| 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?

| There were a couple of changes when analyzing the severity in the windows\_server\_logs.cve |  Informational: went from 93% to roughly 80%  High: Went from 7 to 20% |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| We detected that there was a 1% increase and decrease in success and failure respectfully |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| [Yes, there was some suspicious activity detected |
| --- |

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

| [I was able to count 35 events |
| --- |

* When did it occur?

| [8:00 A.M. March 25 |
| --- |

* Would your alert be triggered for this activity?

| [Yes it would trigger |
| --- |

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

| [No, we will not change the threshold. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| It seems there was suspicious activity regarding the successful logins |
| --- |

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

| The number of activities is around 196-200 |
| --- |

* Who is the primary user logging in?

| User\_j is the primary user |
| --- |

* When did it occur?

| According to the logs the attack happened around 11:00 a.m. and 12:00 p.m. on March 25 |
| --- |

* Would your alert be triggered for this activity?

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

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

| No, we don't believe a change in the threshold would benefit |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| From the logs there weren't any signs of a suspicious volume of deleted accounts |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| An account was locked out” from 12:00 a.m. to 3:00 a.m. on Wednesday, March 25th and with the signature “An attempt was made to reset an accounts password” from 8:00 a.m. to 11:00 a.m. on Wednesday, March 25th. |
| --- |

* 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?

| “A user account was locked out”: Started at 12:00 a.m. on Wednesday, March 25th and stopped at 3:00 a.m. on Wednesday, March 25th.  “An attempt was made to reset an accounts password”: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th. |
| --- |

* What is the peak count of the different signatures?

| For the user account was blocked - 896 signatures  For reset on account password - 1,258 signatures |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| There was suspicious activity at 9 am to 10 am on march 25 |
| --- |

* Which users stand out?

| User\_a and user\_k stand out |
| --- |

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

| user\_a: Started at 12 a.m. on Wednesday, March 25th and stopped at 3 a.m. on Wednesday, March 25th.  user\_k: Started at 8 a.m on Wednesday, March 25th and stopped at 11 a.m. on Wednesday, March 25th. |
| --- |

* What is the peak count of the different users?

| User\_a: the peak count was 984  User\_k: the peak count was 1256 |
| --- |

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

* Does anything stand out as suspicious?

| There is suspicious activity starting at 12 am |
| --- |

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

| Yes they support my findings |
| --- |

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

* Does anything stand out as suspicious?

| User\_a and user\_k stand 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?

| An advantage of a statistical chart is a concise list of the top users accused of suspicious activity. A disadvantage of the statistical chart is that it shows a cumulative perspective of data while other approaches to data representation show a shorter, more specific perspective of data. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| I detected a POST and GET request. |
| --- |

* What is that method used for?

| POST is used to submit information to a web server |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| I couldn't find any suspicious activity in changes to referrer domains |
| --- |

**Report Analysis for HTTP Response Codes**

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

| There was a bit of an increase in the 404 response code |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes, Ukraine had some pretty suspicious activity. |
| --- |

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

| Ukraine had a count of 1369 events during the 8:00p.m timeframe |
| --- |

* Would your alert be triggered for this activity?

| Yes, my alert would be triggered |
| --- |

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

| No, the alert should work as intended so a change is not necessary |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes, there was a suspicious volume of POST activity |
| --- |

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

| The count was 1296 events |
| --- |

* When did it occur?

| 8:00 Pm March 25 |
| --- |

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

| No, a change isn't necessary |
| --- |

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

* Does anything stand out as suspicious?

| There was suspicious activity with the method “GET” from 5 p.m. to 7 p.m. on, March 25th and with the method “POST” from 7 p.m. to 8 p.m. on, Match 25th |
| --- |

* Which method seems to be used in the attack?

| The “GET” and “Post” methods are used in the attack |
| --- |

* At what times did the attack start and stop?

| The attack for “GET” started from 5 pm and ended 7 pm  The attack for “POST” started from 7 pm and ended 8 pm |
| --- |

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

| GET; the peak was 1296  Post; the peak was 729 |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| There's suspicious activity in the country of Ukraine. |
| --- |

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

| The city of Kiev whichh is in Ukraine has a high volume of activity |
| --- |

* What is the count of that city?

| The count of Kiev is 872 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| There was suspicious activity with the URI “/files/logstash/logstash-1.3.2-monolithic.jar” from 6 p.m. to 7p.m. on Wednesday, March 25th and with the URI “/VSI\_Account\_logon.php” from 8 p.m. to 9pm. on Wednesday, March 25th |
| --- |

* What URI is hit the most?

| VSI\_Account\_logon.php was hit the most with 1,415 events |
| --- |

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

| URI VSI\_Logon.php being accessed, the attacker may be trying to brute force the VSI logon page. |
| --- |

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