# Corrigé P1C2

**Note stratégique à l'attention du CoDir d'OmniRoute**

**Objet : Intégration d'un cycle de développement sécurisé (S-SDLC): Opportunité stratégique et impératif business**

Chers membres du Comité de Direction,

Je vous adresse cette note pour alerter sur une évolution critique de notre environnement d'affaires et proposer une feuille de route pragmatique.
Face aux menaces ciblant nos logiciels et au durcissement réglementaire européen, la mise en place d'un **S-SDLC (*Secure Software Development Life Cycle*)** — c'est-à-dire l'intégration de la sécurité à chaque étape de notre cycle de développement — n'est plus un frein, mais un impératif business conditionnant notre accès au marché.

**1. Mutation des menaces : la supply chain applicative comme cible**

Les cyberattaques ne visent plus seulement nos infrastructures, mais notre chaîne de fabrication logicielle elle-même. L'affaire XZ Utils a illustré ce basculement : des attaquants s'infiltrent dans les composants open source et les pipelines CI/CD pour y injecter silencieusement des portes dérobées. Sans démarche S-SDLC, nous risquons de devenir le vecteur de compromission de nos propres clients en leur livrant des produits compromis.

**2. Le cadre réglementaire européen (NIS 2, DORA, CRA)**
Le législateur impose désormais la sécurité by design et la maîtrise des risques tiers. Nos clients majeurs (secteur bancaire, Opérateurs d'Importance Vitale) sont désormais soumis à la directive **NIS 2** et au règlement **DORA**. Ils ont l'obligation légale de reporter leurs risques de *supply chain* sur nous, leurs fournisseurs. Sans preuve formelle de la sécurisation de notre cycle de vie logiciel (S-SDLC), nous serons mécaniquement exclus de leurs appels d'offres.
Par ailleurs, le futur règlement **Cyber Resilience Act (CRA)** imposera le marquage CE sur nos produits numériques. La non-conformité à ses exigences de sécurité "by design" et de transparence (SBOM) expose OmniRoute à des amendes administratives massives, supervisées en France par l'ANSSI, pouvant atteindre 15 millions d'euros ou 2,5 % de notre chiffre d'affaires mondial.

**3. Une stratégie d'implémentation pragmatique, basée sur les standards de l’industrie (OWASP)**
Pour répondre aux inquiétudes légitimes de la part des départements Product et Engineering, le S-SDLC ne viendra pas ralentir la livraison ni bloquer la production. Il s'appuiera sur les standards ouverts de l'OWASP pour automatiser et fluidifier la démarche :

- **Gouvernance** : Nous piloterons notre maturité globale avec **OWASP SAMM**, permettant des avancées progressives et mesurables.
- **Exigences claires** : Nous intégrerons des exigences claires avec **OWASP ASVS** pour rassurer nos clients contractuellement sans réinventer la roue.
- 
- **Intégration DevSecOps** : Nous déploierons des outils automatisés directement dans nos pipelines DevOps existants pour identifier les erreurs sans créer de friction pour les développeurs.

Grâce au concept de *Security-by-Design*, nous économiserons sur le coût exponentiel du changement (une faille corrigée en phase de développement coûte bien moins cher qu'un patch en urgence en production, sans parler de l’impact au niveau de nos clients si nous avons une interruption de service).

Investir dans notre S-SDLC permettra de transformer cette contrainte réglementaire en un avantage concurrentiel décisif. Je me tiens à votre disposition pour vous présenter le détail de cette feuille de route.

Bien à vous,
Le Manager AppSec