Cybersecurity

Project 3 Review Questions

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

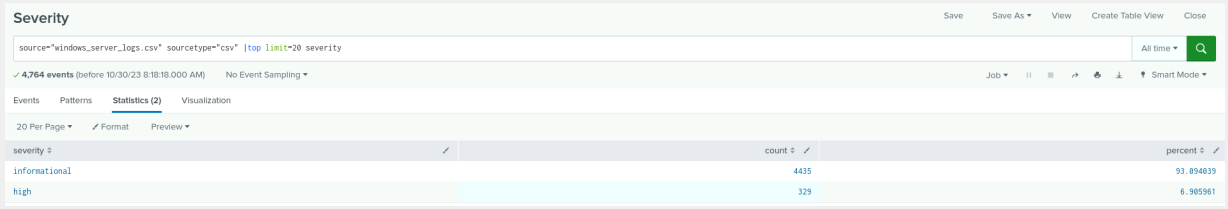
Windows Server Log Questions

Report Analysis for Severity

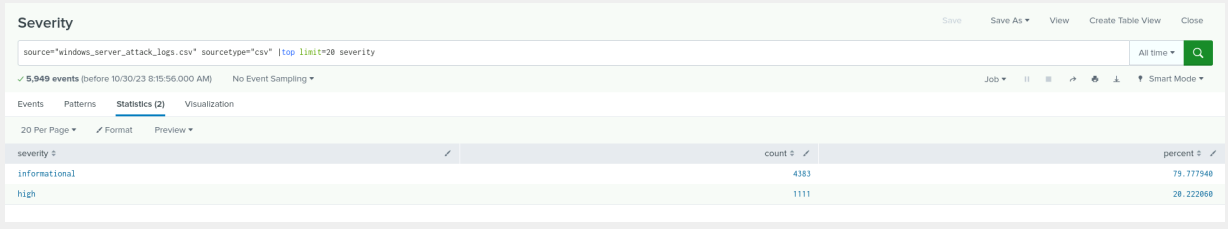
- Did you detect any suspicious changes in severity?

Yes. Increase in ‘High’ Severity by 14% (Count of 329 -> 1111)

Before :



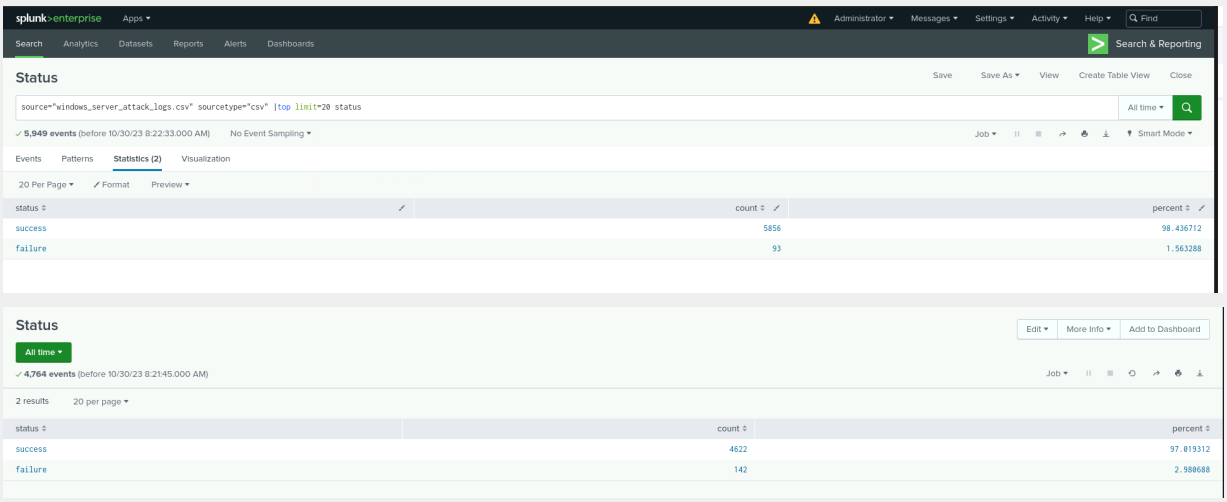
After :



Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Change in count of Failed Activities from 93 -> 142
```



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes. There was a abnormal count of failed activity detected
```

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

```
35 events was detected
```

- When did it occur?

```
Occurred at 9am , 25th of March
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No
```

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
```

- Who is the primary user logging in?

```
User K, User_K attempted 67 times which was suspicious
```

- When did it occur?

