IS 635 – Technology and Startups

Team Cluelez

Project using a Disruptive Tech Idea – Artificial Intelligence

Ayush Vij
026647502

Sadan Iqbal
026622646

Madhur Ingle
026595853

Introduction

For this project we have developed a game like who wants to be a millionaire to see if the user can find a correct answer where the questions are based upon phishing emails and common questions which should be known to any internet user to avoid getting scammed . The way this game works is, when a user starts a game, they are presented with a set of questionnaires and the user must select a correct answer amongst the four given options to proceed further. The language of questions is like that of a potential phishing email where the users are sometimes unaware about the legitimacy of the email and often, they get scammed for it. The is the new type of cybercrime, which is increasing a lot recently, and people are getting scammed due such types of email. As the game progresses, the users are given points out of 10 for each question and they are assessed based upon their final tally. Based on the different types of emails we have gathered over the span of more that 5 years, we have designed a questionnaire as close as we can to all varieties of potential threats in an entertaining way so that the user can enjoy the game at the same time. Upon completing the game, every user would be given a score, and depending upon their final score, they would be assessed. This would be done by the Artificial intelligence technology that we have implemented in this project, that would determine that how much of a threat the user has from a potential fraudulent email. The AI would then make a brief report on the performance of a user score, and it would be sent back to the user describing their performance where they were strong and where they had room for improvement. Every individual's score would be stored, so that if the user tries to play the game again the AI would know about the user's previous score and it would then assess based upon the new score and compare the progress that has been made by the user. This would in turn help the user understand their strength and weakness, so that they can do better the next time. We have made this product using Flutter and it is available across all platforms.

