DevSecOps

Pourquoi placer le “Sec” dans le DevOps ?

Pierrick Prévert
Security Solutions Architect, Qualys, Inc.

La sécurité à la traîne

Pour des raisons historiques comme organisationnelles, la sécurité est encore trop souvent ce qui arrive en bout de chaîne. Elle est posée autour d'applications "boîtes noires".

Le principal enjeu des entreprises est encore de savoir ce qu'elles ont, avant même de souhaiter le sécuriser : on ne peut sécuriser que ce que l'on connaît.

La sécurité consiste dans ce modèle à trouver et patcher les vulnérabilités avant qu'elles ne soient exploitées par d'autres.

Les développeurs sont souvent confrontés à la sécurité à posteriori : sollicités par un DSO, un CSO qui vient signaler des problèmes.

Qualys.

Un schéma habituel

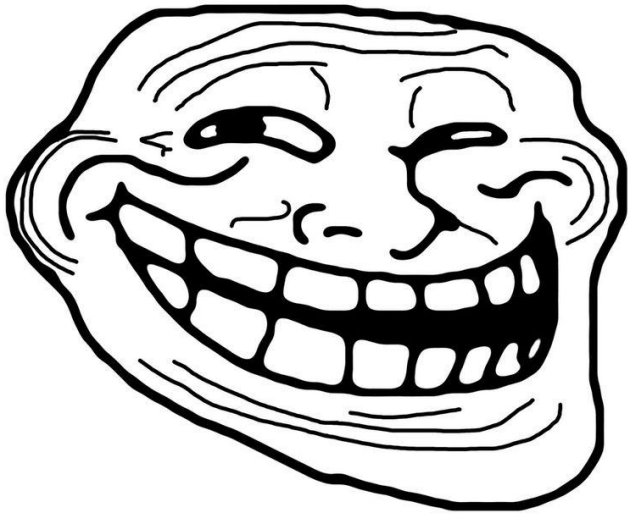
L’équipe développement livre une application complète

L’équipe opérationnelle la met en (pré-)production

L’équipe sécurité effectue un audit régulier ou ponctuel
et *signale les problèmes*

Qualys.

La sécurité



Qualys.

Les mentalités évoluent

Par l’effet médiatique et financier des failles révélées dans la presse

Par le biais de contraintes réglementaires (eg. RGPD)

Par les nouveaux techniciens et ingénieurs, mieux formés

Par l’arrivée de nouvelles méthodologies

Qualys.

Le DevOps invite au changement

Qualys.

DevOps, un concept récent

Créé en 2009 ce concept représente un changement organisationnel et culturel, poussé par la technologie, qui vise à associer les équipes de développement et les équipes opérationnelles.

Vise à résoudre le conflit entre les équipes de dév qui ont pour charge l' évolution d'un projet et les équipes d'ops qui ont pour charge la stabilité.

Les méthodes de développement Agile, originellement centrées sur le développement sont ici généralisées à la production.

Basé sur des cycles courts, des tests en amont, de l'intégration continue et une livraison continue (CI/CD), une évolution rapide par des retours utilisateurs.

Qualys.

Le DevOps s’impose… lentement

Si ce concept s’est imposé dans les startups, les grandes entreprises “traditionnelles” commencent tout juste la transition.

Notamment poussé par l’utilisation de technologies de containerisation, de cloud computing, le DevOps s’impose progressivement dans toutes les entreprises.

Mais ces entreprises ont une forte inertie, avec des centaines ou milliers de projets développés par des équipes différentes, avec des méthodologies différentes.

Le DevOps invite à une véritable révolution interne, plus organisationnelle que technologique.

Qualys.

Avec de nouveaux défis de sécurité

Qu’est-ce qui est en production ?

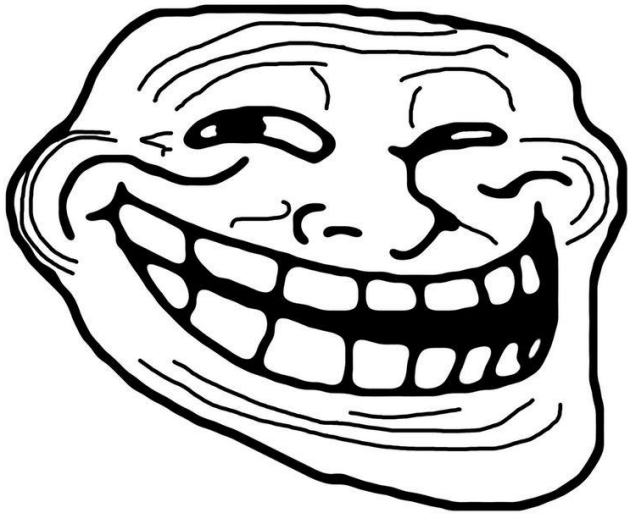
Quels sont les droits de la chaîne CI/CD ?

