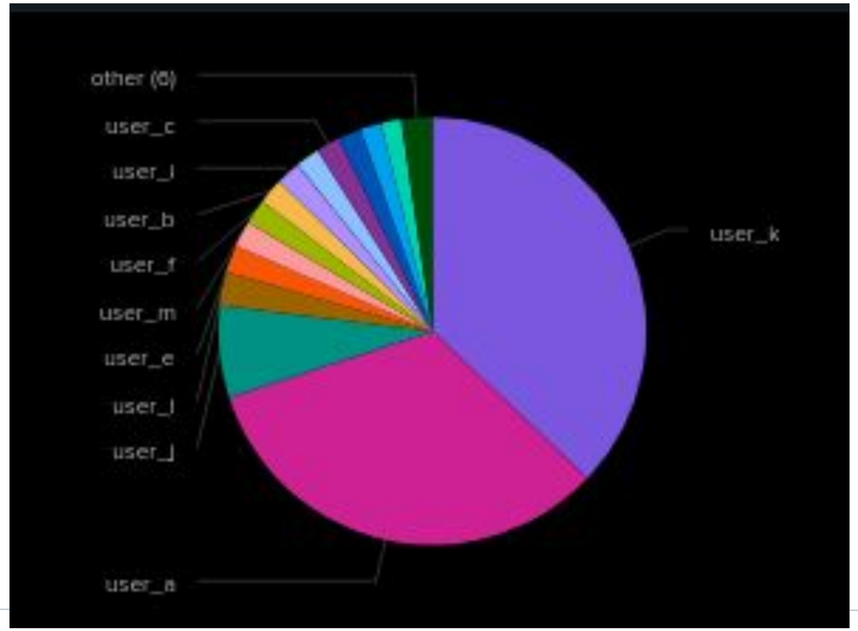


The above images show a comparison between 2 different charts against the established baseline. The top image is the baseline of all signatures and the two images below show various spikes in the data against the established baseline. This indicates there was a possible attack.

Screenshots of Windows User Attack Logs



The area chart here shows the number of events per user over a span of ~12hrs. As you can see, the chart indicates that 2 users have an increase number of events from 12am-3am(user A) and an increase in the number of events from 8:00am-11:00am(user k).



The pie chart indicates that User A and user K were both attempting separate events at different times. These two charts together show a direct correlation between the pie chart data and the data for users. Together, they confirm that there was suspicious activity occurring on these 2 user accounts.

Attack Summary-

- What signatures stand out?
  - Password resets and User account lockouts
- What time did it begin and stop for each signature?
  - User accounts were locked out - 25 March 2020 00:00-03:00
  - An attempt was made to reset an accounts password - 25 March 2020 08:00-11:00
- What is the peak count of the different users?
  - User A - 984
  - User K - 1256
- When did it occur?
  - User A was logging in over 1600 times between 0100-0300
  - User K was logging in over 1900 times between 0900-1100
- The graphs provides an illustration of the significant number of attacks via Brute Force and password reset attempts were made. Resulting in user lockout.

Attack Summary—Apache

Report Analysis for Methods

- Did you detect any suspicious changes in HTTP methods? If so, which one?

On March 25, changes in HTTP methods activity were observed:

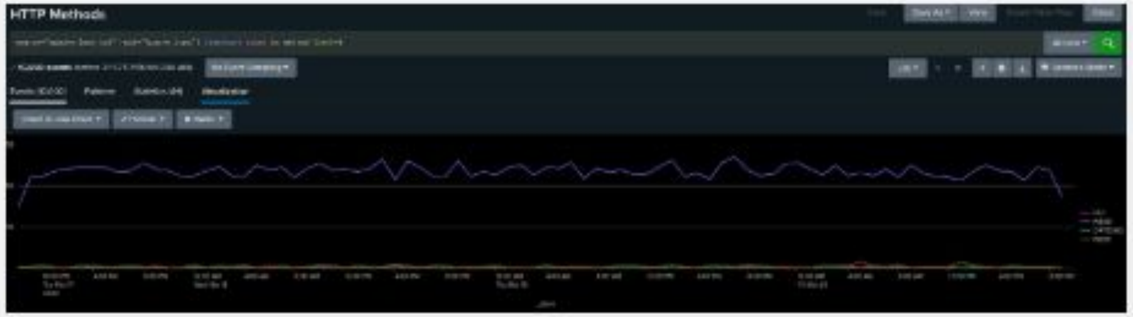
6:00 PM – An increase in GET requests, increasing from 117 to 729.

