Defensive Security Project
by: BootCon Team 3

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Hired as SOC analyst for Virtual Space Industries (VSI), a company specializing in virtual-reality programs for businesses
- VSI suspects potential cyberattacks from a competitor, JobeCorp, aiming to disrupt their operations.
  - Later VSI experienced several cyberattacks, likely from its adversary JobeCorp with several of VSI’s systems down.
- Our Task: use Splunk to monitor and analyze potential threats targeting VSI’s systems and applications
- Key Systems:
  - Apache web server (hosting the administrative webpage)
  - Windows server (running back-end operations and storing intellectual property)

Whois XML Website Categorization API for Splunk

Whois XML Website Categorization API for Splunk

- Integrates IP geolocation in Splunk
- Enables users to enrich logs + events with geographic info about IP addresses
  - Insights like
    - Country, city, region, and timezone of an IP
- Helps detect
  - Patterns, anomalies, and identify potential threats based on geolocation
- Particularly useful in enhancing security investigations for understanding the geographic distribution of network activity

Whois XML Website Categorization API for Splunk

A large corporation's IT security team uses Splunk to monitor and analyze their network traffic. They've recently noticed an increase in employees accessing unfamiliar websites, raising concerns about potential security risks.This implementation allows the security team to quickly identify and respond to potential threats, enforce content filtering policies, and gain deeper insights into their organization's web traffic patterns. The daily updates to the categorization intelligence ensure that the team always has access to the most current website classification data2, enhancing their ability to protect the company's digital assets and maintain a secure online environment for employees.

Logs Analyzed

1 Windows Logs

- Detailed records of events related to the system, security, and applications on a Windows operating system of the company.
- These contains the intellectual property of the organization’s next generation Virtual-reality programs.
- Track critical activity, including:
  - signature_id
  - signature
  - user
  - status
  - severity

2 Apache Logs

- Track critical activity, including
  - HTTP methods,
  - Referer domains,
  - Response status codes,
  - Client IPs
  - User agents
- These fields help identify traffic patterns, detect errors, and monitor for potential cyber threats, enabling effective server security analysis.

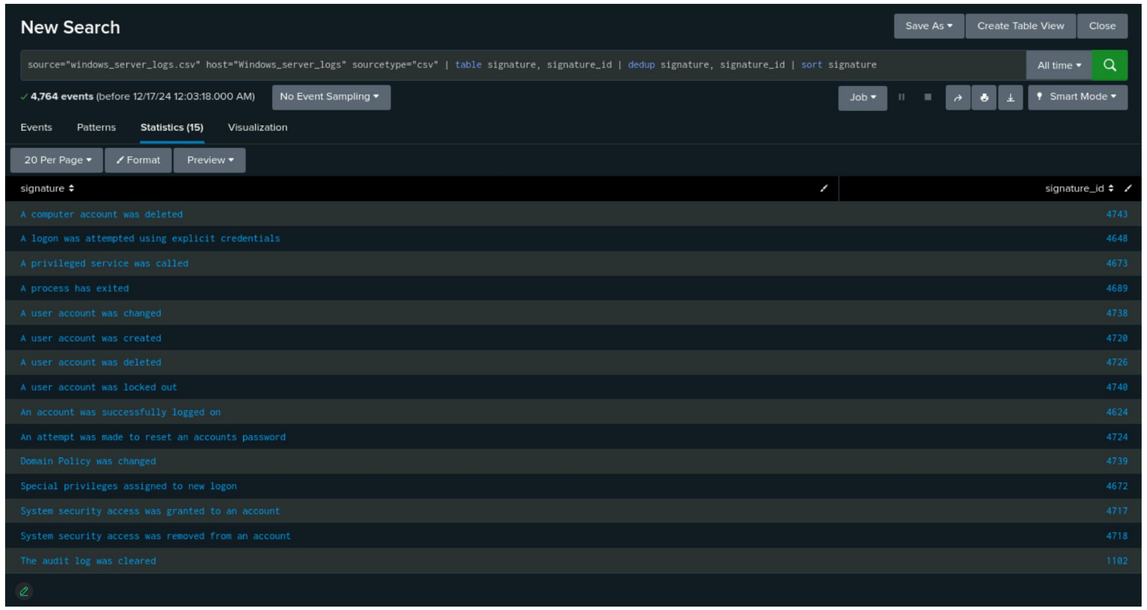
Windows Logs

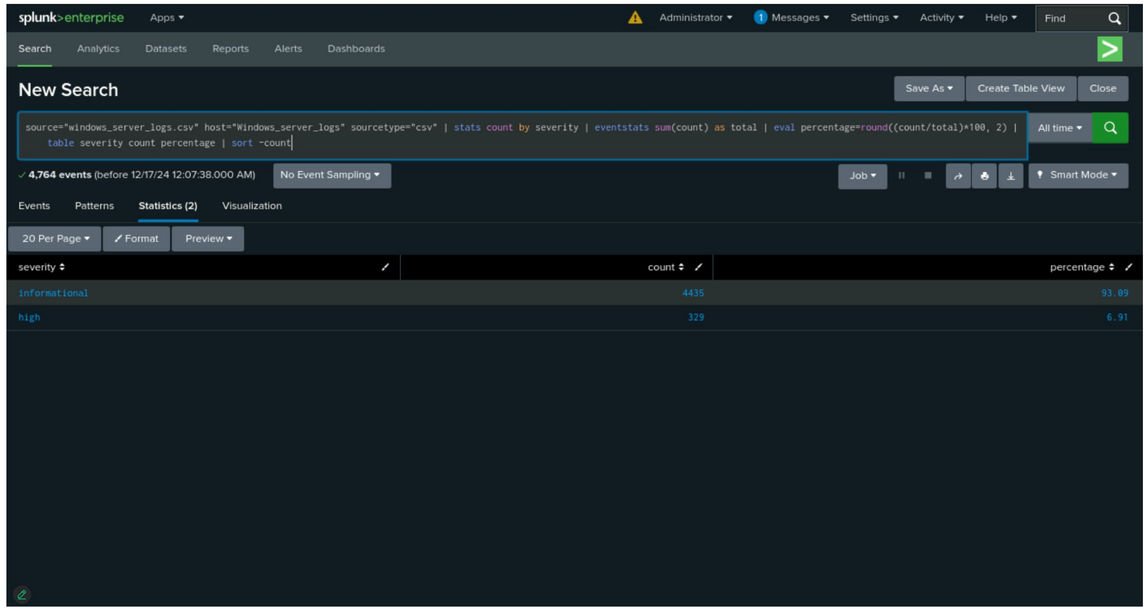
Reports—Windows

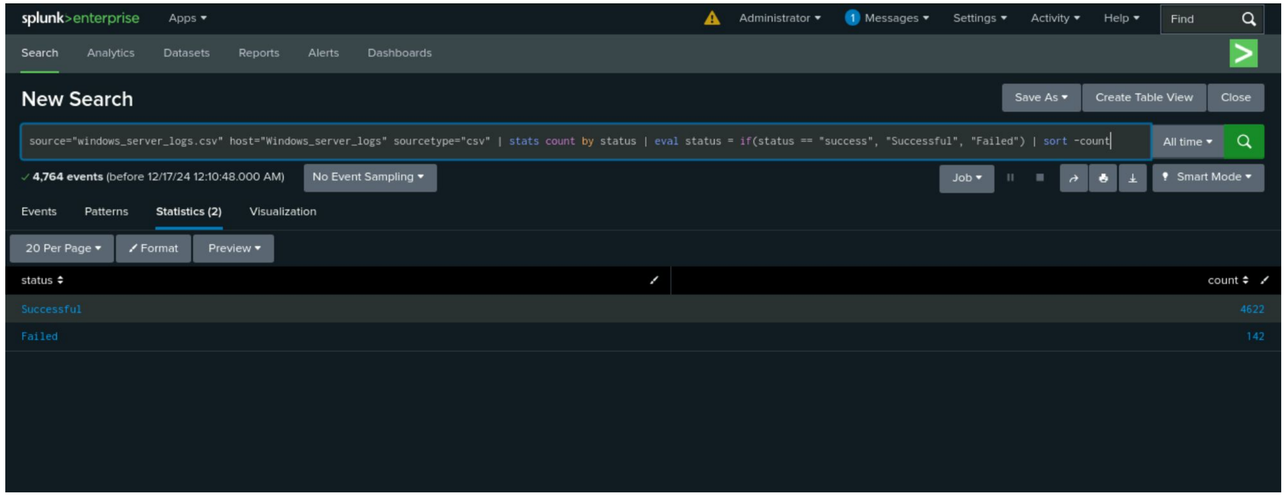
Designed the following reports:

Report Name	Report Description
Signature Information Report	A report with a table of signatures and associated signature IDs.
Severity Level Report	A report that displays the severity levels, and the count and percentage
Success/Failure Report	A report that provides a comparison between the success and failure of Windows activities.

Images of Reports—Windows







Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Brute Force Attack Alert	Login failure count is more than the threshold amount	10	Greater than 12

JUSTIFICATION: The average login failure prior to the attack is around 10, so we put baseline as 10 and threshold as 12.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logon Count Exceeds	Warning for “an account was successfully logged on” count is more than the threshold	10	Greater than 15

JUSTIFICATION: As the most successful logon are from the signature id goes upto 23 and lowest to 9.

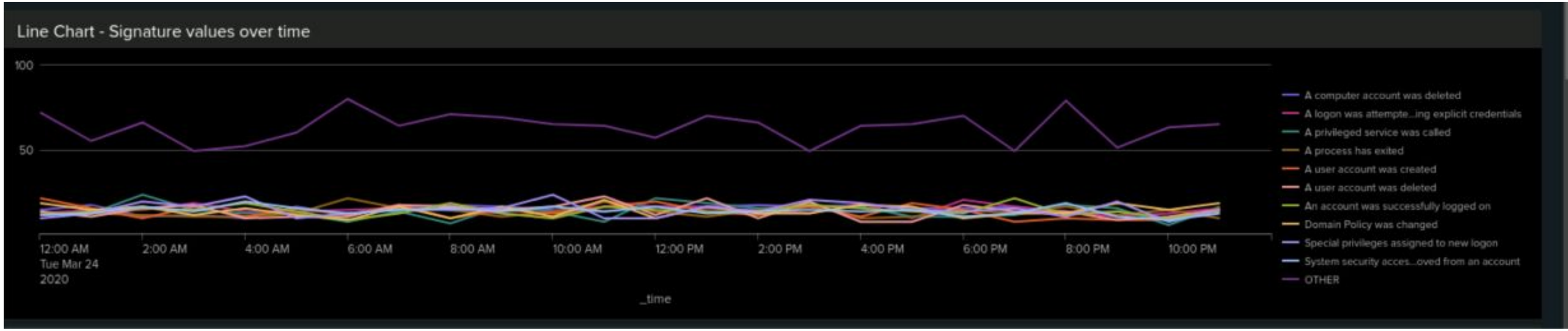
Alerts—Windows

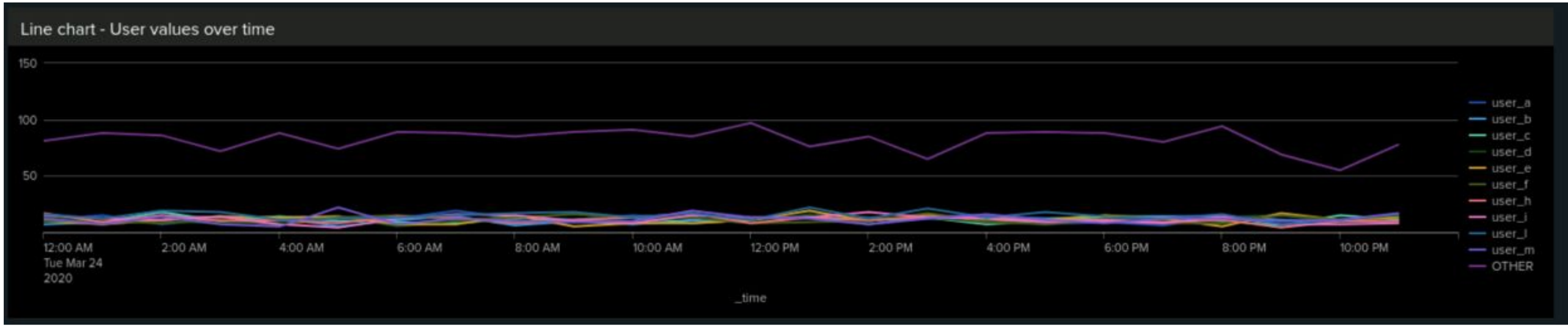
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Deletion Alert	Warning for “A user was deleted” count is more than threshold	9	11

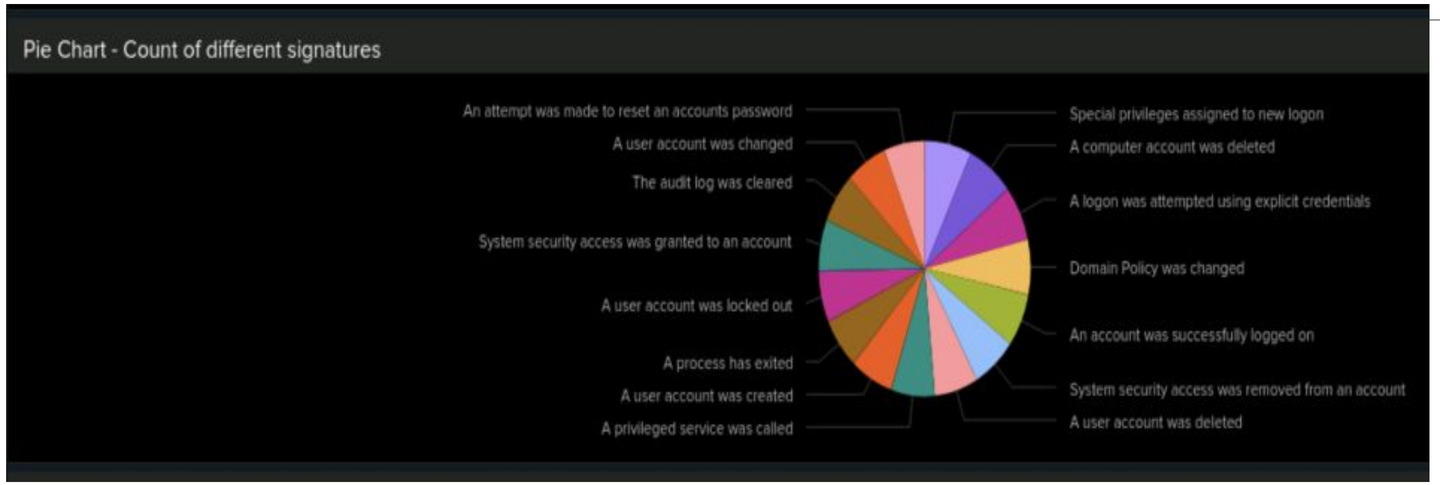
JUSTIFICATION: account being deleted is average around 9-10 and so we set the threshold as 11.

