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?

```
Both Informational and High categories increased and decreased by 13% which would tell us that this is something suspicious happening
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
There was no area of suspicious activities due to only having change of 1% for both informational and high categories
```

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
```

- When did it occur?

```
8:AM March 25
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No - our threshold > 10
```

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?

```
94
```

- Who is the primary user logging in?

```
User_A
```

- When did it occur?

```
This occurred at 2am
```

- Would your alert be triggered for this activity?

```
Yes this would have flagged our threshold alert
```

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

```
No there is no need to change the threshold
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
There was no noticeable volume of deleted accounts that would raise
suspicions
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
The Other Section was the most up top on the chart showing us that There was
something in that field raising suspicions
```

- What signatures stand out?

```
A User accounts was locked out and An attempt was made to rest an accounts
password
```

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

```
8am for Password Rest that ended 11am
12am for account being locked out which ended at 3am
```

- What is the peak count of the different signatures?

```
Account being locked out peaked at 856
Password Rest peaked at 1258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
There were two users who stood out that raised our suspicions. One user had a high activity from 12am to 3am on Wed. March 25th and the other user had high activity from 8am to 11am on Wed. March 25th as well.
```

- Which users stand out?

```
User A and User K were the two who stood out the most.
```

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

```
User_a started at 12am and ended at 3am on March 25th
User_K started at 8am and ended at 11am on March 25th
```

- What is the peak count of the different users?

```
User_a had a peak count of 984
User_k had a peak count of 1,256
```

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

- Does anything stand out as suspicious?

```
There were activities that raised concerns between two different instances. The first one was between 12am and 3am while the other event was between 8am to 11am. Both occurred on the date March 25.
```

- 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?

```
Similar suspicious activity was being displayed (12am - 3am and 8am to 11am)
on March 25th
```

- 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?

```
An advantage for statistical chart is that we are able to have it return to
us a list of all the top users which can then give us a better idea overall
who is causing the suspicious activity. While a disadvantage is the results
that is gives us through a large set of data while other methods of going
through the data can give us more specific focus points of where the data is
coming from and where it is going.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes
```

- What is that method used for?

```
POST and GET
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
No
```

Report Analysis for HTTP Response Codes

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

```
Small Change to just 404 code but nothing to have raised suspicious
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes a large spike in activity occurred at 8pm on March 25th
```

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

```
The count came from Ukraine with a 1,369 count during the spike at 8pm on
March 25th
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No changes needed
```

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?

```
Total count of 1269 at 8pm
```

- When did it occur?

```
8:00PM
```

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

```
No changes needed
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes - spike in activity
```

- Which method seems to be used in the attack?

```
GET
```

- At what times did the attack start and stop?

```
5:00PM - 7:00PM
```

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

```
729
```

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.)

```
Kiev, Ukraine + Kharkiv, Ukraine
```

- What is the count of that city?

```
439 + 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes
```

- What URI is hit the most?

```
/VSI_Account_logon.php
files/logstash/logstash-1.3.2-monolithic.jar
```

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

```
Account logon PHP
```