Business Model Canvas

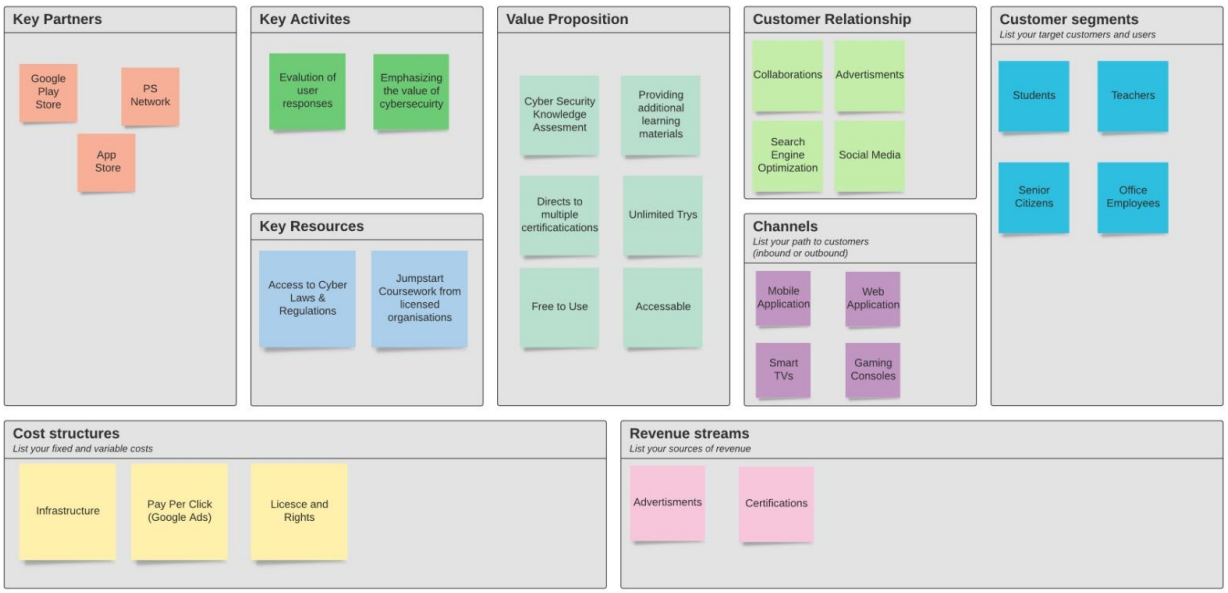

Fig 1. Business Model Canvas

Value Proposition Model

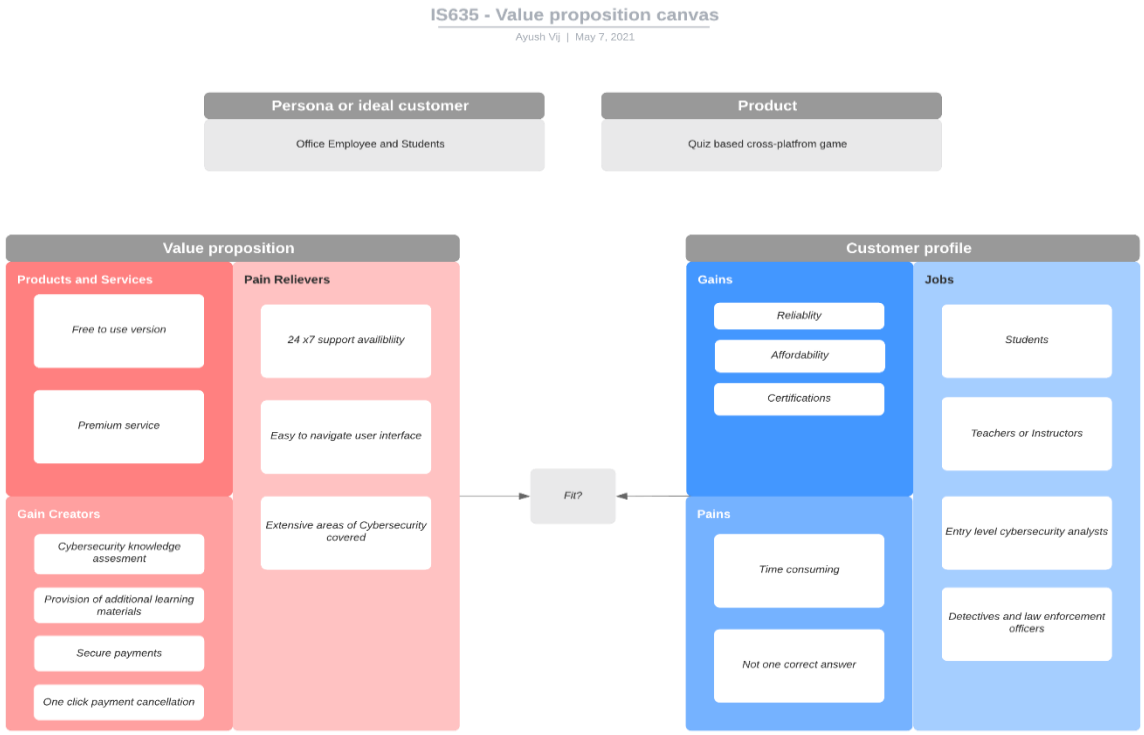

Fig 1. Business Model Canvas

Hypothesis

Over the years, there has been innumerable cases where people have received various emails, which sounds like legit emails concerning the user's safety whether it is online, device safety, bank account details, corrupt operating system and many more. All these alerts, emails have led people getting scammed in one way or the other. Weather it is people getting scammed for a huge amount of money, or people losing data, or their data getting corrupt. This has happened from individual level till big organizational level as well. The simple goal we wish to deliver via Cluelez is to aware the people in general as to how to avoid getting scammed and how to be alert to a possible situation for future purposes. We deliver this is an entertaining and educational way where people select a single response from four different response when asked a question. These questions are updated to the current language of the frequent emails received as well as some old tricks which were used some years before. Some answers maybe be partially correct, but for the user to be fully aware, they need to select the correct answer. At the end of the questionnaire, the user would be assessed by an AI tool to calculate, how much a user understands about potential threats for him and upon completion the user would receive a certification as well. Hopefully, after using Cluelez the user would be able to understand how to avoid getting scammed and they can hopefully educate their partner / colleague about the same.

Data Description

This dataset looks at the data security incidents which have been reported to the Information Commissioner's Office (ICO). Data security incidents are a major concern for those affected and a key area of action for the ICO. This dataset includes figures on brute force attacks, malware, phishing, ransomware, and a range of other cyber and non-cyber security incidents. This dataset contains the number and type of security incidents reported to the ICO for each quarter from April 2019 to September 2020, as reported on the ICO website. Please note that these figures are based on the number of reports submitted by the data controller, not necessarily the number of incidents.