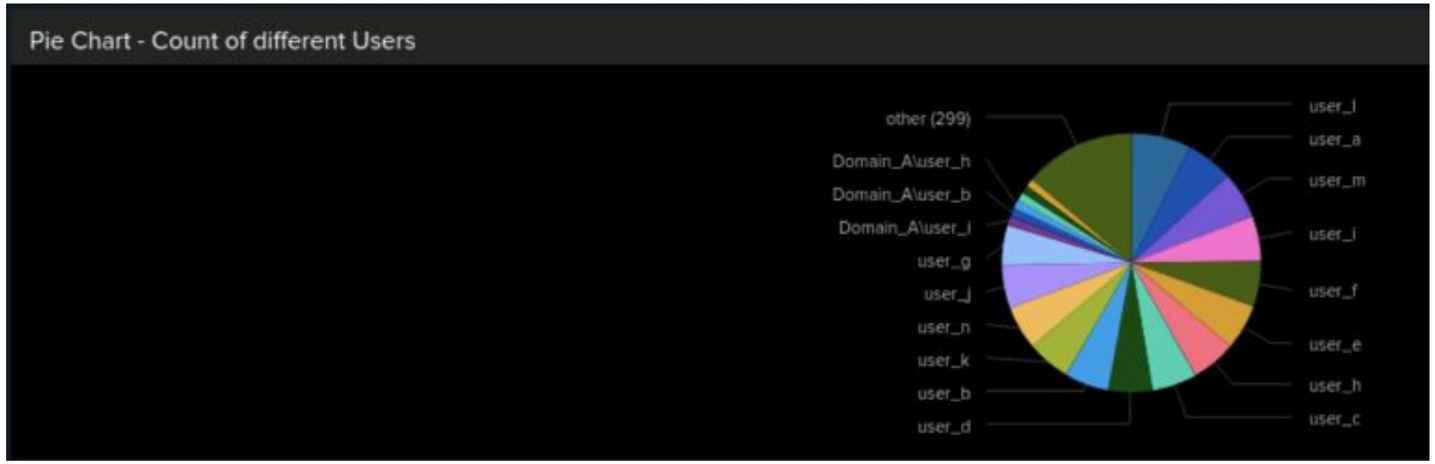
Dashboards—Windows





Dashboards—Windows





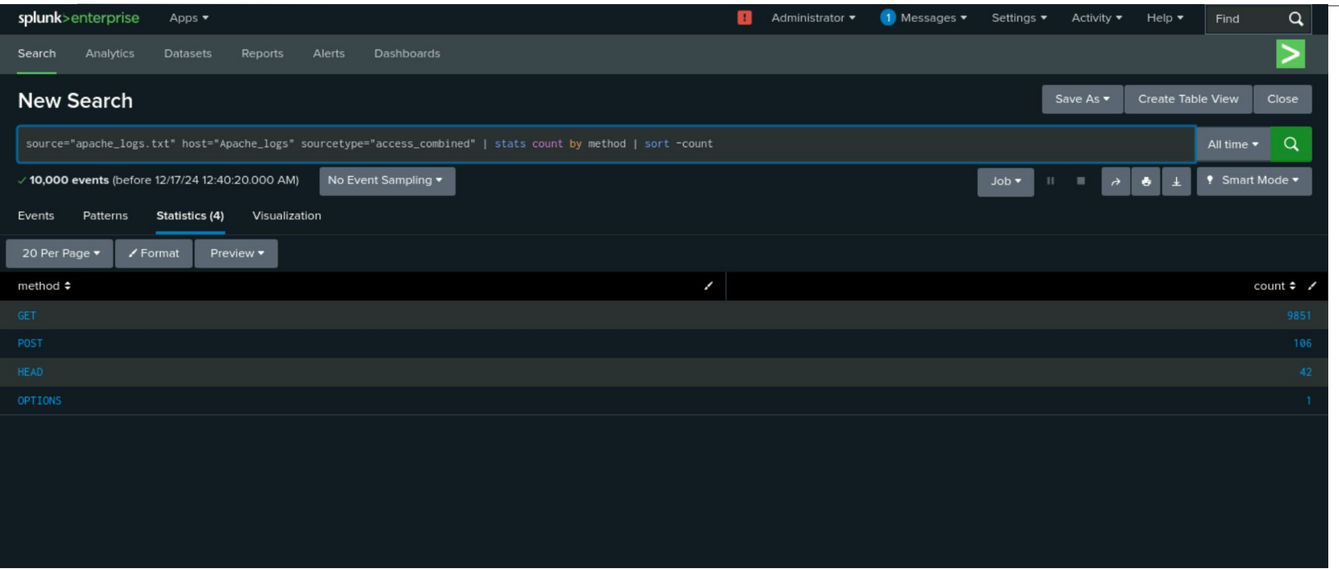
Apache Logs

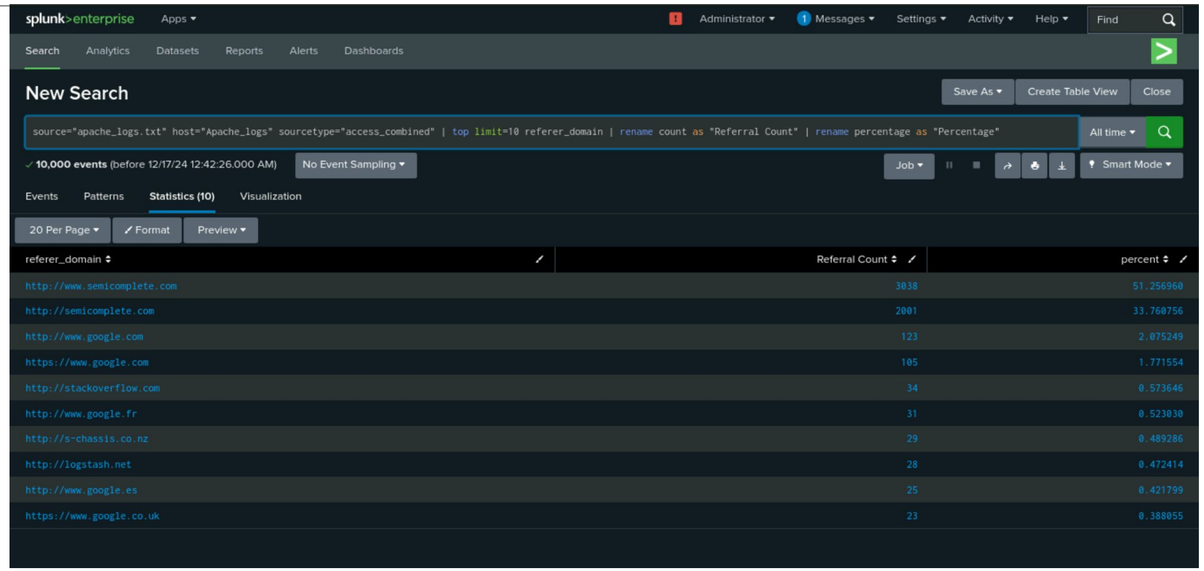
Reports—Apache

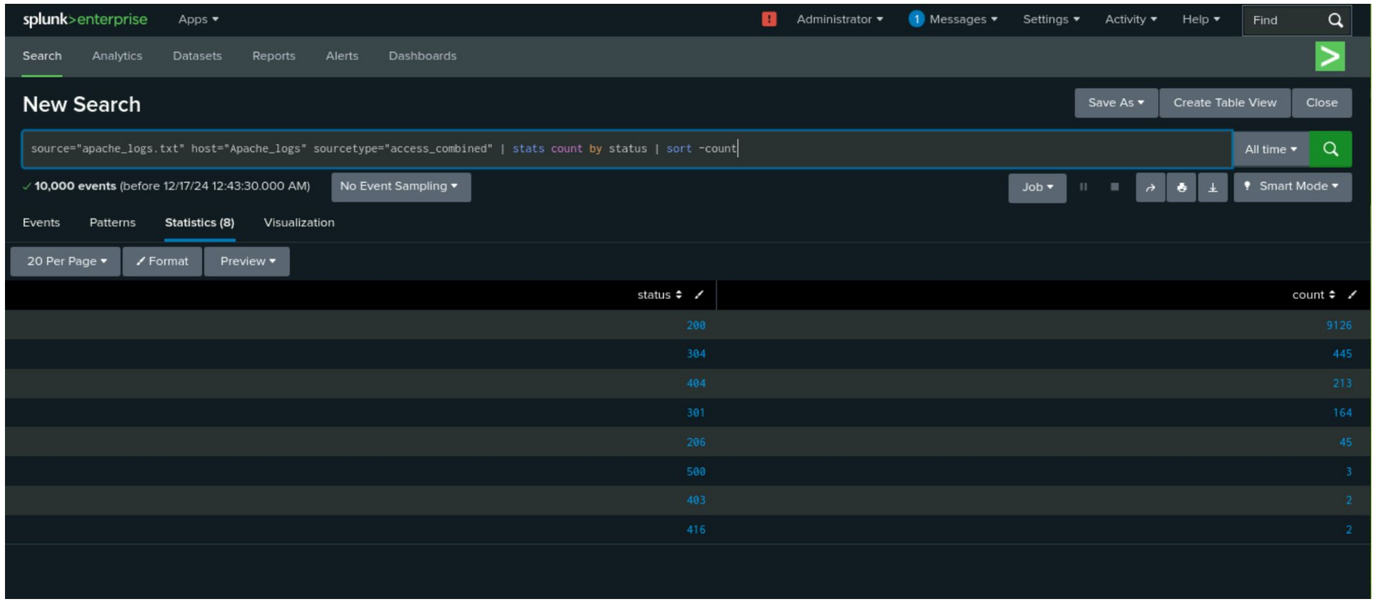
Designed the following reports:

Report Name	Report Description
HTTP Methods Report	Displays a table of HTTP methods (e.g., GET, POST, HEAD) to analyze the types of requests made to VSI's web server
Top 10 VSI Website Domains	Lists the top 10 referring domains to identify potential suspicious sources directing traffic to VSI's website
HTTP Response Code Report	Shows the count of each HTTP response code to detect unusual patterns or errors in server responses

Images of Reports—Apache







Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity from Non-US IP addresses	An alert for IP addresses from other countries.	100	Greater than 120 as immediate action

JUSTIFICATION: Using this we can find out the activity from other countries through IP Addresses.

