Faculté des Sciences

Descriptif du projet

Sujet :
Développement d'une plateforme capable de détecter les cyberattaques, les prédire, et y répondre en temps réel.

Membre d'équipe : Fatna ERRAMLI
Hiba ECHCHIA
Naoual KHELLOUFI
Hamza BOUGHANIME
Mohammed Imrane GRICHE

2024 - 2025

Fonctionnalités du système :

- Détection et prédiction d'attaques (intrusion, phishing, malware, etc.)
- Réponse automatique aux attaques (bloquer des IPs, activer des firewalls, etc.)
- Chatbot capable de résoudre des problèmes de cybersécurité et donner des conseils aux utilisateurs.
- Interface utilisateur via texte, parole, et images.

Architecture du projet :

- Frontend : Développer l'interface utilisateur avec React pour le frontend et Bootstrap pour la conception responsive.
- Backend : Utiliser Node.js (ou Express.js) pour le backend afin de gérer la logique des interactions avec le système.
- Base de données NoSQL : Utiliser MongoDB pour stocker les données, telles que les journaux d'attaques, les interactions utilisateur avec le chatbot, et les réponses automatiques.
- IA et sécurité :
  -Utilisation de NLP pour l'analyse des textes et les prédictions d'attaques.
  -Utilisation de Computer Vision pour analyser des images (comme la détection d'attaques à partir d'images de journaux ou captures d'écran).
  -Modèles de deep learning pour la détection des anomalies dans le réseau.

Étapes de création du projet :

- **Étape 1 :** Mise en place de l'infrastructure
  -Créez le projet React pour le frontend et intégrez Bootstrap pour le design.
  -Configurez le backend en utilisant Node.js et connectez-le à une base de données MongoDB (NoSQL).
- **Étape 2 :** Détection et prédiction d'attaques
  - NLP pour la détection d'attaques :

Collectez des données sur des attaques de cybersécurité (e.g. attaques par phishing, injections SQL) pour entraîner un modèle de deep learning.
Utilisez un modèle de classification NLP (par exemple BERT, GPT ou RNN) pour détecter et prédire les attaques à partir des logs de sécurité.

Exemple GitHub - Cybersecurity Attack Detection with NLP

-Computer Vision pour la détection :

Utilisez Convolutional Neural Networks (CNN) pour analyser les images des journaux (ou captures d'écran d'attaques) et détecter des modèles suspects.
Un modèle comme YOLO ou ResNet peut être utilisé pour la détection d'anomalies visuelles.

Exemple GitHub - Cybersecurity with Computer Vision

- **Étape 3 :** Chatbot multimodal (Texte, Voix, Image)

-Text :

Utilisez des techniques de NLP pour permettre à votre chatbot de répondre aux questions en texte sur les bonnes pratiques en cybersécurité ou la résolution d'incidents.

Un modèle pré-entraîné comme Dialogflow ou Rasa peut être utilisé pour développer des réponses contextuelles intelligentes.

Exemple GitHub - Cybersecurity Chatbot

- Voix :

Intégrez la reconnaissance vocale (comme Google Speech-to-Text API ou DeepSpeech) pour permettre à l'utilisateur de communiquer par voix.

Utilisez des frameworks comme TensorFlow pour traiter la parole et transformer en texte pour analyse.

-Image :

Utilisez Computer Vision (avec un modèle de CNN comme VGGNet ou YOLO) pour permettre à l'utilisateur de télécharger des images (comme des captures d'écran) que le chatbot peut analyser et donner des retours.

Exemple GitHub - TensorFlow Computer Vision