| 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?

| The amount of high severity level counts increased by roughly 60.4% (329 to 1111) |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| The amount of average failures when down and successes up. Failures went from 142 to 93. Successes went from 4622 to 5856. If the baseline for success is surpassed by 21.1% and failures decreased by 35.6% |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes, the baseline was roughly 6 failed activities on average and the alert was set to 8 for triggering as a buffer. There was a spike of up to 35 failed activity |
| --- |

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

| From 7-8am, March 25 2020 there was a spike of up to 35 failed activities and then no failures from 8am to 12pm, a span of 4 hours |
| --- |

* When did it occur?

| From 7-8am, March 25 2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes |
| --- |

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

| No I would not since 8 is considered normal activity |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| There were no suspicious increase of logins but a suspicious decrease in logins |
| --- |

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

| There were was a severe decrease in average logins from 8-9am (16 to 4) March 25 2020 then 0 logins from 9am-12pm |
| --- |

* Who is the primary user logging in?

| ACME-002 |
| --- |

* When did it occur?

| 8-9am March 25 2020 |
| --- |

* Would your alert be triggered for this activity?

| No |
| --- |

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

| Maybe if we were detecting successful logins under a threshold since according to the graph there were no logins at all. Perhaps if a specific user tries logging in over the span of time, this would be a better alternative. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| The baseline trigger condition is 21 since this is just a little above the average, however from 8-9am there is a significant decrease in account deletions during work hours (from 11 to 3) then non from 9am to 11am (2 hour span) |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Between 12Am-3Am there was a peak of 896 user lockouts (2am), between 8am-11AM there was a peak of 1258 of attempts to change a user password (9am), as well as between 10 - 12am there was a peak of 196 successful logins (11am - where there were none on reports) |
| --- |

* What signatures stand out?

| Primarily User was locked out and Password change attempts |
| --- |

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

| Between 12Am-3Am for user lockouts, 8am-11am for attempted password resets and 10am-1pm for successful logins during an outage. |
| --- |

* What is the peak count of the different signatures?

| peak of 896 user lockouts (2am), peak of 1258 of attempts to change a user password (9am),peak of 196 successful logins (11am) |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Cross referencing the signature chart, the spikes in activity correlate with specific users at those times. User\_a from 12am-3am (lockouts), User\_k from 8am-11am for password change attempts and User\_j between 10am to 1pm for successful logins |
| --- |

* Which users stand out?

| User\_a, User\_j, User\_k |
| --- |

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

| User\_a from 12am-3am, User\_k from 8am-11am, User\_j between 10am to 1pm |
| --- |

* What is the peak count of the different users?

| User\_a (984), User\_k (1256), User\_j (196) |
| --- |

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

* Does anything stand out as suspicious?

| The same three signatures spikes correlate with time charts |
| --- |

* 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?

| The same three users spikes correlate with time charts |
| --- |

* 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?

| Depending on the chart |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| The GET and POST methods had drastic changes in their numbers. GET 9851 > 3151 and POST 106 > 1324 |
| --- |

* What is that method used for?

| GET is used to request data from a specified resource whereas POST is used to send data to a server to create/update a resource |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| There was a significant drop in referrer domains |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Significant drop in all response codes (primarily 200 codes) - 404 codes drastically increased |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes, around 10pm on March 25, 2020 there were roughly 937 events from international compared to the rest of the day which were 120 or less |
| --- |

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

| 937 |
| --- |

* 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?

| There were two instances of high POST activity: 6PM (730) and 8PM (1415) |
| --- |

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

| 6PM (730) and 8PM (1415) |
| --- |

* When did it occur?

| 10/25/2025 6PM (730) and 8PM (1415) |
| --- |

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

| No, the threshold would have triggered in a live environment. |
| --- |

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

* Does anything stand out as suspicious?

| There are large spikes of GET requests and then one large POST method at 8pm (1296) |
| --- |

* Which method seems to be used in the attack?

| POST |
| --- |

* At what times did the attack start and stop?

| The attack starts around 7PM to 9PM |
| --- |

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

| 8PM |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| There was a huge increase in locational access from Ukraine |
| --- |

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

| Kharkiv and Kiev, Ukraine |
| --- |

* What is the count of that city?

| Kharkiv is 432 and Kiev is 439 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| There was a large chunk that appeared on the chart for /VSI\_Account\_logon.php and /files/logstash/logstash-1.3.2-monolithic.jar |
| --- |

* What URI is hit the most?

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

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

| It seems like a Bruteforce attack based on the number of failed logins, POST methods and vector of /VSI\_Account\_logon.php |
| --- |

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