OPENCLASSROOMS

Corrigé P1C3

Plan de remédiation de la pratique "Secure Build" (Objectif Niveau 2)

Phase 1 : Atteindre le Niveau de Maturité 1 (Initial et Ad-hoc - Objectif : 3 à 6 mois)
L'objectif du Niveau 1 est de supprimer le build artisanal local et d'obtenir une visibilité claire sur le processus de compilation et les composants intégrés.

- **Activités principales (Build & Dépendances) :**
  1. Interdire la compilation d'artefacts de production sur les postes locaux des développeurs.
  2. Centraliser et automatiser le processus de *build* à l'aide d'outils standardisés (comme GitLab CI ou GitHub Actions) exécutés sur des serveurs dédiés et sécurisés.
  3. Établir la liste de l'ensemble des bibliothèques tierces et open source utilisées par OmniRoute, et identifier leurs vulnérabilités connues (Software Composition Analysis - SCA).
- **Intégration de "Quick Wins" (Recommandations ANSSI S-SDLC) :**
  1. Intégrer un scanner léger de pré-commit (ex. Gitleaks) pour bloquer la fuite de secrets (clés API, identifiants).
  2. Protéger la branche principale (main) : interdire les pushs directs et imposer une revue par les pairs (Peer Review) sur chaque Merge Request.

Phase 2 : Atteindre le Niveau de Maturité 2 (Optimisé et Intégré - Objectif : 6 à 12 mois)
Le Niveau 2 vise à automatiser la sécurisation du pipeline de livraison, à rendre les builds répétables et à imposer des contrôles de sécurité bloquants.

- **Activités principales (Build & Dépendances) :**
  - Intégrer des vérifications automatiques d'intégrité dans le workflow CI/CD à chaque *commit* (génération de *checksums* ou signatures numériques des artefacts).
  - Déployer des outils de scan automatisés pour détecter les vulnérabilités dans le code (SAST) et dans les bibliothèques tierces (SCA) directement au sein du pipeline.

- Mettre en œuvre la génération systématique et automatisée d'un SBOM (*Software Bill of Materials*) au format standard (CycloneDX/SPDX) pour chaque *build* applicatif généré.
- Configurer des *Security Gates* bloquantes pour interrompre le build si une vulnérabilité critique est détectée.
- Désactiver l'usage du tag « latest » sur les images de conteneurs pour verrouiller explicitement les versions des dépendances, assurant ainsi la stabilité et la prédictibilité des environnements.

Assurez-vous que chaque étape de votre plan d'action correspond scrupuleusement aux critères de réussite exigés par la documentation SAMM pour le niveau visé. Pour valider formellement un niveau SAMM, chaque étape de votre plan doit satisfaire aux grilles de questions d'auto-évaluation OWASP. *Par exemple : avoir un outil de build (GitLab CI) ne suffit pas pour valider le Niveau 1 de Secure Build ; il faut aussi prouver que la compilation sur poste local est techniquement impossible pour les livrables de production.*

N'intégrez pas d'activités complexes relevant du niveau 3 (comme le *build* parfaitement hermétique ou reproductible) ; consolidez d'abord le niveau 2 de manière réaliste et soutenable pour les équipes.