Synapsys

Réaliser un audit DevOps et DevSecOps

Réaliser un audit DevOps ou DevSecOps offre une analyse complète et approfondie des pratiques en place, identifiant les opportunités d'amélioration.

Pour le **DevOps**, cela se traduit par l'automatisation et l'optimisation des processus entre les équipes de développement et d'exploitation pour une livraison continue plus rapide.

Le **DevSecOps**, quant à lui, ajoute une dimension de sécurité proactive en intégrant des contrôles de sécurité dès les premières phases du développement, un concept connu sous le nom de Shift-Left. Cette approche permet de prévenir les vulnérabilités tout au long du cycle de vie de l'application.

93%*

des entreprises ont déclaré avoir constaté une amélioration de la sécurité de leurs applications dès les premières étapes de développement après avoir intégré le DevSecOps.

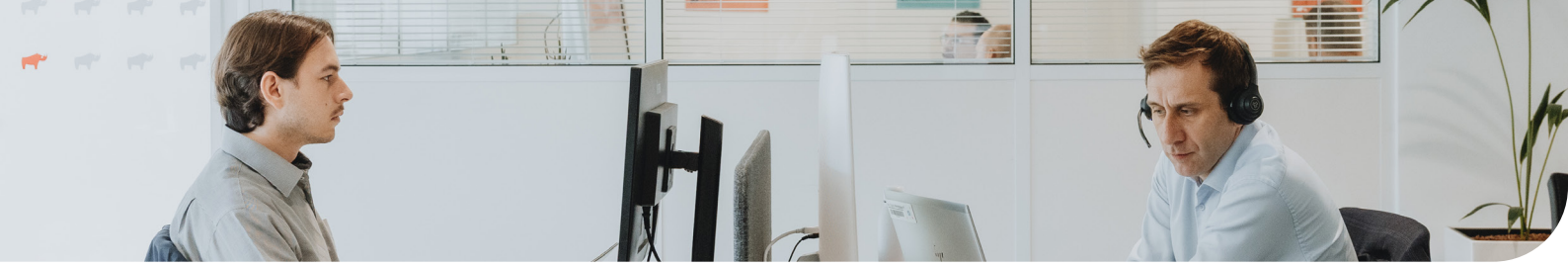
*Source : GitLab DevSecOps Survey

Que couvre un audit DevOps / DevSecOps ?

Le DevSecOps, tout comme le DevOps, intègre la sécurité et l'efficacité à chaque étape du cycle de vie du développement logiciel, de la conception à la livraison continue. L'objectif est de fluidifier la collaboration entre les équipes tout en automatisant les processus et en intégrant des contrôles de sécurité dès le début.

L'audit peut couvrir les dimensions suivantes, selon les objectifs définis :

- **Culture et collaboration** : Évaluer la synergie entre les équipes Dev, Ops et Sec pour garantir des objectifs communs.
- **Automatisation des processus** : Examiner l'intégration des outils dans les pipelines CI/CD pour la livraison continue et la sécurité automatisée.
- **Gestion des vulnérabilités** : Contrôler la détection, le suivi et la résolution des vulnérabilités sur l'ensemble du cycle de vie applicatif.
- **Conformité et gouvernance** : Valider l'alignement des pratiques sur les réglementations et politiques internes, qu'il s'agisse de DevOps ou DevSecOps.
- **Monitoring et retour d'information** : Analyser les systèmes de surveillance et de retour d'information pour optimiser les performances et identifier les anomalies post-déploiement.



Les piliers de la méthode d'audit DevOps / DevSecOps

Contrôle

Gouvernance : évaluation des structures de gouvernance IT et sécurité, ainsi que des mécanismes de décision.

Collaboration : analyse de l'efficacité de la coopération entre les équipes (développement, exploitation, sécurité).

Processus : examen des processus opérationnels, de la livraison continue (DevOps) à la sécurité intégrée (DevSecOps).

Outillage : évaluation des outils en place pour l'automatisation des pipelines CI/CD et la gestion de la sécurité.

Etude documentaire

Gouvernance et sécurité : processus de gouvernance, organisation, RACI, PSSI, KPI, standard et pratique DevOps...

Document d'architecture : cartographie du SI, DAT infrastructure, réseau, manuel opérationnel...

Pratique DevOps : DAT DevOps, outils collaboratifs, méthodologie et comitologie...

Application et développement : principe et standard de développement, liste des stacks techniques, DAT applicatifs...

Co-construction

Interviews : discussions approfondies avec les parties prenantes pour comprendre les pratiques existantes et les objectifs.

Ateliers : sessions collaboratives pour une présentation approfondie de la pratique existante.

Evaluation

Fournir un état de la pratique actuelle : évaluer le niveau de maturité et d'efficacité des pratiques DevOps ou DevSecOps.

