Corrigé Activité P1C3

Voici une politique prescriptive que vous pourriez formuler à votre équipe IAM pour intégrer les principes Zero Trust. Ce document illustre parfaitement votre rôle de pilote exigeant des résultats :

1. **Exigences d'Authentification (MFA)** :
    - **Utilisateurs standards** : MFA obligatoire pour tout accès distant, avec une tolérance pour les applications d'authentification sur smartphone. Le SMS est formellement interdit.
    - **Admins et VIP** : Application immédiate du niveau AAL3 du NIST. L'authentification doit se faire par un MFA résistant au phishing (FIDO2 ou carte à puce) en raison de la criticité de leurs accès et des données qu'ils manipulent.
2. **Règles d'Accès Conditionnel** :
    - L'évaluation du contexte de connexion est obligatoire pour tous.
    - **Exigence de conformité** : Blocage systématique de l'accès si l'appareil (ordinateur ou smartphone) n'est pas identifié, enregistré et déclaré "conforme" par la politique de sécurité (antivirus à jour, système patché). Le principe est clair : pas d'appareil sain, pas d'accès aux données.
3. **Gestion du moindre privilège et SLA (Service Level Agreement)** :
    - **Accès JIT/JEA** : Les administrateurs n'ont aucun droit permanent. Ils doivent élever leurs privilèges uniquement en cas de besoin, pour une durée limitée.
    - **Révocation** : En cas de départ d'un collaborateur, désactivation totale des accès dans un délai strict de 4 heures maximum.
    - **Revue des droits** : Une revue trimestrielle obligatoire est imposée pour auditer et nettoyer les droits des populations Admins et VIP.