

Université de la Manouba
Ecole Nationale Des Sciences De L'informatique



**Cahier des charges du Projet de Conception et de
Développement**

Sujet

Assistant intelligent de cybersécurité

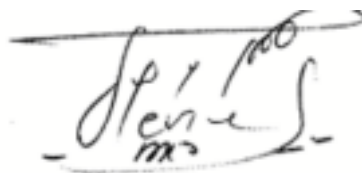
Réalisé par

Jammeli Yasmine

Ben Rejeb Oumeyma

Encadré par

Madame Beji Feriel



1. Introduction

Certainement, la cybersécurité se pose comme une préoccupation primordiale dans le paysage technologique en constante évolution d'aujourd'hui. Des menaces conventionnelles telles que la compromission des courriels professionnels (BEC), les menaces internes et le phishing évoluent, soutenues par l'intelligence artificielle (IA). L'utilisation de Large Language Models (LLMs) pour élaborer des courriels de phishing a atteint un niveau de sophistication où distinguer entre un message authentique d'un collègue et une tentative malveillante devient une tâche exceptionnellement difficile lors de l'infiltration du réseau d'une entreprise. Alors, pourquoi ne pas exploiter cette capacité pour renforcer activement nos défenses ?

Le projet consiste à développer un assistant intelligent en cybersécurité pouvant être intégré de manière fluide au sein des start-ups. Cet assistant vise à protéger les employés contre les courriels de phishing et à accroître la sensibilisation aux menaces de cybersécurité.

2. Travail demandé

2.1. Acteurs

Nous avons 2 types d'acteurs principaux :

- Admin : La start-up qui vise à protéger ses employés et son business éventuellement.
- User : L'employé qui interagit avec l'assistant en exploitant les fonctionnalités du système pour la gestion des menaces en temps réel.

2.2. Besoins fonctionnels

- Authentification de l'utilisateur :
 - Objectif : Assurer un accès sécurisé à l'application. –
 - Exigences :
 - * Authentification à deux facteurs pour une sécurité renforcée.
 - * Politiques de mot de passe pour des mots de passe d'utilisateur forts et uniques.
- Gestion de compte :
 - Objectif : Rationaliser les tâches administratives liées aux comptes utilisateurs.
 - Exigences : Interface d'inscription et de création de compte utilisateur.
- Détection de phishing :
 - Objectif : Détecter et prévenir les attaques de phishing.
 - Exigences :
 - * Intégration avec des modèles d'apprentissage automatique pour une analyse avancée des menaces.
 - * Mises à jour régulières et formation des modèles pour les menaces en évolution.

- Intégration de chatbot :
 - Objectif : Améliorer l'interaction utilisateur et la récupération d'informations.
 - Exigences :
 - * Intégration transparente de chatbots d'IA pour les requêtes de sécurité.
 - * Compréhension du langage naturel pour une communication efficace.
- Tableau de bord et Rapports :
 - Objectif : Fournir des informations sur les activités du système.
 - Exigences :
 - * Tableau de bord convivial affichant l'état de sécurité en temps réel.
 - * Rapports personnalisables sur les activités des utilisateurs et les tendances des menaces.

2.3. Besoins non fonctionnels

- Convivialité :
 - Objectif : Garantir que la solution soit facile à utiliser et à comprendre.
 - Exigences :
 - * Interfaces utilisateur intuitives pour les administrateurs et les utilisateurs normaux.
 - * Formation des utilisateurs et documentation de support.
- Accessibilité :
 - Objectif : Rendre la solution accessible à des utilisateurs divers.
 - Exigences :
 - * Compatibilité avec différents appareils et navigateurs.
 - * Support pour des utilisateurs ayant des niveaux de compétence technique variés.
- Rentabilité :
 - Objectif : Équilibrer les mesures de sécurité avec les considérations de coût.
 - Exigences :
 - * Stratégies de mise en œuvre rentables.
 - * Options de mise à l'échelle en fonction des besoins organisationnels.

2.4. Besoins du domaine

Le développement de notre système s'appuie sur une solide infrastructure de cybersécurité, mettant particulièrement l'accent sur la détection des attaques de phishing par courrier électronique. Pour assurer une expérience utilisateur fluide avec notre chatbot, l'intégration d'un Large Language Model (LLM) est indispensable. De plus, l'incorporation du Machine Learning (ML) demeure cruciale pour une détection proactive des menaces.

En résumé, nos principaux prérequis englobent la sécurité informatique, la détection du phishing, l'utilisation de LLM, ainsi que l'intégration de ML. Ces éléments forment la base essentielle de notre assistant intelligent.

3. Environnements du travail

Listez tous les matériels et les outils que vous allez utiliser :

3.1. Environnement Matériel

- PC 1 :
 - Marque: ASUS,
 - Processeur: 11th Gen Intel(R) Core(TM) i7-1165G7
 - Mémoire RAM : 24 GO,
 - Type du système: Système d'exploitation 64 bits, processeur x64,
 - Système d'exploitation : Windows 11 Professionnel.
- PC 2:
 - Marque: HP,
 - Processeur: Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
 - Mémoire RAM : 12.0 Go
 - Type du système: Système d'exploitation 64 bits, processeur x64,
 - Système d'exploitation : Windows 10 Professionnel.

3.2. Environnement Logiciel

- Langages de programmation
 - Python
 - HTML, CSS, JS
- Bibliothèques particulières et frameworks
 - Docker
 - Flask
 - Numpy
 - Tensor flow
- Environnements de développement intégré
 - Visual Studio Code
 - Jupyter
- Outil pour mesures et reporting
 - StarUML
 - Overleaf

4. Chronogramme prévisionnel du projet

Le projet se déroule pendant une durée de 4 mois et s'étend sur la période entre les mois de Février et Mai. La figure suivante illustre un planning prévisionnel, représentant les étapes principales permettant d'aboutir à une solution fonctionnelle répondant aux critères définis par le présent cahier des charges.

Mois	Février				Mars				Avril				Mai	
Semaine	1	2	3	4	1	2	3	4	1	2	3	4	1	
Documentation et familiarisation avec les outils de travail														
Analyse et spécification des besoins														
Conception														
Implémentation														
Tests et intégration														
Rédaction du rapport														