DevSecOps : la cybersécurité entravée ?

Le fournisseur canadien de solutions Security Compass a publié un rapport concernant l'adoption du DevSecOps au sein de grands groupes.

250 dirigeants et professionnels des fonctions IT et Risque employés au sein de grandes entreprises (plus de 1 M$ de chiffre d'affaires annuel) ont été interrogés*.

Quels sont les principaux résultats de cette enquête anglophone ?

Globalement, 96% des répondants considèrent que l'automatisation des processus de sécurité informatique et de conformité est la voie à suivre.

En outre, 74% utilisent l'approche DevSecOps (regroupant développement, sécurité et opérations informatiques) pour l'ensemble des projets applicatifs internes de leur entreprise. Il s'agit en priorité d'améliorer la sécurité et la qualité des développements logiciels (pour 54% du panel) et d'accélérer la mise à disposition d'applications (30%).

D'autres (19%) utilisent l'approche DevSecOps pour une minorité des développements applicatifs internes. 5% prévoient de le faire. 2% n'ont pas cette intention.

Pour quelles raisons ?

Déficit de compétences

Les défis techniques (cités par 60% des répondants) sont considérés comme le principal obstacle à l'adoption étendue du DevSecOps. Le coût (40%), le manque de temps (39%), le déficit de formation (38%) et de compétences internes (36%) sont d'autres arguments.

Selon une autre étude (Veracode), la formation à la cybersécurité de profils techniques est irrégulière. En outre, 15% seulement des professionnels IT ont rapporté que tous les développeurs de leur entreprise sont conviés à participer à ces sessions de formation.

* Enquête menée par Golfdale Consulting pour Security Compass, source : « The 2021 State of DevSecOps ».

(crédit photo © Shutterstock)