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- 337% increase (329 to 1111 “high” severity events)

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes- 38 events occurred at 03.25.2020 08:00:00

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes

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

38 events

- When did it occur?

```
Occurred at 03.25.2020 08:00:00
```

- Would your alert be triggered for this activity?

```
Yes- our threshold was 15
```

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

```
We would not change the threshold, as the volume increase was detected
```

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 (11:00:00)
77  (12:00:00)
```

- Who is the primary user logging in?

```
ACME-002 user_n
```

- When did it occur?

```
Occurred on 03.25.2020 from 11:00:00 to 12:00:00
```

- Would your alert be triggered for this activity?

```
Yes- our threshold was 25
```

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

We would not change the threshold, as the volume increase was detected

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?

Yes

- What signatures stand out?

1. “An attempt was made to reset an account’s password”
2. “A user account was locked out”
3. “An account was successfully logged on”

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

1. 03.25.2020 08:00:00-11:00:00
2. 03.25.2020 00:00:00-03:00:00
3. 03.25.2020 10:00:00-13:00:00

- What is the peak count of the different signatures?

1. 1,258
2. 896
3. 196

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes- several user logon volumes were unusual
```

- Which users stand out?

```
   1. user_a
   2. user_k
   3. user_j
```

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

```
   1. 03.25.2020 00:00:00-03:00:00
   2. 03.25.2020 08:00:00-11:00:00
   3. 03.25.2020 10:00:00-13:00:00
```

- What is the peak count of the different users?

```
   1. 984
   2. 1,256
   3. 196
```

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

- Does anything stand out as suspicious?

```
Yes- several sections changed
```

- 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- 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?

A visualization simplifies quick review of data while a chart allows easier access to specifics but minimizes the scale of changes.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes- GET, POST (POST had the most significant changes, but GET had substantial changes, too)

- What is that method used for?

1. GET- retrieve content from web server
2. POST- sends content to web server from local host

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No

Report Analysis for HTTP Response Codes

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

```
Yes- 318% increase in 404 response codes
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes
```

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

```
Ukraine 03.25.2020 19:00:00-21:00:00
```

- Would your alert be triggered for this activity?

```
Yes- our threshold was 150
```

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

```
We would not change the threshold, as the volume increase was detected
```

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?

```
03.25.2020 19:00:00-21:00:00 (2)
```

- When did it occur?

Occurred at 03.25.2020 21:00:00

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

We would not change the threshold, as the volume increase was detected

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes- POST methods increased

- Which method seems to be used in the attack?

POST

- At what times did the attack start and stop?

Occurred on 03.25.2020 from 20:00:00-21:00:00

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

1,296

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Yes

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

Kharkiv, Ukraine

- What is the count of that city?

```
432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes
```

- What URI is hit the most?

```
/VSI_Account_Login.php
```

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

```
Brute force logging in users
```