Soit la sécurité arrive trop tard

Soit la sécurité ralentit les livraisons

Qualys.

La sécurité



Qualys.

DevSecOps (2012)

Qualys.

Redéfinir la place de la sécurité

La sécurité ne doit plus être une action punitive, ou bloquante, qui arrive en fin de cycle. Elle doit être intégrée tout au long du cycle. Chacun est responsable de la sécurité.

Du point de vue du développeur

Inviter les équipes sécurité à réfléchir dès l'initialisation d'un projet

Intégrer des outils de sécurité dans la chaîne CI/CD

Similaire à l'approche DevOps "Shift Left Testing"

Qualys.

Les outils DevSecOps

Static Application Security Testing (SAST)

Dynamic Application Security Testing (DAST)

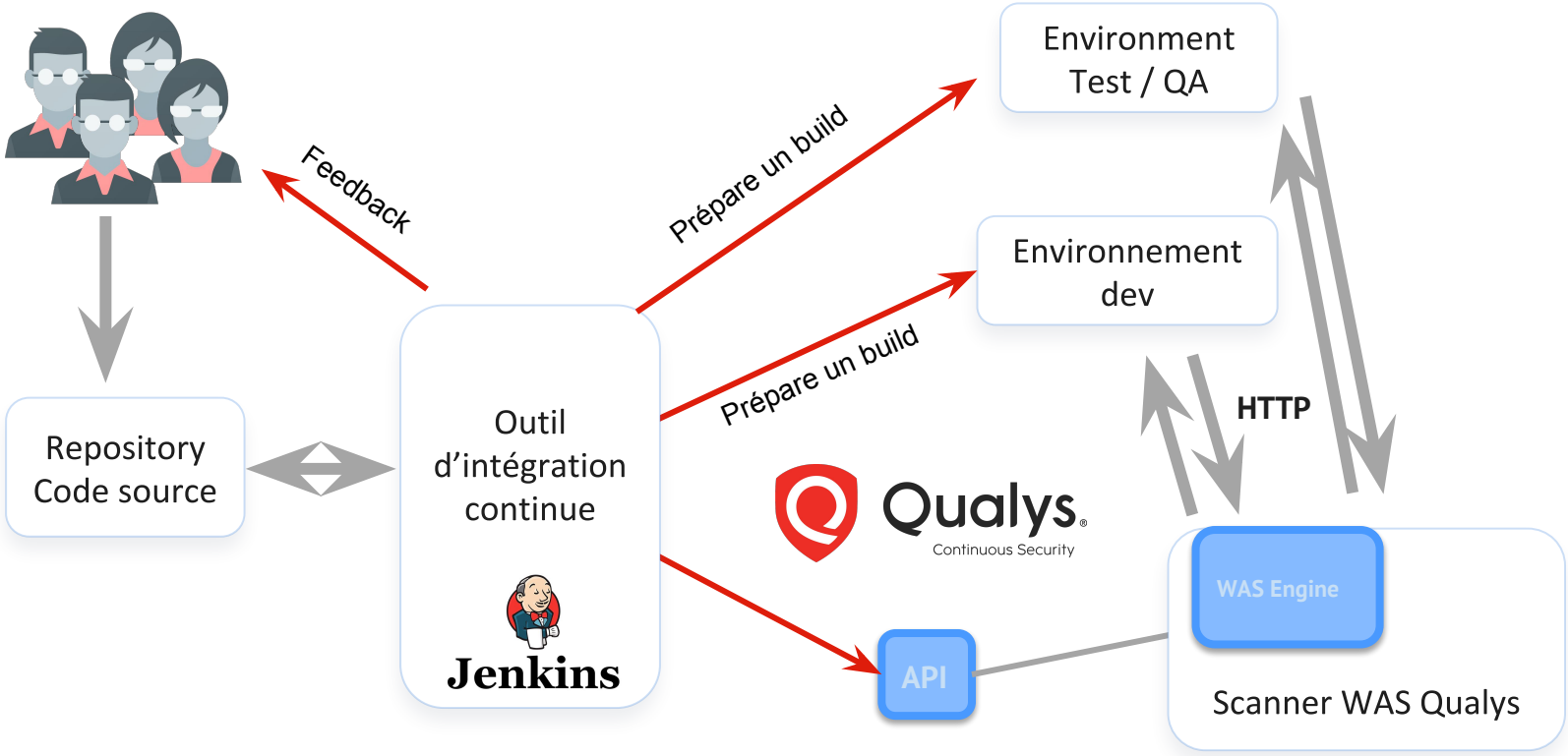
Container security testing

Cloud security assessment

Agent-based security (IOC / FIM…)

Qualys.

CI/CD avec un DAST



Pour conclure

La révolution DevOps commence. La révolution DevSecOps aura nécessairement lieu, car il en va de la survie de l’entreprise.

Qualys.

Merci

pprevert@qualys.com