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?

```
[The severity of information went from 93% to 80%, which is a 13%
decrease.The severity level of high went from 7% to 20%, which is a 13%
increase.The results suggest suspicious changes in severity.]
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
[The success activities went from 97% to 98%, which is a 1% increase.
The failure activities went from 3% to 2%, which is a 1% decrease.These
results suggest no suspicious changes in failed activities.]
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
[At around 8:00 a.m. on Wednesday, March 24th, there appeared to be a
suspicious volume of failed activity.]
```

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

```
[The count of events in the hour it occurred was 35.]
```

- When did it occur?

```
[It occurred at 8:00 a.m. on Wednesday, March 25th]
```

- Would your alert be triggered for this activity?

```
[Yes, my alert would be triggered within the threshold.]
```

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

```
[No, I would not change the threshold. The current threshold successfully
alerted to a high level of failed activity, which was suspicious and
warranted attention. This indicates that the threshold is set at an
appropriate level to detect unusual activity.]
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
[There was a suspicious volume of successful logins at 11:00a.m. and
12:00p.m. on Wednesday, March 25th]
```

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

```
[196 events occurred at 11:00a.m., and 77 events occurred at 12:00p.m]
```

- Who is the primary user logging in?

```
[The primary user logging in is " user_j".]
```

- When did it occur?

[It occurred at 11:00a.m. and 12:00p.m. on Wednesday, March 25th.]

- Would your alert be triggered for this activity?

[yes, my alert would not be triggered for this.]

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

[No, based on the data provided, there doesn't appear to be a need to change the threshold. The maximum count of successful logins by the primary user in an hour is below the current threshold, suggesting that the current threshold is appropriate.]

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

[No, there doesn't appear to be a suspicious volume of deleted accounts. The counts of deleted accounts in the attack logs are within the same range as those in the regular logs. In fact, there seems to be a decrease in the number of deleted accounts during certain hours in the attack logs compared to the regular logs.]

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

[Yes, there are two signatures that stand out as suspicious: "attempt to reset account password" and "user account locked out". The counts for these signatures are significantly higher than in the previous log.A suspicious activity happened from 12:00 a.m. to 3:00 a.m. on Wednesday, March 25th with the signature “An account was locked out”. Another suspicious activity was detected later that day from 8:00 a.m. to 11:00 a.m. with the signature “An attempt was made to reset an accounts password”.]

- What signatures stand out?

[The signature “A user account was locked out” and “An attempt was made to reset an accounts password” signature]

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

[It started from “A user account was locked out” started at 12:00 a.m. and ended at 3:00 a.m.on Wednesday, March 25th.
“An attempt was made to reset an accounts password” started at 8:00 a.m. and ended at 11:00 a.m. on Wednesday, March 25th.]

- What is the peak count of the different signatures?

[“A user account was locked out” has a peak count of 896.
“An attempt was made to reset an accounts password” has a peak count of 1258.]

Dashboard Analysis for Users

- Does anything stand out as suspicious?

[Yes,There was suspicious activity at 12:00 a.m., 3:00 a.m., 9:00 a.m., and 10:00 a.m. on Wednesday, March 25th.]

- Which users stand out?

[The users that stand out are user_a and user_k.]

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

[For user_a, it started at 12:00 a.m. and stopped at 3:00 a.m. on Wednesday, March 25.For user_k, it started at 8:00 a.m. and stopped at 11:00 a.m. on Wednesday, March 25th.]

- What is the peak count of the different users?

```
[The peak count was 984 for user_a and 1256 for user_k.]
```

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

- Does anything stand out as suspicious?

```
[Yes,  on Wednesday, March 25th, there was a suspicious activity detected
from 12:00 a.m to 3:00 a.m., and another one from 8:00 a.m. to 11:00 a.m.]
```

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

```
[yes, the data results match my findings in my time chart for signatures.]
```

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

- Does anything stand out as suspicious?

```
[Yes, two users, user_a and user_k, stand out as suspicious due to their
high counts and large proportions in the pie chart.Yes, on Wednesday, March
25th, there was a suspicious activity detected from 12:00 a.m. to 3:00 a.m.,
and another one detected from 9:00 a.m. to 10:00 a.m.]
```

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

```
[Yes, the results match my findings in my time charts for users.]
```