```
25th March - 9am
```

- Would your alert be triggered for this activity?

```
Yes, The alert would be triggered
```

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

```
No.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes. During the timeframe where suspicious login activities occurred there
was an increase in volume of user accounts being deleted
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes. There was an Increase in Password Change Attempt + User Locked
```

- What signatures stand out?

```
Account Locked Out + Attempt to Change/Reset Password Stood out the most
```

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

```
Locked Out - March 25th between 12am and 3am
Reset password - March 25th between 8am and 11am
```

- What is the peak count of the different signatures?

```
User accounts being locked out - 896  (at 2am)
Attempts to reset account - 1258 counts (at 9am)
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes
```

- Which users stand out?

```
User A, User K, User J
```

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

```
User A - Between 12am - 3am
User K -Between 8am - 11am
User J - Between 10am - 1pm
```

- What is the peak count of the different users?

```
User A - Peak count of 984 at 2am
User K - Peak count of 1256 at 9am
User J - Peak count of 196 at 11am
```

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

- Does anything stand out as suspicious?

```
yes
```

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

```
Yes
```

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

- Does anything stand out as suspicious?

```
Yes. Shows user A and K were very active
```

- 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?

The visualization of the data allows us to understand and interpret the data more easily allowing us to see any changes that may occur when comparing two different reports. The use of Pie Charts for example can help easily show the changes in data as it represents it all as a percentage and can easily show any major statistical shifts in data.

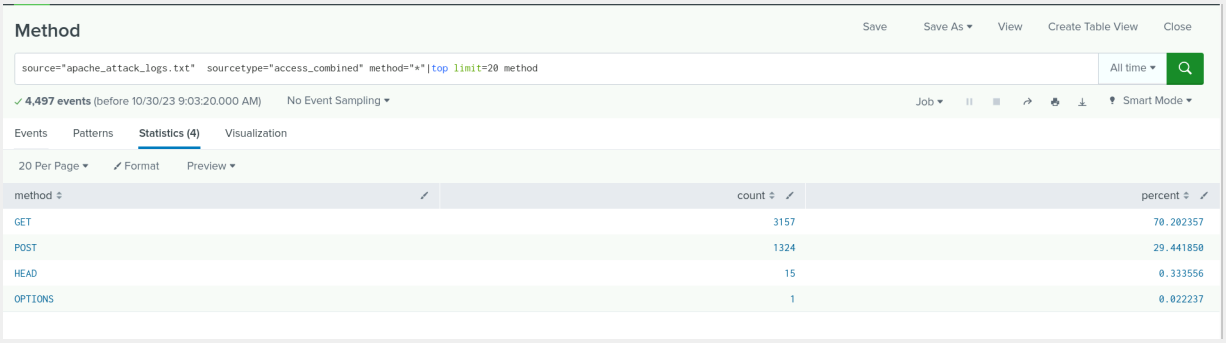
Apache Web Server Log Questions

Report Analysis for Methods

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

Suspicious changes were detected. GET requests decreased while Post requests jumped dramatically. Head requests dropped slightly

After



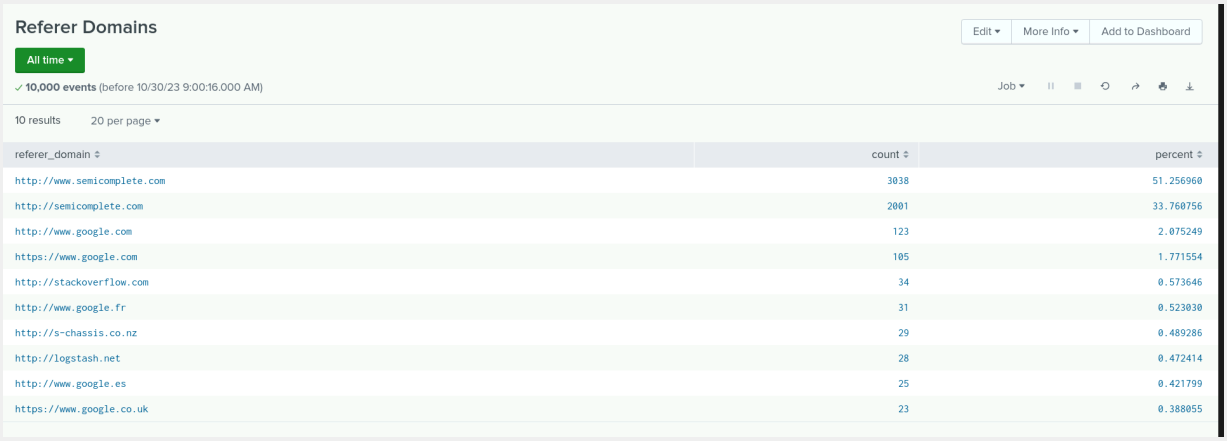
- What is that method used for?

GET request - Used to request data from a specified resource.
POST request - Used to send data to a server to create/update a resource.
HEAD request - Head is almost identical to GET, without the response body.

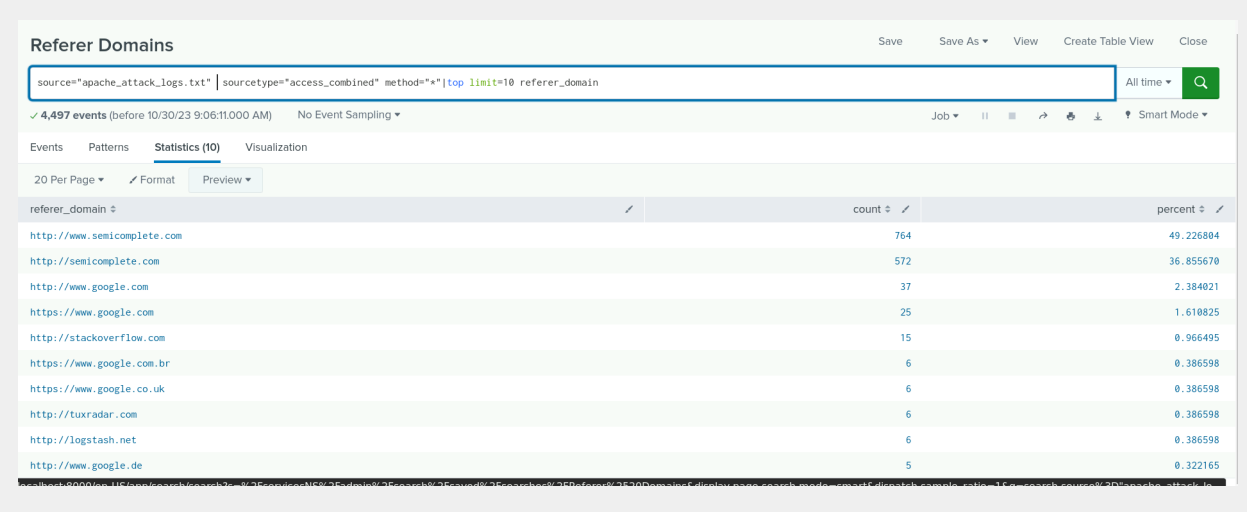
Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Slight suspicious activity detected in the drop in count from Semicomplete.com dropping from 3038 to 764. However due to the different scale/ratio the drop is not as suspicious (10000 events vs 4497 events)
Before:



After

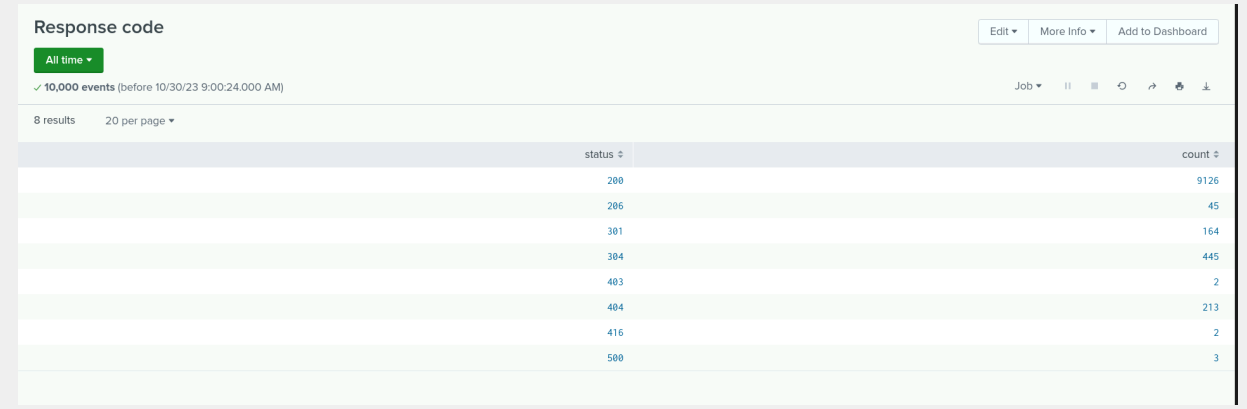


Report Analysis for HTTP Response Codes

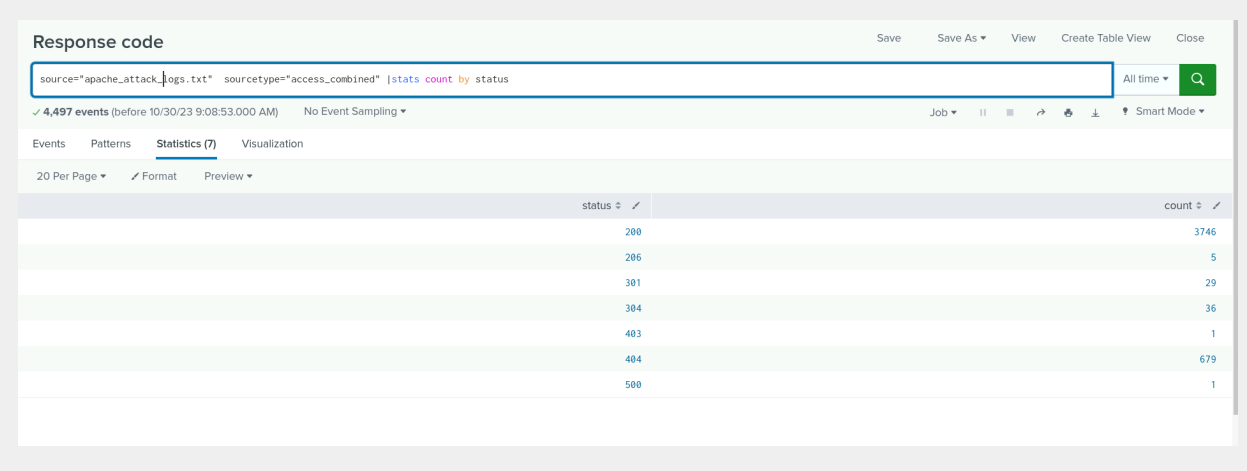
- Did you detect any suspicious changes in HTTP response codes?

We saw some of the numbers dramatically different. For example, status **200** codes went from a count of 9126 down to 3746,. But status **404** codes increased going from 213 up to 679

Before:



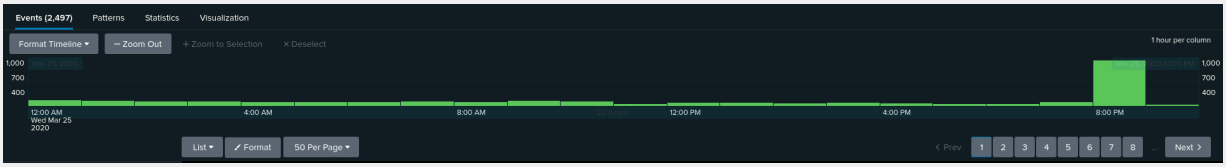
After:



Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes. There was an abnormal count of international activity
```



