| 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 incidents increased from 6.91% to 20.22% |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| Yes. A suspicious fall has taken place in the Failed Activities which almost halved from 2.98% down to 1.56% |
| --- |

**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?

| 192, 12am, Wed March 25, 2020  973, 1am, Wed March 25, 2020  1007, 2am, Wed March 25, 2020  174, 3am, Wed March 25, 2020  187, 4am, Wed March 25, 2020  192, 5am, Wed March 25, 2020  178, 6am, Wed March 25, 2020  207, 7am, Wed March 25, 2020  205, 8am, Wed March 25, 2020  1293, 9am, Wed March 25, 2020  784, 10am, Wed March 25, 2020  196, 11am, Wed March 25, 2020  197, 12pm, Wed March 25, 2020  164, 1pm, Wed March 25, 2020 |
| --- |

* When did it occur?

| From 12am to 1pm Wed, Wed March 25, 2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes. Ours is set at >17 |
| --- |

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

| No. Our alert was based on normal activity and allowed for a limited amount of spikes in failed logins and would have triggered investigations. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| No because our threshold was >29 events per hour. Normal activity was an average of 13 with a high of 22, so we set >29 events including some buffer for spikes in activity. The attack data did not exceed 16 events in any one hour. |
| --- |

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

| The count of events was from 8 to 21 per hour which falls within the range of normal activity. |
| --- |

* Who is the primary user logging in?

| User\_a logging in approx. 14% of the time |
| --- |

* When did it occur?

| We didn’t see a high volume of activity in the data so do not see an attack using this vector. |
| --- |

* Would your alert be triggered for this activity?

| No because our threshold is set at >29 events. |
| --- |

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

| No because the normal activity range (average 13 and high of 22) was not exceeded in this data. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| Our threshold was set at >29 so we did not detect a suspicious volume of deleted accounts. The average number of deletions was 13 and the high was 22. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| An increase to very high percentages for certain categories of signature for:   * **A user account was locked out** * **An attempt was made to reset an accounts password** |
| --- |

* What signatures stand out?

| Signatures stand out for:   * **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?

| **A user account was locked out** 12am-3am  **An attempt was made to reset an accounts password** 8am-11am |
| --- |

* What is the peak count of the different signatures?

| **A user account was locked out** = peak count 896  **An attempt was made to reset an accounts password** = peak count 1258 |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes **user\_a** and **user\_k** have increased their logins |
| --- |

* Which users stand out?

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

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

| User\_a 12am-3am.  User\_k 8am-11am. |
| --- |

* What is the peak count of the different users?

| User\_a = peak count of 984.  User\_k = peak count of 1256. |
| --- |

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

* Does anything stand out as suspicious?

| A user account was locked out increased to approx. 30%  An attempt was made to reset an accounts password increased to approx. 35% |
| --- |

* 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 increased to 1878, 31.5% logins  User\_k increased to 2118, 35.6% logins |
| --- |

* 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?

| Reports are good for showing historical data, however they can be difficult for seeing the changes indicating an attack and the vector(s) being used to do it.  The statistical charts made it immediately obvious that there was a problem and who or what was the source of the problem. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| GET 200 dropped from 8994 down to 2416  POST 200 increased greatly from 99 to 1323  GET 404 increased from 202 to 671 |
| --- |

* What is that method used for?

| POST method sends data to the server  GET method retrieves data from the server, requesting pages, etc. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| Yes. The overall traffic from Referrer Domains decreased by just over 87% |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Yes. Generally a drop in responses, in total by approximately 59%. I.e. the 200 Response dropped from 9126 to 3746 events. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| There was a significant spike in activity of 937 events at 8pm, Wed 25 March, 2020 |
| --- |

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

| 937 events at 8pm Wed 25 March, 2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes. Our threshold is >100 which would trigger an alert. |
| --- |

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

| No. The normal hourly average was 62 events with a high of 84, so our alert level of >100 was appropriate for this data. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes a significant spike in activity at 8pm, 25 March, 1296 events |
| --- |

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

| 1 hour at 8pm, 25 March, 1296 events |
| --- |

* When did it occur?

| At 8pm, 25 March, 1296 events |
| --- |

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

| No, our threshold was set at >5 events per hour. This would have triggered an alert with this attack data. |
| --- |

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

* Does anything stand out as suspicious?

| Suspicious increase in GET and POST requests. |
| --- |

* Which method seems to be used in the attack?

| GET and POST requests. |
| --- |

* At what times did the attack start and stop?

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

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

| GET = peak count 729 events  POST = peak count 1296 events |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| Heightened amount of activity emanating from Ukraine |
| --- |

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

| Heightened amount of activity emanating from Ukraine in Kiev and Kharkiv |
| --- |

* What is the count of that city?

| Kiev = count of 454, Kharkiv = count of 433 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Suspicious increase in the traffic on VSI\_Account\_logon.php page. This page did not feature at all in the original logs, however, after the attack it accounts for 29.42% of the traffic. |
| --- |

* What URI is hit the most?

| VSI\_Account\_logon.php is hit the most. |
| --- |

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

| The attacker is potentially attempting a brute force attack. |
| --- |

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.