Corrigé Activité P1C10

L'idée de tout journaliser pour faciliter le débogage est une erreur critique qui transforme vos serveurs de logs, censés vous protéger, en une immense base de données vulnérable.

Si l'API journalise les requêtes brutes, elle va inscrire des données personnelles, des numéros de carte de crédit, des mots de passe en clair ou des jetons de session valides directement dans de simples fichiers texte. L'équipe SOC ou un attaquant interne qui a accès aux logs aura alors accès à tous les secrets de l'entreprise.

Pour corriger ce processus, voici la règle stricte que vous devez imposer dans la politique de développement :

"Le système NE DOIT JAMAIS journaliser en clair des données personnelles, médicales ou des secrets d'authentification (mots de passe, numéros de carte bancaire, jetons de session) sous peine de créer une nouvelle faille de sécurité majeure."

N'oubliez pas d'encoder correctement les données loggées. Si un utilisateur malveillant tape un bout de code JavaScript ou une commande système dans un champ de recherche, et que vous loggez cette entrée sans l'encoder, ce code pourrait s'exécuter sur le poste de l'analyste de sécurité qui lit les logs ! C'est ce qu'on appelle l'injection de log (CWE-117). Prenez toujours soin de neutraliser les caractères spéciaux avant écriture.