DevSecOps : concilier sécurité et agilité en maintenant la productivité

Les équipes DevOps trouvent souvent les processus de sécurité laborieux et manuels, entravant l'agilité qui les aide à commercialiser efficacement leurs solutions. Quant aux équipes IT, elles estiment que leurs collègues risquent de sacrifier la sécurité au nom de l'innovation et du chiffre d'affaires.

Malgré un respect des intentions mutuelles de l'ensemble des équipes, tout conflit pourrait occasionner des retards au niveau des processus. Par exemple, l'équipe IT pourrait devoir apporter des mises à jour importantes à la sécurité du réseau et informer certaines équipes qu'elles risquent d'expérimenter des temps d'arrêt lors de cette implémentation cruciale.

Toutefois, les équipes DevOps ont généralement plus de latitude dans leur fonctionnement dans ce monde piloté par les logiciels et elles pourraient demander à repousser cette mise à jour le temps d'accomplir des tâches ou de tenir des échéances, obligeant l'équipe IT à attendre et à consacrer du temps à reprogrammer leur travail.

Ceci alimente un mythe selon lequel les équipes DevOps préféreraient ignorer la sécurité. Dans la réalité, les développeurs souhaitent savoir que leurs applis et l'environnement dans lequel ils travaillent sont sûrs ; mais dans le même temps, ils ne veulent pas que la sécurité les empêche de commercialiser rapidement de nouveaux produits et fonctionnalités logicielles.

Existe-t-il donc un moyen pour les équipes DevOps, l'une des ressources les plus importantes de nombreuses entreprises modernes, d'embrasser la sécurité sans nuire à l'agilité ? Est-ce que l'intégration de DevOps et de la sécurité peut se faire de façon à alléger les tensions et à promouvoir la collaboration, tout en *améliorant* la sécurité et l'agilité dans le processus ?

La réponse est oui et cela est possible grâce à l'automatisation.

Le rapprochement par l'automatisation

Maintenant que les dirigeants sont plus enclins à se focaliser sur la sécurité, du fait des conséquences financières et de réputation manifestes d'une compromission, les équipes DevOps devraient définir comment elles protègent et sécurisent leurs multiples projets et environnements de production. L'automatisation de la sécurité dans le cadre d'un processus CI/CD permet aux équipes DevOps de suivre facilement les règles de sécurité de l'entreprise intégrées dans la chaîne d'automatisation.

Ce processus peut continuer de tourner sans problème atténuant les inquiétudes concernant la sécurité. Il continue d'automatiser les changements de règles et les activités de façon à réduire le risque d'erreur. Même si la solution d'automatisation reste cachée, elle demeure utilisable à tout moment pour visualiser les données sur les vulnérabilités, les obligations de conformité, les règles de sécurité et la connectivité réseau, via ses capacités d'analyse continue.

De plus, les équipes DevOps sont déjà familiarisées avec les outils automatisés dans leurs

opérations et communications quotidiennes et elles accepteront volontiers de basculer vers une solution de sécurité qui intègre leurs processus existants.

L'automatisation est centrale pour créer des équipes « DevSecOps » fiables, efficaces et connectées, faisant de l'option sécurisée l'option la plus simple. Cette approche combine l'utilisation des outils automatisés DevOps en vue de déploiements continus, dans les délais et dans le budget et la vocation de la sécurité de réduire l'erreur humaine et de maintenir une visibilité continue des vulnérabilités potentielles.

Encourager l'adoption

La collaboration DevOps est un principe directeur, souvent associé à l'idée de responsabilité partagée. Pour intégrer la sécurité dans le processus DevOps, les équipes de sécurité et les développeurs doivent collaborer et instaurer une responsabilité partagée. Mais comment ?

Certaines organisations peuvent assigner un représentant de la sécurité à chaque équipe de développement. Cette personne agit comme un pivot entre les deux équipes, améliorant la communication et établissant un processus équilibré tenant compte des intérêts mutuels de chacun. Un flux continu de partage de connaissances entre les deux équipes garantit un certain degré de maturité qui permet à une entreprise de sécuriser les applications et les services avec une solution automatisée.

Les équipes de sécurité peuvent définir des règles de sécurité permettant aux équipes de développement de déployer en continu, sous réserve d'observer les règles de sécurité et de conformité. C'est critique pour les deux équipes. Cette nouvelle façon de travailler fait que les développeurs vont pouvoir tester leur posture de sécurité à chaque étape de l'enchaînement CI/CD et corriger ce qui doit l'être et que les équipes de sécurité peuvent garantir la sécurité et la conformité tout au long du processus de développement.

Embrasser la collaboration

Toute croyance selon laquelle il y aurait de la discorde entre les équipes DevOps et IT est non fondée. Si l'on ne peut nier que les deux équipes s'influencent, ce n'est pas dû à un conflit, mais aux besoins métier. Si les deux équipes coopèrent, elles peuvent mieux tenir leurs objectifs et s'inscrire dans une entreprise plus sûre, innovante et rentable.

La première étape consiste à accepter la collaboration et en embrassant la sécurité plutôt qu'en la craignant, les équipes DevOps peuvent mieux contrôler le lien entre leurs besoins et les processus de l'équipe IT.
Une solution de sécurité automatisée peut être déployée pour améliorer l'efficacité et les résultats des deux services et ensuite de toute l'organisation. Il est temps pour les DevOps d'embrasser le DevSecOps.

devops apps © sergey nivens shutterstock