Data Cleaning Steps

Fig 3. Data Cleaning Steps from Tableau Prep Builder

As we know that the data which was taken was from April 2019 to Septermber 2020. The initial data was divided into three quarters per year, but there was a mistake in the original data. The quarter 3 of the year 2020/2021 was posted as quarter 4 of the year 2019/2020. So, the values were edited there to clean it up and to properly divide the data according to their given quarter. Later the was edited into two parts, where they were again seperated into three different cleaning steps. The above cleaning step was divied according to the data reported in three different quarters of the year 2020. The data had total complaints reported for malware, virus, phishing emails, ransomware and a bunch of cyber and non cyber incidents. This data was given by the data controller in the ICO. The Clean 2 was divied according to the total complaints recorded in the year of 2019 and they were divided according to the quarters in which they were reported so as to easily understand the frequency of complaints which were reported and which months were the most targeted months and what type of attacks were register in order to understand the frequency and the types of attack reported.

Vizualizations

Some of the images mentioned below are the vizialized data which was cleaned to better understand the data.

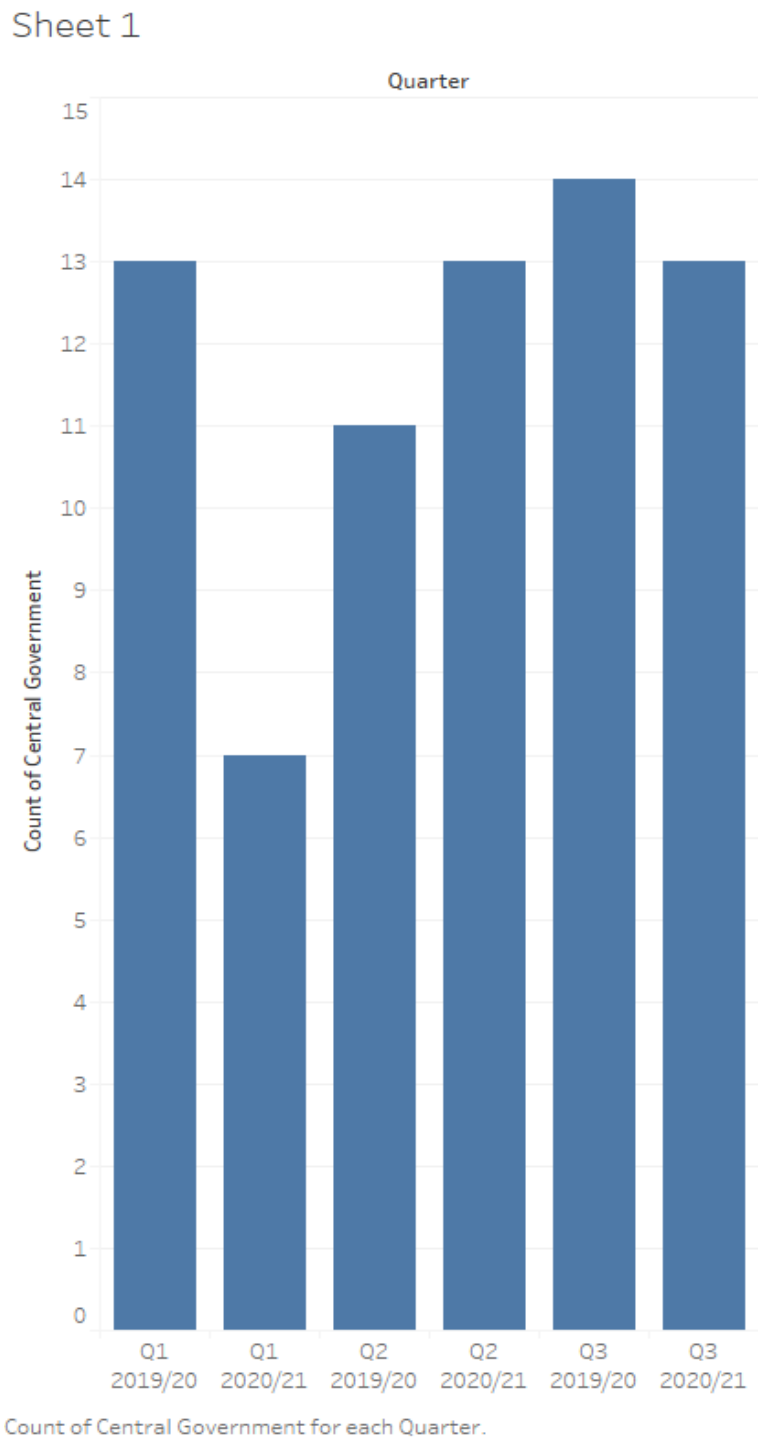

Fig 4. Visualization from Tableau – Number of attacks on the Central / Federal Government by quarter

