Cybersecurity

Project 3 Response Questions from SOC Review

SOC: Backdoor Bouncers

Joseph Efezokhae

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 (Suspicious changes shifted from `6% to 20%`).

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes; Failure rate trended down 1.5% to half its original of about 3%
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, we observed a spike in volume at or around 8:00 AM MST.
```

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

```
35 events were collected during this time event sample.
```

- When did it occur?

```
We observed a spike in volume at or around 8:00 AM MST.
```

- Would your alert be triggered for this activity?

```
Our event capture triggered a total of 6 emails to the SOC.
```

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

```
Yes, based on the discussions on the data, the initial estimate was low (6) and should have been set higher (to possibly 9 or 10) to mitigate some of the extra data coming through (this allows for more human personnel to be spent in tasks more crucial to the system).
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Negative. The data says that no successful logins above the anticipated threshold of 16 were breached at 8:00 AM MST.
```

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

```
16 was the number of triggered items.
```

- Who is the primary user logging in?

```
Upon analysis of the users with successful logins it was determined that user: user_c   was the primary user logging in.
```

- When did it occur?

```
1:00 AM MST, 5:00 AM MST and 8:00 AM MST 3 event login events were recorded at each time interval under user: user_c.
```

- Would your alert be triggered for this activity?

In the run of odds, Our SOC was able to set a threshold that fortunately did alert the SOC of this set of abnormalities noted in the data.It could have easy enough been 17 that Our SOC went with denying our team an honest opportunity to slow it down and confirm access in the system manually.It is a reminder that to set thresholds within ideal target range and adapt frequently with data changes. This is a big item for a weekly (or in some cases, a monthly) meeting to access levels and adjust accordingly.

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

This is definitely before the team at the next SOC meeting. The event trigger time at 8:00 AM MST was a true benefit for Our SOC, but it is a rising concern that needs to be addressed. We plan to talk about Network Segmentation and Biometric sign ins to quickly mitigate the challenges of the pending attack as we transition into a VPN with WAF to better mitigate traffic and deter unwanted access to VPI Enterprise's systems and servers.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes, at 5:00 AM MST. User: **user_c** was also recorded with a logged trigger event as well.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, at 5:00 AM MST. User: **user_c** was also recorded with a logged trigger event as well.

- What signatures stand out?

User: **user_c** was also recorded with a logged trigger event at 5:00 AM MST.

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

```
5:00 AM MST was noted for a deleted account. 1:00 AM MST, 5:00 AM MST and
8:00 AM MST was noted for a noted high number of successful logins.
```

- What is the peak count of the different signatures?

```
3 logins was noted as the highest number of logins per any recorded hour.
This was also awarded to user: user_c.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Our SOC observed users: user_a, user_j and user_k with spikes in volume.
```

- Which users stand out?

```
Our SOC observed users: user_a, user_j and user_k with spikes in volume.
```

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

```
Our SOC observed users: user_a (1:00 AM MST -3:00 AM MST), user_j (11:00 AM
MST - 1:00 PM MST) and user_k (9:00 AM MST - 11:00 AM MST) with spikes in
volume noted at those time intervals.
```

- What is the peak count of the different users?

```
The peak count of total users is established at: 29.
```

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

- Does anything stand out as suspicious?

Bar Graph: Large amount of password reset attempts observed (**2,128** in total over all time) and **1,811** user accounts reflected as: **Locked Out** in total (over all time).

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

In direct correlation the values seem to vary as the SOC compiles the separate tallies of subcolumns, but the chart does add to the decimal the results and they do **match**.

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

- Does anything stand out as suspicious?

Yes, there are several abnormalities identified for the following hours: **1:00 AM MST 2:00 AM MST, 9:30 AM MST, 10:30 AM MST** and **11:45 AM MST** by users:**user_a, user_k and user_j.**

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

The results do match the visualizations in the SOC's pie chart. Users:**user_a, user_k and user_j activity usage spiked to 6% (user_j), 31% (user_a) and 35% (user_k)**

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?

The visualizations may be slightly deceptive when assessing finer data but for the general application of understanding a pie chart demonstrates the correct set of information. A bar chart on the other hand tends to add quick insight into levels much like the pie charts. All stats charts should be taken on a case by case basis.

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, POST method observed a large spike in activity (Used to upload files or
submit web forms; 12 times the amount in increase observed).
```