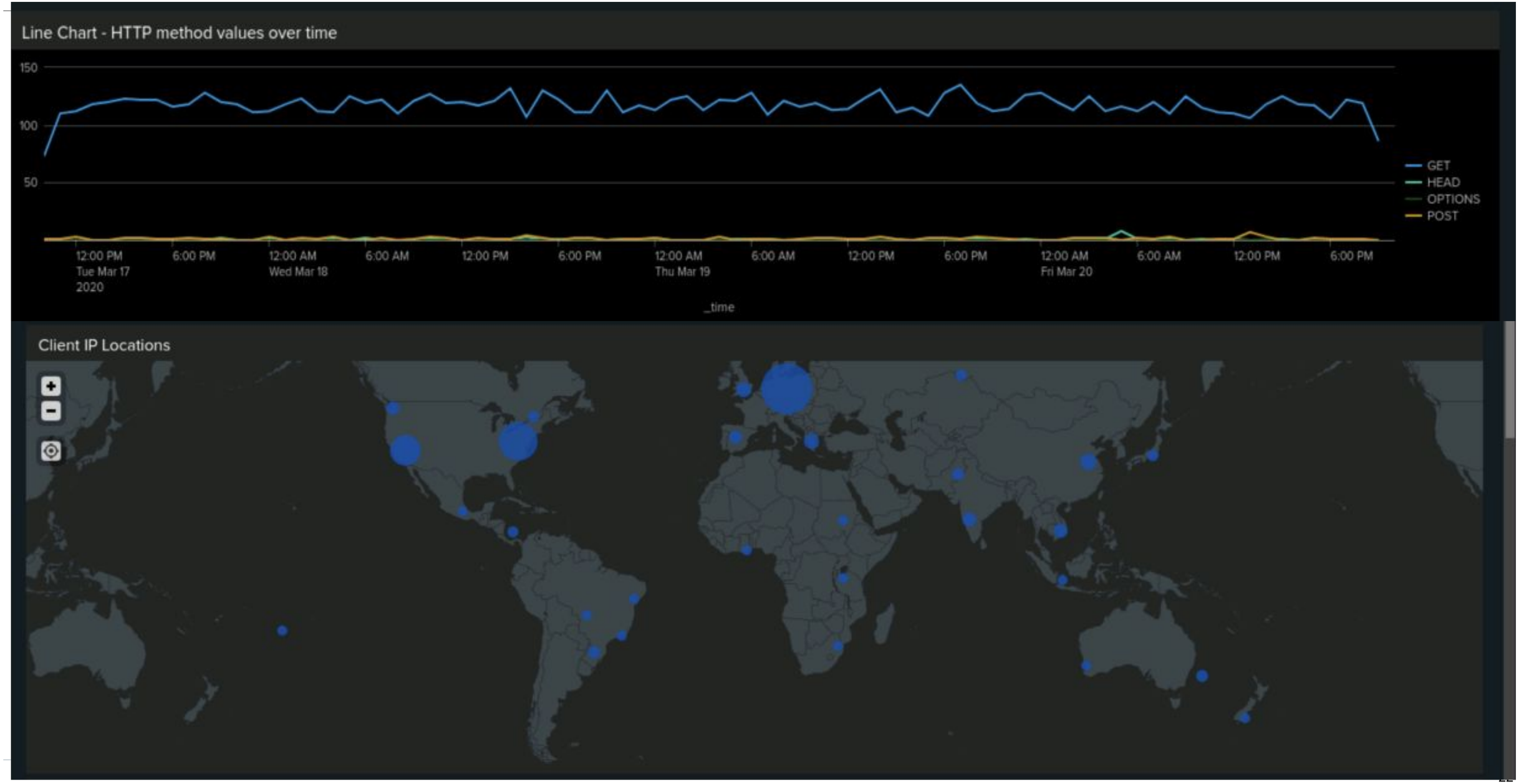
Alerts—Apache

Designed the following alerts:

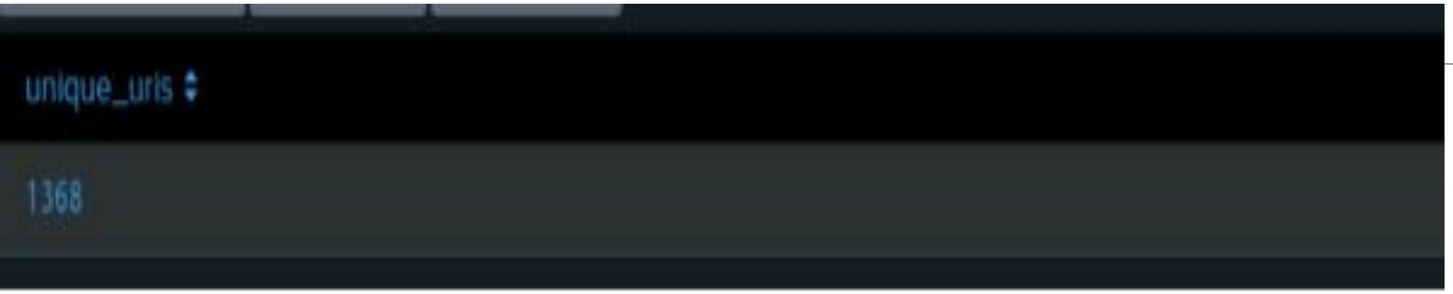
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of HTTP POST Methods Exceeds Alert	The hourly count of HTTP POST method have exceeded the threshold amount	10	20

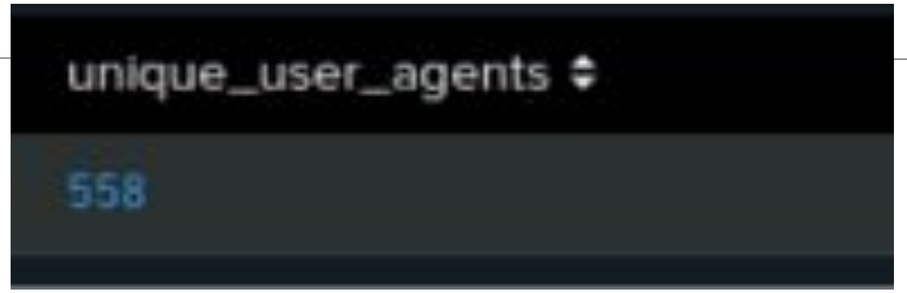
JUSTIFICATION: we don't have any POST requests going beyond 10 per hour prior to the attack.

Dashboards—Apache



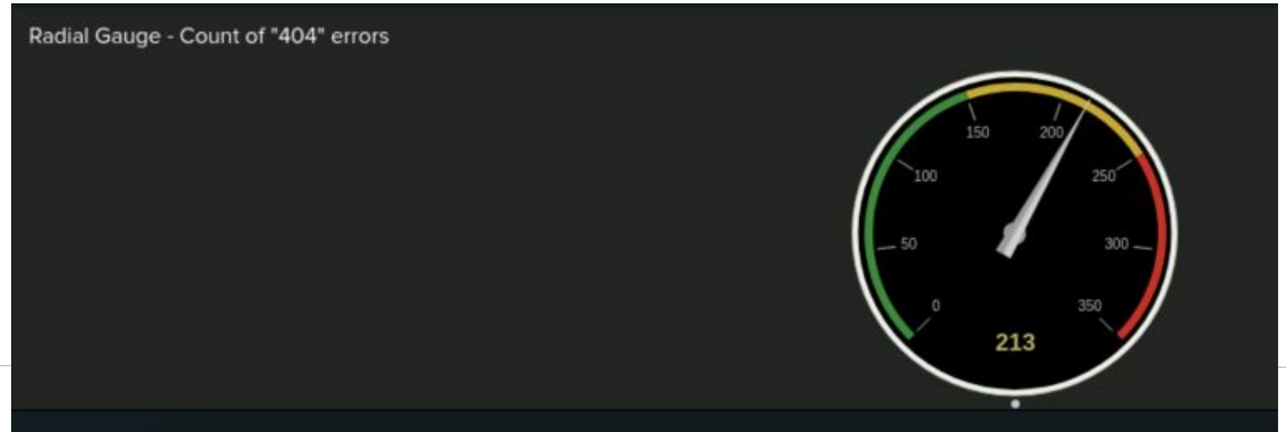
Dashboards—Apache





Count of User Agents

useragent	count
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	1044
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36	369
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/	364
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0	296
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	271
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	268
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	237
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	236
Mozilla/5.0 (X11; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0	229
Tiny Tiny RSS/1.11 (http://tt-rss.org/)	198
-	190
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	175
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0	166
Mozilla/5.0 (compatible; archive.org_bot +http://www.archive.org/details/archive.org_bot)	166
Mozilla/5.0 (compatible; Ezooms/1.0; help@moz.com)	157
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36	152



Attack Analysis

Attack Summary—Windows

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

- Suspicious Changes in Severity: Severity "high" has shown a significant increase in both count and percentage: Count: 329 → 1111 Percentage: 6.91% → 20.22%
- Suspicious Changes in Failed Activities: Failures have decreased: 142 → 93 Successes have increased: 4622 → 5856
- Windows Attack System Analysis: The system reported a noticeable shift in severity distribution: "High" severity increased. Pre-attack severity was predominantly "informational" (~79%). Post-attack, there were more successes than failures, indicating a potential anomaly or change in activity patterns.

Attack Summary—Windows

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

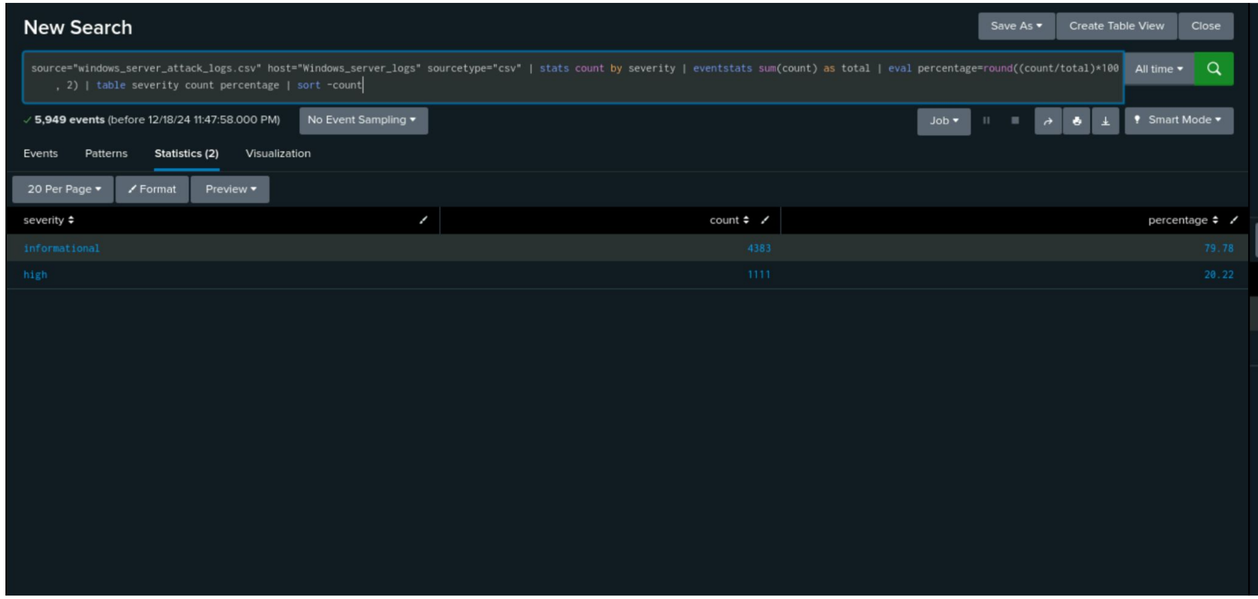
Windows
Alert 1: Failed Windows Activity Our alert was set to anything greater than 6, so it was triggered as there were 35 events at 8AM
Alert 2: Successful Logins Our alert was triggered for this activity, we had set it to anything greater than 15 and there were 196 events at 11am and 77 at 12pm and 15 at 1pm
Alert 3: Deleted Accounts We set our baseline for 11, the highest deleted account events in the logs was 22 and in the attack logs the highest was 17, nothing suspicious noted.

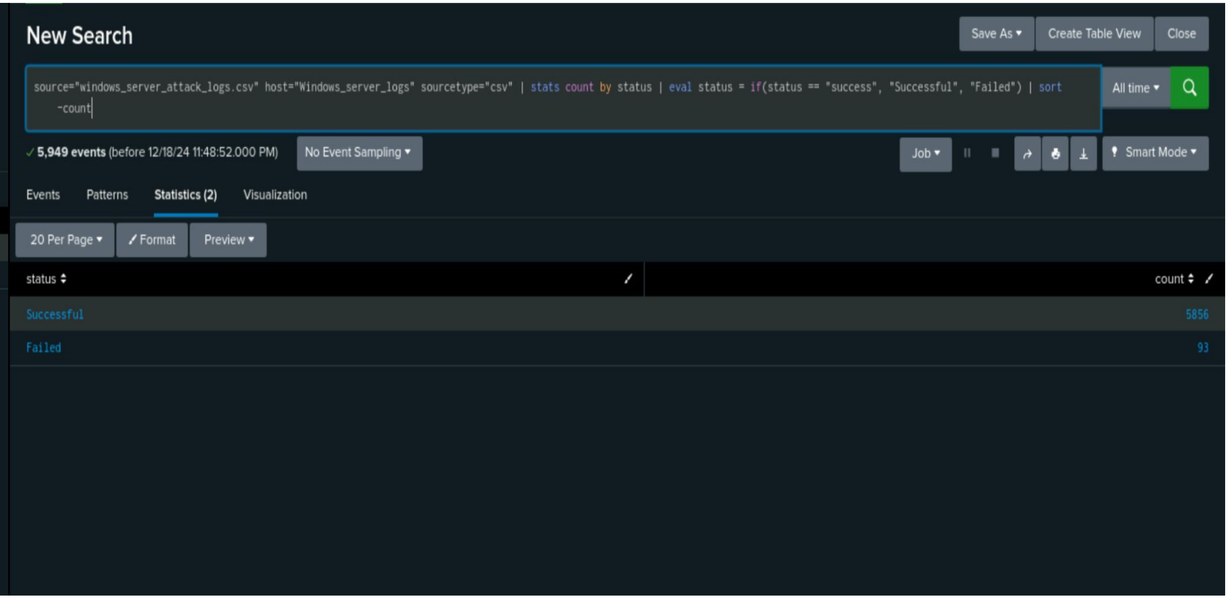
Attack Summary—Windows

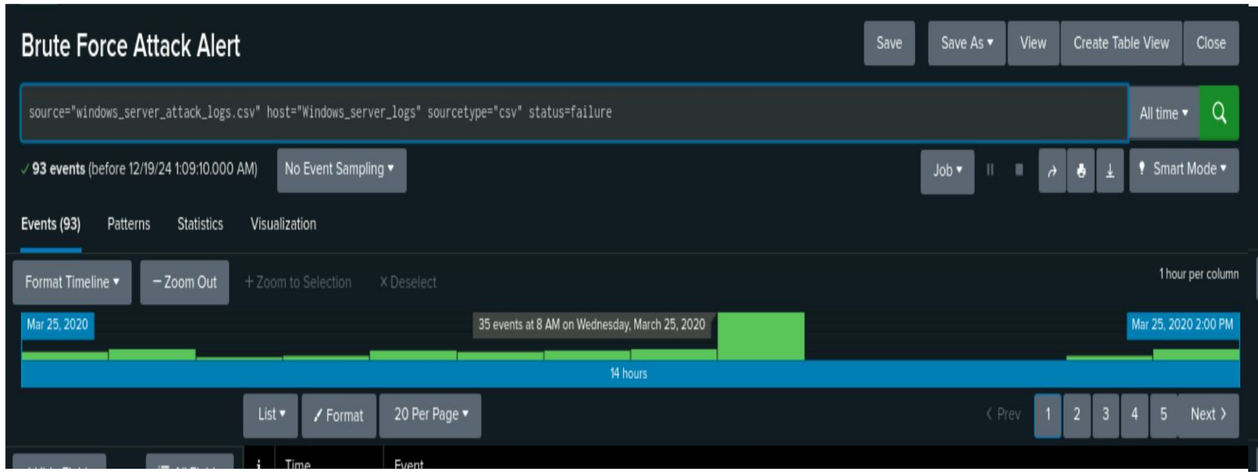
Summarize your findings from your dashboards when analyzing the attack logs.

