Corrigé Activité P1C5

Voici comment vous pourriez structurer votre *Executive Summary* pour allier vision stratégique et pragmatisme opérationnel :

- **1. Justification de l'approche (Optimum visé)**
  - Face aux trois risques critiques de notre analyse EBIOS RM (Usurpation admin, Fuites SaaS, Mouvements latéraux), le modèle traditionnel de défense périmétrique est caduc. Notre stratégie vise un optimum opérationnel en imposant immédiatement l'Identité comme nouveau périmètre exclusif, appliquant ainsi les principes de vérification explicite du Zero Trust.
- **2. Mesures immédiates (Priorités Trimestre 1 - Exigences MUST)**
  - *Action 1* : Déploiement obligatoire du MFA FIDO2 pour 100% des accès Administrateurs et VIP (Couvre le risque d'usurpation).
  - *Action 2* : Configuration de règles strictes (*Deny All*) sur les Network Security Groups (NSG) de nos environnements Cloud IaaS (Couvre l'exposition des services).
  - *Action 3* : Interconnexion de notre application CRM Cloud au SSO central avec accès conditionnel vérifiant la conformité du poste (Couvre le risque SaaS).
- **3. Mesures à venir (Chantier différé à N+1)**
  - *Chantier différé* : La micro-segmentation dynamique complète de notre réseau local On-premise.
  - *Justification* : Cette étape du modèle de maturité (stade Avancé) nécessite un prérequis critique que nous n'avons pas : une cartographie exhaustive et validée de nos flux applicatifs hérités. Un déploiement immédiat risquerait de bloquer la production métier.
- **4. Stratégie d'ajustement (Veille)**
  - *Mise en œuvre* : Revue trimestrielle de la feuille de route appuyée sur la fonction *Govern* du NIST CSF. La veille sera alimentée par les bulletins du CERT-FR ciblant spécifiquement les méthodes de contournement d'identités Cloud, permettant d'ajuster nos règles d'accès conditionnel en temps réel.