



DevSecOps

Intégrer la sécurité dans les pratiques DevOps

Avec la complexité des systèmes d'informations actuels, mêlant cloud, IoT et applications mobiles, « la sécurité ne peut plus être tributaire de la seule infrastructure, elle devient plus proche de l'application. »



Enjeux

La sécurité, parent pauvre des projets de développement

80%

des entreprises françaises ont subi au moins une cyberattaque avérée.

69%

ont rencontré des incidents de sécurité lors d'une mise en production.

85%

des applications présentent au moins une vulnérabilité. En moyenne, il faut un à trois mois pour qu'elle soit corrigée.

30%

Pourtant, seules 30% des équipes de test réalisent des tests de sécurité.

70%

des équipes ne réalisent pas des tests de sécurité.



Besoin

Une demande de sécurité en hausse chez les entreprises et les consommateurs



Améliorer la sécurité, premier objectif de la stratégie IT

47%

35%

Entre 2017 et 2018, les décideurs plaçant la sécurité en tête de leurs priorités est passé de 35% à 47%.

Ce que les consommateurs attendent de leurs produits digitaux :



Sûreté de fonctionnement (fiabilité, performance...)



Protection vis-à-vis des cyber-risques



Solutions

DevSecOps : faire de la sécurité une exigence comme les autres

+68%

68% des entreprises françaises vont intégrer la sécurité dans leurs projets DevOps d'ici 2020

«DevSecOps fait glisser la sécurité vers une "Security as Code"»

Pierre Baumgartner, Capgemini

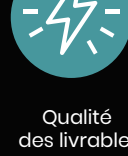
Objectifs de DevSecOps

Comment instaurer une démarche DevSecOps ?

Trouver le bon compromis entre :



Vitesse de livraison



Qualité des livrables



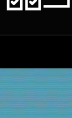
Sécurité des applications



Impliquer les experts sécurité dans l'élaboration de la solution, pour qu'elle soit sécurisée « by design ».



Automatiser les tests de sécurité



Mettre en place des outils d'audit de code afin d'identifier les failles de sécurité le plus tôt possible.



Miser sur des tests de sécurité dans le cloud, plus faciles à intégrer aux démarches DevOps.

« DevSecOps ne vise pas seulement à intégrer la sécurité au cœur même du projet mais, autant que possible, à l'industrialiser. »



Intégrer la sécurité en amont du cycle de vie applicatif

Planification

Optimiser la chaîne de valeur

Tests et développements

Assurer la qualité et la sécurité en continu

Production

Superviser pour améliorer la fiabilité des services

Déploiement

Accélérer avec la livraison continue



Les 3 premiers avantages d'une démarche DevSecOps :

81 %

respect des exigences de sécurité et de conformité

61 %

prévention active de la cybercriminalité

58%

réduction du nombre d'incidents post-déploiement



Futur

Et ensuite ?

76%

Des bots, pour aller plus loin dans l'automatisation des tests et leurs intégrations au pipeline DevOps. 76% d'entreprises en ont mis en place ou l'envisagent.

54%

De l'analyse prédictive : 54% des répondants s'appuient sur l'analyse des sets de tests.

60%

Du Machine Learning : en 2020, 60% des fournisseurs d'AST intégreront dans leurs solutions

Sources :

- Cahiers de ITES Innovation Summit, CRiP, 2018

- Observatoire DevSecOps 2019 de Micro Focus

- Avis d'expert Cap Gemini « Avec DevSecOps, la sécurité retrouve la place qui lui est due »

- Enquête CFTL 2019

- World Quality Report 2018, Cap Gemini, Sogeti et Micro Focus