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, we did not see any changes regarding the severity when we ran the attack logs.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes, we do have more failed activities in the attack logs.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, we did detect a suspicious volume of failed activity.
```

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

```
The count was 35 around 8 am.
```

- When did it occur?

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

- Would your alert be triggered for this activity?

```
Yes, because we had our threshold at 15.
```

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

```
No, based off the information from the attack log we should not change our threshold.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes, we did detect a suspicious volume of successful logins.
```

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

```
We had two different hours with a suspicious volume of successful logins. One was 196 and the other was 77.
```

- Who is the primary user logging in?

```
User J was the primary user.
```

- When did it occur?

```
The count for 196 occurred at 11 am on March 25, 2020, and the count of 77 occurred at noon on the same day.
```

- Would your alert be triggered for this activity?

```
Yes, we had our threshold at 50.
```

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

```
No, with the current threshold that was chosen, we could catch the
suspicious activity.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No, there was no suspicious activity in the alert of deleted accounts.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, the times of 1 am and 2 am were the most suspicious from the log.
```

- What signatures stand out?

```
The signature that stands out is User Account is Locked out, and an attempt
was made to reset an account password.
```

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

```
The signature for a user account is locked out starting around midnight and
it ended around 3 am. An attempt was made to reset an account password that
started 8 am and ended around 11 am.
```

- What is the peak count of the different signatures?

```
A user account is locked out, had a peak count of 896, and an attempt was
made to reset the account password peak count of 1,258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, we had two user A and K had a lot of activity when we ran the attack logs.
```

- Which users stand out?

```
Both users A and K stand out, but user K had a higher count, which is very suspicious.
```

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

```
User A started around midnight and went on till about 3 am. User K started at 8 am and went on till 11 am.
```

- What is the peak count of the different users?

```
User A's peak count was 984, and User K's peak count was 1256.
```

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

- Does anything stand out as suspicious?

```
Yes, both the signature and user pie charts have the highest count in the bar and pie charts on the dashboard.
```

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

```
Yes, both signatures, as stated earlier, have the highest count in the pie chart.
```

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

- Does anything stand out as suspicious?

```
[Enter answer here]
```

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

```
Yes, user K and A have the highest count by far.
```

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 if the count jumps out high, then it is very easy to tell. The disadvantages of Charts can sometimes hide critical details, especially when they aggregate or summarize data, which may lead to missing important context or data.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, we did see a suspicious change in the HTTP methods. We saw a change in POST
```

- What is that method used for?

```
The HTTP method POST is used for sending data.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
No, we did not see any suspicious change in the referee domains.
```

Report Analysis for HTTP Response Codes

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

```
We did see some small changes overall between the regular and attack logs.
The major change we saw was response code 404 from 2% to 15%.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, we did see a volume spike from Ukraine in two cities.
```

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

```
The count was 937. That was around 8 pm on March 25, 2020
```

- Would your alert be triggered for this activity?

```
Yes, because we had our threshold at 170.
```

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

```
No, we would have been alerted by the suspicious activity.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, we detected suspicious activity March 25, 2020
```

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

```
The count was 1296 around 8 pm.
```

- When did it occur?

```
It occurred 8 pm March 25, 2020
```

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

```
No, we had our threshold at 12 which means we would have been alerted about
the suspicious activity.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, we got an increase in the POST methods from 7am to 9am.
```

- Which method seems to be used in the attack?

```
The method used in the attack is POST. POST methods primarily use is for
sending data.
```

- At what times did the attack start and stop?

```
The attack started at 7 am and ended around 9 am.
```

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

```
The peak count for the POST method was 1296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, we ran the attack logs we did see a spike in the activity coming from
Ukraine.
```

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

```
The high volume of activity came from two cities in Ukraine. The one with
the highest activity was Kiev and the second highest came from Karkhiv.
```

- What is the count of that city?

```
Kiev,Ukraine had a count of 440.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, we had very high count of suspicious activity of one URI.
```

- What URI is hit the most?

```
The URI hit the most was /VSI_Account_logon.php. That had a count of 1,323
```

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

```
Based on all my findings, I believe the attacker may be attempting to brute
force user accounts. This is supported by the high volume of activity linked
to the signatures "User Account is Locked Out" and "An Attempt Was Made to
Reset an Account Password", particularly involving Users A and K.
Additionally, the unusual spike in activity from Ukraine suggests that the
attacker could be operating from that region. To protect VSI, it is
recommended to implement multi-factor authentication, enable account lockout
thresholds, and block or closely monitor access attempts from Ukraine.
```