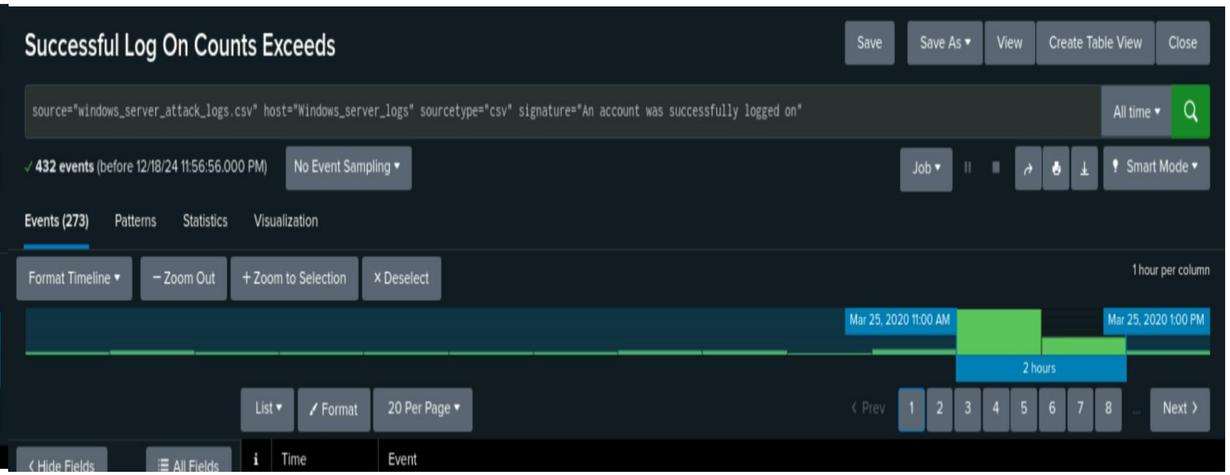
Description	Analysis
Suspicious changes in severity	The severity increased from 329 to 1111. We can see the spike of 13.31% on our second day.
Suspicious changes in failed activities	Though the amount of failed login dropped in number, thus resulting in the increase of successful logins.
Suspicious volume of failed activity	The number of events spiked to 35 events 8am, while in the normal windows logs the events hovered around 5, which is why we set our threshold to 6
Suspicious volume of successful logins	After analyzing our reports we found that one particular user had more successful login and our created alert picked up.
Suspicious volume of deleted accounts	We noted nothing suspicious as the highest level of events in the windows logs was 22 and the highest seen in the windows attack logs was 17

Screenshots of Attack Logs

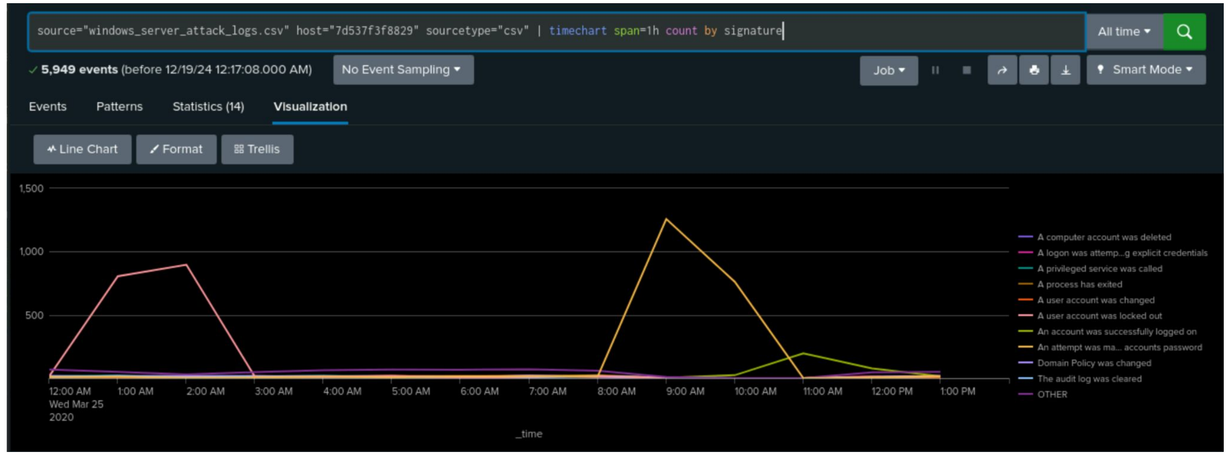


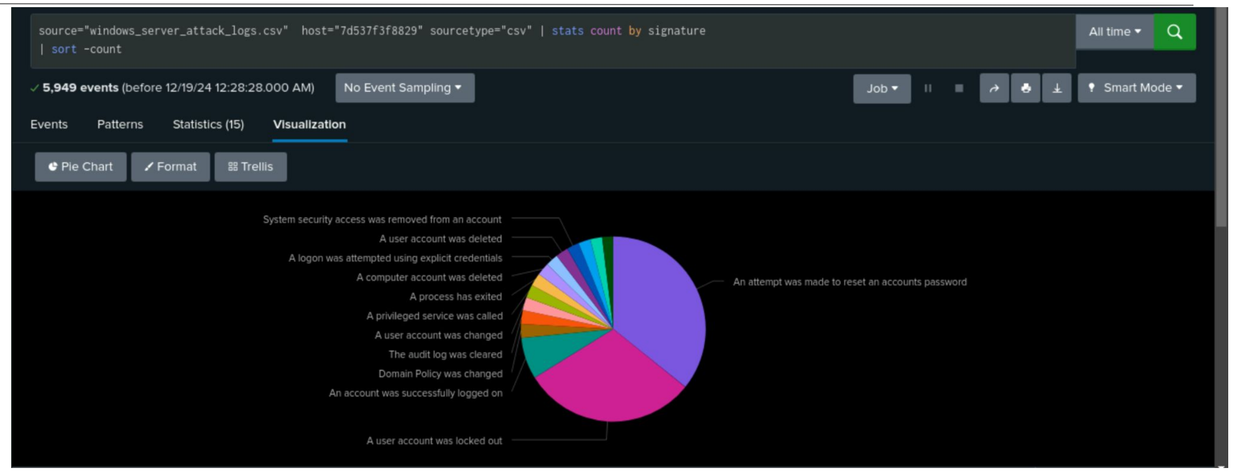


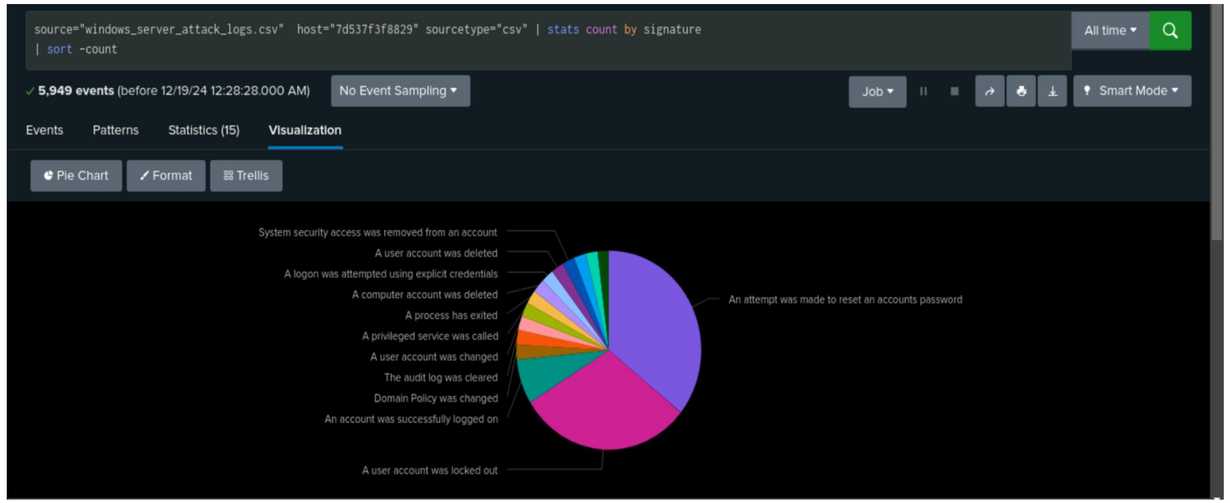


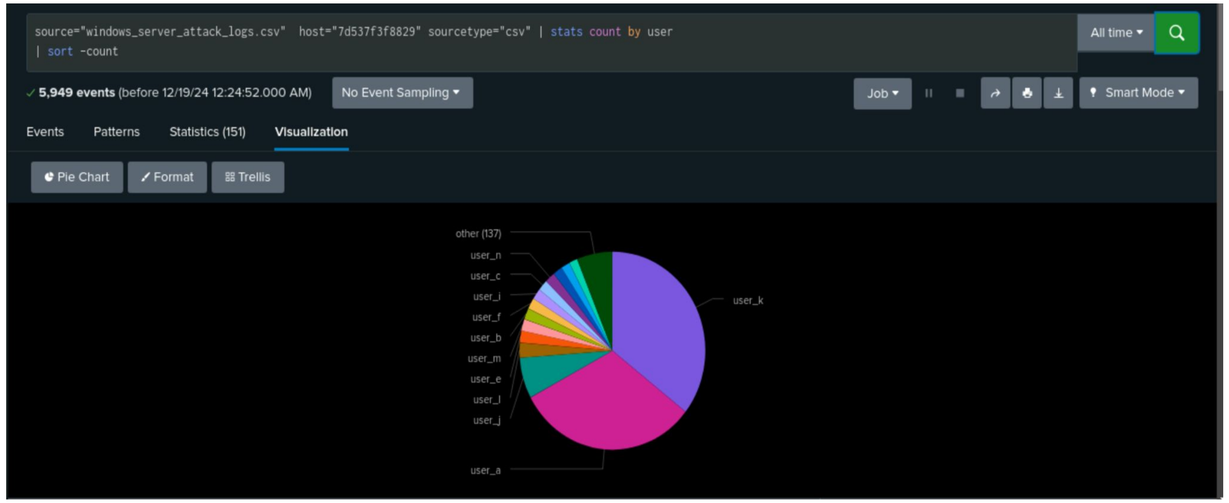


Screenshots of Attack Logs









Attack Summary—Apache

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

- Our Time Chart of HTTP methods revealed suspicious volumes of GET and POST methods.
  - The GET attack went from 5pm to 7pm and peaked with a count of 729.
  - The POST attack went from 7pm to 9pm and peaked with a count of 1,296.
- Our Cluster Map revealed suspicious activity from a couple cities.
  - Kiev (439), Kharkiv (433), D.C. (724), and NYC(881) all had high volumes of activity.
- Our URI Data flagged “/VSI_Account_logon.php” as having suspiciously high volume.

Attack Summary—Apache

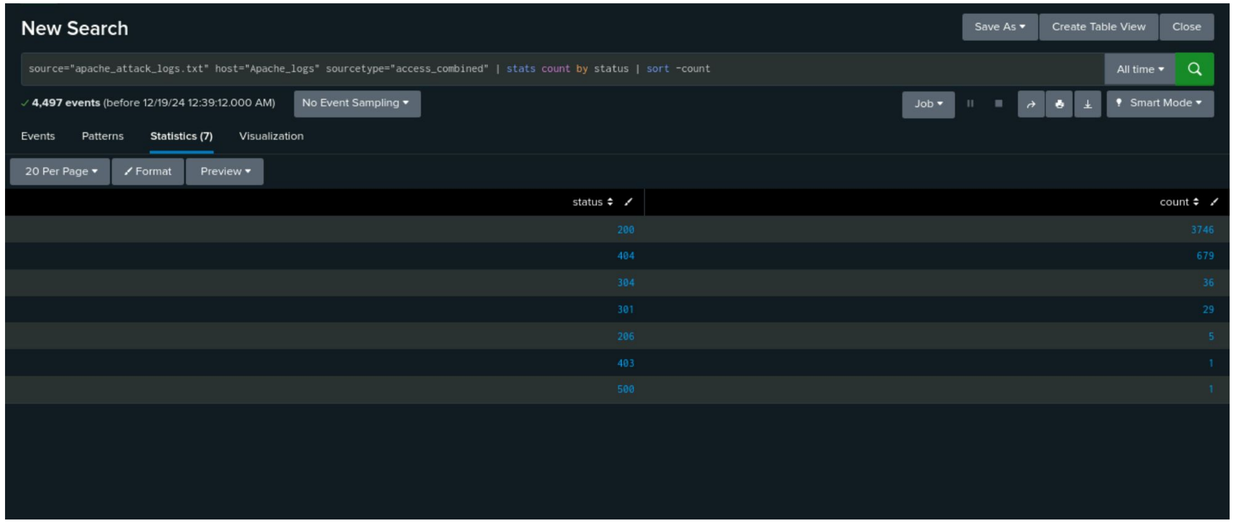
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

