COMPTE RENDU PING 56

3e réunion des membres du groupe

Informations générales :

Date de la réunion : 20/11/2025 08h30-11h **Lieu de la réunion** : En présentiel (D1-254)
Personnes présentes : • Eunice LOKOSSOU (CERT), cheffe de projet • Julie GOUR (CERT), membre du groupe • Ilyas DAOUDA (CERT), membre du groupe • Rizkiath KOUNOU (BDTN), membre du groupe • Kenan AKLE (BDTN), membre du groupe • Julien TANG (IF), membre du groupe
Ordre du jour : • Choisir collectivement l'architecture et les outils nécessaires à la mise en place de l'environnement technique du projet • Organiser le travail technique à venir, en répartissant les tâches liées à cette architecture ainsi que celles relatives à la rédaction du document de spécification.

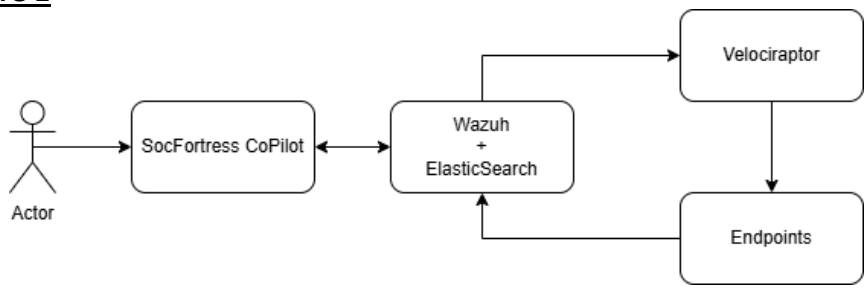
Sujets de la rencontre :

Sujet : Choisir collectivement l'architecture et les outils nécessaire à la mise en place de l'environnement technique

Résumé de la discussion :

Cette première réunion a porté sur le choix de l'architecture du projet. De ce fait, trois architectures ont été proposées.

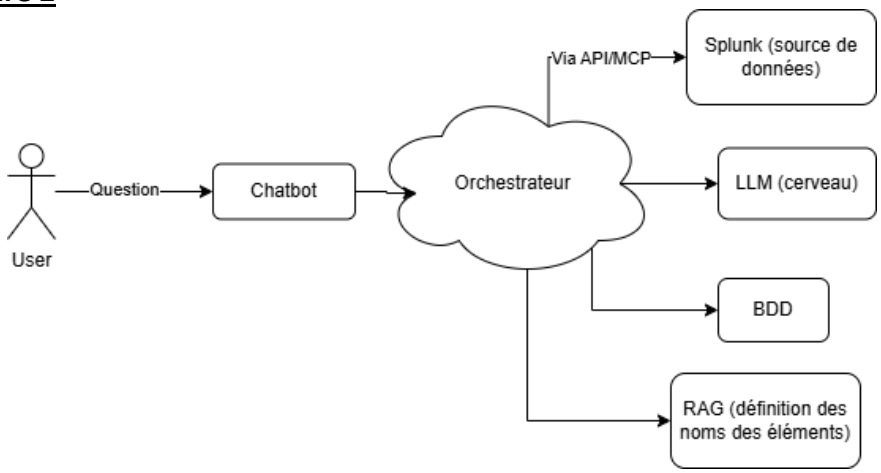
1. **Architecture 1**



Cette architecture se base sur l'utilisation d'outils open-source : **SocFortress CoPilot**, **Wazuh & ElasticSearch** ainsi que **Velociraptor** pour le côté agent.
D'abord, SocFortress CoPilot est une plateforme pouvant unifier plusieurs outils de sécurité en une interface centralisée, notamment via des connecteurs. De plus, l'outil intègre déjà un agent IA qui permet de poser des questions en langage naturel.
Ensuite, Wazuh est le SIEM dans cette architecture, avec un module d'indexation et de

