Cybersecurity

Project 3 Review Questions

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

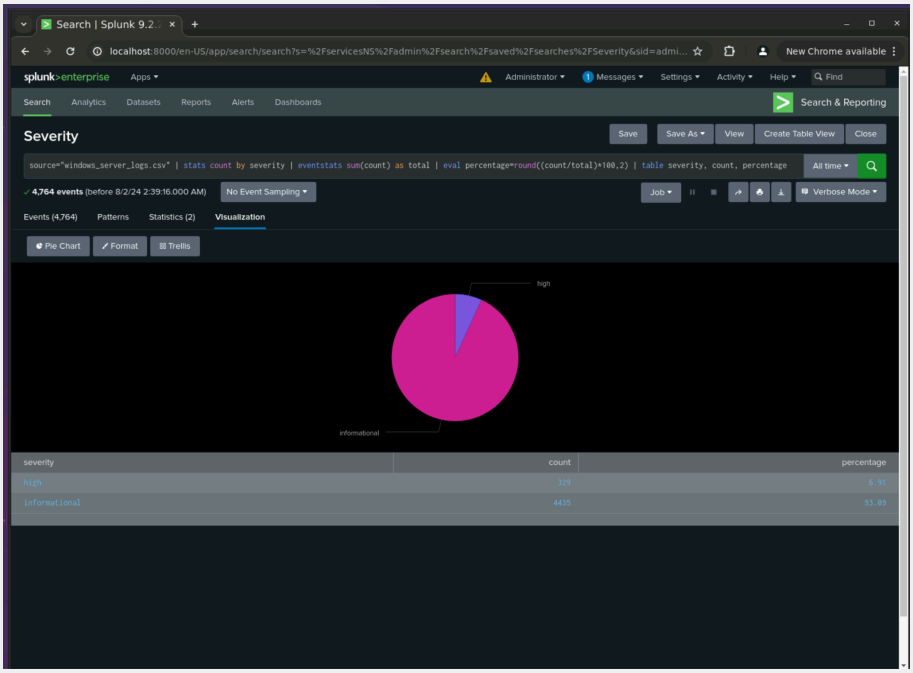
Windows Server Log Questions

Report Analysis for Severity

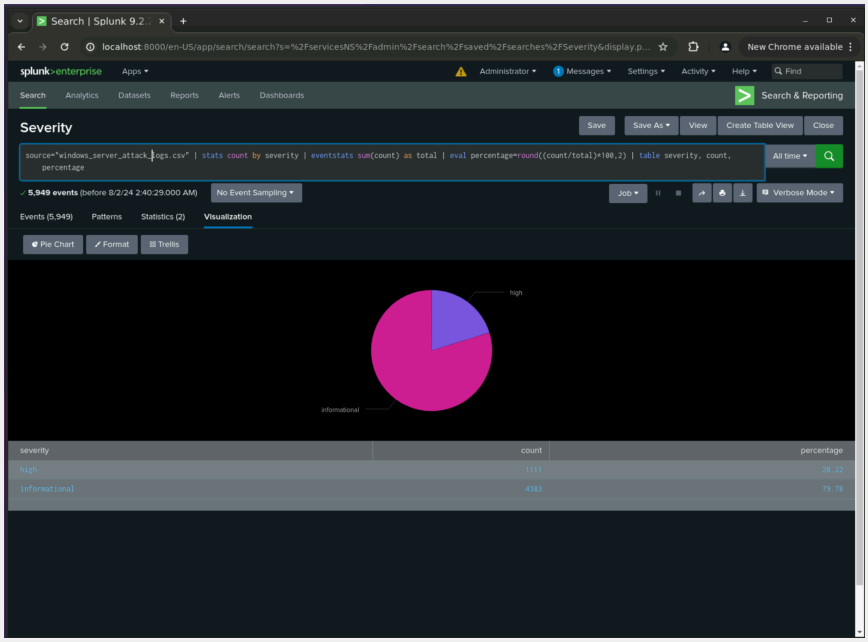
- Did you detect any suspicious changes in severity?

Yes, prior to the attack, the “high” severity count was 329. After the attack the “high” severity jumped up to 1111. This changed the “high” severity percentage from 6.9% to 20.2%.

