HACKATHON-ENSET-2024

Thème : L'IA au Service de la Cybersécurité

Sujet : "Intelligence Artificielle contre les Cyber-Menaces : Vers une Détection Parfaite du Phishing"

Description

Ce challenge propose de développer un système automatisé utilisant l'intelligence artificielle pour détecter les e-mails et sites de phishing, tout en alertant les utilisateurs en temps réel. Les participants devront créer une solution capable d'analyser les e-mails entrants et les URL afin d'identifier les signes de phishing, tels que les liens suspects, les pièces jointes malveillantes et le texte trompeur, en utilisant des techniques de machine learning.

I. Problématique

La montée en puissance des cyber-attaques, en particulier le phishing, menace la sécurité des informations personnelles et des actifs organisationnels. Comment l'intelligence artificielle peut-elle être exploitée pour identifier et neutraliser ces menaces de manière proactive et efficace ?

II. Objectifs

1. Développement d'un modèle d'IA : Créer un modèle d'intelligence artificielle capable de détecter les tentatives de phishing avec une précision élevée.

2. Interface utilisateur : Concevoir une interface intuitive pour visualiser et interagir avec les données de détection.

3. Rapidité et efficacité : Garantir que la solution est rapide et fonctionne en temps réel pour contrer les attaques.

III. Fonctionnalités de la solution

1. Détection en temps réel : Analyse continuelle des e-mails et des sites web pour identifier les signaux de phishing.

2. Apprentissage automatique : Adaptation du système en fonction des nouvelles techniques de phishing identifiées.

3. Tableau de bord interactif : Visualisation des alertes de sécurité, des statistiques de détection, et gestion des fausses alertes.

4. Rapports détaillés : Génération automatique de rapports décrivant les tentatives de phishing détectées et les actions prises.

IV. Les livrables

Les livrables doivent être déposés dans la Classroom avec les liens vers les dépôts GitHub.

https://classroom.google.com/c/NjgzODc5NDAzOTEy?cjc=t2frsvg

1. Code source : Ensemble complet du code développé pendant le hackathon.

2. Documentation : Explication des choix technologiques, architecture du système, et guide utilisateur.

3. Démo du produit : Prototype fonctionnel de la solution avec une démonstration de la détection de phishing.

4. Présentation finale : Support de présentation résumant le travail réalisé, les résultats obtenus, et les perspectives d'amélioration.

V. Présentation

Chaque équipe disposera de 8 minutes pour présenter leur solution devant un jury. La présentation devra inclure :

1. Introduction : Brève description du problème et de la solution proposée.

2. Démonstration : Montrez comment votre solution fonctionne avec des exemples concrets.

3. Résultats : Mettez en avant les performances de votre modèle et les bénéfices de votre interface utilisateur.

4. Conclusion : Récapitulez les points forts de votre projet et discutez des améliorations futures possibles.

Notes pour les participants

Technologies recommandées : Python, TensorFlow, Keras, scikit-learn, Flask/Django pour l'interface web.

Sources de données : Utilisation de bases de données publiques de phishing (par exemple, OpenPhish, PhishTank, kaggle) pour l'entraînement des modèles.

Critères d'évaluation : Précision du modèle, convivialité de l'interface utilisateur, innovation dans l'approche, qualité de la présentation finale.

Bonne chance à toutes les équipes et que le meilleur projet gagne !