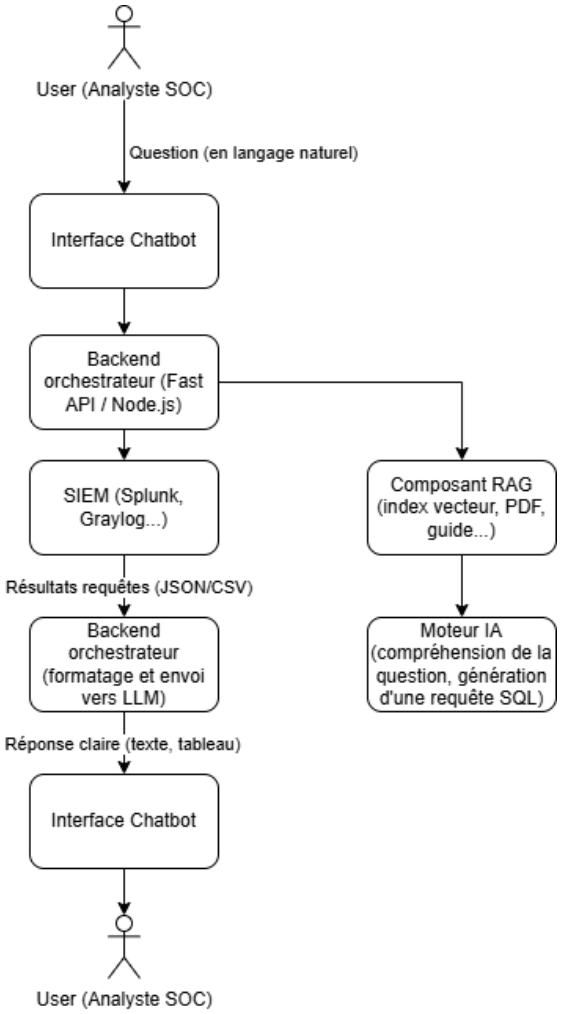
recherche basé sur ElasticSearch.
Enfin, Velociraptor est un outil open-source de forensique et réponse à incident qui servira de complément à Wazuh par exemple pour investiguer un endpoint en cas d'alerte.

2. Architecture 2



Cette deuxième architecture proposée place l'orchestrateur au centre du fonctionnement de l'agent IA car pilotant tous les autres composant.
En gros, lorsque qu'un utilisateur formule un prompt en langage naturel via le chatbot, sa demande est transmise à l'orchestrateur qui s'occupe du traitement.

3. Architecture 3



Cette troisième architecture est similaire à la première mais plus détaillée.

Choix d'architecture

Tout d'abord, nous avons éliminé l'architecture 1 car elle ne correspond pas à notre use case (le SIEM est différent) et l'utilisation d'un agent IA tout fait enlève un plan technique conséquent au projet.
Nous partirons donc sur l'architecture 3, car elle est la même que la 2 mais plus détaillée.

Choix d'orchestrateur

Vu que nous avons choisi l'architecture 3 qui s'axe autour de l'orchestrateur, le choix de l'orchestrateur est une étape plus qu'importante.
Après des recherches sur le sujet, nous avons sélectionné trois outils : n8n, make et LangChain. Ces outils sont, classés dans cet ordre, du plus user-friendly au moins.
Par ailleurs, il est possible de combiner n8n et LangChain, pour jumeler le côté graphique de n8n à la modularité de LangChain. C'est d'ailleurs ce que nous avons décidé de faire.

Autres points clarifiés

- La version gratuite de Splunk sera suffisante pour le projet. Elle permet de collecter 500 Mo de données par jour (environ 50000 logs), ce qui est largement suffisant pour nous.
- Notre BDD servira aussi de journalisation. Elle enregistra l'historique des conversations dans un premier temps du projet, puis les actions effectuées (en tant qu'agent) pour pouvoir effectuer de nouveau ces actions au besoin sans avoir à resuivre tout le processus de réflexion.
- Nous aurons aussi des comptes utilisateurs, de sorte à ce que chaque utilisateur ait ses propres conversations.

Sujet : Organiser le travail technique à venir, en répartissant les tâches liées à cette architecture ainsi que celles relatives à la rédaction du document de spécification

Travail commun :

• Commencer la rédaction du PowerPoint en vue de la prochaine réunion binôme
• Rédiger le document de spécifications
• Se former sur les notions et technologies de l'architecture

Travail individuel :

- **Julie, Rizkiath** : Rédaction du rapport du document de spécifications avant le 03/12/2025
- **Eunice :** Planifier une réunion avec le client pour le 05/12/2025
- **Ilyas, Kenan, Julien :** Se former sur les notions et technologies de l'architecture pour en avoir une compréhension approfondie