| 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 changes for Informational went from 93.09% to 79.77% and the changes for High went from 6.91% to 20.23%. The increase in High cases suggest suspicious activity. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| The change of failed activities went down from 2.98% to 1.56%, we did not detect suspicious activity, at this point. |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes there was suspicious activity. A possible brute force attack. |
| --- |

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

| 35 |
| --- |

* When did it occur?

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

* Would your alert be triggered for this activity?

| With our previous threshold at 15, our Alert would be triggered |
| --- |

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

| For now we will maintain a threshold of 15 for our Alerts, we will review again at a later point. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| There are potential suspicious volume of successful logins happen in the span of 1 hour on March 25 2020 from 11:00 am to 12:00 pm |
| --- |

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

| 392 |
| --- |

* Who is the primary user logging in?

| User\_j with 604 counts of successful log on account and 69.907% |
| --- |

* When did it occur?

| March 25 2020 from 11:00 am to 12:00 pm |
| --- |

* Would your alert be triggered for this activity?

| Yes, because the threshold is only at 20 times |
| --- |

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

| I don't think changes is needed for the threshold as 20 successful logon is a good number |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| There was a significant drop in deleted accounts from roughly 30 each hour to about 12 each hour. This suggests that Admins may not be deleting accounts of ex-employees or transferees, this raises concerns, but further investigation is required to confirm suspicious activity. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| So the signature of "A user account was locked out" and "An attempt was made to reset an accounts password" had high count of activity in a period of time |
| --- |

* What signatures stand out?

| "A user account was locked out" and "An attempt was made to reset an accounts password" |
| --- |

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

| -The signature "A user account was locked out" start from after 12 am March 25 2020 to 3 am the same day  -The signature "An attempt was made to reset an accounts password" start from 8 am and stop at 11 am on March 25 2020 |
| --- |

* What is the peak count of the different signatures?

| The peak count for "A user account was locked out" is 1792 as 2 AM  The peak count for "An attempt was made to reset an accounts password" is 2516 at 9 AM |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| User a and user k with suspiciously high amount of activity in a short term of time |
| --- |

* Which users stand out?

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

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

| User\_a start from 12 am to 3am March 25 2020  User\_k start from 8am to 8am to 11am |
| --- |

* What is the peak count of the different users?

| User\_a peak is 1968  User\_k peak count is 2512 |
| --- |

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

* Does anything stand out as suspicious?

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

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

* Does anything stand out as suspicious?

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

**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?

| [Enter answer here] |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| The biggest change in HTTP methods was GET going from 19,702 all the way down to 3,157. I would say the “suspicious” change would be in regards to the POST method going from 212 all the way to 1,324. |
| --- |

* What is that method used for?

|  |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| All traffic on the websites decreased by quite a large amount. This could show that systems are not working as intended or the sites are being brought down/made inaccessible through a potential inconsistent Distributed Denial of Services (DDOS) attacks. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| These numbers fell drastically as well like the referrer websites. This may be indicative of a Distributed Denial of Service (DDOS) attack since these numbers are nowhere close in comparison. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Very suspicious activity occurred on March 25, 2020 at 8pm. |
| --- |

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

| March 25, 2020 at 8pm there were 937 Non-US registrations of activity within the hour. |
| --- |

* Would your alert be triggered for this activity?

| Yes it would since our alert is set to any number over 118 in an hour. This instance was 937 within an hour. |
| --- |

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

| If anything, our threshold may be a tad low. Although, there was only one other instance of any Non-US logins being over 118 within an hour. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

|  |
| --- |

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

| Yes there was suspicious activity. It occurred on March 25, 2020 at 8pm. THe count was 1,296 within the hour. |
| --- |

* When did it occur?

| March 25, 2020 at 8pm. |
| --- |

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

| I would say no overall. The second highest report of HTTP method activity was 7 within the hour on the apache\_attack\_logs.txt. Our threshold of 10 suffices. If anything, the threshold should be raised, to ~100?, due to the large discrepancy in the hourly volume of POST method activity if overreporting becomes a problem. |
| --- |

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

* Does anything stand out as suspicious?

| [Enter answer here] |
| --- |

* Which method seems to be used in the attack?

| [Enter answer here] |
| --- |

* At what times did the attack start and stop?

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

* What is the count of that city?

| [Enter answer here] |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| [Enter answer here] |
| --- |

* What URI is hit the most?

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

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