| 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 the Windows Server Logs, the informational severity was at 93% and the high severity was at 7%. When changing to the attack logs, we see informational severity drop to 80% and the high severity jump to 20%.(These numbers are rounded up and down). The huge jump in high severity raises suspicious activity. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| In the Windows Server Logs, successful activities were at 97% and failed activities were at 3%. When changing to the attack logs, we see successful activities jumped to 98% and the failed activities dropped to 2%.(These numbers are rounded up and down). No real big changes between the sets of logs that jumps out as suspicious |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Most of the activity was around 1-3 events, so it looked pretty normal. There was a huge spike of 28 events that occurred that looked suspicious. |
| --- |

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

| 28 events |
| --- |

* When did it occur?

| It occurred at about 8:30 AM |
| --- |

* Would your alert be triggered for this activity?

| Yes, the alert that was made would be triggered by this activity |
| --- |

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

| No, the threshold would not be changed as there is only this one occurrence of a large number of events that caused it to be triggered. The rest of the events were in the range of the threshold and baseline. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| There were two spikes of a high count of logins within two different hour ranges. |
| --- |

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

| 196 at 11AM-12PM and 77 @ 12-1PM |
| --- |

* Who is the primary user logging in?

| The primary user logging in was user\_j. |
| --- |

* When did it occur?

| It occurred on March 25, 2020 from 11AM - 1PM. |
| --- |

* Would your alert be triggered for this activity?

| Yes, the alert that was created would be triggered. |
| --- |

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

| No, if we were to change the threshold, we may not be alerted anymore since the threshold is a lot lower than these spikes. We would then see less alerts being triggered when suspicious activity is occurring. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| There was no suspicious volume of deleted accounts. There were slight changes in percentages, but nothing that would raise concerns. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| There are 2 signatures with counts of about 850 and more. |
| --- |

* What signatures stand out?

| “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?

| “User account was locked out”: 12 - 3 AM  “An attempt was made to reset an accounts password”: 8 - 11 AM |
| --- |

* What is the peak count of the different signatures?

| “User account was locked out”: 896 @ 2AM  “An attempt was made to reset an accounts password”: 1,258 @ 9AM |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes there are two big spikes for two users that stand out as suspicious. |
| --- |

* Which users stand out?

| user\_a and user\_k are the two users that stand out. |
| --- |

* 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: 984 @ 2AM  user\_k: 1,256 @ 9AM |
| --- |

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

* Does anything stand out as suspicious?

| The two signatures, “User account was locked out” and “An attempt was made to reset an accounts password”,have a significantly higher count than the rest of the signatures in the chart, as well as from the original logs. |
| --- |

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

| Yes they match, as these were the two signatures that raised concerns from the timechart. |
| --- |

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

* Does anything stand out as suspicious?

| The two users, user\_a and user\_k,have a significantly higher count than the rest of the users in the chart, as well as from the original logs. |
| --- |

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

| Yes they match, as these were the two users that raised concerns from the timechart |
| --- |

**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?

| Using the statical chart allowed us to take a deeper look into a single item, and within that item, one of the subsections to look at. So for the radial gauge, we were able to take a deeper look at severity in the logs and then single in on high severity. The advantage is being able to look at one thing of a specific group of information vs all of it together. A disadvantage of this is that you cannot really compare it to other information within that field. So in this example, we lose the capability of comparing the high severity to the informational severity. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| All of the HTTP Methods had a decrease in percentage, except for one. HTTP POST Method had an increase of a little more than 28 percent. |
| --- |

* What is that method used for?

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

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| There were no suspicious changes in the referrer domains. There were no big changes in percentages, with the most being 2 - 3 percent and the rest were decimal percentage changes. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Response code 200 drops by 8 percent and response code 304 jumps up by 11 percent. Response code 304 means that the requested resource has not been modified since the last time that the resource was accessed. This can raise concerns because of the big increase in percentage of the code appearing. As well as depending on what the resource being accessed is. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| There was one spike of suspicious volume of over 900 events in a particular hour. |
| --- |

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

| It occurred from 8 - 9 PM. |
| --- |

* Would your alert be triggered for this activity?

| Yes the alert that was created would be triggered. |
| --- |

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

| No, the threshold would not be changed as there is only this one occurrence of a large number of events that caused it to be triggered. The rest of the events were in the range of the threshold and baseline. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes there was a suspicious volume of activity that occurred during a single hour with almost 1,300 HTTP POST events. |
| --- |

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

| It occurred from 8 PM - 9 PM. |
| --- |

* When did it occur?

| It occurred on March 25th,2020 |
| --- |

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

| No, the threshold would not be changed as there is only this one occurrence of a large number of events that caused it to be triggered. The rest of the events were in the range of the threshold and baseline. |
| --- |

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

* Does anything stand out as suspicious?

| There are 2 spikes for two different HTTP Methods that stand out as suspicious. |
| --- |

* Which method seems to be used in the attack?

| The HTTP POST and GET methods seem to be in use for the attack. |
| --- |

* At what times did the attack start and stop?

| The attack started at 5 PM with the GET method and ended at 9 PM with the POST method. |
| --- |

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

| POST: 1,296 events  GET: 729 events |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| In the original apache file, there was a big cluster that was around Germany. In the attack file, what stood out was that this cluster moved east and into Ukraine, with the cluster being larger which raised concerns. |
| --- |

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

| The new location is Kiev,Ukraine with a high volume of activity. |
| --- |

* What is the count of that city?

| The count for Kiev was 440. |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes there was information that stood out as suspicious. Two of the URI has a massive jump in percentage increase compared to how they looked in the original apache logs. One of them is almost nearly a third of the URI information now. |
| --- |

* What URI is hit the most?

| The URI that was hit the most was /VSI\_Account\_logon.php. |
| --- |

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

| Based on the URI that is being accessed the most, we can assume the attacker is potentially trying to perform a Brute-Force Attack. |
| --- |

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