Workshop: Using ChatGPT in Cyber Defense

Objective: This workshop provides a practical guide to building a phishing email and social engineering detection system using ChatGPT. Attendees will learn how to set up the environment, collect data, preprocess it, and perform live coding demonstrations to enhance threat detection capabilities.

Step 1: Environment Setup

1. Open a web browser and navigate to chat.openai.com.

2. Log in to the OpenAI platform using your credentials.

Step 2: Obtain the Transfer Model

1. Once logged in, navigate to the ChatGPT section.

2. Look for the option to obtain the transfer model specifically designed for detecting phishing emails.

Step 3: Collecting Phishing Email Data

1. Provide attendees with a sample dataset of phishing emails. This dataset can be obtained from various sources or created for demonstration purposes.

2. Explain the importance of a diverse and representative dataset for training the detection model.

Step 4: Preprocessing Data

1. Demonstrate how to preprocess the collected data to make it suitable for training.

2. Show how to clean and tokenize the text, handle missing values, and perform any necessary feature engineering.

Step 5: Basic Phishing Email Detection

1. Enter a sample phishing email in user prompt.

2. Demonstrate a basic implementation where the detection system checks if the entered text contains known phishing keywords.

Step 6: Addressing Vulnerabilities

1. Discuss common vulnerabilities in the basic phishing email detection system.

2. Provide guidance on how to address these vulnerabilities to improve accuracy and reliability.