Pre Attack



Post Attack

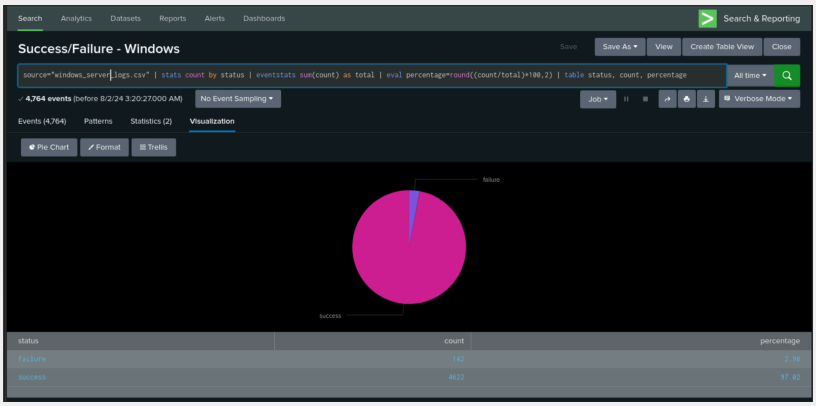


Report Analysis for Failed Activities

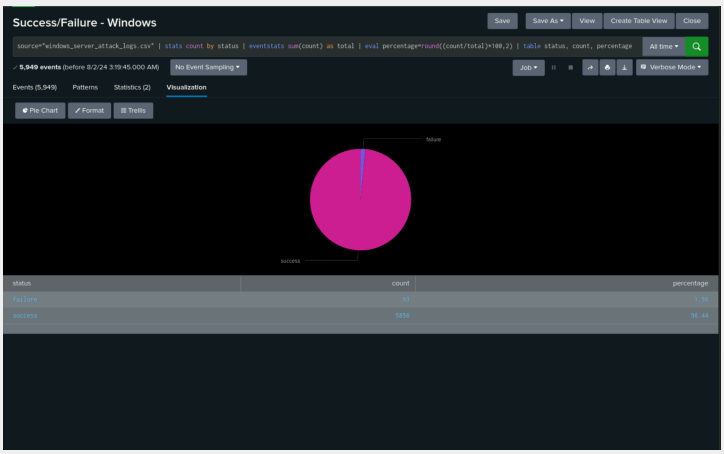
- Did you detect any suspicious changes in failed activities?

Yes - Pre Attack, there was double the failures we saw in the post attack and the success rate went up (from 4622 to 5856), which means the attacker had a lot of successful attempts which caused the failure rate to skew the numbers a bit.

Pre Attack



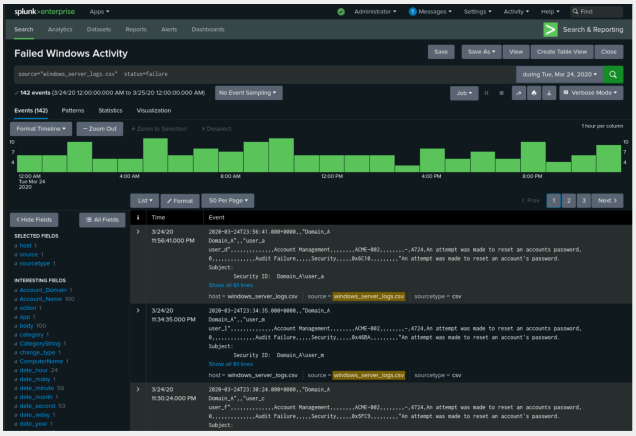
Post Attack



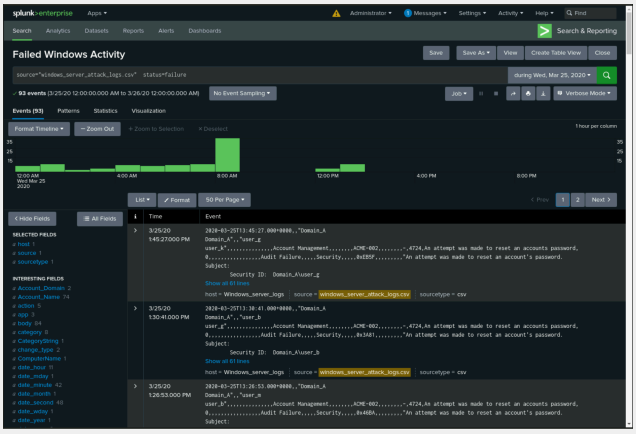
Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

`Yes - Pre Attack`



`Post Attack`



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

```
35 events
```

- When did it occur?

```
8:00am on March 25, 2020
```

- Would your alert be triggered for this activity?

```
Yes, it was set to greater than 8 events
```

