**Projet PFE**

**Titre :** Développement d’un agent IA pour l’automatisation et l’optimisation des processus de sécurité dans SOC.

**Résume :**

Dans un environnement de cybersécurité marqué par une explosion du volume d’alertes à traiter, Les centres de sécurité des opérations (SOC) font face à des défis croissants en matière de réactivité, d’efficacité et de charge de travail. Le traitement manuel des incidents reste lent, répétitif et sujet à l’erreur, ce qui nuit à la détection rapide des menaces critiques. Ce projet propose de développer un agent intelligent basé sur un large language model (LLM), capable d’interagir avec la plateforme TheHive, largement utilisée pour la gestion des incidents de sécurité. En combinant des techniques avancées telles que le prompt engineering, le tool calling, l’architecture ReAct (Reasoning + Acting), ainsi que le Model Context Protocol (MCP), cet agent sera en mesure de comprendre des requêtes en langage naturel, de générer ou d’analyser automatiquement des alertes, et d’agir sur les données en temps réel (ex. : création de tickets, extraction d’indicateurs de compromission, classification des alertes, etc.).

**Mots clés utilisés :**

LLM (Large Language Model), agent, cybersécurité, SOC (Security Operations Center), automatisation des alertes, prompt engineering, tool calling, ReAct (Reasoning and Acting), Model Context Protocol (MCP), gestion des incidents, indicateurs de compromission (IOC), réduction du temps de réponse, assistance intelligente, intégration API.

**Problématique :**

Les centres de sécurité des opérations (SOC) sont confrontés à une surcharge croissante d’alertes de sécurité à traiter, ce qui rend le travail des analystes long, répétitif et vulnérable aux erreurs humaines. Cette pression nuit à la réactivité face aux menaces, complique la priorisation des incidents critiques et freine l’efficacité globale des opérations. Il devient donc nécessaire d’automatiser certaines tâches, tout en gardant une capacité d’analyse fine et adaptée au contexte, pour améliorer la détection, l’investigation et la réponse aux cybermenaces.

**Objectif :**

Développer un agent conversationnel intelligent basé sur un Large Language Model (LLM), capable d’interagir avec les outils d’un Security Operations Center (SOC) tels que TheHive, les SIEM, SOAR, TIP, etc., afin d’automatiser la création, l’analyse et le traitement des alertes de sécurité. Cet agent exploitera des techniques avancées telles que le prompt engineering, le tool calling, l’architecture ReAct (Reasoning + Acting) et le Model Context Protocol (MCP) pour comprendre des requêtes en langage naturel, agir en temps réel sur les données de sécurité, améliorer la productivité des analystes, réduire le temps de réponse aux incidents et renforcer la fiabilité des opérations.