Livrable 7: Rapport de synthèse

La réalisation de la plateforme prédictive sécurisée pour l'usine Benin Moto Industry (BMI) s'est articulée autour d'une approche de **Défense en Profondeur (Defense in Depth)**. Plutôt que de s'appuyer sur une seule barrière de sécurité, notre groupe a interconnecté plusieurs couches de protection indépendantes :

1. **Sécurité Périmétrique et Accès (Livrable 1 & 3) :** Le système vérifie de manière stricte l'identité de chaque acteur via une authentification forte (MFA, JWT rotatifs) couplée à un moteur de règles granulaire (Casbin). Un opérateur ne peut mathématiquement pas accéder aux privilèges d'un administrateur, limitant ainsi la surface d'attaque interne.
2. **Confidentialité des Flux et du Stockage (Livrable 2) :** L'encapsulation du réseau dans un tunnel VPN (Tailscale), le chiffrement des bases de données (AES-256 via pgcrypto) et la sécurisation des communications (TLS 1.3) garantissent la protection contre l'espionnage industriel et limitent l'impact d'un potentiel Ransomware.
3. **Protection du Noyau IA (Livrable 4) :** Le modèle de Machine Learning, cœur de la propriété intellectuelle de BMI, a été blindé contre les attaques spécifiques à l'IA. L'utilisation d'algorithmes de détection d'anomalies (Isolation Forest), de limitation de débit (Rate Limiting) et de bruitage mathématique (Confidentialité Différentielle) empêche l'empoisonnement des données et l'extraction du modèle par des concurrents.
4. **Validation Offensive (Livrable 5) :** La robustesse de cette architecture a été éprouvée par un audit Red Team rigoureux, basé sur les standards internationaux **OWASP Top 10 2025** et **OWASP Machine Learning 2023**. Les vulnérabilités identifiées ont immédiatement fait l'objet de remédiations au niveau du code et de la configuration.

La synergie de ces livrables démontre qu'il est possible de concilier l'hyper-connectivité de l'Industrie 4.0 avec un niveau de sécurité maximal.