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?

```
[Advantages:
- Comprehensive View: The statistical charts provide a comprehensive
view of user activities, allowing for a deeper understanding of the
data.
- Identification of Outliers: They can help identify outliers or unusual
activity, as these will stand out from the typical statistical
```

```
patterns.
- Comparison: They allow for a more detailed comparison of user
behavior, as they can show distributions, averages, and other
statistical measures that are not apparent in other types of charts.
Disadvantages:
- Interpretation Difficulty: Statistical charts can be more difficult to
interpret for those who are not familiar with statistical measures and
concepts.
- Lack of Temporal Context: Unlike line graphs, statistical charts do
not provide a temporal context, making it harder to understand how
user behavior changes over time.
- Less Intuitive: They may not be as visually intuitive as pie charts or
bar graphs, which provide a straightforward visual comparison of
different categories of data.]
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
[Yes, there is a suspicious change in the HTTP methods..Yes, the GET
activity was decreased by about 29%. The POST activity was also increased by
29%.]
```

- What is that method used for?

```
[GET is a request method supported by HTTP used to request data from a
specified resource. It retrieves information from the server and should have
no other effect.
POST is a request method supported by HTTP used to send data to a server to
create/update a resource. The data is included in the body of the request.
This may result in the creation of a new resource or the updates of existing
resources or both.]
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
[No, there were no suspicious changes detected in referred domains.]
```

Report Analysis for HTTP Response Codes

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

```
[Yes,there was one significant change that was suspicious, and it was the
404 response code increasing from 2% to 15%.]
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
[Yes, there is a suspicious volume of international activity from Ukraine at
8:00 p.m. was detected on March 25th.]
```

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

```
[The Ukraine had a count of 1369 events during the attack on 8:00 p.m]
```

- Would your alert be triggered for this activity?

```
[Yes, my alert would be triggered by this activity.]
is higher than my threshold of 140.]
```

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

```
[Yes, considering the significant increase in the count of events on
2020-03-25, it might be beneficial to lower the threshold to detect such
spikes in international activity earlier. However, it's also important to
consider the risk of false positives. The new threshold should be determined
based on the normal range of international activity and the risk tolerance
of the organization.]
```

Alert Analysis for HTTP POST Activity

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

```
[Yes, there is a suspicious volume of HTTP POST activity. The count of HTTP POST requests on 2020-03-25 is significantly higher than any other hour.]
```

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

```
[The count of events on 2020-03-25 was 1296, which is significantly higher than any other hour.]
```

- When did it occur?

```
[It occurred at 8:00 p.m. on Wednesday, March 25th.]
```

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

```
[Yes, I would consider raising the threshold. The current threshold of 10 was exceeded by a large margin during the suspicious activity. However, the new threshold should still be set at a level that would detect smaller, but still potentially significant, spikes in HTTP POST activity.]
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
[Yes, there is a significant increase in the use of the HTTP POST method during the attack.There was suspicious activity with the GET method from 5:00 p.m. to 7:00 p.m. on Wednesday, March 25th. Later that day, there was another suspicious activity from 7:00 p.m. to 8:00 p.m]
```

- Which method seems to be used in the attack?

```
[The HTTP POST method seems to be used in the attack.]
```

- At what times did the attack start and stop?

```
[]The GET attack started at 5:00 p.m and ended at 7:00 p.m. on Wednesday, March 25.The POST attack started at 7:00 p.m. and ended at 8:00 p.m. on the same day.]
```

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

```
[The peak count of GET was 1296.The peak count of POST was 729.]
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
[There was suspicious activity from Kiev, Ukraine.]
```

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

```
[There was a high volume of activity from the cities of Kiev and Kharkiv.]
```

- What is the count of that city?

```
[From Kiev there was a count of 872, and from Kharkiv there was a count of 432.]
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
[Yes, the URI "VSI_Account_logon.php" stands out as it has the highest count in the pie chart.]
```

- What URI is hit the most?

```
[The URI that is hit the most is "VSI_Account_logon.php".]
```

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

```
[The "VSI_Account_logon.php" URI suggests that the attacker is attempting to
log in to an account. This could indicate a brute force attack where the
attacker is trying to guess the password of an account. The high number of
POST requests supports this, as POST is typically used to send data (like a
password) to a server.]
```