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?

```
[We Detected some accounts were deleted, created and some people got access granted to accounts. Some accounts were given special privileges and some accounts were successfully logged onto. Also, we detected account management password policy was changed]
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
[System security access was granted to an account, A user account was deleted and the audit logs were cleared, Special privileges assigned to new login, a user account was created, a computer account was deleted and an account was successfully logged onto.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
[On March 25th, 2020, 8AM we detected suspicious failure login attempts, the count was 35 attempts for the hour. Yes our alert would be triggered and we
```

```
would keep our threshold the same.We also see multiple attempts to reset
account password]
```

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

```
[35]
```

- When did it occur?

```
[March 25th 2020 8AM]
```

- Would your alert be triggered for this activity?

```
[Yes]
```

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

```
[No]
```

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?

```
[196 ]
```

- Who is the primary user logging in?

```
[user f]
```

- When did it occur?

```
[ March 25th 2020 11 AM]
```

- Would your alert be triggered for this activity?

```
[yes]
```

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

```
[No i would keep it the same]
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
[no]
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
[some accounts are deleted but nothing over or close to the threshold ]
```

- What signatures stand out?

```
[4726]
```

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

```
[12 AM to 2PM]
```

- What is the peak count of the different signatures?

```
[17]
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
[Yes]
```

- Which users stand out?

```
[Users A,K, and J ]
```

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

```
[User A - started after 12 AM and stopped by 3 AM on March 25th.
User K - started after 8 AM and stopped by 11 AM on March 25th.
User J - started after 10 AM and stopped by 1 PM on March 25th.
```

- What is the peak count of the different users?

```
[User A - 984
User K - 1,256
User J - 196]
```

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

- Does anything stand out as suspicious?

```
[yes, an attempt was made to reset account password and a user account was
locked out is very high between the ranges of 1,800 to 2,100]
```

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

```
[yes some of the results do ]
```

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

- Does anything stand out as suspicious?

```
Yes user K and user a, counts are high]
```

- 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?

```
[it gives you the specific stats, counts and percentages. Then it also
details out what's issue is happening on the left side. Also it just looks
different as in format and imagery compared to the charts]
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
[Yes we detected a change in the GET and POST. The POST method had an
increase of almost 30%. The GET method increased past our baseline on
Wednesday March 25th.]
```

- What is that method used for?

```
[GET- request information from a particular source. POST - carries updated
message request parameter in the body to a web server]
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
[The top domain activity came from semicomplete.com, but didnt show signs of it being suspicious.]
```

Report Analysis for HTTP Response Codes

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

```
[The response codes were initially 200 but noticed the 404 codes saw amax increase of 15%]
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
[High volume of POST method at 8 p.m on wednesday march 25th, with 939 events.]
```

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

```
[2 hours with 83 events in the 7pm hour and 939 in the 8pm hour.
```

- Would your alert be triggered for this activity?

```
[Yes]
```

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

```
[Yes, I would lower the threshold]
```

Alert Analysis for HTTP POST Activity

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

```
[Yes there was an increase of POST at 8PM wednesday march 25th with 1296 events. ]
```

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

```
[1 hour]
```

- When did it occur?

```
[The 8PM hour of Wednesday march 25th ]
```

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

```
[I would lower my threshold range.]
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
[Yes, there was an increase in POST and GET methods.]
```

- Which method seems to be used in the attack?

```
[The POST method and the GET method]
```

- At what times did the attack start and stop?

```
[POST - 7PM - 9PM
GET - 5PM - 7PM]
```

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

```
[The peak count for POST - 1296 and the peak count for GET - 729]
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Suspicious activity from Ukraine
```

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

```
Kharkiv, Ukraine
Kyiv, Ukraine
```

- What is the count of that city?

```
Kharkiv - 433
Kyiv - 439
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
[Yes, we found suspicious activity from /VSI_Account_logon.php.]
```

- What URI is hit the most?

```
[VSI logon page]
```

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

```
[This shows signs of a brute force attack on the VSI logon page.]
```