Corrigé P1C6

Charte d'engagement du Security Champion d'OmniRoute

La présente charte d'engagement, co-signée par le développeur volontaire, son directeur produit et le Manager AppSec, formalise les trois piliers indispensables à la réussite du programme de sécurité applicative :

1. Rôle, Co-responsabilité et Matrice RACI (Anti-Silo)

Pour éviter que la désignation d'un Champion ne déresponsabilise le reste de l'équipe agile, la charte pose le principe fondamental d'une **sécurité comme responsabilité collective** :

- **Les Développeurs de l'équipe :** Restent collectivement **Responsibles & Accountable (R & A)** de la qualité de leur code, de l'application des standards de sécurité (ASVS L1/L2), et des revues de code initiales croisées par les pairs (*peer review*).
- **Le Security Champion :** Intervient comme **Facilitateur et Coach (R/C)**. Il est *Responsible (R)* de l'animation culturelle de son équipe et du tri initial des alertes de sécurité (réduction des faux positifs et calibrage des outils en console). Il est *Consulté (C)* par ses pairs pour les aider à résoudre leurs blocages techniques. **Il n'a pas vocation à corriger seul les vulnérabilités de l'équipe ni à porter seul le fardeau des tickets cyber.**
- **Le Manager AppSec :** Reste **Accountable (A)** de la cohérence des politiques, de l'animation transverse de la communauté des Security Champions, et de la validation finale des critères d'acceptation (*security gates*) lors des jalons de livraison critiques.

2. Modalités pratiques d'engagement et de protection

- **Temps sanctuarisé :** Le Champion dispose d'un crédit-temps de **15 % de son temps homme mensuel** dédié exclusivement à sa mission d'animation cyber (veille, guilde, assistance aux pairs).
- **Ajustement de la charge :** Pour éviter le surmenage ou le rejet du rôle, la capacité de production de fonctionnalités (*features*) du développeur est officiellement réduite de 15 % par son directeur produit dans les sprints.

- **Valorisation de carrière :** Cet investissement est formellement intégré dans ses objectifs annuels et valorisé comme un accélérateur d'évolution technique au sein d'OmniRoute.

3. Plan d'apprentissage actif, contextuel et partagé

Pour ancrer les compétences dans la pratique et stimuler la motivation intrinsèque (plutôt que d'imposer des cours théoriques descendants stériles) :

- **Pratique par les pairs (Peer learning) :** Organisation de revues croisées de sécurité de bout en bout et de sessions de *Threat Modeling* (modélisation des menaces) collectives sur l'architecture de l'équipe.
- **Apprentissage par l'impact (Analyse Post-Mortem) :** Sessions de décryptage conjoint d'incidents réels ou passés d'OmniRoute (ou de cas d'école de la supply chain comme *XZ Utils* ou *Log4Shell*) pour comprendre concrètement les chemins d'attaque.
- **Gamification et Hackathons :** Participation régulière de l'équipe à des ateliers interactifs de simulation d'attaque et de défense (ex. Capture The Flag ou Serious Game AppSec).

Insistez lourdement sur la co-responsabilité de l'équipe et la valorisation du rôle de Champion dans la carrière des ingénieurs de l'éditeur.

N'érigez jamais le champion en "flic" de la sécurité ou en simple scribe administratif chargé de remplir des rapports de vulnérabilités, au risque de voir le programme échouer par manque de motivation intrinsèque.