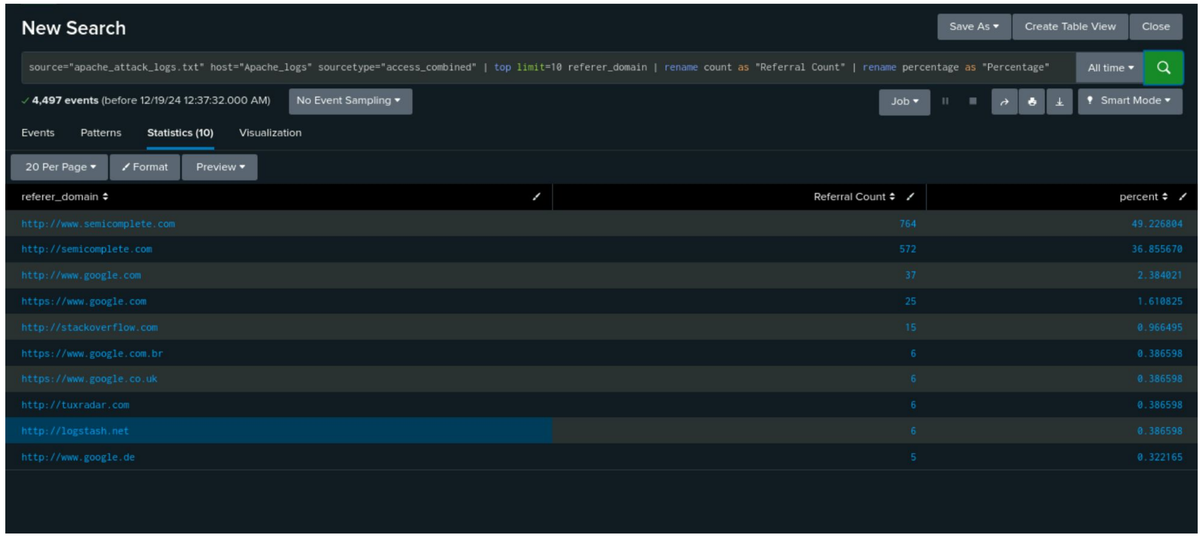
Apache
Alert 1: Other Logins from Non-US countries Our alert was set to anything greater than 120, but later we changed our threshold to 300 after analyzing our reports.
Alert 2: Hourly count of HTTP POST method We set our alert to anything greater than 10 as the regular values hovered around 7, our threshold did get triggered as there were 1296 events on March 25th at 8PM.

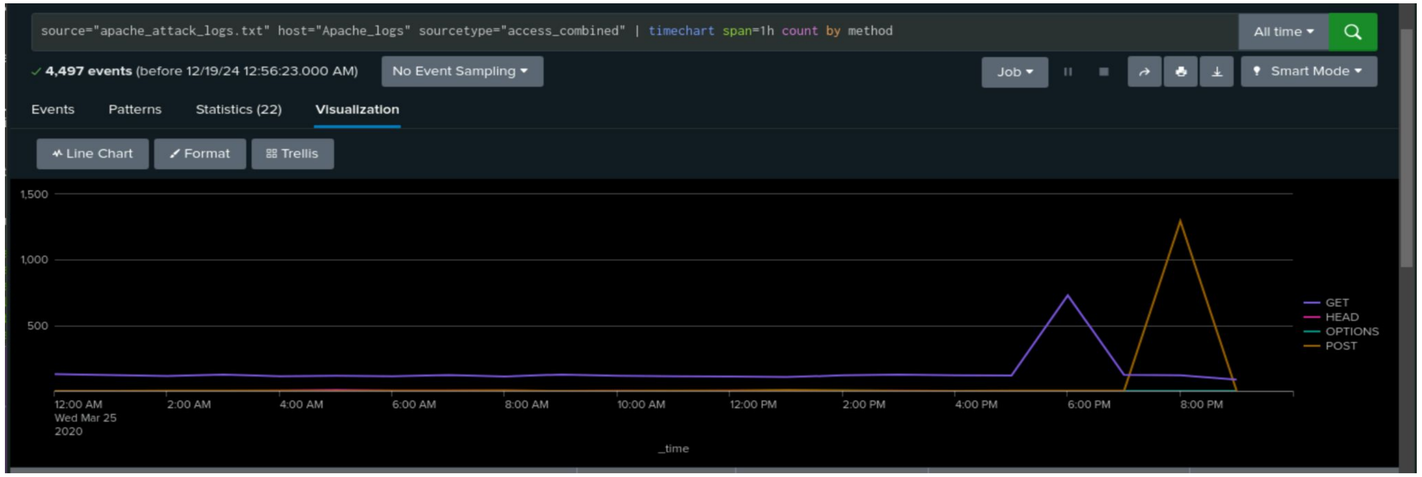
Attack Summary—Apache

Description	Analysis
Suspicious changes in HTTP methods	The GET and POST requests were suspicious. The count for GET requests requests was reduced and POST requests has increased.
Suspicious changes in referrer domains	there has been increase in the domains in comparison with day1
Suspicious changes in HTTP response codes	the HTTP response codes has their numbers doubled.
Suspicious volume of international activity	initially the activity from other countries was recorded at 136 however it increased to 1415.
Suspicious volume of HTTP POST activity	HTTP Post activity flow has increased tremendously from 7 to 1296
Time Chart of HTTP Methods	The GET and POST requests increased around 6:00 pm and 8 pm respectively.
Analysis for Cluster Map	The login activity has increased from Ukraine and certain cities of USA
Analysis for URI Data	The VSI_Account_logon.php page has been for used for attack and the others column has been reduced to half.

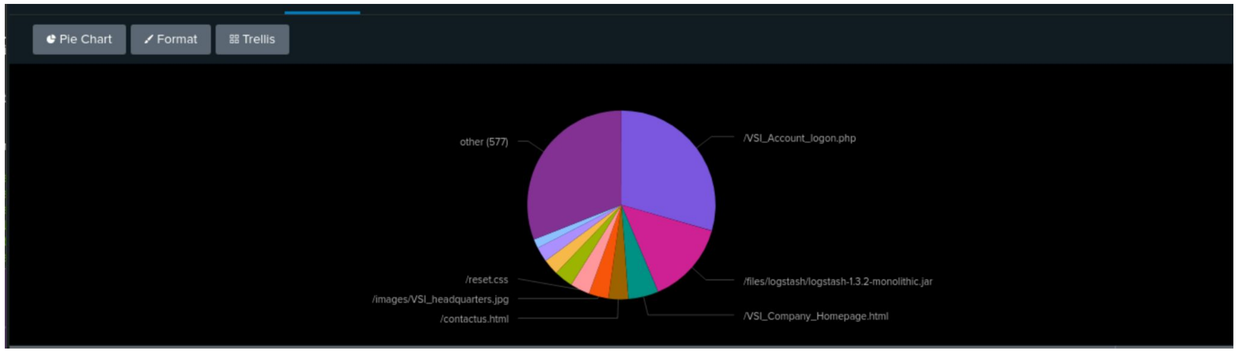
Screenshots of Attack Logs

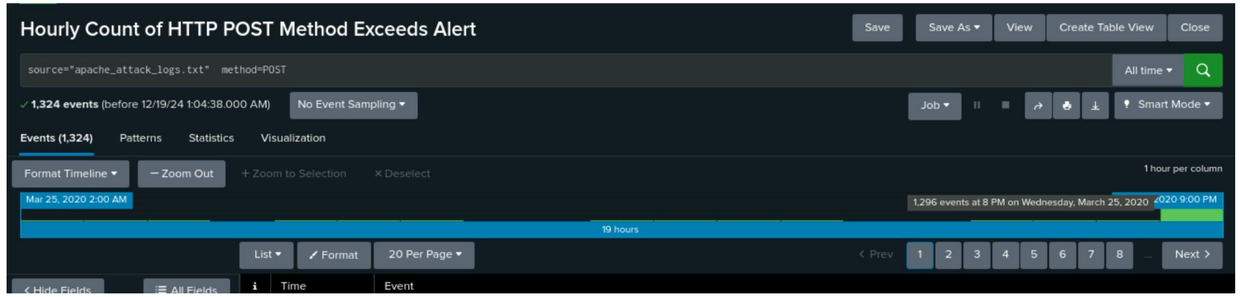






Screenshots of Attack Logs

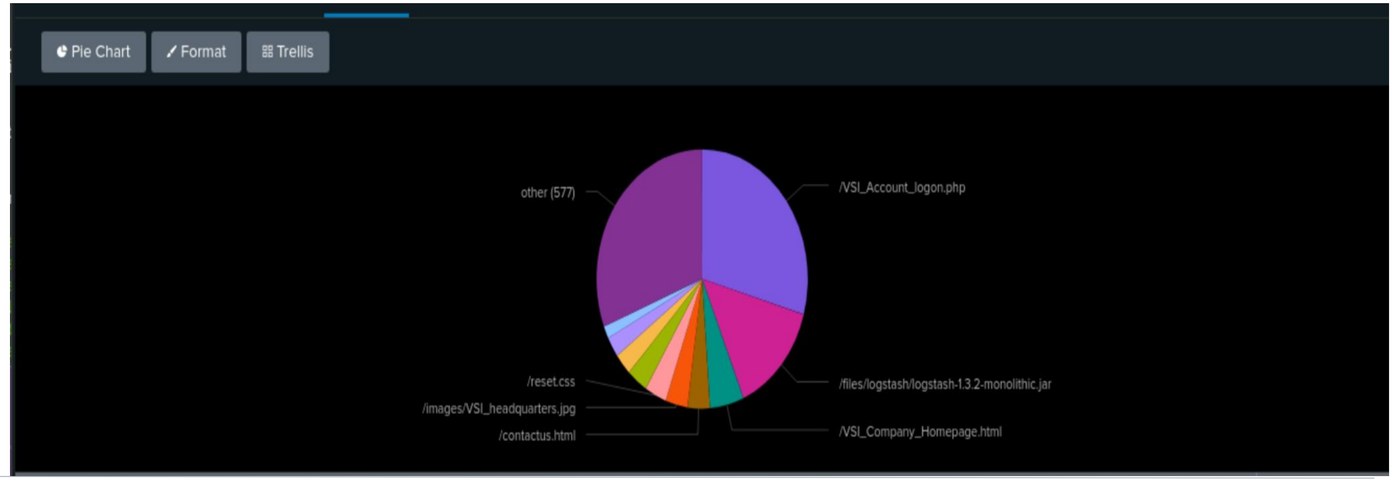




Screenshots of Attack Logs

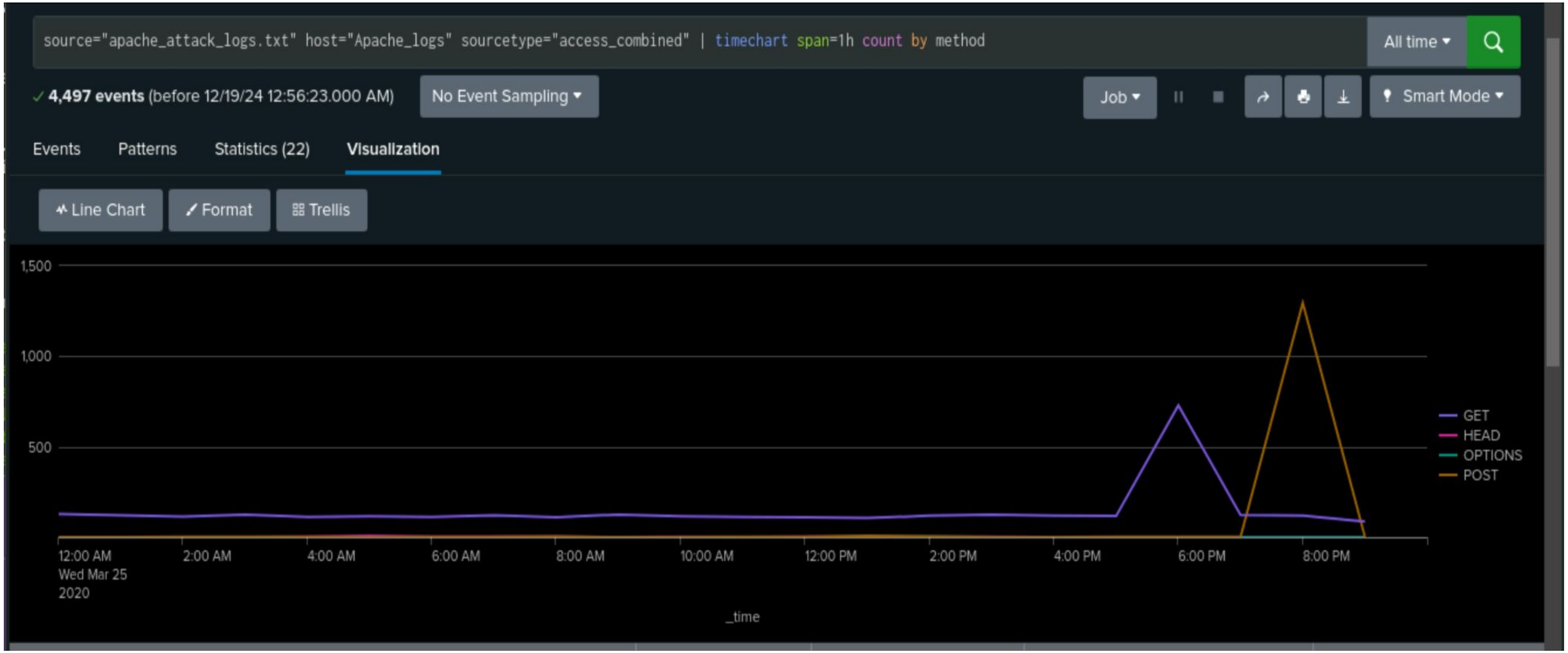
International Activity

URI Analysis



Screenshots of Attack Logs

Time Chart Analysis



Summary and Future Mitigations

Project 3 Summary

- What were your overall findings from the attack that took place?
  - Our overall findings from these attacks is that on March 25, VSI experienced enhanced number of attacks on there Windows and Apache Servers.
  - The attack targeted user authentication with spikes in POST requests and GET requests, high activity on VSI_Account_logon.php, and unusual activity from Ukraine and Washington. It also had high failed login attempts, account lockouts, and password resets. This can mean that a coordinated brute force and enumeration attempts were made

