DevSecOps : une implémentation en dents de scie

S'appuyer sur un bon programme de sécurité des applications ne signifie pas pour les entreprises la fin des déploiements de code « vulnérable ». C'est l'un des enseignements d'une enquête nord-américaine promue par l'éditeur spécialisé de logiciels Veracode.

378 professionnels de l'IT, de la cybersécurité et du développement applicatif ont été interrogés en juin 2020 par Enterprise Strategy Group (ESG) pour Veracode.

La plupart des professionnels interrogés jugent le programme de sécurité applicative de leur organisation plutôt bon. Ils lui attribuent une note moyenne de 7,92 sur 10. Plus d'un tiers des répondants (36%) leur accordent même une note de 9 ou 10 sur 10.

Tout est pour le mieux dans le meilleur des mondes numériques ?

Gérer le risque

Investir dans un logiciel de sécurité applicative est une chose. En finir avec les vulnérabilités du code d'applications et de microservices livrés en est une autre.

Ainsi, 48% des répondants reconnaissent pousser « régulièrement » du code « vulnérable » (le code hérité inclut des composants obsolètes, des correctifs ne sont pas appliqués, le nouveau code est déployé hors d'un cadre rigoureux de développement…).

31% disent le faire « occasionnellement ».

Tous déclarent agir pour respecter une échéance de livraison jugée « urgente », avec l'ambition de corriger la faille ultérieurement. L'argument est mentionné par 54% des répondants concernés. Ils peuvent aussi considérer le risque très modéré (49%) ou arguer d'une découverte tardive de failles dans le cycle de développement (45%).

Former, qui et pour quels résultats ?

La formation à la sécurité cyber (le Sec du DevSecOps) des développeurs et d'autres profils techniques est irrégulière.

35% des répondants déclarent que moins de la moitié des équipes en charge du développement applicatif participent à des sessions de formation sur la sécurité. 15% seulement rapportent que tous les développeurs son conviés à participer à ces sessions.

Investir dans l'AppSec limiterait le risque. Malgré tout, pour 6 répondants sur 10, des applications déployées en production ont été exposées aux 10 principales vulnérabilités du référentiel OWASP (Open Web Application Security Project) ces derniers mois.

« Ces failles ne sont pas nécessairement liées au code dans lequel des vulnérabilités connues ont été identifiées. Toutefois, elles mettent en évidence l'attention requise, notamment en ce qui concerne le suivi du code et la fréquence des tests sur l'ensemble du cycle de vie du développement logiciel (SDLC) », ont indiqué les auteurs du rapport.

(crédit photo via Pixabay)