

RUSSIA

Thibault Ferrand

thibault.p.ferrand@protonmail.com

Sujet : Conception d'un Assistant RSSI Virtuel basé sur un LLM

Contexte

Les Responsables de la Sécurité des Systèmes d'Information (RSSI) doivent gérer un volume croissant d'informations, de risques et de réglementations. Un assistant virtuel intelligent, basé sur un Large Language Model (LLM), pourrait faciliter leur travail en automatisant certaines tâches, en fournissant des réponses aux questions de conformité et en aidant à la gestion des incidents de cybersécurité.

Objectifs

Développer un assistant RSSI virtuel capable de :

- Répondre aux questions sur les normes et réglementations en cybersécurité (ISO 27001, NIST, RGPD, LPM, etc.).
- Analyser et synthétiser des alertes de cybersécurité.
- Assister dans la rédaction de rapports et de politiques de sécurité.
- Effectuer une veille sur les nouvelles menaces et vulnérabilités.
- Interagir via une interface web ou un chatbot (ex. Slack, Teams, Web UI).

Cahier des charges

1. Architecture

L'assistant devra être conçu avec une architecture modulaire comprenant :

- **Un moteur LLM** (exploitable via API ou modèle open-source affiné sur un corpus spécialisé).
- **Une base de connaissances** contenant des documents de référence (normes, guides, bonnes pratiques).
- **Une interface utilisateur** sous forme de chatbot ou web app.
- **Un module de veille** collectant les dernières alertes CVE et incidents de cybersécurité.
- **Un mécanisme d'auditabilité** pour tracer et vérifier les réponses fournies par l'IA.

2. Contraintes techniques

- Déploiement sur serveur local.
- Utilisation d'un LLM open-source (ex : Llama, Falcon, GPT-J).
- Intégration d'un moteur de recherche documentaire (ex : Elasticsearch).
- Respect des contraintes de confidentialité et de sécurité des données.

3. Fonctionnalités clés

- **FAQ automatisée** sur les bonnes pratiques de cybersécurité.
- **Analyse des alertes** (parsing et résumé d'incidents à partir de sources comme CVE, CERT-FR).
- **Aide à la conformité** (réponses sur ISO 27001, SOC 2, RGPD, etc.).
- **Synthèse de documents** (résumé de rapports de cybersécurité).
- **Personnalisation** en fonction des besoins du RSSI (ajout de documents internes).

Livrables attendus

1. Rapport de conception détaillant :

- L'architecture technique.
- Le choix du modèle LLM et des outils associés.
- Les mécanismes de gestion des données et des logs.

2. Prototype fonctionnel comprenant :

- Un chatbot ou une interface web permettant d'interagir avec l'assistant.
- Une démonstration des fonctionnalités clés.

3. Documentation utilisateur expliquant comment utiliser l'assistant et l'intégrer dans un environnement d'entreprise.

4. Code source et instructions de déploiement sous format Docker ou script d'installation.

5. Rapport final et présentation orale avec démonstration du système.

Critères d'évaluation

- Qualité des réponses fournies par l'assistant.
- Pertinence des sources et capacité d'adaptation aux nouvelles informations.
- Robustesse de l'architecture et respect des contraintes de sécurité.
- Expérience utilisateur et ergonomie de l'interface.
- Documentation claire et exhaustive.