| 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?

| In terms of severity, there were not any visible changes or suspicious looking activity. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| We did detect suspicious changes in failed activities. |
| --- |

**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?

| The count was 70 events at 8 AM. |
| --- |

* When did it occur?

| It occurred on March 25, 2020 at 8 AM. |
| --- |

* Would your alert be triggered for this activity?

| Yes, the alert would have been triggered. |
| --- |

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

| No, our alert was set for 15 in an hour. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes, we did detect a suspicious volume of logins. |
| --- |

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

| The count was 392. |
| --- |

* Who is the primary user logging in?

| user\_j |
| --- |

* When did it occur?

| March 25, 2020 at 11:00 AM. |
| --- |

* Would your alert be triggered for this activity?

| Yes, our alert would be triggered. |
| --- |

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

| No, we would not change our threshold. It is set at 40. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| No we did not. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Yes, there were a couple of signatures. |
| --- |

* What signatures stand out?

| “An attempt was made to reset an accounts password”  “A user account was locked out”  “AN account was successfully logged on” |
| --- |

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

| “An attempt was made to reset an accounts password” : 8 AM - 11 AM  “A user account was locked out” : 12 AM - 3 AM  “AN account was successfully logged on” : 10 AM - 1 PM |
| --- |

* What is the peak count of the different signatures?

| “An attempt was made to reset an accounts password” : 1,258  “A user account was locked out” : 896  “AN account was successfully logged on” : 196 |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which users stand out?

| user\_k, user\_j, and user\_a |
| --- |

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

| user\_k : 8 AM - 11 AM  User\_j : 10 AM - 1 PM  user\_a : 12 AM - 3 AM |
| --- |

* What is the peak count of the different users?

| user\_k : 1,255  User\_j : 196  user\_a : 896 |
| --- |

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

* Does anything stand out as suspicious?

|  |
| --- |

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

| Yes they do |
| --- |

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

* Does anything stand out as suspicious?

|  |
| --- |

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

| Yes they do |
| --- |

**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 pie chart was easier to read and visually tell which user had more activity in comparison to everyone else. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes, POST had suspicious changes. |
| --- |

* What is that method used for?

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

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| Yes |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Yes, the count dropped 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?

| 7 PM - 9 PM |
| --- |

* Would your alert be triggered for this activity?

| Yes it would have |
| --- |

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

| No, the alarm would have triggered correctly. |
| --- |

**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 |
| --- |

* When did it occur?

| March 25, 2020 at 7 PM - 9 PM |
| --- |

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

| No, the threshold was correct. |
| --- |

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

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which method seems to be used in the attack?

| It seemed to be a potential XSS attack. |
| --- |

* At what times did the attack start and stop?

| It happened between 7 PM to 9 PM. |
| --- |

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

| 439 |
| --- |

**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 |
| --- |

* What is the count of that city?

| 439 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes |
| --- |

* What URI is hit the most?

| Account logon was hit the most with 1,322 counts. |
| --- |

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

| The user was potentially doing a brute force attack. |
| --- |

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