Corrigé Activité P1C2

Voici une analyse détaillée que vous pourriez présenter à votre DSI pour justifier le passage au Zero Trust :

1. **Risque 1 : Usurpation d'identité d'un administrateur (Spoofing)**

    - **Limite du modèle périmétrique** : La confiance est uniquement liée à la présence sur le réseau interne. Une fois le mot de passe de l'administrateur volé, le pare-feu laisse passer l'attaquant car il considère que tout ce qui vient de l'intérieur (ou d'un VPN) est légitime.
    - **Principe Zero Trust mobilisé** : La vérification explicite de l'identité en continu. Le Zero Trust exige une authentification forte (MFA) dynamique.
        i. Le PDP vérifiera non seulement l'identité, mais aussi le contexte (l'appareil utilisé est-il connu de l'entreprise ? L'heure de connexion est-elle habituelle ?)
        ii. Chaque session sera donc validée via le PEP.
2. **Risque 2 : Accès SaaS non maîtrisé (Fuite de données)**

    - **Limite du modèle périmétrique** : Le pare-feu est aveugle face aux ressources hébergées à l'extérieur. Le périmètre physique ne protège pas les applications Cloud utilisées par des collaborateurs en télétravail depuis leurs réseaux personnels.
    - **Principe Zero Trust mobilisé** : L'identité comme nouveau périmètre et la protection centrée sur la ressource. Le Zero Trust déplace les contrôles de sécurité directement devant la ressource SaaS (via des passerelles logiques ou des intégrations d'identité) et évalue la posture de sécurité du terminal (sain ou compromis) avant d'autoriser l'accès aux données de l'entreprise.

3. **Risque 3 : Mouvement latéral après compromission (Élévation de privilèges)**

    - **Limite du modèle périmétrique** : Le réseau interne est "à plat". Une fois le périmètre franchi (via un *phishing* réussi par exemple et la connexion d'un attaquant au réseau interne wia des identifiants valides), il n'y a plus de cloisons internes. L'attaquant navigue librement d'un poste de travail vers un serveur critique.
    - **Principe Zero Trust mobilisé** : La micro-segmentation et l'application stricte du moindre privilège. Chaque ressource devient un micro-périmètre isolé. L'accès à une application ne donne absolument aucun droit d'accès aux autres applications du réseau, bloquant net la propagation de l'attaquant.