| 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, the high severity went up by 15% |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| The amount of failed activities decreased by 1.5% |
| --- |

**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 |
| --- |

* 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 I wouldn’t. Our predefined baseline of 7 was spot on due to other hourly events being less than 8. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| There was an increase in volume, which is worth checking out. |
| --- |

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

| 16 |
| --- |

* Who is the primary user logging in?

| User\_c |
| --- |

* When did it occur?

| 8am on March 25th, 2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes, because our baseline was 15. |
| --- |

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

| No I wouldn’t. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| Yes, 17 accounts were deleted at 5am on Wednesday, March 25th, 2020. The threshold/baseline was 15. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| YES |
| --- |

* What signatures stand out?

| Accounts locked out, attempts made to reset passwords, and user account successfully logging on. |
| --- |

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

| 12-3am on March 25th, 2020 - User accounts being locked out.  8am-11am on March 25th, 2020 - Reset account passwords.  10am-1pm on March 25th, 2020 - Accounts were successfully logged on. |
| --- |

* What is the peak count of the different signatures?

| 896 - User accounts locked out 1,258 - Reset account passwords 196 - An account was successfully logged on |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which users stand out?

| User A, User K, User J |
| --- |

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

| User A - 1:40am to 2:50am User K - 9am to 11am User J - 10:45am - 12:30pm |
| --- |

* What is the peak count of the different users?

| User A - 745 User K - 397 User J - 35 |
| --- |

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

* Does anything stand out as suspicious?

| Yes. - A user account was locked out. - An attempt was made to reset an account 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, User A and User K have significantly higher amounts. |
| --- |

* 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?

| Line charts are great for showing volumes over time, whereas pie charts are limited to only showing values. Pie charts do help visualize smaller quantities in comparison to a line chart, where the lines for low amounts are hard to see. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes, POST. |
| --- |

* What is that method used for?

| POST submits an entity to the specified resource. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| Yes, the number decreased significantly. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Yes, code 404 went up significantly. |
| --- |

**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 at 8pm on Wednesday, March 25th, 2020 |
| --- |

* 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?

| 8-9pm |
| --- |

* When did it occur?

| March 25th, 2020 |
| --- |

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

| No |
| --- |

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

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which method seems to be used in the attack?

| GET and POST |
| --- |

* At what times did the attack start and stop?

| GET- 5pm - 7pm POST- 7pm - 9pm |
| --- |

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

| GET - 729 POST - 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 & Kharkiv, Ukraine |
| --- |

* What is the count of that city?

| 2 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes |
| --- |

* What URI is hit the most?

| /VSI\_Account\_logon.php |
| --- |

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

| Brute force attacking the logon page. |
| --- |

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