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?

```
No, the total number of high and informational totals increased to 1111 and
4383. Percentages remained unchanged.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
The number of failures decreased from 2.980688% on the
windows_server_logs.csv to 1.563288% when viewing the
windows_server_attack_logs.csv. Still, this value should be investigated.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, there was an increase of failed activity.
```

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

```
There were 35 failed activity events recorded.
```

- When did it occur?

```
This occurred on 8am March 25th 2020
```

- Would your alert be triggered for this activity?

```
Yes, our alert would have been triggered.
```

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

```
Yes, we may increase our threshold a small amount to account for normal
activity.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes, suspicious volume of successful logins were detected.
```

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

```
15 events were recorded at 1am
14 events were recorded at 2am
15 events were recorded at 7am
16 events were recorded at 8am
15 events were recorded at 1pm
```

- Who is the primary user logging in?

```
The primary user logging in was User A.
```

- When did it occur?

```
11 times at 2am on 3/25/2020
```

- Would your alert be triggered for this activity?

```
No, our alert would not have been triggered. Our threshold was 13.
```

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

```
Yes, we agree that we would change our threshold to be closer to 10.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, we detected a suspicious volume of deleted accounts. Our threshold was
set to trigger anything greater than 13 deleted accounts per hour.
14 events at 12am on 3/25/2020
14 events at 4am on 3/25/2020
17 events at 5am on 3/25/2020
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, at 9am on 3/25/2020, 1,258 attempts were made to reset an account's
password. At 2am on 3/25/2020 a user account was locked out 896 times.
```

- What signatures stand out?

```
“User account was locked out” and “An attempt was made to reset an account’s
password.”
```

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

```
“User account was locked out” signature began at 12am and concluded at 3am
“An attempt was made to reset an account’s password” signature began at 8am
and concluded at 11am.
```

- What is the peak count of the different signatures?

```
“An attempt was made to reset an accounts password” peaked at 1,258 times
“User account was locked out” peaked at 896 times
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes. It appears two users had excessive activity during this time period.
```

- Which users stand out?

```
User A and User K
```

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

```
User A started at 1:40am and stopped at 2:50am
User K started at 9:10am and stopped at 11am.
```

- What is the peak count of the different users?

```
The peak count for User A is 785.
The peak count for User K is 397
```

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

- Does anything stand out as suspicious?

```
Yes, again the data shows the “attempts to reset an accounts password” and
“user account lockouts” take up a significant portion of the pie chart.
```

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

```
The numbers in the pie chart show an increase of count of events compared to the number of events in the time chart. This is possibly because we used different SPL queries to retrieve the data.
```

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

- Does anything stand out as suspicious?

```
Yes, User A and User K had the most event counts.
```

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

```
The same users (User A and User K) were both isolated as the users with the highest counts represented in the data. However, the exact values were not consistent between the two charts. This is because in the time chart we are tracking users by time and in the column chart we are tracking users by count.
```

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 advantages of using this report are that it shows the data all in one place and can show a creative visual representation of the data. Areas of concern are easily identifiable and can be shared with people who may not be well versed in reading technical logs.

The disadvantages of this report is that it may be a little too much data in one place and can be confusing to navigate. Also, while some of the data can be easily isolated and represented, the data does not show direct parallels to the same conclusions on different visualizations because of the utilization of the different SPL queries constructed.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, POST requests increased from 106 to 1324.
```

- What is that method used for?

```
POST requests are requests that send data to a specified resource. This
occurs when files are uploaded or when a user fills out information on a
website.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes, all of the referrer domains decreased in count.
```

Report Analysis for HTTP Response Codes

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

```
Yes, All status codes decreased except status code 404. This increased from
213 to 679. This is the error code.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, there is a suspicious volume of international activity.
```

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

```
937 events were recorded at 8pm
```

- Would your alert be triggered for this activity?

```
Yes, our alert would be triggered. Our threshold was set to alert anything
over 250.
```

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

```
No, we agreed we would keep our threshold the same. Regular activity is
normally below our threshold.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, we detected suspicious volumes of HTTP POST activity.
```

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

```
1296 POST requests
```

- When did it occur?

```
20:00 at 3/25/2020
```

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

```
No, our current threshold of 4 would have triggered the alert. We agreed not
to change it.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, particularly with POST methods.
```

- Which method seems to be used in the attack?

```
The POST method appears to be used in the attack,
```

- At what times did the attack start and stop?

```
The attack began at 7pm and concluded at 9pm
```

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

```
The peak count was 1,296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, we saw increased activity over Europe, specifically over the areas of
Ukraine.
```

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

```
Kiev, Ukraine showed the highest number of activities.
```

- What is the count of that city?

```
Kiev had a count of 444.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes. We see a spike in URI counts that were well over 1,000.
```

- What URI is hit the most?

```
/VSI_Account_logon.php had a count of 1,323
```

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

```
The attacker could potentially be scanning for vulnerabilities, conducting a brute force attack or they could have automated a script or bot to make the requests happen.
```