**Ideation Phase**

**Defining the Problem Statements**

|  |  |
| --- | --- |
| **Date** | **26-09-2023** |
| **Team ID** | **671** |
| **Project Name** | **Machine Learning Model Deployment using IBM Cloud Watson Studio** |

**Phishing Detection Model Deployment with IBM Watson Studio**

**Problem Definition and Design Thinking**

**Introduction**

Our project revolves around deploying a machine learning model for phishing detection using IBM Cloud Watson Studio. Phishing detection plays a pivotal role in safeguarding digital security by identifying fraudulent and malicious activities. In this document, we will articulate the problem statement, outline the steps to address it, and detail our design thinking approach to guide the project.

**Problem Statement**

Objective: Develop a robust machine learning model deployment pipeline for phishing detection with IBM Cloud Watson Studio.

Data: We possess a dataset comprising various email attributes, URLs, and user behaviors, along with their classification as either phishing or legitimate. This dataset will be instrumental in training and evaluating our machine learning model.

**Key Challenges:**

1. Data Preprocessing: Ensuring the dataset is cleaned, standardized, and free from inconsistencies.

2. Feature Engineering: Identifying and engineering relevant features to enhance model accuracy.

3. Model Selection: Choosing the most suitable machine learning algorithm(s) for effective phishing detection.

4. Model Evaluation: Evaluating the model's performance through relevant metrics.

5. Deployment: Creating a user-friendly interface or API for seamless model utilization by security professionals.

**Design Thinking Approach**

**Empathize:**

Prior to addressing the problem, empathizing with end-users is paramount. Our primary users include cybersecurity experts and IT professionals. Understanding their priorities and how precise phishing detection can empower them is essential.

**Actions:**

- Conduct interviews and surveys with cybersecurity experts to grasp their needs and insights.

- Analyze historical phishing attack data to identify critical patterns and features.

- Collaborate with industry professionals to gain domain-specific knowledge.

**Define:**

Based on insights from the empathy phase, we will define clear objectives and success criteria for our project.

**Objectives:**

- Develop a phishing detection model with a false-positive rate of less than X%.

- Create a user-friendly web application for security professionals to input suspicious emails or URLs for immediate analysis.

**Ideate:**

Brainstorm creative solutions and techniques to tackle the problem. This phase involves exploring various machine learning algorithms and strategies for phishing detection.

**Actions:**

- Experiment with different machine learning algorithms, including decision trees, random forests, and deep learning models.

- Investigate feature selection methods to enhance model precision.

- Consider incorporating threat intelligence feeds for real-time phishing threat updates.

**Prototype**

Develop a prototype of the machine learning model and the user interface for phishing detection.

**Actions:**

- Build a Jupyter Notebook or Python script for data preprocessing, model training, and evaluation.

- Create a user-friendly web interface using tools like Flask or Django to allow users to submit email or URL data for analysis.

- Test the prototype with a subset of the dataset to verify it meets performance objectives.

**Test**

Evaluate the model's performance using relevant metrics and gather feedback from users.

**Actions:**

- Split the dataset into training and testing sets.

- Train the model on the training set and evaluate it on the testing set.

- Utilize metrics like accuracy, precision, recall, and F1-score to assess model performance.

- Collect user feedback on the web interface for usability and effectiveness.

**Implement**

Once the prototype aligns with the defined objectives and garners positive feedback, proceed with full implementation.

**Actions:**

- Train the final machine learning model using the complete dataset.

- Deploy the model within a production-ready web application.

- Execute rigorous testing to ensure the application's resilience and ease of use.

**Iterate**

Continuously gather user feedback and iterate on the model and interface to improve accuracy and user experience.

**Actions:**

- Monitor the model's performance and update it as new phishing threats emerge.

- Address user feedback promptly and make necessary enhancements to the web interface.

- Stay informed about advancements in cybersecurity and phishing detection for potential improvements.

**Conclusion**

In this document, we've presented our approach to solving the challenge of deploying a phishing detection machine learning model using IBM Cloud Watson Studio. We've defined the problem, identified key challenges, and introduced a design thinking approach that includes empathizing with users, defining objectives, ideating potential solutions, prototyping, testing, implementing, and iterating.

Our ultimate aim is to deliver an accurate and user-friendly solution that bolsters cybersecurity efforts by identifying phishing threats effectively. By following this structured approach, we endeavor to create a valuable tool that enhances digital security for organizations and individuals.