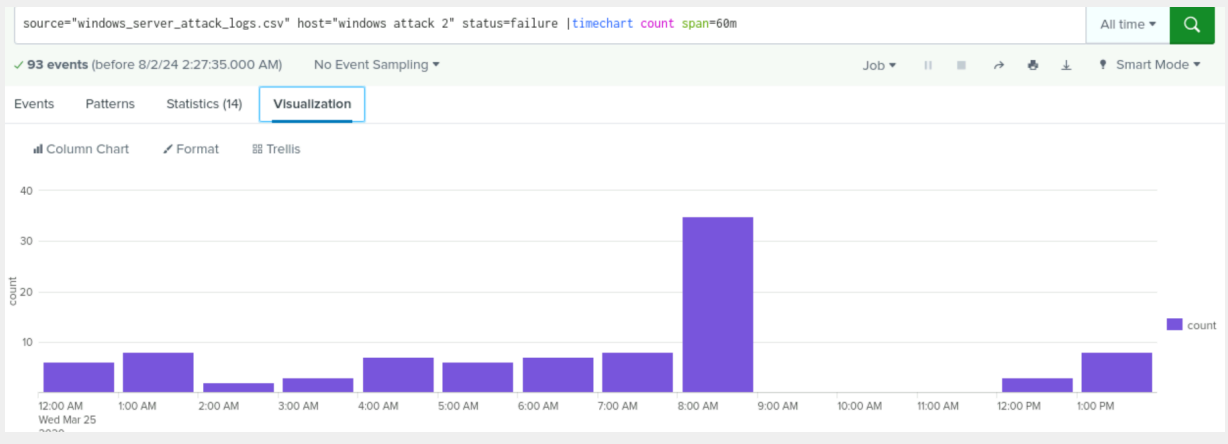
- After reviewing, would you change your threshold from what you previously selected?

```
No, based on the attack logs, this was within range and won't provide too
many alerts.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes, there is suspicious logins due to lack of logins.
```



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

```
There are zero logins between 9 and 11.
```

- Who is the primary user logging in?

```
User_a is the primary user
```

- When did it occur?

```
2am one Wed Mar 25 2020
```

- Would your alert be triggered for this activity?

```
No, our alert would not be triggered.
```

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

```
I would change the threshold number slightly.
```

Alert Analysis for Deleted Accounts

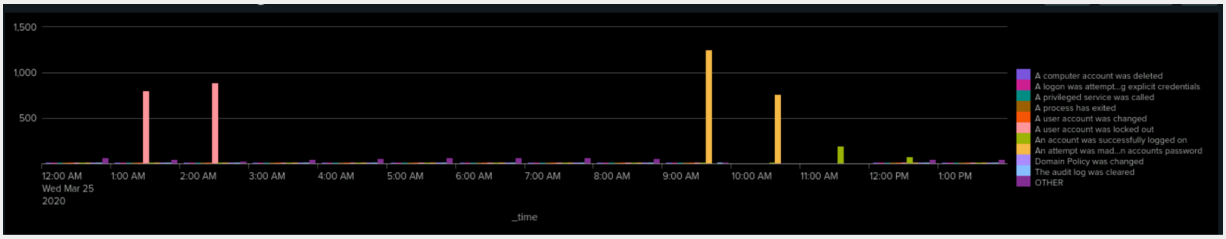
- Did you detect a suspicious volume of deleted accounts?

```
No, there were fewer user accounts being deleted during the attack than
there were on the original server logs. 318 user accounts were deleted on
March 24th. 131 user accounts were deleted on March 25th.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes
```



- What signatures stand out?

```
A user account was locked out & An attempt was made to reset an accounts
password
```

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

```
1:00am - 2:00am = A user account was locked out
9:00am - 10:00am = An attempt was made to reset an accounts password
```

- What is the peak count of the different signatures?

```
896 count = A user account was locked out
1258 count = An attempt was made to reset an accounts password
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes there is an increase in two users.

- Which users stand out?

User_a and user_k

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