Project 3 Summary

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

  - The user must be logged out after certain number login attempts.
  - Implement MFA, rate limiting, and CAPTCHA to mitigate brute force and bot attacks.
  - Enforce stricter password policies and monitor high-risk URIs for unusual traffic.
  - Use geo-blocking and alert thresholds tuned to detect anomalies while reducing false positives. - Strengthen defenses with input validation, regular penetration testing, and real-time threat detection systems

Cybersecurity

Project 3 Review Questions

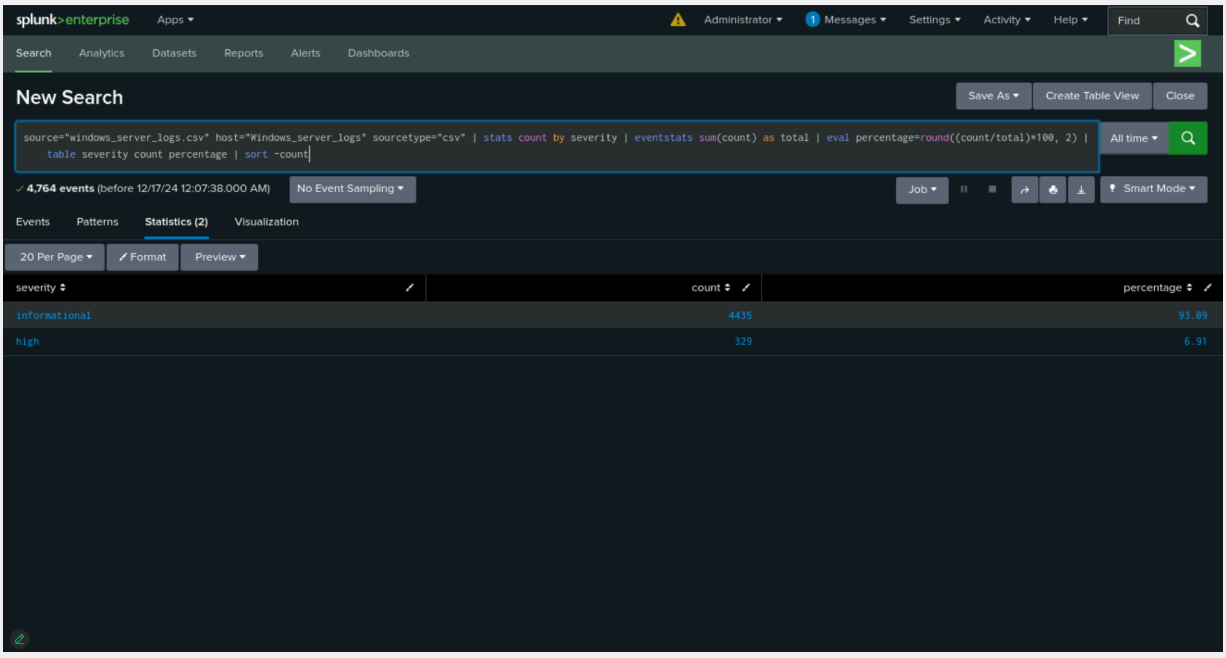
Make a copy of this document before you begin. Place your answers below each question.

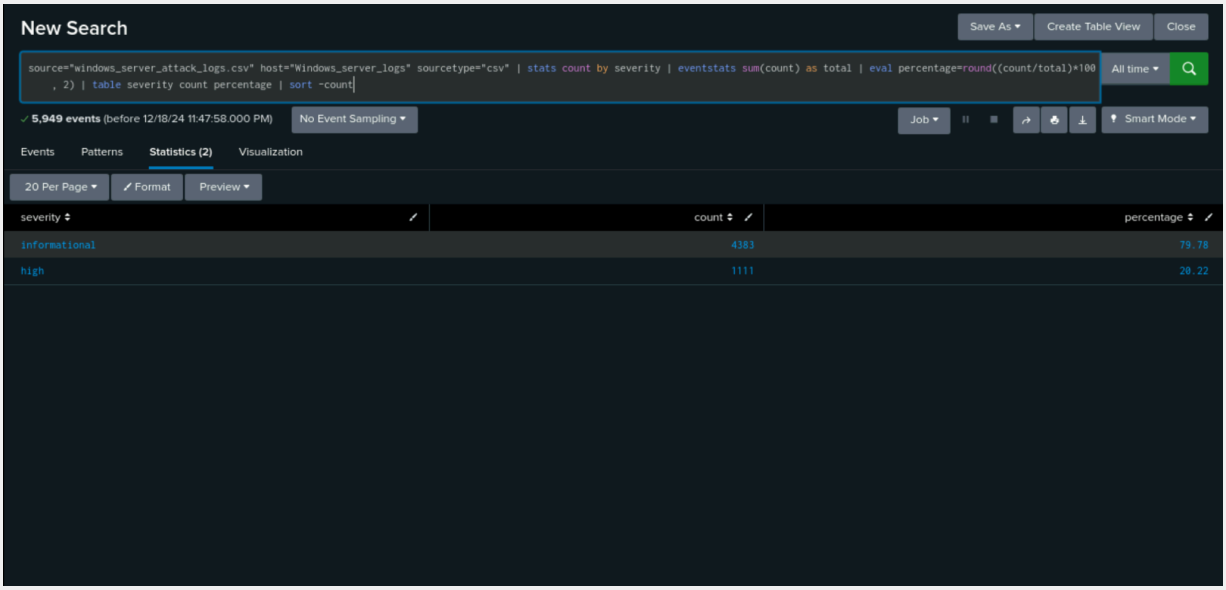
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes,severity “high” increases from 329 to 1111 and from 6.91% to 20.22%.

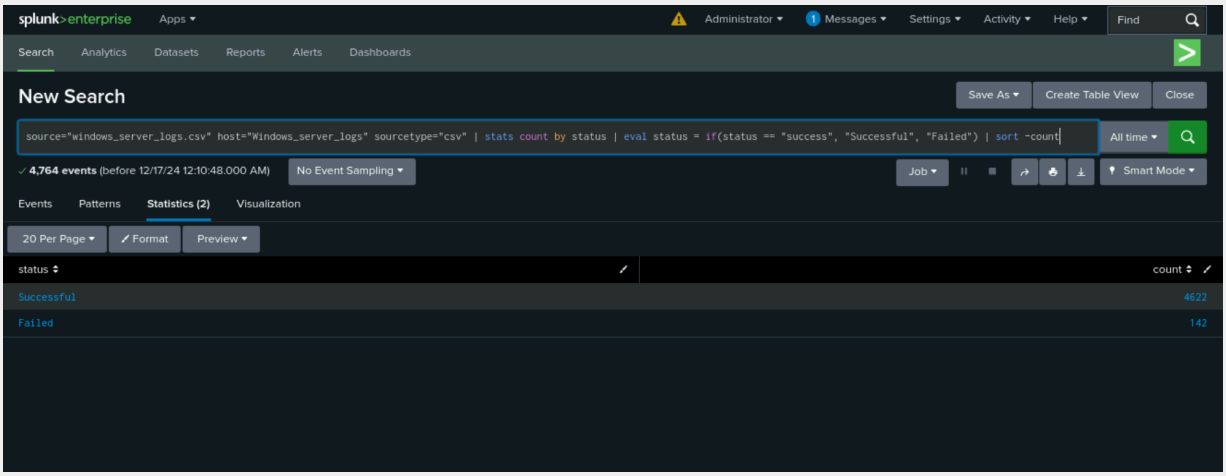


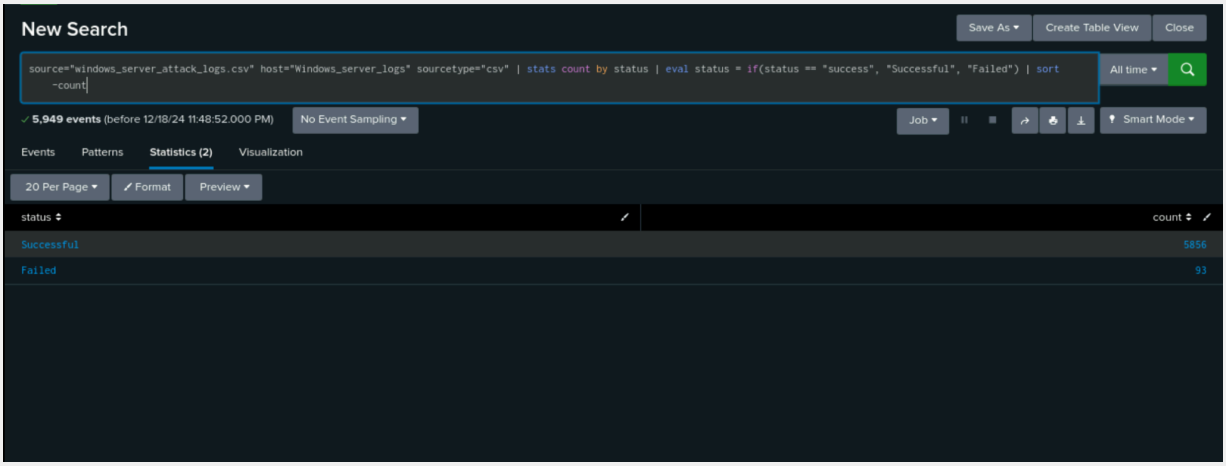


Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes. The amount of failure has dropped from 142 to 93 and the amount of success has increased from 4622 to 5856.

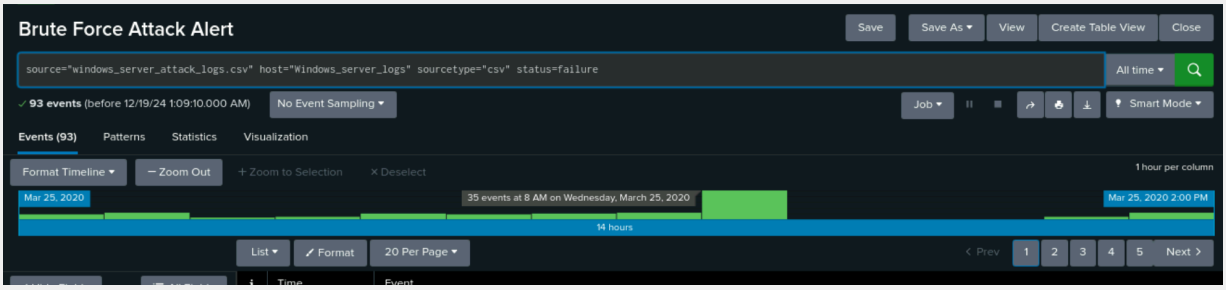




Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes



- If so, what was the count of events in the hour(s) it occurred?

35 events

- When did it occur?

```
8am on March 25, 2020
```

- Would your alert be triggered for this activity?

```
Our alert is anything greater than 6, so it would be triggered
```

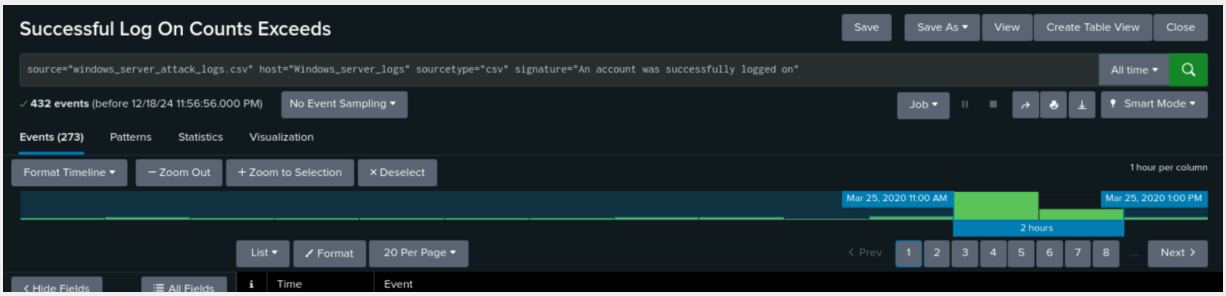
- After reviewing, would you change your threshold from what you previously selected?

```
We would bump up our number to 12
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes
```



- If so, what was the count of events in the hour(s) it occurred?

```
196 events at 11am and 77 at 12pm and 15 at 1pm
```

- Who is the primary user logging in?

```
User_j
```

- When did it occur?

```
11am, 12pm, 1pm
```

- Would your alert be triggered for this activity?

```
Yes, our alert was triggered for this activity
```