- What is that method used for?

```
POST method observed a large spike in activity (Used to upload files or
submit web forms)
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes, the baseline was observed at 3,000 but the Attack Data shows about 570
which is drastically less.
```

Report Analysis for HTTP Response Codes

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

```
Code 404 and 200 showed changes in comparison.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
65 was our set threshold; the event came back with 800+ but we observed a
pocket of low balled information to encourage the SOC to increase the
threshold from 65 to 70.
```

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

```
8:00 PM MST was the target Window Wednesday, March 25, 2025.
```

- Would your alert be triggered for this activity?

```
Yes, thankfully the 800+ events would have been triggered by our lower end threshold.
```

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

```
65 was our set threshold; the event came back with 800+ but we observed a pocket of low balled information to encourage the SOC to increase the threshold from 65 to 70.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, at 8:00 PM MST we observed 1296 events that did trigger our SOC email trigger alert set within system (threshold number was 4).
```

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

```
8:00 PM MST we observed 1296 events that did trigger our SOC email trigger alert set within system (threshold number was 4).
```

- When did it occur?

```
8:00 PM MST we observed 1296 events that did trigger our SOC email trigger alert set within system (threshold number was 4).
```

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

```
Negative. The total number of actions triggered was 1; it was technically a perfect collection.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Two spikes in the data did stand out as abnormalities as collected for POST (1,296 events) and GET (729 events) at **6:00 PM MST (GET)** and **8:00 PM MST (POSTS)**.

- Which method seems to be used in the attack?

Two spikes in the data did stand out as abnormalities as collected for POST (1,296 events) and GET (729 events) at **6:00 PM MST (GET)** and **8:00 PM MST (POSTS)**.

- At what times did the attack start and stop?

Two spikes in the data did stand out as abnormalities as collected for POST (1,296 events) and GET (729 events) at **6:00 PM MST (GET)** and **8:00 PM MST (POSTS)**. The conclusion of these events, respectively, was **7:00 PM MST** and **9:00 PM MST**.

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

Two spikes in the data did stand out as abnormalities as collected for POST (1,296 events) which was the top event number total.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

GET (729 events) at **6:00 PM MST (GET)** showed an abnormality in comparison as well.

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

Kiev, Ukraine had 8 more with 440 events.

- What is the count of that city?

```
The count for the city jumped 10X from 35 to 440 in comparison to the
baseline data.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
The total URI changed by over 55% in comparison between the pool data and
the attack data summary.  We lost a batch of unique URIs.
```

- What URI is hit the most?

```
Accountlogin.php was hit the most with 1,323 events in comparison to the
baseline data.
```

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

```
Brute Force Attack and/or Password Spraying.
```


READ ME:
All information was sourced in ASU Class training for Cybersecurity Bootcamp Class of 2025. The information breakdown on CIM Add-on was specifically issued by ChatGPT 4.0. All remaining information bases have been pulled from class notes, project work time and ChatGPT 4.0 for additional sourced information. Plagiarism is a serious crime.

Submitted by: JEfezokhae@GMail.com
Linked IN: www.linkedin.com/in/joseph-efezokhae-933612148
Google Drive for Project #3:
https://drive.google.com/drive/folders/1IEB0LO0uFOudmd2eSSOnT7C2235F5lWL?usp=sharing

Be Safe! Be well! Be Informed!

Backdoor Bouncers Inc ***VSI logo care of Vehicular Solutions Innovated