Corrigé Activité P1C3

Pour poser un cadre d'exigence robuste et prévenir 80 % des erreurs de configuration initiales, voici la checklist opérationnelle « Cloud & Serveur » que vous devez transmettre à l'équipe DevOps :

1. **Désactiver le listing des répertoires et modifier tous les mots de passe par défaut :** L'infrastructure NE DOIT exposer aucun compte, paramètre, ou mot de passe par défaut (que ce soit pour le système d'exploitation, les bases de données ou les consoles d'administration). La navigation libre dans l'arborescence des fichiers (directory listing) DOIT être désactivée sur tous les serveurs web pour empêcher l'exploration par des attaquants externes. De plus, les permissions des buckets cloud doivent être explicitement restreintes, appliquant le principe de moindre privilège.
2. **Masquer les traces d'erreurs techniques aux utilisateurs finaux :** Les serveurs applicatifs DOIVENT être configurés pour intercepter globalement les erreurs. Aucune "stack trace", message de débogage ou version de framework ne doit être renvoyée à l'utilisateur final. Le système doit afficher une page d'erreur générique et conviviale, tandis que les détails techniques complexes doivent être journalisés uniquement de manière sécurisée en interne.
3. **Déployer les en-têtes de sécurité HTTP (Security Headers) :** Les serveurs web et les répartiteurs de charge (Load Balancers) DOIVENT être configurés pour envoyer les directives de sécurité HTTP aux navigateurs des clients (par exemple, les en-têtes forçant l'utilisation exclusive de connexions sécurisées HTTPS ou protégeant contre le clickjacking). Ces directives complètent la protection de l'infrastructure en sécurisant le canal de communication avec l'utilisateur final.

Ne privilégiez jamais la rétrocompatibilité (backward compatibility) au détriment d'une configuration sécurisée moderne. Si une ancienne application nécessite des paramètres de sécurité obsolètes ou affaiblis pour fonctionner sur le nouveau cloud de TechNova, il faut corriger l'application, et non abaisser le niveau de sécurité global du serveur.