- After reviewing, would you change your threshold from what you previously selected?

```
No, our alert caught the activity
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Highest previously was 22, in the attack logs the highest was 17, nothing
suspicious noted.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

March 25 2020 1:00AM 805 and at 2:00 am 896 user accounts locked out March 25 2020 at 09:00am 1258 attempts were made to reset an accounts password.

- What signatures stand out?

805 at 1am and 896 at 2am user accounts were locked out. March 25 2020 at 9am 1258 attempts were made to reset an accounts password

- What time did it begin and stop for each signature?

12am-3am for user accounts being locked out and 8am - 11am for attempts were made to reset an accounts password

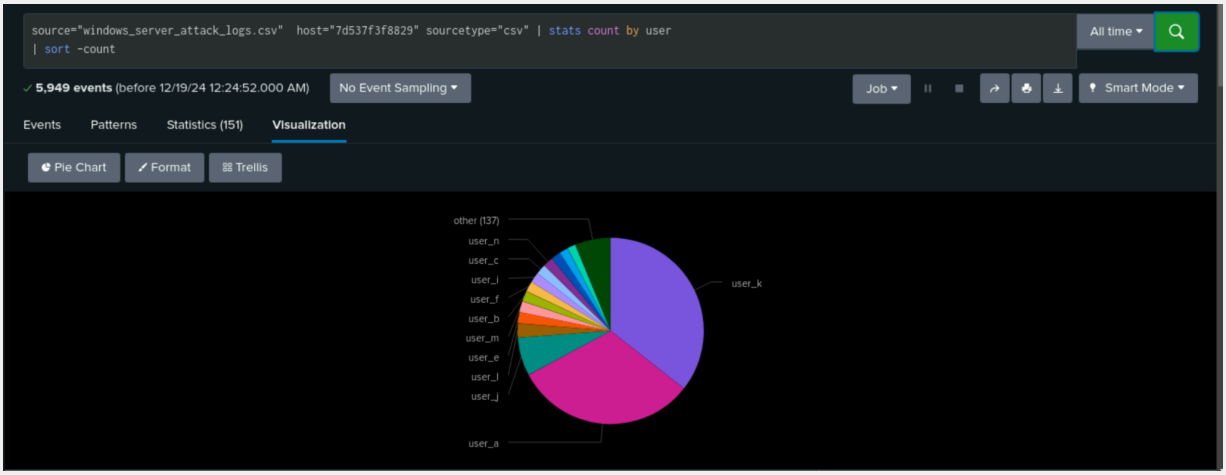
- What is the peak count of the different signatures?

896 for user accounts being locked out and 1258 for attempts were made to reset an accounts password

Dashboard Analysis for Users

- Does anything stand out as suspicious?

USER_K 35% AND USER_A 31.5%



- Which users stand out?

```
User K and User A
```

- What time did it begin and stop for each user?

```
User_K 09:00 am 1256 events; 761 at 10:00am stops at 11:00am
User_A 01:00 am 799 events; 984 02:00 am stops at 03:00 am
```

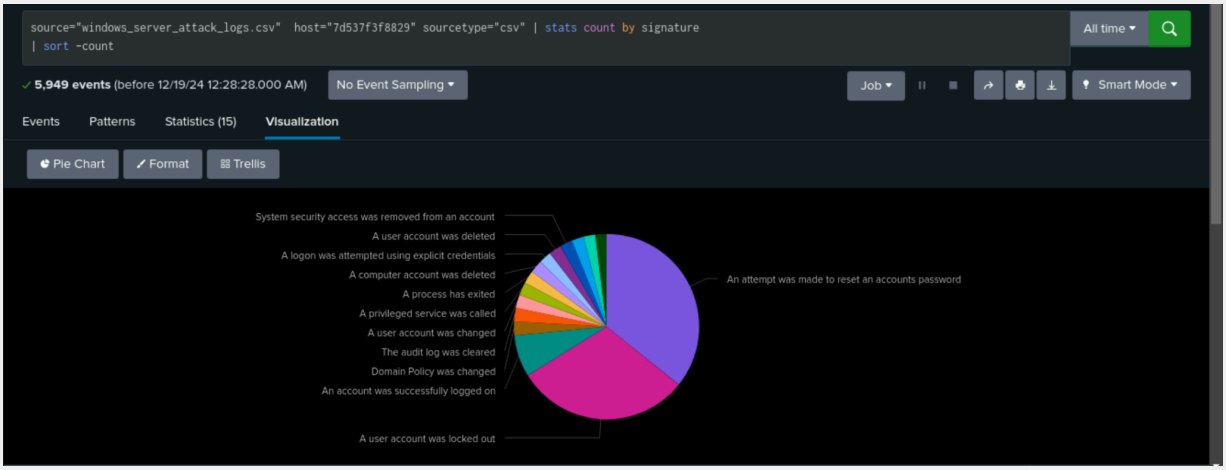
- What is the peak count of the different users?

```
User_K peak is 1256 events at 9:00AM
User_A peak is 984 events at 2:00AM
```

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
User_A 30.44% 1811
User_K 35.77% 2128
```



- Do the results match your findings in your time chart for signatures?

```
Yes. They match.
```

Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Nothing suspicious.
```

- Do the results match your findings in your time chart for users?

```
No, the results do not match.
```

Dashboard Analysis for Users with Statistical Charts

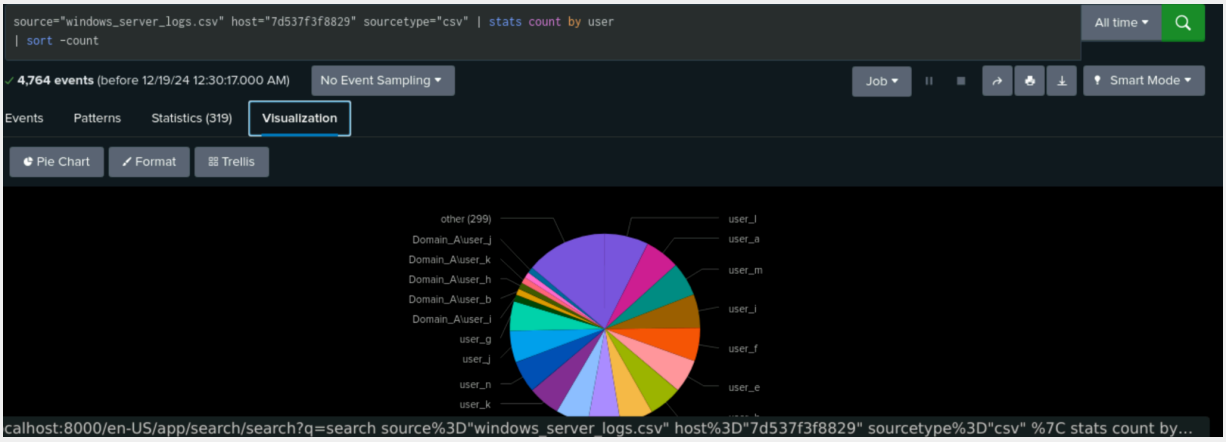
- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

```
Statistical Reports:
Advantages
   -  Provides precise and granular data insights
   -  Tailored to technical audiences for specific reporting needs
   -  Include explanations and advanced metrics for deeper understanding
Disadvantages
```

- Harder for non-technical audiences to interpret
- Takes longer to analyze and derive conclusions compared to visualizations

Visualizations:
Advantages
- Highlights key trends and relationships instantly
- Appealing and accessible to a broad audience
- Focuses on critical data points without excessive detail

Disadvantages
- May oversimplify complex data or miss nuanced insights
- Can mislead if poorly designed or improperly scaled
- Needs supplementary information for thorough analysis

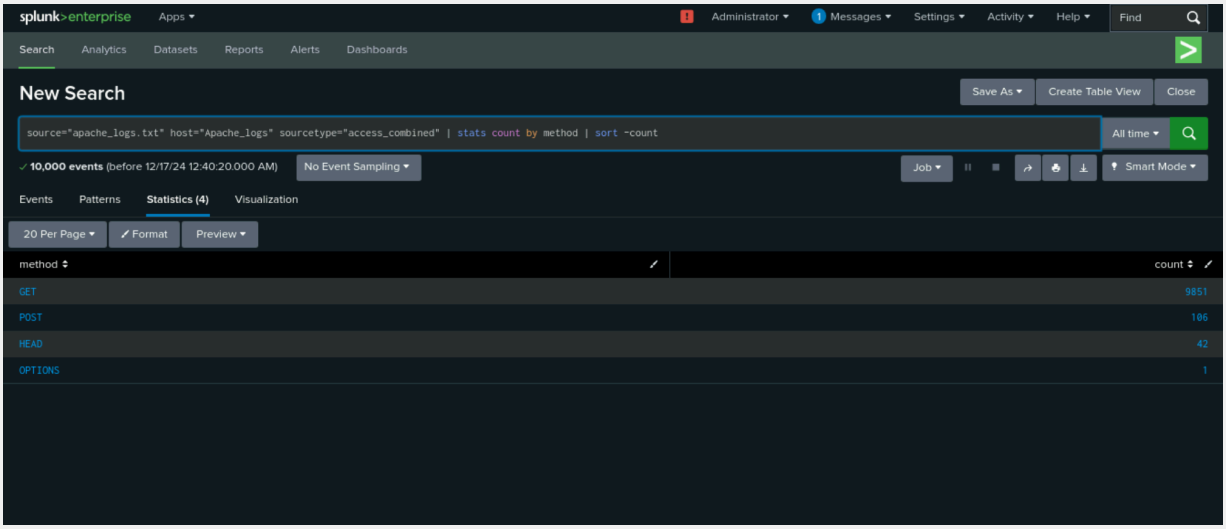


Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, `GET went down, POST went up.`



- What is that method used for?

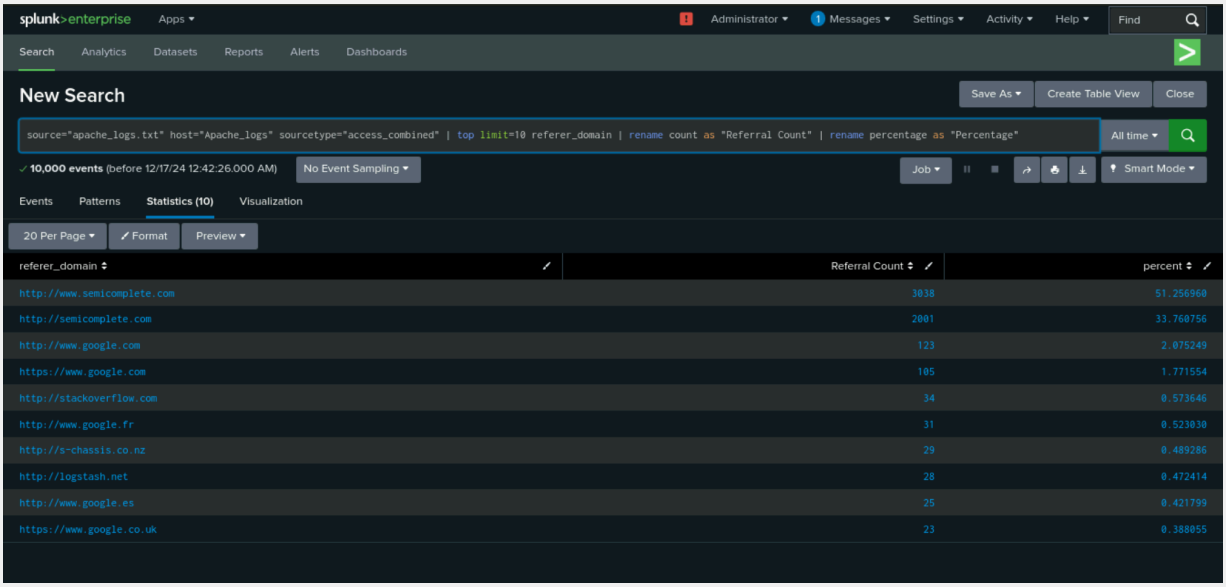
`GET requests: used for retrieving data from a server without modifying any resources.`

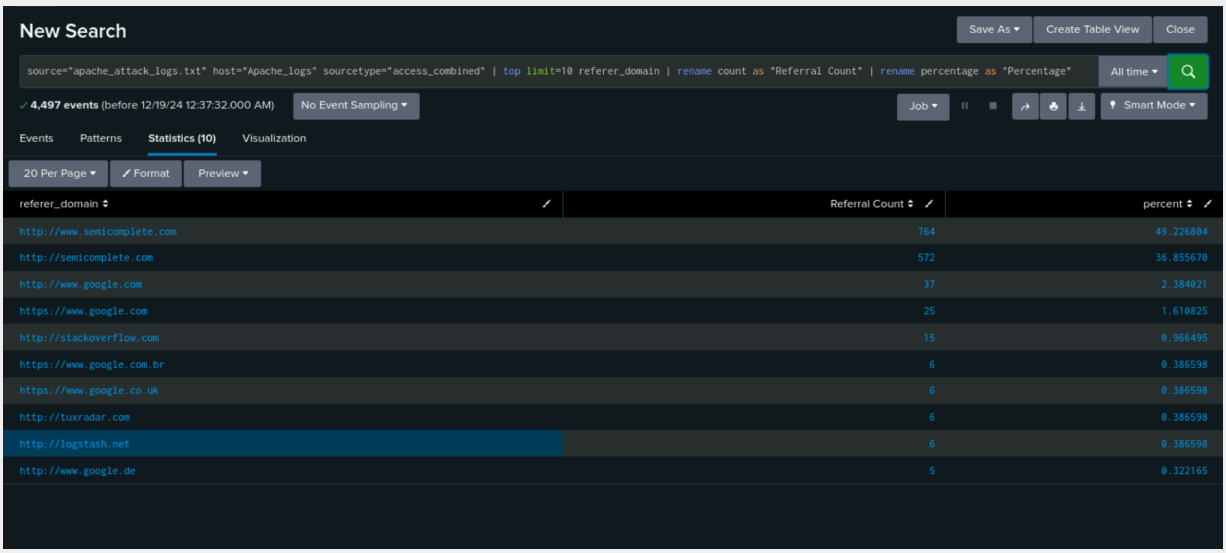
`POST requests: used for sending data to the server to create or update resources.`

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No major changes to the domains.





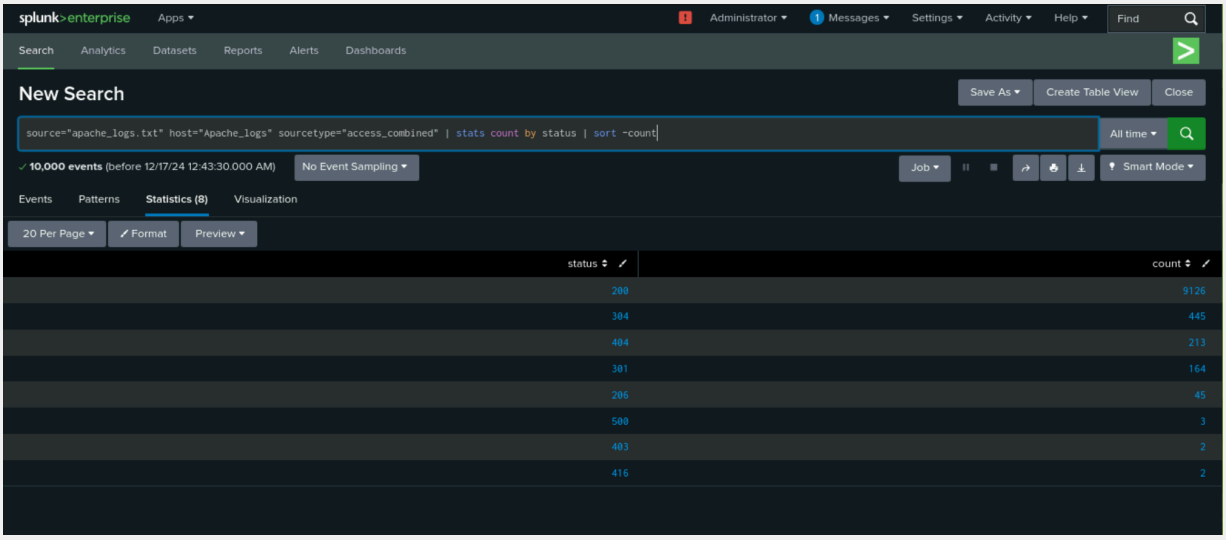
Report Analysis for HTTP Response Codes

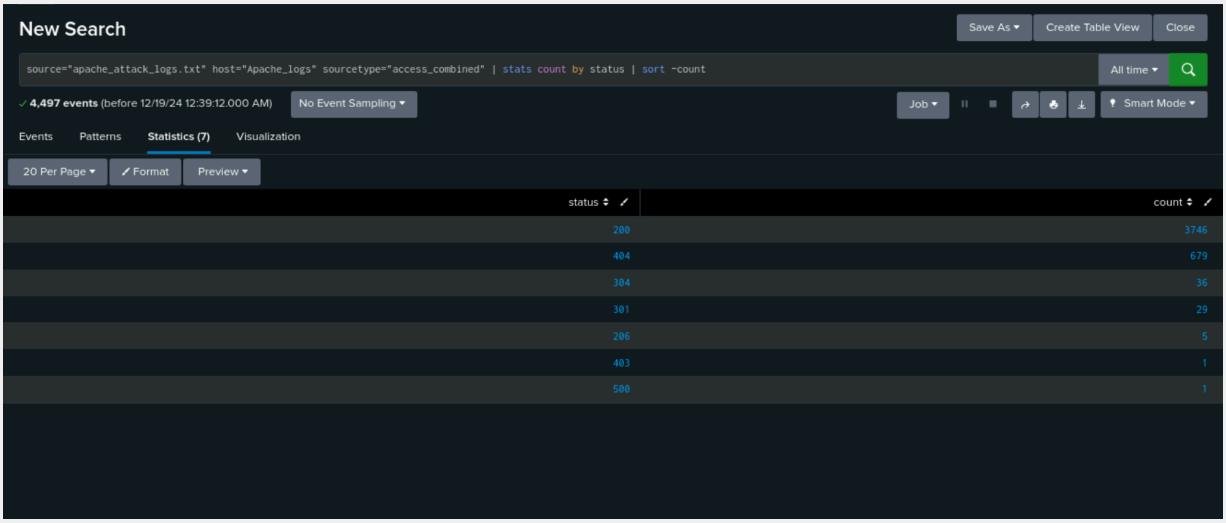
- Did you detect any suspicious changes in HTTP response codes?

Yes. There are several changes:

1. 200 went down by more than half
2. 404 went up around 400
3. 304 went down 400
4. 301 went down 100

5. 206 went down 40

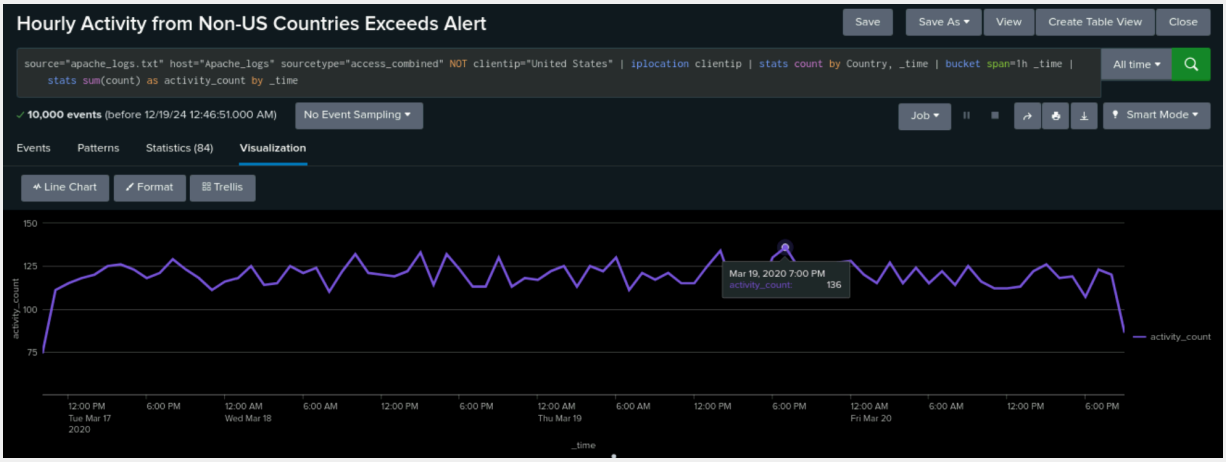




Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes. We see a spike from international volume.
```



