Engineer Conseil

Programme continu d'analyse de sécurité

Mis en place un programme continu de sécurité — analyse du code, DAST, contrôles des dépendances et des vulnérabilités, génération de SBOM, détection de secrets et actions épinglées par SHA — accompagné de 21 audits de sécurité écrits.

2025

21

audits de sécurité écrits, en
plus des contrôles automatisés

Situation. Les protections de l'application — politique de sécurité du contenu, rôles de base au moindre privilège, nouvelle vérification des droits — défendent la plateforme à l'exécution. Elles ne renseignent pas sur ce qui est livré : vulnérabilité connue apparue dans une dépendance mardi dernier, identifiant commité puis retiré ou action tierce épinglée sur une étiquette devenue discrètement un autre code.

Tâche. La sécurité du code et de la chaîne d'approvisionnement devait être continue et automatisée, pour que son état soit un résultat de compilation plutôt qu'une opinion.

Action. CodeQL assure l'analyse statique, ZAP les tests dynamiques contre une instance en service et govulncheck la vérification des dépendances Go. Un inventaire logiciel SBOM est généré à chaque compilation avec Anchore et Syft pour savoir ce qui a été livré sans le reconstituer après coup. Gitleaks cherche les identifiants dans l'historique. Chaque GitHub Action tierce est épinglée à un hash de commit plutôt qu'à une étiquette, ce qui fige la référence à cette dépendance, même si l'étiquette est déplacée. Dependabot surveille 6 écosystèmes. À cette automatisation s'ajoutent 21 audits de sécurité écrits, dont un modèle de menaces et une évaluation selon le guide de test OWASP : les scanners reconnaissent les catégories déjà décrites, tandis que le modèle de menaces nomme celles propres à cette plateforme.

Résultat. Une vulnérabilité reconnue par les contrôles configurés peut faire échouer la compilation. Le volume de constats constitue le coût réel : un scanner signalant tout apprend aux gens à l'ignorer. Maintenir un signal exploitable demande un tri continu plutôt qu'une configuration unique.

Mettez cette expérience au service de votre projet

Prenez « Programme continu d'analyse de sécurité » comme point de départ pour un défi similaire dans votre organisation. Les prestations mobilisées pour cette réalisation sont disponibles pour votre projet. Des transmissions, procédures d'exploitation et manuels qui permettent à votre équipe de faire fonctionner le système sans rappeler ses concepteurs.

Découvrir nos prestations Contactez-nous →

Examinez ce qui a conduit au résultat

Découvrez la situation, les décisions et le résultat de cet exemple. Nous pouvons discuter des éléments transposables à vos contraintes et de ceux qui nécessitent une autre démarche.
Programme continu d'analyse de sécurité — 21 audits de sécurité écrits, en plus des contrôles automatisés

Découvrir nos prestations Contactez-nous →

Envie de vérifier la sécurité à chaque compilation ?

Discutez de votre projet avec l'ingénieure responsable de sa réalisation. Nous convenons par écrit du périmètre, de la base tarifaire et de la transmission avant le début des travaux.

Rôle exercé dans ce contexte : Ingénieure sécurité. Cette réalisation fait appel à DevOps, Automatisation et CI/CD, Fiabilité et sauvegardes, Sécurité et Documentation. Et puisque vous êtes ici, nous sommes aussi plutôt doués en DevOps et automatisation CI/CD, Sécurité et gestion des accès, Sécurité des agents d'IA et Documentation technique.

Contactez-nous Découvrir nos prestations

Un élément **d'un parcours plus long** — entièrement présenté sur ce site.

Chaque entrée suit la même structure : la situation, la tâche, ce que nous avons fait et ce qui a changé.

Voir l'ensemble du parcours

Définissez l'amélioration nécessaire

Présentez la décision, les personnes concernées et les options déjà envisagées. Nous pouvons expliciter les compromis et laisser une recommandation documentée.

Consulter les tarifs Contactez-nous →

Envie de vérifier la sécurité à chaque compilation ?

Interrogez-nous sur les décisions qui sous-tendent « Programme continu d'analyse de sécurité ». Vous parlerez aux personnes capables d'expliquer le travail et d'évaluer votre propre projet.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://advisory.engineer.company/fr/portfolio/ran-a-continuous-security-scanning-programme/