|  |
| --- |
| 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, an increase of 13.32% (from 6.905961% to 20.222060%)(from 658 to 1111) |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

|  |
| --- |
| Yes, a decrease of 1.42% (from 2.980688% to 1.563288%) (from 284 to 93) |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

|  |
| --- |
| Yes, at hour 8 there was 70 failures. |

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

|  |
| --- |
| 70 failures at hour 8 |

* When did it occur?

|  |
| --- |
| 8:39am is when the trigger was alerted (hypothetically) |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes |

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

|  |
| --- |
| No, based on my baseline data, my threshold was appropriate |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

|  |
| --- |
| While my alert would not have been triggered, the count of successful logins is dramatically lower. |

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

|  |
| --- |
| N/A |

* Who is the primary user logging in?

|  |
| --- |
| user\_a |

* When did it occur?

|  |
| --- |
| N/A, my alert would not have been triggered |

* Would your alert be triggered for this activity?

|  |
| --- |
| No |

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

|  |
| --- |
| Based on the baseline, I might lower it a little, but not too much because it would initiate Alert Fatigue and this is for successful logins. |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

|  |
| --- |
| No, the volume decreased a lot. |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes, 1,811 user accounts were locked out and 2,128 attempts to reset the password. |

* What signatures stand out?

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

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

|  |
| --- |
| 1am “A user account was locked out”  9am “An attempt was made to reset an accounts password” |

* What is the peak count of the different signatures?

|  |
| --- |
| 1,811 “A user account was locked out”  2,128 “An attempt was made to reset an accounts password” |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes |

* Which users stand out?

|  |
| --- |
| user\_a and user\_k had a dramatic increase in events |

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

|  |
| --- |
| user\_a START: 0100 hrs END: 0300 hrs  user\_k START: 0900 hrs END: 1100 hrs |

* What is the peak count of the different users?

|  |
| --- |
| user\_a 1,878  user\_k 2,118 |

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

* Does anything stand out as suspicious?

|  |
| --- |
| Yes, by 2am the account lockouts reduced, between 9 and 11am the attempts to reset accounts passwords happened, and then between 11am and 1pm there was a large increase in successful logins. |

* 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, accounts user\_a and user\_k had very abnormal amount of events. |

* 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?

|  |
| --- |
| The Pie Chart was probably not the best for overall user count. It may have been better to do a Bar graph like the signature count which successfully exposed suspicious activity. The Pie chart is probably best for a small number of differing variables to measure. |

## 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?

|  |
| --- |
| It is used for uploading/publishing content to the website. |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

|  |
| --- |
| There is a dramatic decrease in activity coming from the referer domains. |

**Report Analysis for HTTP Response Codes**

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

|  |
| --- |
| Yes, a large increase in Error 404 messages. (from 213 to 679) |

**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?

|  |
| --- |
| 937 in hour 20 (8pm) |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes |

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

|  |
| --- |
| No, it was based off the baseline and this increase is significant. |

**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?

|  |
| --- |
| 1296 POST events in hour 20 (8pm) |

* When did it occur?

|  |
| --- |
| 8pm |

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

|  |
| --- |
| No, it was based off the baseline and this increase is significant. |

**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 |

* At what times did the attack start and stop?

|  |
| --- |
| START 7pm END 9am |

* 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?

|  |
| --- |
| Many countries have decreased significantly while Ukraine has increase significantly. |

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

|  |
| --- |
| Ukraine |

* What is the count of that city?

|  |
| --- |
| 877 |

**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 Attack |

© 2024 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.