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

```
Occurred 8pm on 25th March
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No
```

Alert Analysis for HTTP POST Activity

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

```
Yes
```

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

```
Count of 1296 reported
```

- When did it occur?

```
8pm on the 25th March , 2020
```

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

```
No
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, we saw that before the attack, the GET method was the most requested,
hovering between 110-120 per hour.  This was well below our alert threshold
> 150, so no alert triggered.  Then between 5:00pm -7:00pm on Wednesday,
25th of March, 2020, it increased drastically, reaching a high of 729 at
06:00pm.
```

- Which method seems to be used in the attack?

```
Get and Post
```

- At what times did the attack start and stop?

```
GET - Between 5:00pm -7:00pm.
POST - Between 7:00pm -9:00pm.
```

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

```
GET - Peak count was 729.
POST - Peak count was 1,296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
A spike in logins was detected from the Ukraine region
```

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

```
Kiev & Kharkiv
```

- What is the count of that city?

```
Kiev - Count was 440.
Kharkiv - Count was 433.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, we saw that ‘VSI_Account_login.php’ became prominent and was the most
used URI during the attack, making a total of 1,323 counts .  Before the
attack it was registering 101 .
```

- What URI is hit the most?

```
VSI_Account_login.php
```

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

```
Brute Force attack to gain access with stolen account credentials
```

```
Gain Access to the server to cause malicious harm such as backdoor and/or
steal information
```