**Rapport de Projet : Étape 3 - Supervision**

1. **Métriques de Qualité :**

1.1 *Sécurité* :

Mesure la résistance du système aux menaces externes et internes. Inclut la conformité aux normes de sécurité, l'efficacité des pare-feux et la gestion des identités et des accès pour assurer une protection optimale contre les attaques potentielles.

1.2 *Évolutivité*  :

Évalue la capacité du système à maintenir ses performances lorsqu'il est agrandi pour supporter une croissance future. La capacité à évoluer sans compromettre la qualité du service est essentielle pour garantir une expérience utilisateur constante.

1.3 *Maintenabilité* :

Mesure la facilité avec laquelle le système peut être maintenu, réparé et amélioré. Cela inclut la clarté du code, la documentation précise et la facilité de mise à jour, éléments essentiels pour une gestion efficace à long terme du système.

*1.4 Taux de Disponibilité du Système* :

Mesure le temps pendant lequel le système est opérationnel et accessible pour les utilisateurs. Un haut taux de disponibilité garantit un accès continu aux fonctionnalités, minimisant ainsi les interruptions et assurant une expérience utilisateur fluide.

*1.5 Expérience Utilisateur* :

Comprend les évaluations des utilisateurs, le taux de satisfaction et les retours d'expérience. Ces métriques captent directement la perception des utilisateurs, offrant une indication précieuse sur la convivialité, la pertinence et la qualité du système du point de vue de l'utilisateur.

Ces mesures permettent d'évaluer non seulement la sécurité, mais également la disponibilité, les performances,l’évolutivité, et l'expérience utilisateur, garantissant ainsi un système robuste, réactif et conforme aux attentes des utilisateurs.

1. **Menaces de Sécurité :**

2.1 *Injection SQL* :

L'injection SQL, c'est un peu comme si un pirate informatique rusé parvenait à s'infiltrer dans une application web en introduisant des codes SQL interdits. Une fois à l'intérieur, il peut causer des ravages en compromettant, manipulant, voire supprimant des données, mettant ainsi en péril la sécurité et l'intégrité du système. C'est un genre de cambriolage numérique qu'on n'apprécie vraiment pas.

2.2 *Hijacking de Session* :

Le hijacking de session, c'est un peu comme si un intrus s'invitait à votre soirée privée en ligne. Il prend le contrôle de votre session utilisateur, se glissant dans votre identité pour mener des actions louches à votre insu.

2.3 *Attaques de l'Homme du Milieu (Man-in-the-Middle)* :

Imaginez une conversation en ligne entre deux personnes. Maintenant, ajoutez à cette scène un individu indésirable qui se faufile secrètement entre elles. Il écoute, manipule et peut même altérer la conversation sans que personne ne le sache. C'est un peu comme si quelqu'un se mêlait de vos affaires sans permission.

2.4 *Exfiltration de Données* :

L'exfiltration de données, c'est comme le cambriolage numérique où des informations confidentielles sont volées et sortent du système sans permission. C'est un peu comme si quelqu'un emportait des secrets dans l'ombre, mettant en danger la confidentialité et l'intégrité des informations. Pas vraiment sympa.

1. **Se Protéger des Menaces :**

3.1 *Prévention et Détection des Attaques* :

Hijacking de Session : Nous paramétrons Security Onion pour détecter les comportements d'authentification anormaux ou les tentatives d'accès non autorisées, renforçant ainsi notre prévention du hijacking de session.

3.2 *Attaques de l'Homme du Milieu (Man-in-the-Middle)* : Nous utilisons les capacités d'inspection du trafic de Security Onion pour détecter les anomalies dans les communications réseau, signalant potentiellement une attaque de l'homme du milieu, renforçant ainsi notre détection précoce de ces attaques.

3.3 *Exfiltration de Données* : Nous paramétrons Security Onion pour surveiller les flux de données sortants et détecter les modèles de transfert inhabituels ou non autorisés, renforçant ainsi notre détection de l'exfiltration de données.

Cette approche intégrée, utilisant Security Onion, assure une surveillance proactive des menaces de sécurité tout en tenant compte des métriques de qualité. Cette combinaison garantit notre résilience et notre robustesse, renforçant ainsi notre capacité à détecter, prévenir et répondre efficacement aux menaces actuelles et émergentes.

Dans le cadre des contraintes de temps, notre engagement envers la sécurité demeure prioritaire. Malgré le délai serré, notre équipe est pleinement investie dans l'amélioration de la robustesse et de la sécurité de notre solution. Nous restons déterminés à protéger les données et le réseau entier en mettant en place des mesures visant à renforcer la sécurité informatique en passant par la procédure suivante : Détecter → Alerter → Agir .