5:00 AM – A slight rise in HEAD requests from 0 to 8, possibly reconnaissance activity.

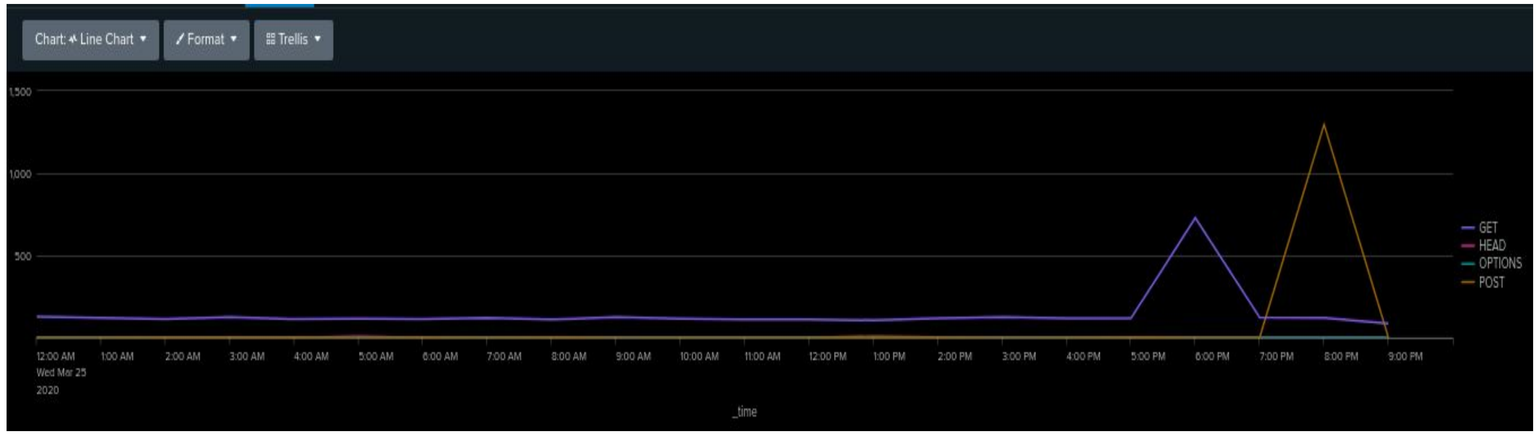
8:00 PM – A significant spike in POST requests, surging to 1,296.

These anomalies may indicate suspicious activity, including reconnaissance, server capability testing, or potential attempts to exploit vulnerabilities. Further investigation into the sources and intent of these requests is recommended.

Baseline:



Attack Summary—Apache



After the attack we can see the spike on GET and POST requests between 5 pm and 9 pm

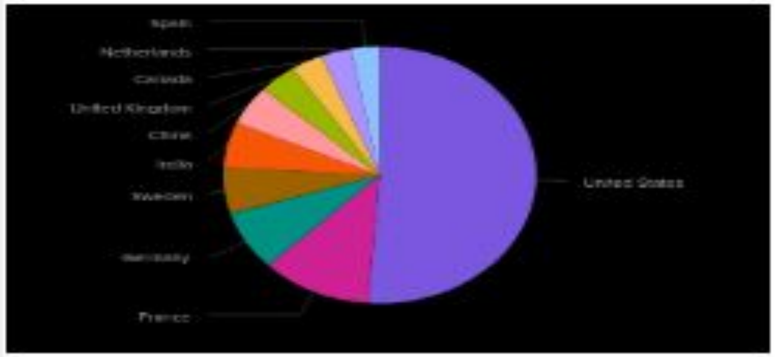
Attack Summary—Apache Geographical

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

At 8:00 PM on March 25, a significant increase in traffic was detected, totaling 937 requests from Ukraine.