```
User_a is between 1am and 2:00am
User_k is between 9am and 10am
```

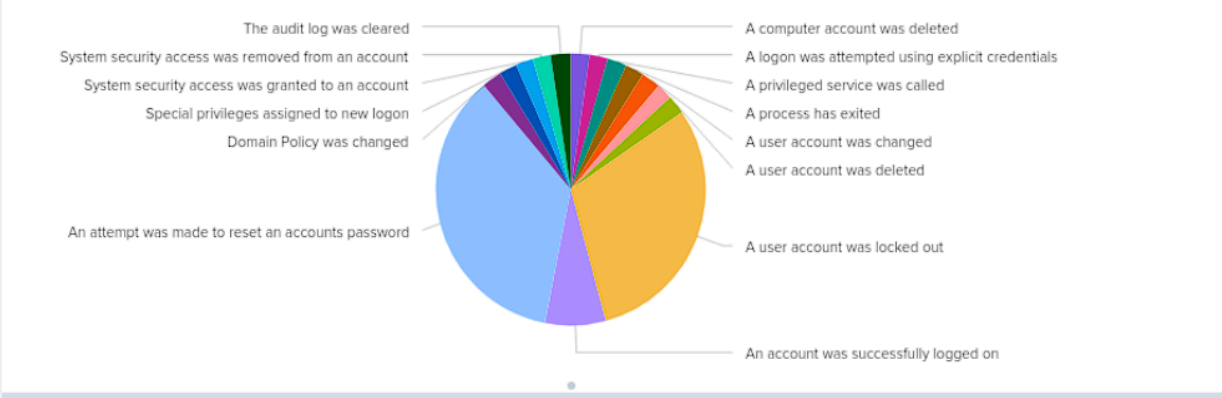
- What is the peak count of the different users?

```
User_a 984
User_k 1256
```

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

- Does anything stand out as suspicious?

```
Yes the spike in amount of users that were locked out of their accounts and
the amount of attempts to reset an accounts password were higher than
normal.
```

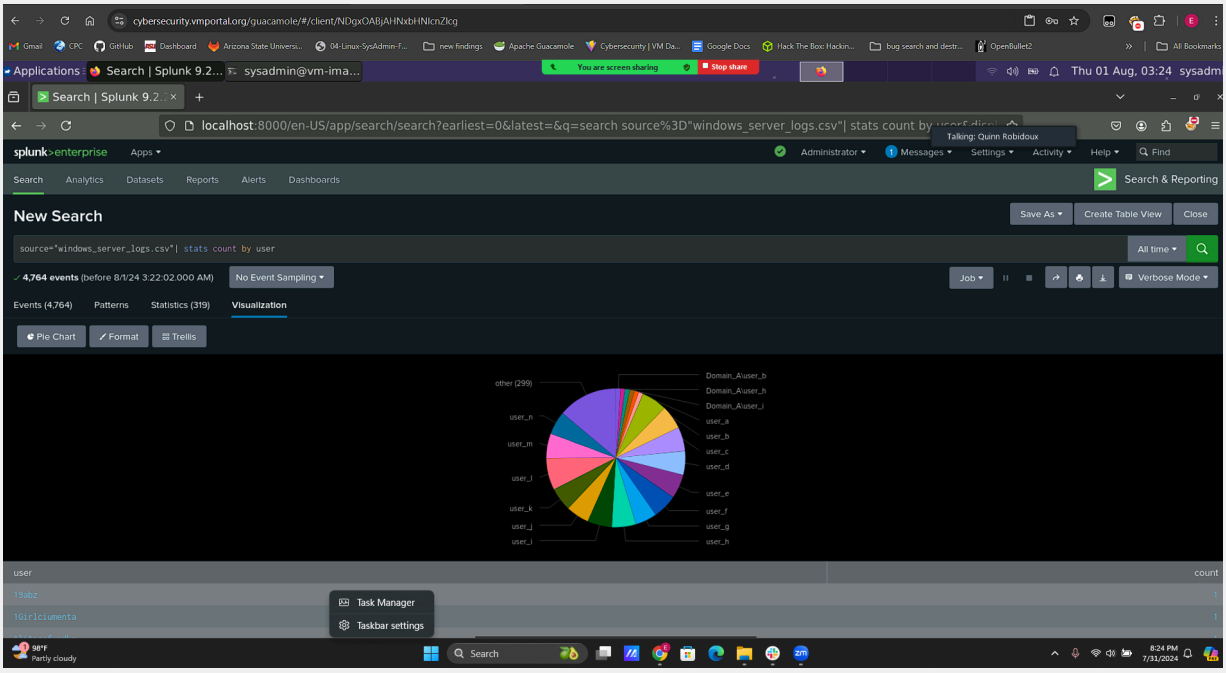


- Do the results match your findings in your time chart for signatures?

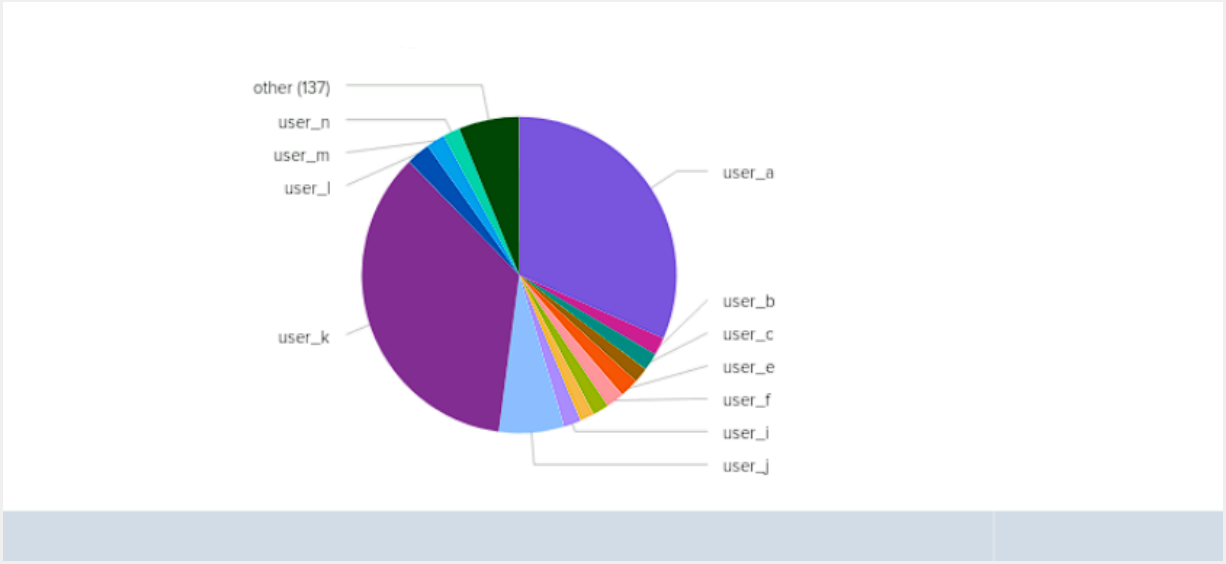
```
Yes the results match my findings in my time chart as shown in the
screenshot above.
```

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

- Does anything stand out as suspicious?



Yes that there was 3 domain users that were no longer in after the attack



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

yes

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?