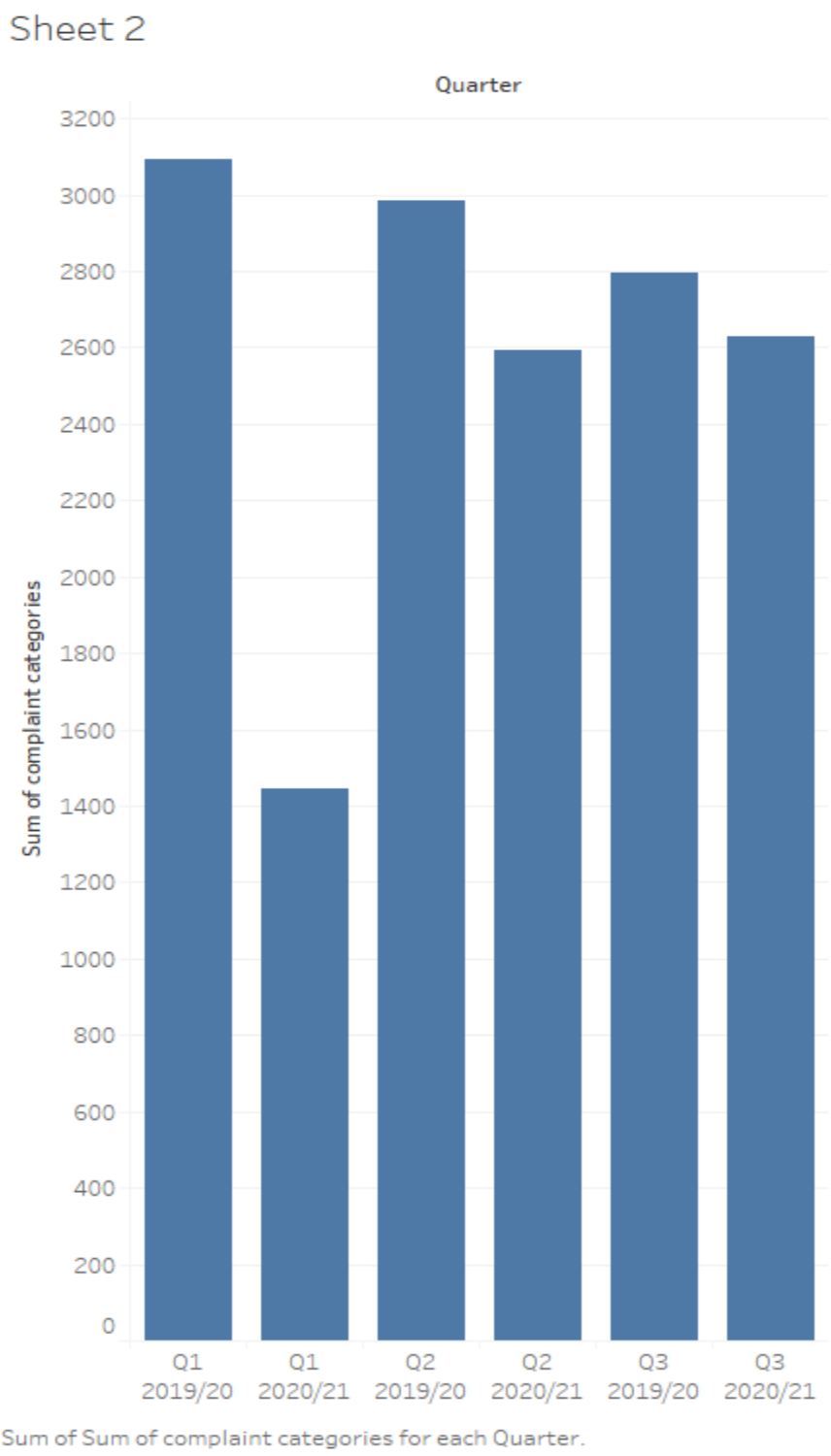

Fig 5. Visualization from Tableau – Total number of cyberattacks by each quarter

