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, the severity for high went way up into the thousands
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes the number of successes went up while the number of failures went down.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes there was a spike in activity.
```

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

```
There was a total count of 35
```

- When did it occur?

```
at 8:00 am to 9:00 am on Wednesday March 25, 2020
```

- Would your alert be triggered for this activity?

```
Yes it would because my threshold is “anything greater than 15”
```

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

```
No I would not, because the average baseline is normal and less than
threshold.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
No, it was not a suspicious volume however, it was slightly outside of the
average
```

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

```
The total count was 16
```

- Who is the primary user logging in?

```
User_c was primary user logging in during this time
```

- When did it occur?

```
Mar 25 2020, at 8:00 am
```

- Would your alert be triggered for this activity?

```
No it would not because my threshold was set “anything greater than 30”
```

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

```
No I would not
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, there are 2 spikes.
```

- What signatures stand out?

```
High count of attempted account password resets and a high count of user
accounts locked
```

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

```
Attempted account password reset: 8 am to 11 am
User account locked out: 12 am to 3 am
```

- What is the peak count of the different signatures?

```
Attempted account password reset: 1258
User account locked out: 896
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, 2 users seem to stand out as ones logged in the most over a time
```

- Which users stand out?

```
User_a and user_k
```

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

```
User_a: 12 am to 3 am
User_k: 8 am to 11 am
```

- 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 Account locked and account password reset are both high
```

- 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?

```
Yes, 2 users log in way more than the others
```

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

```
Yes, they 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?

```
With the statistical chart you can just view the count or the number of logins only, with the line graph visualization as well as the pie chart, you can clearly see which times the bulk of the logins occurred as well as which users had a greater amount of logins.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, there was a significant spike in POST method
```

- What is that method used for?

```
It is used to send data to a server or create/update a resource
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes, other than the top 5 domains that refer VSI, the rest of the top 10 changes.
```

Report Analysis for HTTP Response Codes

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

```
Yes, there was a spike in status code 404
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, a spike around Europe, specifically Ukraine in the cities of Kiev and
Kharkiv
```

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

```
It occurred for 1 hour at 8:00 pm for a total count of 877
```

- Would your alert be triggered for this activity?

```
Yes, because my threshold is “anything greater than 150”
```

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

```
I would not change the threshold, looking at the average around for the
baseline before the attack, the threshold is still good.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, a spike in activity
```

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

```
It occurred for an hour for a count of 1,296 events
```

- When did it occur?

```
8:00 pm to 9:00 pm on Wednesday March 25 2020
```

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

```
No, because with the threshold set, there is a clear spike in activity
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There is a spike for the POST method
```

- Which method seems to be used in the attack?

```
POST method
```

- At what times did the attack start and stop?

```
The attack started around 7:00 pm and stopped around 9:00 pm
```

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

```
The top count is 1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
There is an abnormal amount of 404 status codes as well as a great amount of
status code 200 from ukraine which wasn't there before the attack
```

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

```
In the United States, Washington DC = abnormal amount of status 404 errors
In Ukraine, Kiev and Kharkiv = great amount of status 200 codes
```

- What is the count of that city?

```
Washington DC = Status code 404: 643
Kiev = status 200: 439
Kharkiv = status 200: 433
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, there is a spike among one of them.
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
Attempting to login to VSI via Brute Force
```