```
That it shows by name of signature and by user specifically.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, both GET and POST had serious spikes during the hours of the attack.
729 GET events occurred at 6pm more than 3 times the average per hour.

1,296 POST events came through at 8pm more than 1000 times the average per
hour.
```

- What is that method used for?

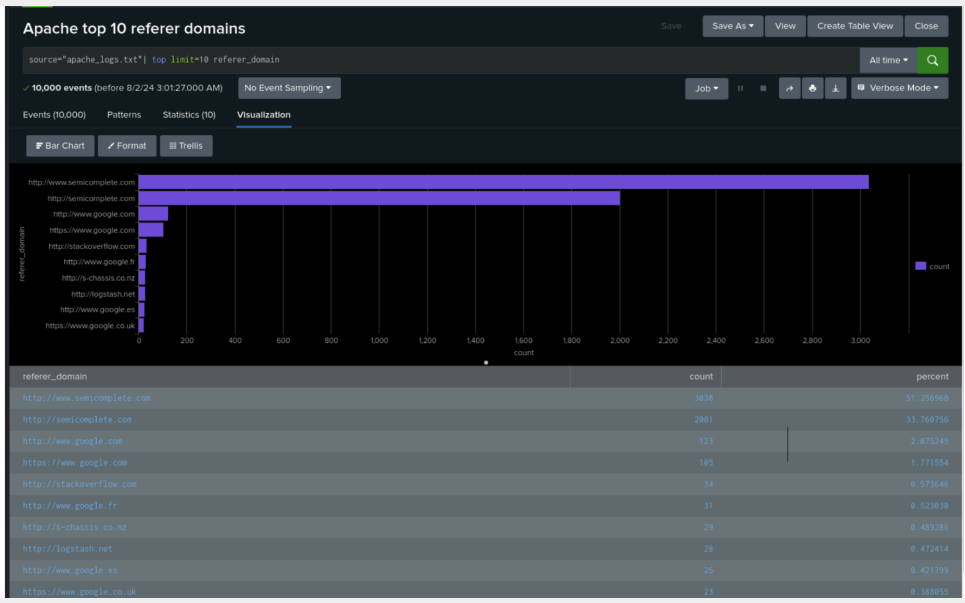
```
GET is a request for resources or data, trying to fetch something from our
servers.

POST is a method to submit data.