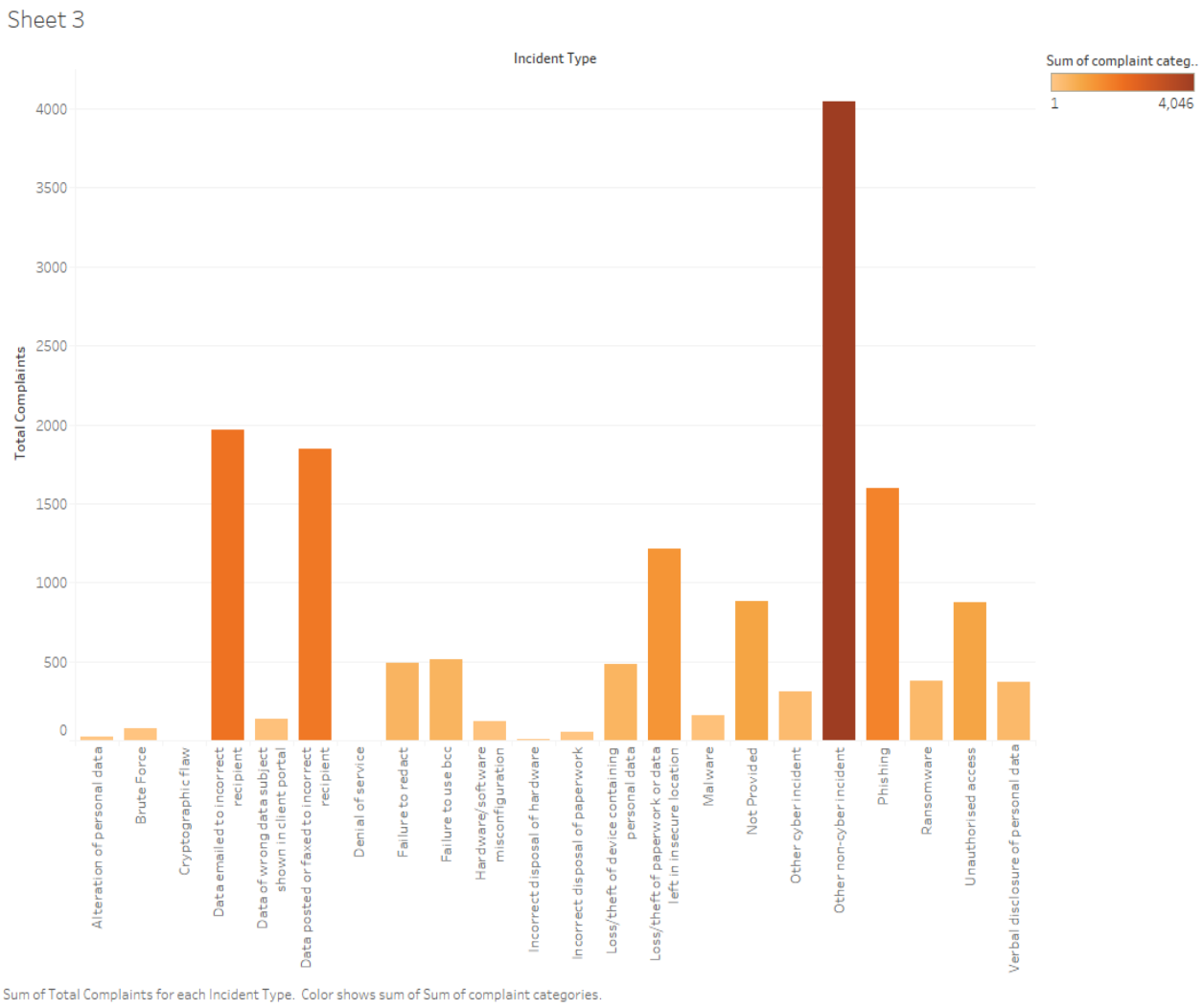

Fig 6. Visualization from Tableau – Total number of complaints for all quarters by category