Baseline:



Attack Summary—Apache Geographical

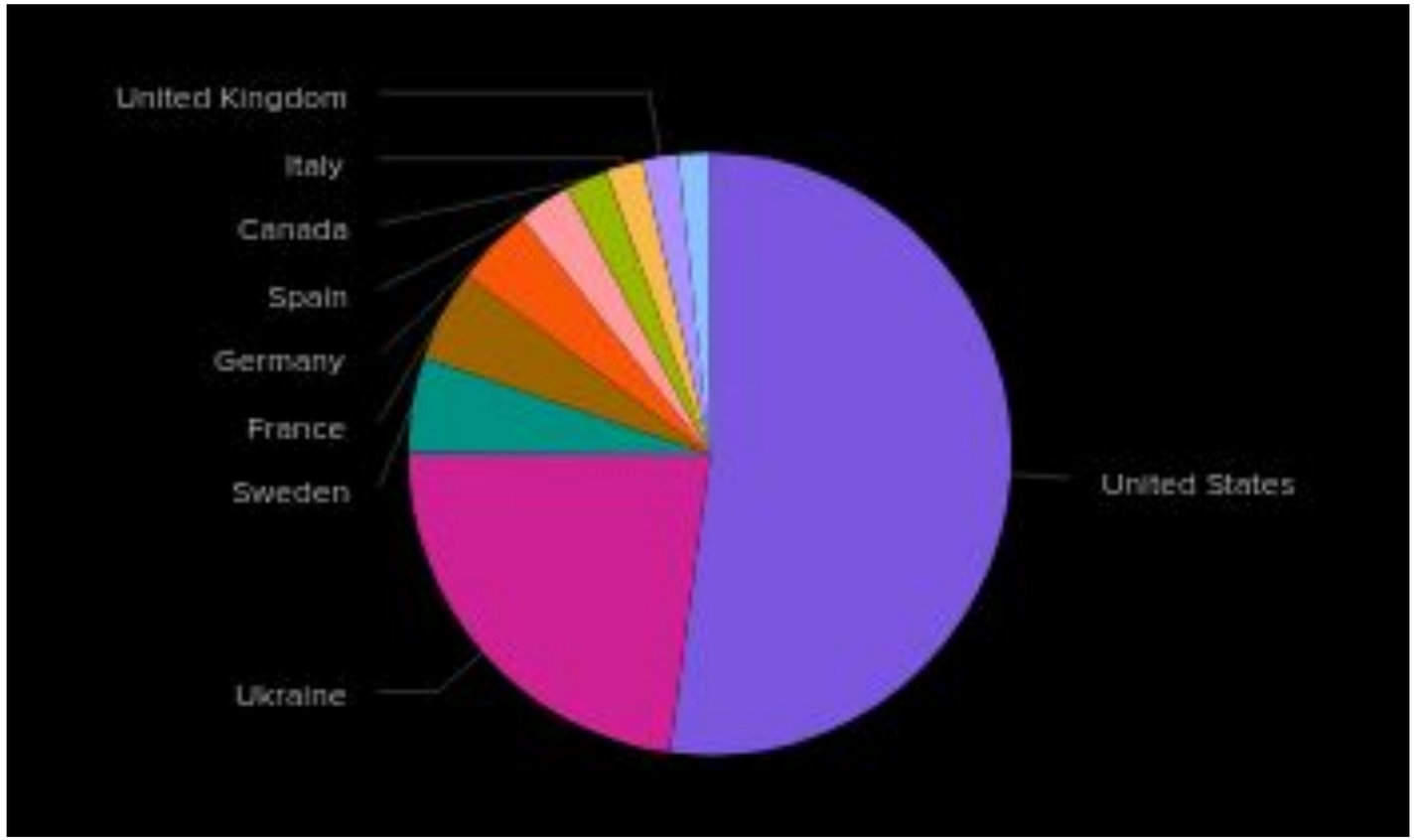
Ukraine in the cities of Kiev and Kharkiv

Kiev has 439 events

And Kharkiv has 432 events

Attack Summary—Apache Geolocation

Country	count	percent
United States	2000	44.474094
Ukraine	877	19.501890
Sweden	198	4.402935
France	190	4.225039



After the attack we can clearly see a spike in traffic from Ukraine, making it the most reasonable location from where the attacks were made

Screenshots of Non US-IP alert

- Would your alert be triggered for this activity?

Yes because the limit was set at 73.

- After reviewing, would you change the threshold that you previously selected?

No I would not change the hourly activity because it effectively captures usual activity. I may increase to 100 if too many false positives come in.

