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?

```
Informational severity made up 93%, and High severity was 7%. When reviewing the attack logs, Informational severity jumped to 14000, and High dropped by 6000.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
With the status labeled as a fascinating field, failure was 2.9%. When reviewing the attack logs, failures dropped to 1.5% at 186, from 710 successes, dropped from 23820 to 11898. This could be a dangerous mix when we have higher-severity traffic and more successful logins.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, it dropped from 23,820 to 11,898 on the attack log, and when you use
status=failure, you see the attack logs dropped and the primary user changed
from user_l in logs to user_b in attack logs.
```

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

```
11,898
```

- When did it occur?

```
March 25, 2020, at 2 pm had the highest activity.
```

- Would your alert be triggered for this activity?

```
We set our baseline to 8 for this alert.
```

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

```
No its accurate
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
We don't know how many employees the company has, which is essential, but
the log-ins went from 1615 to 864 in the attack logs.
```

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

```
392 in the attack logs
```

- Who is the primary user logging in?

```
User_J
```

- When did it occur?

```
March 25, 2020 at 2 pm
```

- Would your alert be triggered for this activity?

```
Yes, my alert will be triggered for this activity because it is accurate.
```

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

```
No, we wouldn't change our threshold.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
The volume dropped from 1590 to 260 when compared to the attack log.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, there was a sharp increase and decrease in three signature events.
```

- What signatures stand out?

```
A user account was locked out
An attempt was made to reset an account's password
An account was successfully logged in.
```

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

```
A user account was locked out: Wednesday, March 25, between 12:00 AM and
3:00 AM.
```

```
An attempt was made to reset an account’s password: Wednesday, March 25, between 8:00 AM and 11:00 AM.
An account was successfully logged on: Wednesday, March 25, between 10:00 AM and 1:00 PM.
```

- What is the peak count of the different signatures?

```
A user account was locked out: 896
An attempt was made to reset an account's password: 1,258
An account was successfully logged on: 196
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, there was a sudden increase in activity levels for three users.
```

- Which users stand out?

```
User “a”
User “k”
User “j”
```

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

```
User “a”: From 1:40 AM to 2:40 AM
User “k” from 9:10 AM to 11:00 AM
User “j” from 10:50 AM to 12:30 PM
```

- What is the peak count of the different users?

```
User “a” : 785
User “k” : 397
User “j” : 35
```

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

- Does anything stand out as suspicious?

```
Yes. After analyzing the column chart, there was a sporadic increase in the
count of events for three signatures compared to usual. The following
changes in signature count were suspicious:
   1.  An attempt was made to reset an account's password that increased
      from 295 to 2,128
   2. A user account was locked out, rising from 309 to 1,811
   3. An account was successfully logged on that increased from 323 to 432
```

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

```
Yes. Findings from the column chart show a sudden increase in the number of
signatures for the identical three signatures identified in the time chart
for signatures. These are ‘A user account was locked out’, ‘An attempt was
made to reset the account's password’, and ‘An account was successfully
logged on’.
```

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

- Does anything stand out as suspicious?

```
The pie chart analysis of the number of users shows a massive increase in
the activity count for three users. User_k has the highest increase from 260
to 2,118, followed by user_a, which increased from 282 to 1878, and finally
user_j has a slight increase from 256 to 398
```

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

```
Yes. The results from the time chart for users revealed that user_a and
user_j experienced a sudden increase in activity over a period, which is
confirmed by the findings from the count of users that shows a massive rise
in count for the same user_k, user_a, and user_j.
```

Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels you created?

```
Advantages:
   1. Ability to sort from highest to lowest.
   2. The report shows any abnormality in user events.
   3. The percentage of each user activity is displayed and well-arranged.
   4. The simplicity of the statistical table makes it easier to understand
      the data.
      Disadvantages:
         1. Not efficient when analyzing users' activity over a period of
            time.
         2. Data is too bulky, which makes it difficult to handle large data
            sets.
         3. Does not show trends and will not be suitable for trend
            analysis.
         4. Visually not appealing.
         5. Difficulty comparing two or more data sets.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
There were some drastic changes to the HTTP POST and HTTP HEAD. Both methods
Experienced a sharp increase.
```

- What is that method used for?

```
Http Post and Head
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
We noticed a significant drop in referrer domain levels within a few hours
of the day. The typical traffic for the referrer domain is around 75, and we
had hours in the 45-55 range.
```

Report Analysis for HTTP Response Codes

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

```
The number of 404 codes was suspicious. There was a total of 679 for the
status
404. A possible DDoS attack is occurring.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, we had a spike in traffic from Ukraine.
```

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

```
864 events, from 3:30 pm to 4:30 PM
```

- Would your alert be triggered for this activity?

```
Yes, my alert would have been set to 55 events. The normal baseline for
international activity is 45 events.
```

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

```
No, my threshold would have been triggered with this level of activity.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, we experienced a spike in activity on one particular day.
```

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

```
The count was 1296 between 4 pm and 5 pm.
```

- When did it occur?

```
March 25th, 2020
```

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

```
No, I would not change my threshold because my alert would have been
triggered at five events.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, the flood of HTTP POSTs suggests brute force attempts.
```

- Which method is used in the attack?

```
HTTP Post
```

- At what times did the attack start and stop?

```
March 25, 2020, from 2 pm to 5 pm on the same day.
```

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

```
1296 Post Methods
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, we have experienced a spike in activity from Ukraine.
```

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

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

- What is the count of that city?

```
438 for Kyiv, Ukraine, and 433 for Kharkiv, Ukraine
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, we have a ton of traffic going to the VSI company homepage and login
screen.
```

- What URI is hit the most?

```
VSI_Account_logon.php
```

- What could the attacker be doing based on the URI being accessed?

```
The attacker is trying to brute force his way into the account logon page.
```