Justification des choix techniques :

1. MISP :

- MISP est une plateforme open source dédiée au partage d'informations sur les menaces, permettant aux organisations de collecter, stocker, partager et analyser des données relatives aux incidents de cybersécurité

- Intégration avec d'autres outils : MISP peut facilement s'intégrer avec d'autres outils de sécurité via son API, ce qui nous permet d'automatiser des processus de sécurité

2. Suricata :

- Détection d'intrusion : Suricata est un système de détection d'intrusion (IDS) qui offre une analyse en temps réel du trafic réseau, permettant de détecter et de bloquer les menaces potentielles sur un réseau. En intégrant Suricata avec MISP, il est possible de générer dynamiquement des règles de blocage d'adresses IP identifiées comme malveillantes, ce qui renforce ainsi la défense du réseau contre les attaques

- Performance et flexibilité : Suricata est connu pour sa performance élevée, tout en permettant à l'utilisateur de la flexibilité dans la création de règles de détection

3. Wazuh :

- Surveillance et gestion des ressources : Wazuh est une plateforme de sécurité open-source qui offre du monitoring de ressource, de la détection des intrusions et de la gestion des vulnérabilités. Elle collecte et analyse les logs, détecte les anomalies et génère des alertes, permettant une réponse rapide aux incidents

- Intégration avec d'autres outils : Wazuh peut être intégré avec d'autres outils de sécurité pour donner une vue plus globale du réseau, par exemple avec Slack avec accès au réseau extérieur pour envoyer des alertes en temps réel et permettre une communication instantanée

- Dashboard : Le tableau de bord de Wazuh permet une visualisation en temps réel des alertes et des ressources, facilitant ainsi la prise de décision rapide

4. Slack :

- Communication en temps réel : L'intégration de Slack avec Wazuh, nous permet d'envoyé des alertes en temps réel, pour une communication facile et rapide avec tous les membres du projet

- Facile à mettre en place : la mise en place du service Slack était rapide et simple

- Mise en place de différents canaux : les canaux nous permettent de gérer l'informations qui doit y être (ex : canal alerts-soc → toutes les alertes soc …)

5. Architecture globale :

- Centralisation des informations : En hébergeant le MISP et l'agent Wazuh (pas le manager) dans Suricata, nous centralisons les informations de sécurité, facilitant ainsi leur corrélation et leur analyse

- Scalabilité et évolutivité : L'architecture choisie permet d'ajouter de nouvelles sources de données ou de nouveaux outils de sécurité, assurant ainsi l'évolutivité du système