Cybersecurity

Project 3 Review Questions

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

```
There was suspicious activity, the percentage for events with high severity
went from 6.9% to 20.2%
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
No suspicious activity, failed activities percentage actually dropped from
2.98% to 1.56%
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
There was a day and time where we saw a surge of suspicious failed activity
```

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

```
The count was 35
```

- When did it occur?

```
It occurred on March 25th, 2020 at 8 am
```

- Would your alert be triggered for this activity?

```
Yes it would have, we set our threshold at 15 originally
```

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

```
Considering that every other event was still below 20 I think I would keep
the threshold the same.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes there was a time that I noticed suspicious activity
```

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

```
It was 196 events
```

- Who is the primary user logging in?

```
User j
```

- When did it occur?

```
March 25th at 11 am
```

- Would your alert be triggered for this activity?

```
Yes it would’ve, our threshold was set at 40
```

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

```
I don’t think I would change our threshold.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No suspicious activity, alert would have not been triggered.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, we had a couple signatures that stood out from the rest as well as
activity occurring outside normal business hours.
```

- What signatures stand out?

```
“An attempt was made to reset an accounts password” “A user account was
locked out” (“Account was successfully logged on” was another to note but
wasn’t as big as the other two signatures)
```

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

8 am to 11 am for an attempt to reset password and 12 am to 3 am for a user account was locked out (10 am to 1 pm for successful logins)

- What is the peak count of the different signatures?

```
Peak count for attempt of password reset is 1,258 and peak for user account
locked out was 896 (196 for successful logins).
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes we have two users that stand out from the rest in terms of activity.
```

- Which users stand out?

```
User a and user k (user j also noted but not as big as the other two).
```

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

```
12 am to 3 am for user a and 8 am for 11 am user k (10 am to 1 pm for user
j).
```

- What is the peak count of the different users?

```
984 is peak for user a, 1,256 for user k (196 for user j).
```

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

- Does anything stand out as suspicious?

```
The same signatures that we noted in the timechart were also visibly
suspicious with the graphs and charts
```

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

```
Yes they do
```

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

- Does anything stand out as suspicious?

```
The same users that we noted in the timechart were also suspicious in the
chart.
```

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

```
Yes they do
```

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 charts you really get to see the breakdown of all the numbers while with bar charts or line charts or other visuals it does a good job at pointing out the peaks and you get to visually see what looks like suspicious activity.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes we noticed that POST had suspicious changes, it went from 106 to 1324
```

- What is that method used for?

```
POST is used to send data to the server.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes and no, it seems like for all top 10 domains the count decreased for all of them with the most significant being http://www.semicomplete.com which initially had a count of 3038 then dropped to 764, although, when we look at the percentages they weren't a drastic difference like for example the top domain even though dropped a lot in count it only went from 51.25% to 49.22%. So its something to note but not a big deal.
```

Report Analysis for HTTP Response Codes

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

```
Yes we did notice that the count for HTTP response codes dropped
significantly.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes they was suspicious activity
```

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

```
937
```

- Would your alert be triggered for this activity?

```
Our alert would have been triggered
```

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

```
No I think it was an appropriate threshold to have to trigger the alert that
we got.
```

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?

```
1,296
```

- When did it occur?

```
March 25, 2020 at 8pm
```

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

```
I would not have changed the threshold
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes we noticed a spike
```

- Which method seems to be used in the attack?

```
Primarily it is the POST method
```

- At what times did the attack start and stop?

```
From 7pm-9pm for POST
```

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

```
1,296 for POST
```

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
```

- What is the count of that city?

```
439
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes
```

- What URI is hit the most?

```
Account logon with 1,322 counts
```

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

```
A potential brute force attack or sql injection
```