This likely means the attacker used GET events to prob the defenses before
unleashing their POST events trying to exploit a found weakness,
unfortunately we don't know based off this info just what kind of attack it
is, though it does narrow the list down.
```

Report Analysis for Referrer Domains

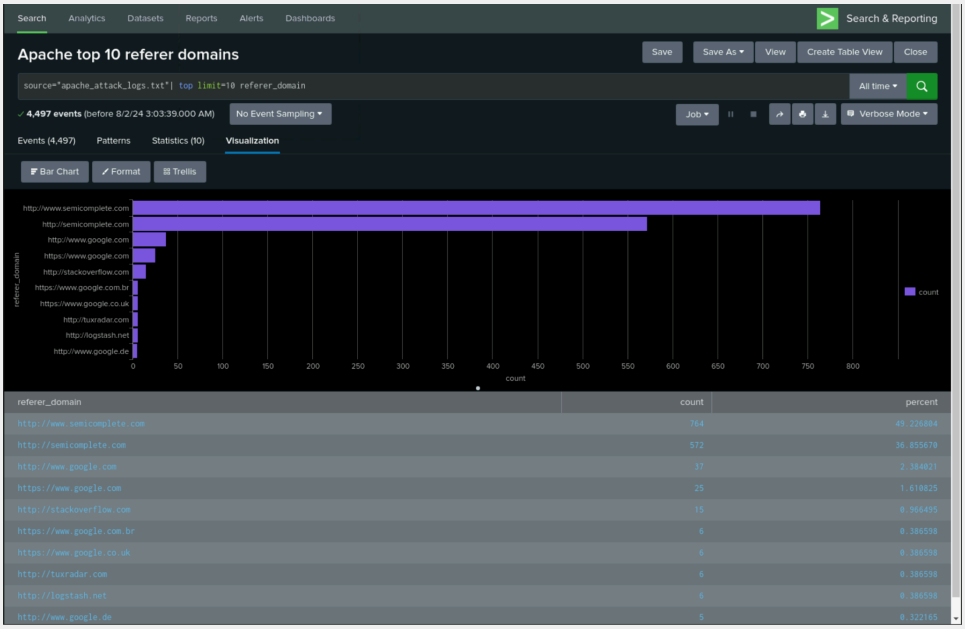
- Did you detect any suspicious changes in referrer domains?

