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?

```
Yes, high severity events increased from 329 to 1111 while informational
events were relatively the same.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes, we set our threshold for failed password resets at 4.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes we set our threshold for failed passwords reset at 4. We saw a count of
35 in one hour.
```

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

```
35.
```

- When did it occur?

```
3 am Wednesday March 25, 2020.
```

- Would your alert be triggered for this activity?

```
Yes, the alert would be triggered and we would alert on 4 failed password
resets.
```

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

```
No, I would not change the threshold, but we might consider loosening a
little to not have too many alerts.
```

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?

```
7:00pm March 24, 2020 - 8:00am March 25,2020
```

- Who is the primary user logging in?

```
User_b with 10 and user_n with 9.
```

- When did it occur?

```
1AM March 24 to 5 pm March 24, 2020.
```

- Would your alert be triggered for this activity?

```
No it would not by a single user.
```

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

```
No, because it would trigger too many alerts.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, we saw multiple events.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
There were a large number of deleted accounts during the same time frame of
the other events.
```

- What signatures stand out?

```
Special privileges assigned to new logon, A computer account was deleted,
system security access was removed from an account, A user account was
deleted.
```

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

```
Special privileges assigned to new logon 7pm Mar23 to 7pm Mar 24, alert @11
A computer account was deleted 7pm Mar 23 to 6 pm Mar 24, alert @ 10
System security access was removed from an account 7pm Mar 23 to 6 pm Mar
24, alert @ 10
A user account was deleted 7pm Mar 23 to 6 pm Mar 24, alert @ 11
```

- What is the peak count of the different signatures?

```
Special privileges assigned to new logon 23
A computer account was deleted 17
System security access was removed from an account 18
A user account was deleted 22
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, there was a significant amount of logins from three users.
```

- Which users stand out?

```
User_k, user_a and user_j
```

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

```
user_k :03/25/2020 04:00am - 06:00am
user_a :03/24/2020 8:00pm - 10:00pm
User_j :03/25/2020 06:00am - 08:00am
```

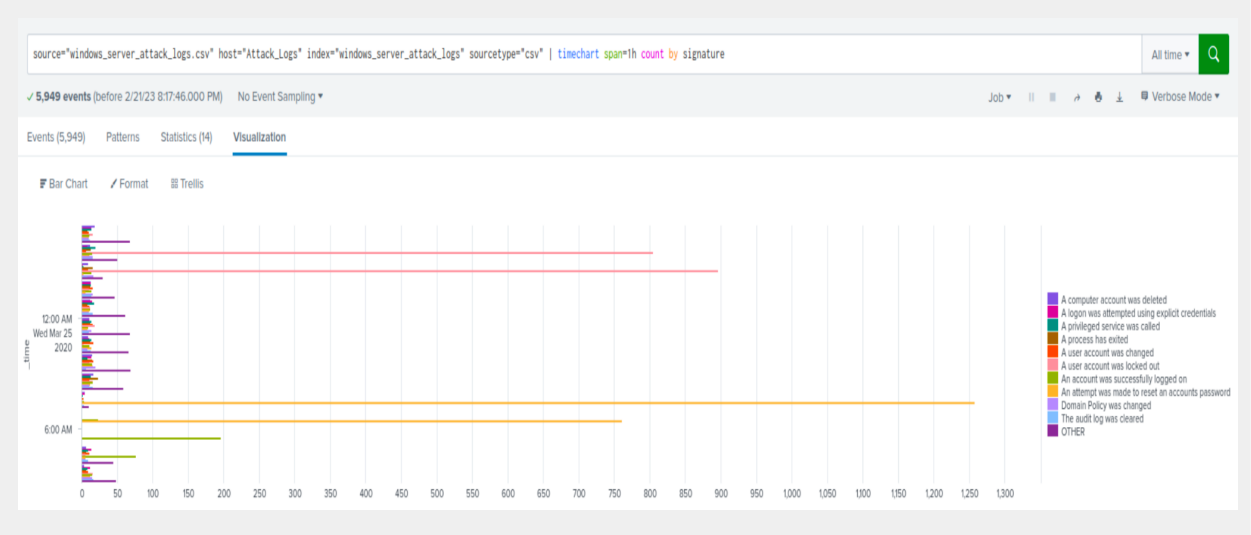
- What is the peak count of the different users?

```
User_k :1256
User_a :984
User_j :196
```

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

- Does anything stand out as suspicious?

```
Yes, a high amount of “A user account was locked out” and “An attempt was
made to reset an accounts password”.
```



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

```
Yes
```

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

- Does anything stand out as suspicious?

```
Yes, there's an increase in user_a, user_k and user_j.
```

- 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?

```
While using the statistical charts an advantage was using the time charts.
These charts helped quickly find data for the events or for the user per
hour. A disadvantage was using the bar graphs. These would slow down the
process immensely because it isn’t obvious to see change in activity. The
different graphs show ups
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes there were suspicious changes, especially POST.
```

- 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?

```
I definitely noticed changes. The count of the last 5 domains dropped
drastically.
```

Report Analysis for HTTP Response Codes

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

```
We detected suspicious changes with response code 200 and 404.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

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

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

```
At 8:00 PM, the count was 939.
```

- Would your alert be triggered for this activity?

```
Our alert was set to more than 140, so it would have been triggered.
```

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

```
I would not change the threshold.
```

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?

```
At 8:00 PM on March 25th, 2020, the count was 1296.
```

- When did it occur?

```
8:00 PM on March 25th, 2020.
```

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

```
No I would not. We set the threshold to 15 which should be perfect.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There is a variation in the HTTP method time charts which is suspicious.
```

- Which method seems to be used in the attack?

```
POST.
```

- At what times did the attack start and stop?

```
Between 7:00 PM and 9:00 PM.
```

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

```
1296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, one city has a high volume of activity.
```

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

```
Kiev has a high volume.
```

- 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?

```
VSI_Account_logon.php is hit the most.
```

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

```
The attacker is likely conducting a brute force attack.
```