Corrigé P1C5

Playbook de Réponse à une Vulnérabilité Critique (Zero-Day)

Phase 1 : Déclenchement par le CSIRT et réactivation de la gouvernance CI/CD

- **Réception de l'alerte et cadrage :** Le **SOC/CSIRT** réceptionne le bulletin du CERT-FR, ouvre l'incident de sécurité et convoque la cellule de crise technique (SOC, AppSec, Lead Dev).
- **Rétablissement de la politique de sécurité CI/CD :** Face à la désactivation non autorisée des contrôles, la règle d'interdiction absolue de débrayage (*deny-by-default*) est réaffirmée. Les administrateurs DevOps réactivent immédiatement les scanners SCA/SAST sur le pipeline. Une *Security Gate* bloquante est verrouillée : aucun build ne peut être déployé en production sans validation automatique des contrôles ASVS.

Phase 2 : Cartographie d'impact et pilotage via la plateforme ASPM

- **Recherche d'exposition via Dependency-Track (AppSec & CSIRT) :** Le CSIRT s'appuie sur l'AppSec Manager pour interroger la base centralisée des SBOMs dans **Dependency-Track**. En quelques minutes, l'AppSec identifie avec précision les versions applicatives et les conteneurs en production intégrant le composant vulnérable.
- **Orchestration et suivi du MTTR via DefectDojo (AppSec & Dev) :** L'AppSec consolide et déduplique l'alerte dans **DefectDojo**, créant un ticket d'urgence assigné aux Lead Developers. DefectDojo sert de tableau de bord central pour suivre le temps de résolution (*MTTR - Mean Time To Remediation*), mesuré par rapport au SLA de crise fixé à 48 heures pour les vulnérabilités de sévérité critique.

Phase 3 : Correctif de code, investigation SOC et qualification réglementaire

- **Remédiation technique (Développeurs & AppSec) :** Les développeurs mettent à niveau la dépendance vulnérable dans un environnement isolé, valident le comportement applicatif et font passer le correctif à travers la CI/CD réactivée pour validation automatique.

- **Investigation d'exposition en production (SOC / CSIRT) :** En parallèle du développement du patch, le SOC/CSIRT analyse les logs d'accès pour vérifier si la vulnérabilité a fait l'objet de tentatives d'exploitation avant la mise à jour.
- **Qualification réglementaire (GRC, RSSI & Juridique) :**
    - *Cas A (Pas d'exploitation décelée par le SOC) :* Il s'agit d'une vulnérabilité traitée dans le cadre du SLA d'urgence. Aucune notification d'incident DORA n'est requise auprès des autorités financières, mais une note d'information technique est transmise aux 50 clients bancaires.
    - *Cas B (Exploitation avérée avec impact sur les services) :* La vulnérabilité est qualifiée en **Incident**. L'équipe GRC déclenche immédiatement la notification légale aux clients concernés sous les délais réglementaires imposés.

N'entrez pas dans l'écriture de scripts de déploiement Ansible ou dans le codage détaillé des correctifs Java. L'AppSec Manager orchestre le flux et l'organisation, il ne code pas techniquement la remédiation.