```
Yes - pre attack, the count was higher (3038 for www.semicomplete.com & 2001
for semicomplete.com). After the attack the traffic reduced (764 for
www.semicomplete.com & 572 to semicomplete.com). Reduced traffic means not
as many people are directed to our site.
```

Pre Attack



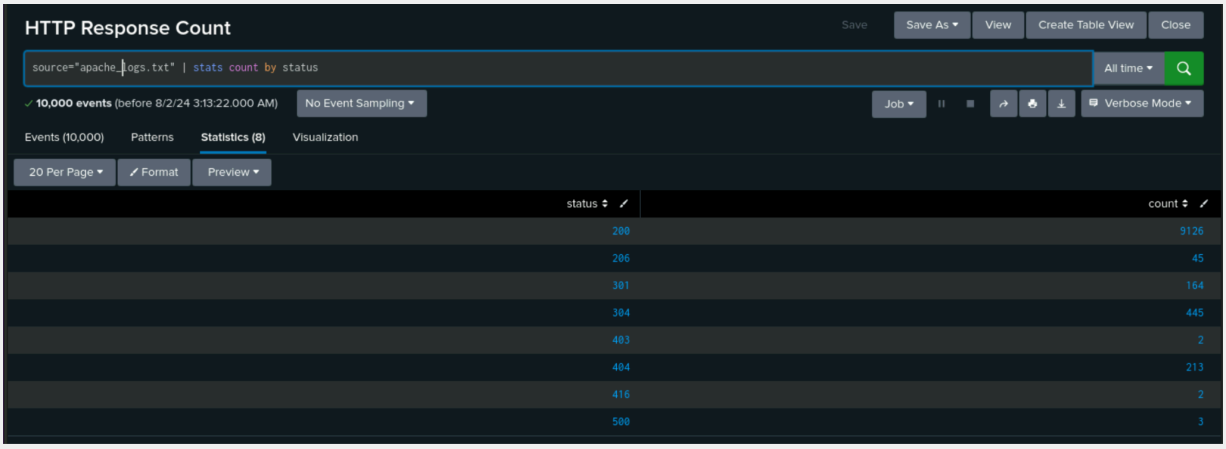
Post Attack



Report Analysis for HTTP Response Codes

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

Yes - Before the attack, the response code count (200) was much higher (9126) which signifies a successful connection. After the attack, the successful connections/responses went down (3726) signifying that getting a good connection was not as common/easy.
Pre Attack



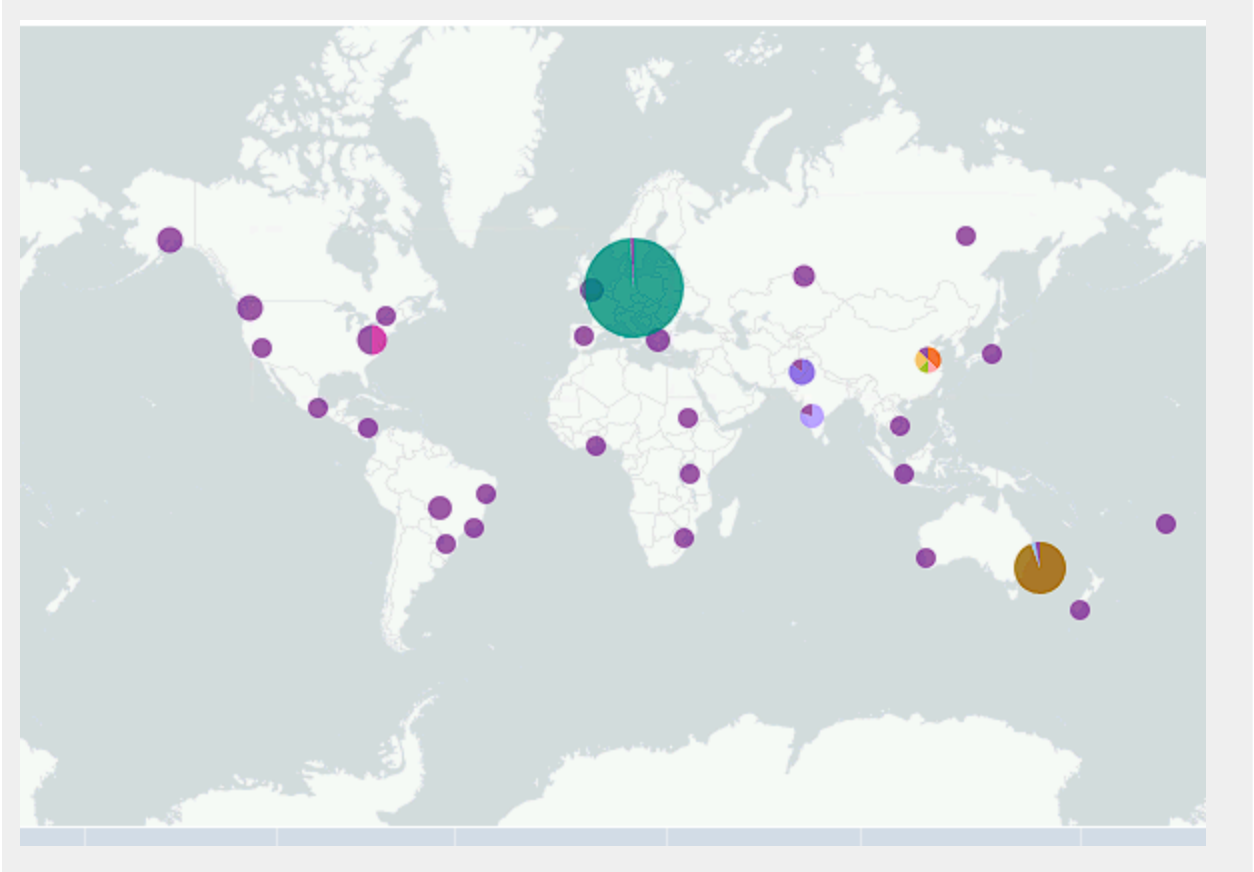
Post Attack

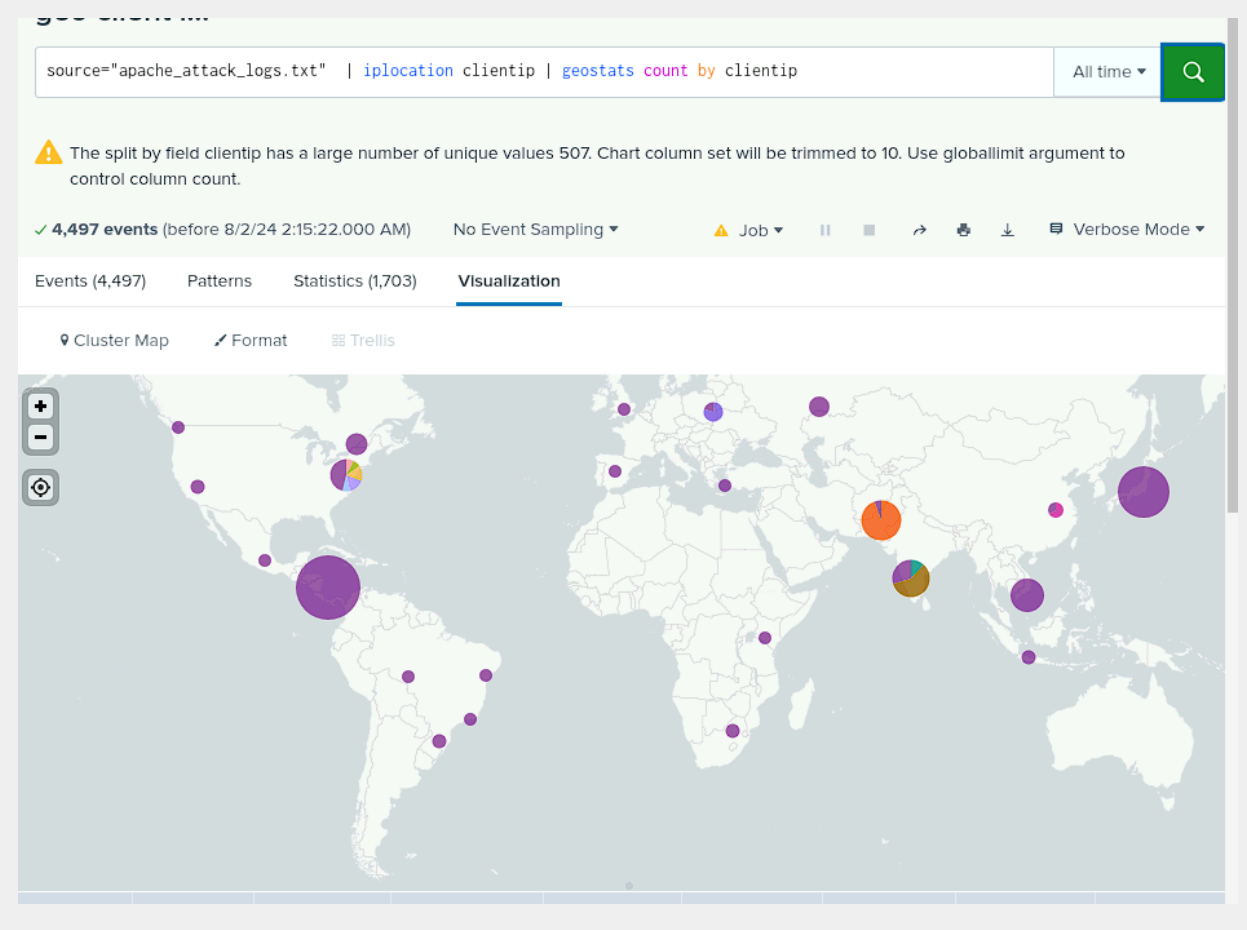
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

International activity was starkly different from normal levels, normally europe is the location for the vast majority of traffic, however during the time around the attack large quantities of interactions came from India, Afghanistan, Japan, Vietnam and primarily from Central America.

These locations normally make up very little of standard traffic and could either be origin points of attacks, or more likely, the location of servers meant to hide the true location of the attackers.





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