- If so, what was the count of the hour(s) it occurred in?

730 at 6pm, decreased 123 (normal baseline) at 7pm and increased to 1415 at 8pm

- Would your alert be triggered for this activity?

Yes, our alert is triggered for anything above 120

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

We would increase our threshold to 300

Alert Analysis for HTTP POST Activity

- Did you detect any suspicious volume of HTTP POST activity?

```
Yes. There is a spike of POST requests.
```

- If so, what was the count of the hour(s) it occurred in?

```
1,296 counts
```

- When did it occur?

```
8 PM on March 25th, 2020
```

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

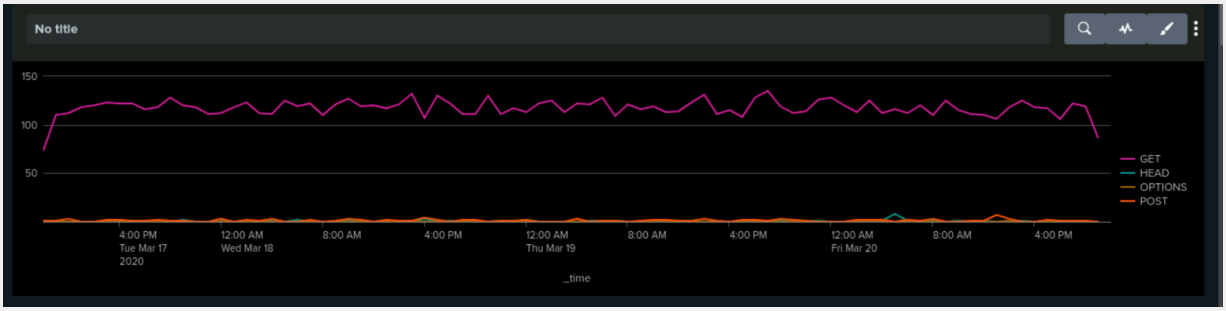
```
Yes, we will change it to 300-400
```

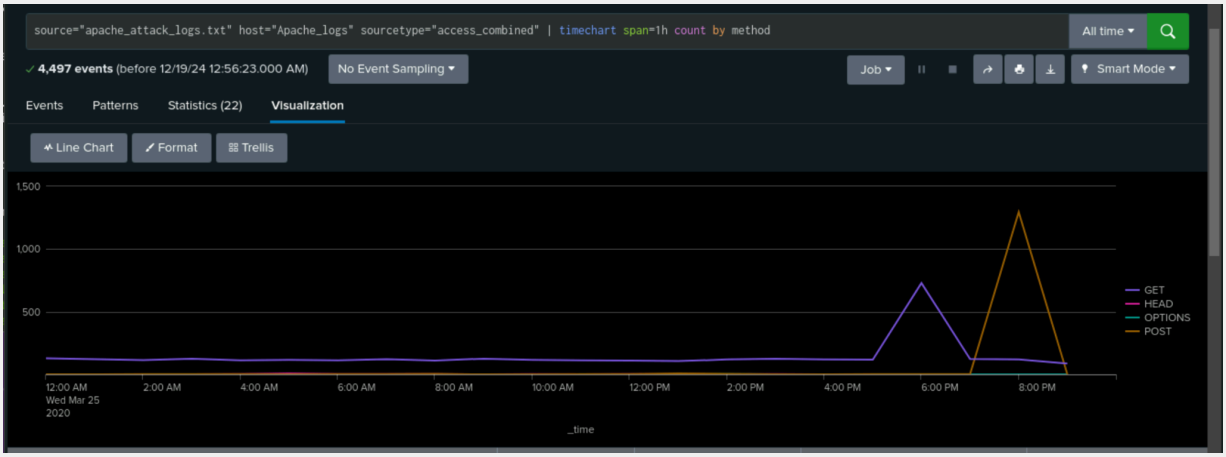
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
The GET spiked at 6 pm to 729 requests.
```

The POST requests spikes to 1296 requests at 8 pm





- Which method seems to be used in the attack?

The POST Method

- At what times did the attack start and stop?

Starts at 5:00 pm and ends at 09:00 pm

- What is the peak count of the top method during the attack?

POST at 1296

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

San Francisco 1143, New York 881 Germany 992

```
Attack: washington 724, New York 670 Ukraine 911
```

- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

```
Ukraine(Kiev and Kharkiv) and Washington DC, USA
```

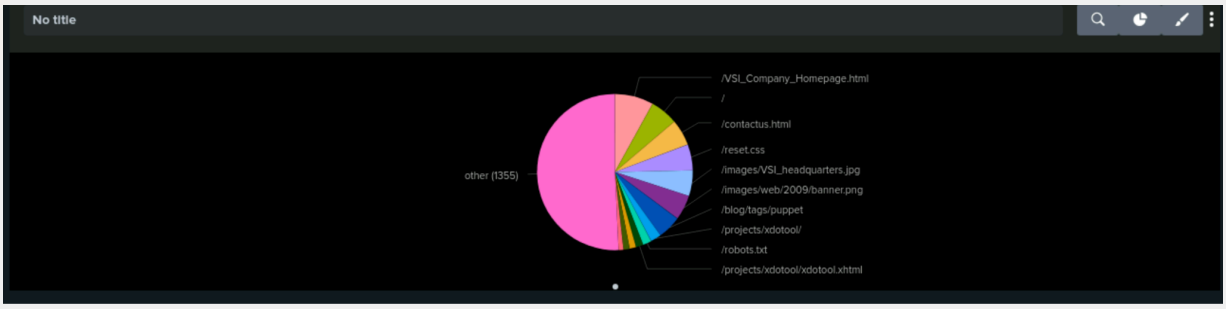
- What is the count of that city?

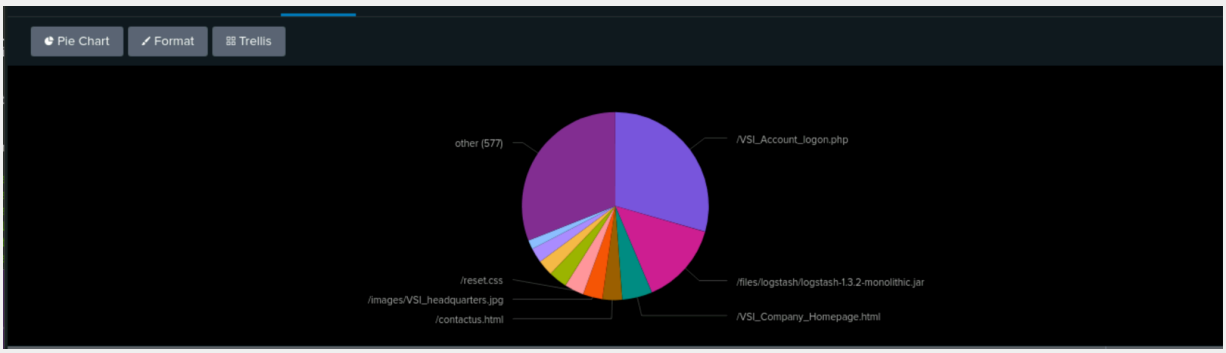
```
Washington 724

Kiev 440

Kharkiv 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes
```





- What URI is hit the most?

```
VSI_Account_logon.php 29.42% 1323 count
```

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

```
The attacker was trying to access our server with brute force attack and SQL injection.
```