| 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?

| Percentage wise, there were far more queries labeled as “high” as opposed to the basic Windows logs. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| The number of failed activities was almost halved. |
| --- |

**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?

| 35 events across a single hour. |
| --- |

* When did it occur?

| 8AM on Wednesday, March 25th, 2020 |
| --- |

* 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?

| No, based on metrics provided by original Windows Server logs, and using the Signature ID of 4624, “an account was successfully logged on”, no suspicious activity was detected.  However, by further examining the attack logs and sorting by “user” I was able to determine there was suspicious activity. |
| --- |

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

| 11 events in 1 hour. |
| --- |

* Who is the primary user logging in?

| user\_a |
| --- |

* When did it occur?

| 2AM on Wednesday, March 25th, 2020. |
| --- |

* Would your alert be triggered for this activity?

| No. |
| --- |

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

| Yes. I would adapt the alert to account for successful logins per user rather than as a collective. Subsequently, I would adjust the threshold to match this new alert. |
| --- |

**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?

| Absolutely, yes, there was a dramatic spike in accounts being locked out and subsequently a dramatic spike in attempting to reset accounts’ passwords. |
| --- |

* What signatures stand out?

| * “A user account was logged out.” * “An attempt was made to reset an account's password.” |
| --- |

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

| * “A user account was logged out.” - Started at roughly 1AM on March 25th, ended between roughly 2AM and 3AM on March 25th. * “An attempt was made to reset an account's password.” - Started at roughly 9AM on March 25th, ended between roughly 10AM and 11AM on March 25th. |
| --- |

* What is the peak count of the different signatures?

| * “A user account was logged out.” - Peak count is 896. * “An attempt was made to reset an account's password.” - Peak count is 1,258. |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| The values for user\_k and user\_a are drastically inflated compared to the other users. |
| --- |

* Which users stand out?

| User\_k and user\_a |
| --- |

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

| User\_a - started at roughly 1AM on March 25th, and ended between the hours of 2AM and 3AM on March 25th.  User\_k - started at roughly 8AM on March 25h, and ended between the hours of 9AM and 10AM on March 25th. |
| --- |

* What is the peak count of the different users?

| User\_a - 984  User\_k - 1,256 |
| --- |

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

* Does anything stand out as suspicious?

| Yes. |
| --- |

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

| Yes, the pie chart of signature values shows the same increase in activity for two signature values, “A user account was logged out” and “An attempt was made to reset an account's password.” |
| --- |

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

* Does anything stand out as suspicious?

| Yes. |
| --- |

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

| Yes, the user count using the bar chart reflects the same spike for user\_a and 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?

| Advantages of using a statistical chart to track Users is that you can get more detailed metrics alongside the count, such as percentages. You can also sort the counts and percentages by ascending or descending values with more ease. A disadvantage of using a statistical chart is that proper usage of visualizations, such as a bar chart, allows for more immediately identifiable information and discrepancies, which can be useful in situations where an analyst is monitoring numerous graphs, charts, and metrics. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes, there was a drastic increase in POST methods. |
| --- |

* What is that method used for?

| HTTP POST method is used to send data to a server. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| No, there were no suspicious changes. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| There was a drastic increase in the percentage of “404” HTTP 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?

| 939 events in 1 hour. |
| --- |

* Would your alert be triggered for this activity?

| Yes. |
| --- |

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

| No. |
| --- |

**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?

| 1,296 events in 1 hour. |
| --- |

* When did it occur?

| 8PM on Wednesday, March 25th, 2020. |
| --- |

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

| I would likely raise the threshold some to reduce alert fatigue. |
| --- |

**Dashboard Analysis for Time Chart of HTTP Methods**

* Does anything stand out as suspicious?

| Yes. |
| --- |

* Which method seems to be used in the attack?

| POST method. |
| --- |

* At what times did the attack start and stop?

| Between the hours of 7PM and 9PM. |
| --- |

* 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.)

| Kiev, Ukraine. Kharkiv, Ukraine. |
| --- |

* What is the count of that city?

| Kiev - 439  Kharkiv - 433 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes. |
| --- |

* What URI is hit the most?

| The VSI account logon page - /VSI\_Account\_logon.php |
| --- |

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

| Attempting a brute force attack against VSI. |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.