```
730 events at 6pm on Wednesday, march 24, 2020
1415 events at 8 pm on wednesday march 24, 2020

This is over the average per hour of 120 events.
```

- Would your alert be triggered for this activity?

```
Our alert would be triggered as the threshold was set for 150 events per
hour.
```

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

```
No our threshold was adequate for catching such large events
```

Alert Analysis for HTTP POST Activity

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

```
Yes at 8pm on Wednesday, March 24th, 2020 the number of hourly HTTP POST
increased over 1000 times.
```

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

```
1,296 times between 8-9pm
```

- When did it occur?

```
8-9pm Wednesday, March 24th,2020
```

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

```
The threshold was blown passed as it was set to 10 being well above the
hourly average.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
yes.
```

- Which method seems to be used in the attack?

```
Both GET and POST
```

- At what times did the attack start and stop?

```
GET attack at 6pm
POST attack at 8pm

Wednesday, March 24th, 2020
```

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

```
Get = 729
POST = 1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes
```

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

```
Ashburn = 668 count 14.854%
New York= 516 count 11.474%
Kyiv = 438 count 9.74%
Kharkiv = 432 count 9.606%
```

- What is the count of that city?

```
Four cities that normally don’t appear in the top ten cities dominated the
top of the list during the time of the attacks.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, there were several URI’s belonging to the VSI website that was being
viewed.
```

- What URI is hit the most?

```
/VSI_Account_logon.php was hit the most at 1323.
```

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

```
Based on the account logon page, it could be a potential brute force attack.
```