Corrigé Activité P1C4

L'initiative du développeur, bien qu'orientée vers l'efficacité, représente un risque majeur pour la chaîne d'approvisionnement de TechNova. Un composant téléchargé sur un forum non officiel, sans maintenance depuis deux ans, coche toutes les cases de la vulnérabilité A03 : source non fiable, risque de code malveillant altéré, et absence de correctifs futurs en cas de faille découverte.

Pour corriger ce comportement de manière systémique, vous devez intégrer l'exigence documentaire suivante dans le guide des pratiques de développement :

"Afin de garantir l'intégrité de notre produit, toute nouvelle dépendance logicielle DOIT impérativement provenir d'un registre officiel et faire l'objet d'un scan de vulnérabilités automatisé (outil SCA) avant intégration. Le composant DOIT obligatoirement figurer dans le SBOM centralisé du projet. Enfin, son activité de maintenance et ses alertes de sécurité (CVE) doivent être monitorées en continu par l'équipe."

En imposant ce critère, vous interdisez de fait l'utilisation de la bibliothèque du forum. Le développeur devra rechercher une alternative sur un registre officiel (comme npm ou Maven), s'assurer que le projet est activement maintenu par une communauté, et laisser la chaîne CI/CD valider son innocuité via la génération du SBOM.

Ne déployez jamais de mises à jour de dépendances massivement sur tous vos systèmes de production en une seule fois. En cas de compromission silencieuse d'un composant de confiance, utilisez toujours des déploiements progressifs (staged rollouts) sur une petite partie de vos serveurs pour limiter l'impact d'une potentielle attaque.