Cahier des Charges : Système de Détection et de Prévention des Cyberattaques Basé sur l'IA

Contents

1 Contexte et Objectifs

1.1 Contexte

Avec l'augmentation des cyberattaques sophistiquées, les entreprises doivent se doter de solutions avancées pour protéger leurs infrastructures. Ce projet vise à développer un système intelligent capable de :

- Détecter et prévenir les cyberattaques en temps réel.
- Identifier les menaces avancées, y compris les attaques quantiques.
- Offrir des fonctionnalités comparables à celles de Cybereason.

1.2 Objectifs généraux

- Proposer une plateforme intégrant des algorithmes d'IA pour la détection proactive des menaces.
- Incorporer des mécanismes de réponse rapide aux incidents.
- Fournir une interface utilisateur intuitive et détaillée pour l'analyse des menaces.

2 Description Fonctionnelle

2.1 Fonctionnalités principales

1. **Détection des cyberattaques (IDS)**
   - Utilisation de modèles IA basés sur des techniques de Machine Learning (ML) et Deep Learning (DL) pour détecter les comportements anormaux.
   - Identification des attaques classiques (DDoS, ransomware, phishing, etc.) et émergentes.
2. **Prévention des cyberattaques (IPS)**
   - Mécanismes automatiques pour bloquer les menaces identifiées.
   - Gestion des politiques de sécurité pour minimiser les vulnérabilités.
3. **Surveillance continue**
   - Collecte et analyse en temps réel des logs réseau, des endpoints, et des applications.
   - Gestion des alertes avec des niveaux de criticité.
4. **Gestion des incidents et analyse post-mortem**
   - Fonctionnalités d'investigation avancées pour comprendre les attaques passées.
   - Recommandations automatisées pour renforcer la sécurité.
5. **Détection et défense contre les attaques quantiques**

- Intégration d'algorithmes résistants aux attaques basées sur la cryptographie quantique.
- Veille technologique sur les avancées dans le domaine des attaques quantiques.

6. **Autres fonctionnalités**

   - Détection comportementale avancée : Analyse des comportements pour identifier des activités suspectes et anticiper les menaces.
   - Cartographie visuelle des attaques : Une vue graphique interactive montrant les vecteurs d'attaque et leur propagation dans le réseau.
   - Corrélation des événements : Regroupement d'alertes pour détecter des attaques complexes basées sur plusieurs événements disparates.
   - Réponse automatisée : Actions correctives en temps réel comme l'isolation des endpoints compromis ou la suppression de fichiers malveillants.

2.2 Fonctionnalités supplémentaires

- Tableau de bord interactif : Affichage en temps réel des alertes, des indicateurs de performance, et des rapports.
- Compatibilité multi-plateforme : Fonctionnement sur des systèmes Windows, macOS, et Linux.
- Rapports avancés : Génération de rapports détaillés pour les administrateurs et équipes de sécurité.
- Modèle SaaS ou On-Premise : Option d'installation locale ou dans le cloud.

3 Contraintes Techniques

3.1 Technologies utilisées

- **Backend** : Python (Django ou Flask), Java, ou Go.
- **Frontend** : React.js, Angular, ou Vue.js.
- **IA** : Frameworks comme TensorFlow, PyTorch, ou Scikit-learn.
- **Base de données** : PostgreSQL, MongoDB ou Cassandra (pour les grands volumes de données).

3.2 Performance

- Analyse des données en temps réel avec une latence minimale (< 1 seconde).
- Gestion de volumes massifs de données générées par les logs et événements réseau.

3.3 Interopérabilité

- Intégration avec des solutions tierces (SIEM, SOC).
- API REST pour permettre une extensibilité et une intégration dans des environnements existants.

3.4 Sécurité

- Chiffrement : Utilisation de SSL/TLS pour toutes les communications.
- Authentification multi-facteurs (MFA) : Sécurisation des accès.