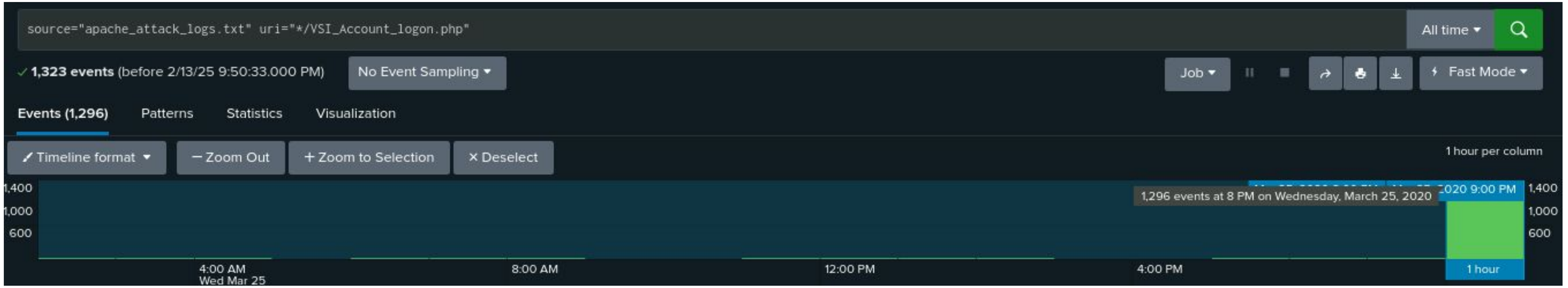
Attack Summary—URI's

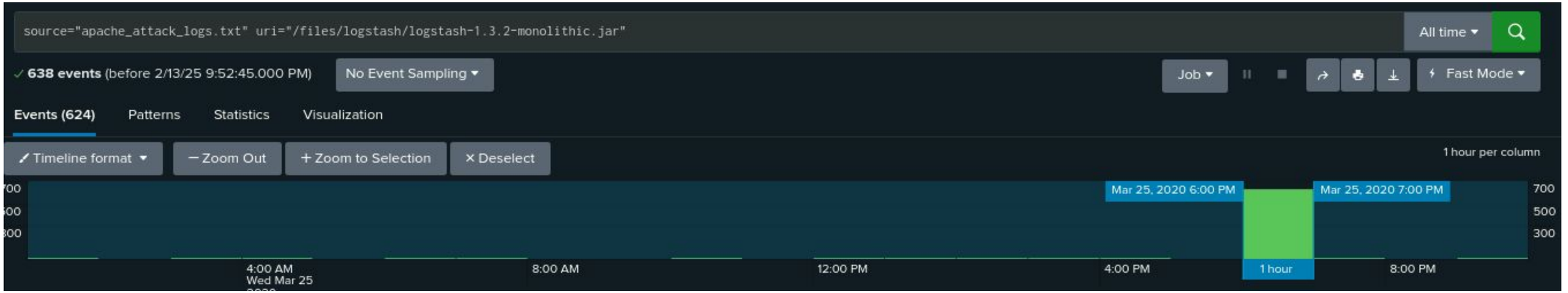
Upon analyzing the uri logs we found that:

URI "/VSI_Account_logon.php" - Between 8:00 PM and 9:00 PM was pinged 1296 times

URI "/files/logstash/logstash-1.3.2-monolithic.jar" - Between 6:00 PM and 7:00 PM was attempted access 624 times

Attack Summary—URI's





Attack Summary—URI's

- Based on the URI being accessed, what could the attacker potentially be doing?

This raises the possibility of a brute force attack, where numerous login attempts are being made in an effort to gain unauthorized access.

There are known vulnerabilities associated with **Logstash 1.3.2**:

1. **CVE-2014-4326**: This vulnerability allows remote attackers to execute arbitrary commands via a crafted event in specific output plugins, such as `zabbix.rb` or `nagios_nsca.rb`.
   nvd.nist.gov
2. **CVE-2021-23358**: This issue pertains to the `underscore` package used in Logstash versions up to 1.3.2. It allows arbitrary code injection via the template function when a variable property is passed as an argument without proper sanitization.
   nvd.nist.gov

This should be patched immediatley.

Summary and Future Mitigations

Project 3 Summary

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

  Brute force attack on apache servers, trying to exploit different web urls to gain access to resources; that can be seen through increase in 404 errors.

  Recon was conducted through a series of GET requests

  Potential Exploit on Logstash 1.2.3

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

  Frequent software updates, applying SIEM tools with finer tuning alerts perhaps hourly or 30-min intervals to better identify or monitor suspicious activity, enforce 2-factor authentication.