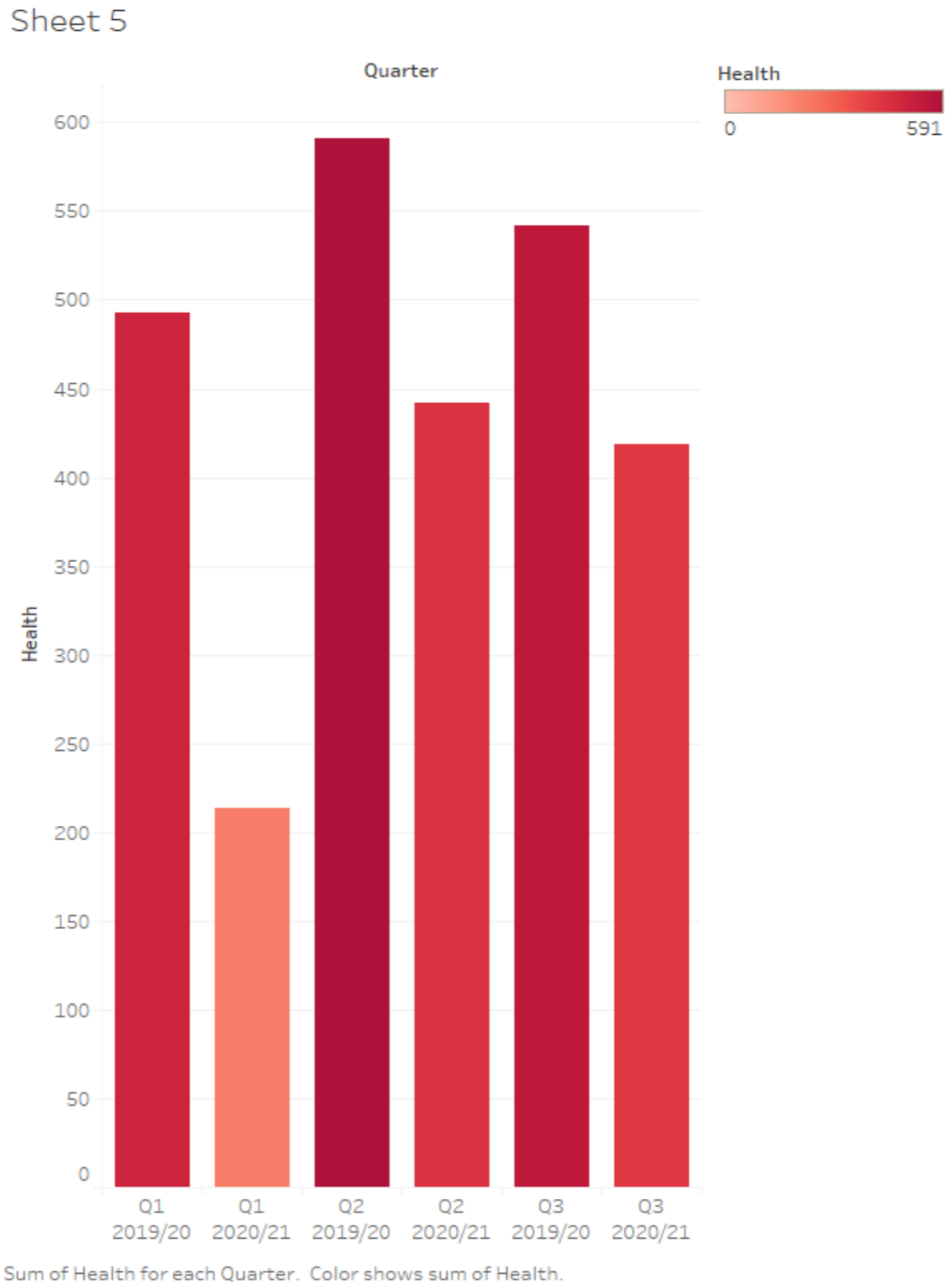

Fig 7: Visualizations from Tableau – Total attacks on healthcare sector by quarter

Monetization

The revenue model for Cluelez is a very simple one. People willing to take the test can take a sample test to see the types of questions and the level of the questions. If they like the sample test, they can buy the product through app store or google play store where they would be given the real questions. This in turn would give the user a certificate of completion if they successfully take the question and give the correct answer which would be decided by the AI. Another way of earning, would be through advertisments, where the user would be given with advertisments when the user gives a sample text. Based on the result provided for a particular user, the AI would assess the strong and weak points of the user. The application would then recommend the particular user to a third party's (Udemy, Coursera, YouTube) platform where they can do a certification which would be hand crafted by us. Every user which decides to undergo this course, would be paying us, thus making it another mode of revenue generation.