Synapsys

Mesurer sa maturité DevSecOps

Le DevSecOps est une culture dérivée du DevOps qui vise à introduire la sécurité dès le début du cycle de vie du développement logiciel.

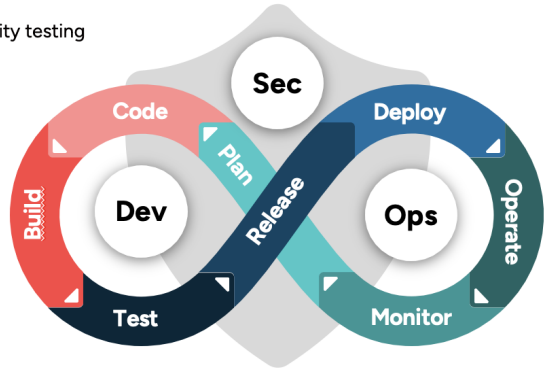
Le DevSecOps étend également la collaboration entre les équipes de développement et d'exploitation et intègre les équipes de sécurité dans le cycle de livraison des logiciels. Cela nécessite des changements dans la culture, les processus et les outils de ces équipes fonctionnelles de base pour faire de la sécurité une responsabilité partagée.

Tous les collaborateurs impliqués dans le développement et le maintien de l'état opérationnel sont responsables de l'intégration de la sécurité dans la chaîne d'intégration / livraison continue.

Pourquoi évaluer sa maturité DevSecOps ?

- Optimiser l'efficacité
- Mettre en conformité (normes et réglementation)
- Réduire les coûts
- Time to Market
- Amélioration continue et innovation
- Aligner la sécurité et le business
- Meilleure gestion des ressources

Les principes du DevSecOps



Release
- Access and configuration management
- Secret Management

Code
- Static application security testing
- Pre-commit hooks

Deploy
- Chaos engineering
- Pen Test

Build
- Software component analysis
- Static application security testing

Operate
- Log collection
- Patching
- Treat Intelligence

Test
- Dynamic application security testing
- Authentication
- Pen Test

Plan
- Threat landscape
- Compliance validation

Monitor
- Runtime Application self-protection
- Security information and event management
- Runtime application self-protection

Les modèles de maturité spécifiques à la sécurité

Idéal pour les organisations qui cherchent à renforcer leur intégration de la sécurité dans DevOps, mais peuvent être limités par leur spécialisation.

OWASP DevSecOps Maturity Model (DSOMM)

AVANTAGES

- **Spécifique à la sécurité :** Conçu spécialement pour le DevSecOps avec une forte orientation sur la sécurité.
- **Structure claire** : Facile à comprendre et à appliquer.

INCONVÉNIENTS

- **Complexité croissante :** Peut devenir complexe à gérer pour les grandes entreprises.
- **Pas de support officiel continu.**

SAMI (Security Assurance Maturity Model for DevOps)

AVANTAGES

- **Centré sur la sécurité** : très orienté vers l'intégration de la sécurité dans DevOps.
- **Flexible** : peut être appliqué à différents environnements DevOps.

INCONVÉNIENTS

- **Usage limité :** moins connu et utilisé que d'autres modèles.
- **Documentation limitée :** moins de ressources disponibles.

Sonatype DevSecOps Maturity Model

AVANTAGES

- **Gestion des composants :** excellente couverture de la gestion des dépendances logicielles.
- **Spécifique au DevSecOps :** ciblé pour les pratiques DevSecOps.

INCONVÉNIENTS

- **Spécifique à un domaine :** se concentre principalement sur la gestion des composants.
- **Portée limitée** par rapport à d'autres modèles plus larges.

Les modèles de maturité généraux

Offrent une grande flexibilité et sont souvent plus faciles à adapter, mais peuvent manquer de détails spécifiques à DevSecOps.

Gartner DevSecOps Maturity Model

AVANTAGES

- **Reconnaissance du marché :** Très respecté et souvent utilisé comme standard.
- **Flexibilité :** Peut être adapté à différents types d'organisations.

INCONVÉNIENTS

- **Accès restreint :** Souvent derrière un paywall, ce qui peut limiter l'accès aux détails du modèle.
- **Moins détaillé.**

Microsoft DevSecOps Maturity Model

AVANTAGES

- **Adaptabilité :** Facile à adapter selon la taille et le type d'organisation.
- **Simplicité :** relativement simple à mettre en œuvre.

INCONVÉNIENTS

- **Focus limité :** plus adapté aux écosystèmes Microsoft.
- **Pas aussi détaillé** que certains autres modèles.

NIST Cybersecurity Framework (Adaptation for DevSecOps)

AVANTAGES

- **Réputation solide :** basé sur un cadre largement reconnu et accepté**.**
- **- Alignement réglementaire :** aide à respecter les normes de sécurité.

INCONVÉNIENTS

- **Non spécifique à DevSecOps :** nécessite une adaptation importante pour une application DevSecOps.
- **Complexité** : peut être difficile à adapter sans expertise.

DevOps Institute DevSecOps Capability Maturity Model

AVANTAGES

- **Approche holistique :** Couvre culture, automatisation, gouvernance, et résilience. entreprises.
- **Formation continue :** Favorise l'amélioration continue à travers la formation.

INCONVÉNIENTS

- **Documentation limitée :** Moins de documentation disponible comparé à d'autres modèles.
- **Nouveauté relative :** Moins mature que d'autres.

Les modèles de maturité bien établis

Fournissent une couverture complète et sont bien reconnus, mais peuvent nécessiter des efforts supplémentaires pour une application DevSecOps.

BSIMM (Building Security In Maturity Model)

AVANTAGES

- **Large couverture :** Évalue une vaste gamme de pratiques de sécurité logicielle.
- **Benchmarking :** Permet de comparer les pratiques avec celles d'autres entreprises.

INCONVÉNIENTS

- **Non spécifique à DevSecOps :** Nécessite une adaptation pour une application DevSecOps.
- **Complexité :** Modèle très détaillé.

NIST Cybersecurity Framework (Adaptation for DevSecOps)

AVANTAGES

- **Réputation solide :** basé sur un cadre largement reconnu et accepté.
- **- Alignement réglementaire :** aide à respecter les normes de sécurité.

INCONVÉNIENTS

- **Non spécifique à DevSecOps :** nécessite une adaptation importante pour une application DevSecOps.
- **Complexité** : peut être difficile à adapter sans expertise.

Comment choisir son modèle de maturité DevSecOps ?

Critères
Objectifs de sécurité
Conformité réglementaire
Débutant
Maturité avancée
Taille de l'organisation
Culture d'entreprise
Automatisation
Ressources humaines limitées
Flexibilité pour les grandes entreprises
Mesure et suivi de la performance
Focus sur l'amélioration continue

Notre accompagnement DevSecOps

Audit et Conseil DevSecOps

Réaliser un audit des pratiques actuelles de développement et de sécurité pour identifier les risques et proposer des stratégies DevSecOps adaptées.

Intégration des outils de sécurité

Déployer et configurer des outils de sécurité automatisés qui s'intègrent dans les pipelines CI/CD existants.

Mise en place de la gouvernance

Élaborer des politiques de gouvernance de sécurité qui alignent les objectifs de sécurité avec les opérations de développement.

Formation et sensibilisation

Accompagner les équipes de développement et de sécurité sur les outils et les pratiques de DevSecOps.

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