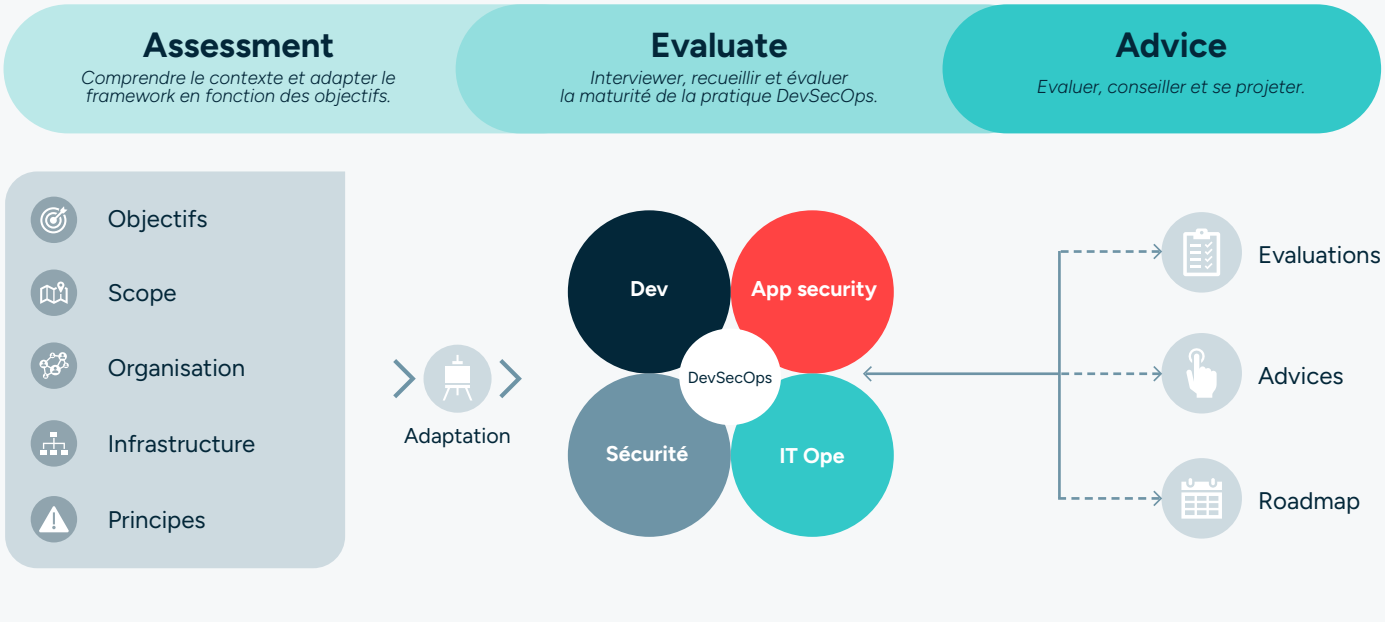
Proposer une méthodologie reproductible : garantir que les résultats de l'audit peuvent être utilisés comme base de référence pour des améliorations continues.

Livrables

Recommandations et conseils : propositions détaillées pour améliorer les pratiques DevOps ou DevSecOps.

Priorisations et feuille de route : définition, en collaboration avec le client, d'un plan d'action priorisé pour renforcer l'efficacité opérationnelle ou la sécurité.

Les étapes de l'audit DevOps / DevSecOps



Etape 1 : Assessment ou état de l'art de la gestion du SI

L'assessment repose sur des entretiens et des ateliers permettant de **cartographier l'écosystème existant** et d'**identifier les pratiques en place**. Elle couvre les aspects suivants :

- Gouvernance IT et sécurité
- Contraintes organisationnelles, réglementaires, métiers et technologiques
- Méthodologies de gestion de projet (Agile, Scrum, SaFe)
- Processus DevSecOps ou DevOps
- Automatisation des processus de livraison et de déploiement
- Efficacité de la collaboration et fluidité des échanges

Adaptation de la méthodologie d'évaluation

Pour proposer des recommandations optimisées, il convient d'aligner l'évaluation au niveau de maturité DevSecOps de l'entreprise :

- Niveau débutant : notation basée sur les capacités à couvrir
- Niveau intermédaire : notation basée sur les fonctions à couvrir
- Notation basée sur un domaine spécifique pour les clients souhaitant concentrer leur évaluation sur un pilier particulier (Culture, Automatisation, Lean, Mesure).

Etape 2 : Evaluation

La méthodologie d'évaluation se basera sur le système de notation définie en phase précédente.
Elle permettra de **mettre en exergue les points forts et faibles** de la pratique actuelle, qui permettra de **faire une analyse d'écart** entre l'état actuel et idéal, afin de **définir les axes d'amélioration et les priorités**.

Etape 3 : Recommandations et feuille de route

Les résultats de l'évaluation déboucheront sur des **recommandations précises**, accompagnées d'une **feuille de route**. Cette feuille de route présentera les actions à entreprendre pour renforcer la posture DevSecOps et les étapes pour les implémenter efficacement.

Pourquoi se faire accompagner par Synapsys ?

Confiance

Une culture grand compte et un large portefeuille de clients qui nous renouvellent leur confiance depuis des années.

Collectif

Une organisation structurée autour de “Squads” techniques pour partager et renforcer les expertises.

Humain

Un modèle d’entreprise et une organisation qui veillent au développement du savoir-être et du savoir-faire de nos consultants.

Ils nous font confiance

sodexo · CA · SAINT-GOBAIN · DECATHLON · METRO

TOTAL direct energie · GROUPE BPCE · EIFFAGE · MONOPRIX · Essonne TERRE D'AVENIRS

ENGIE · SOCIETE GENERALE · VINCI · adeo · CA TECHNOLOGIES & SERVICES

Contactez-nous

Tél : 01 84 16 49 71
Email : lerhino@synapsys-groupe.com
Paris • Lille • Lyon • Kuala Lumpur
www.synapsys-groupe.com

Découvrez nos ressources