AYI NEDJIMI Consultants

Métriques DevSecOps : KPI pour la maturité sécurité

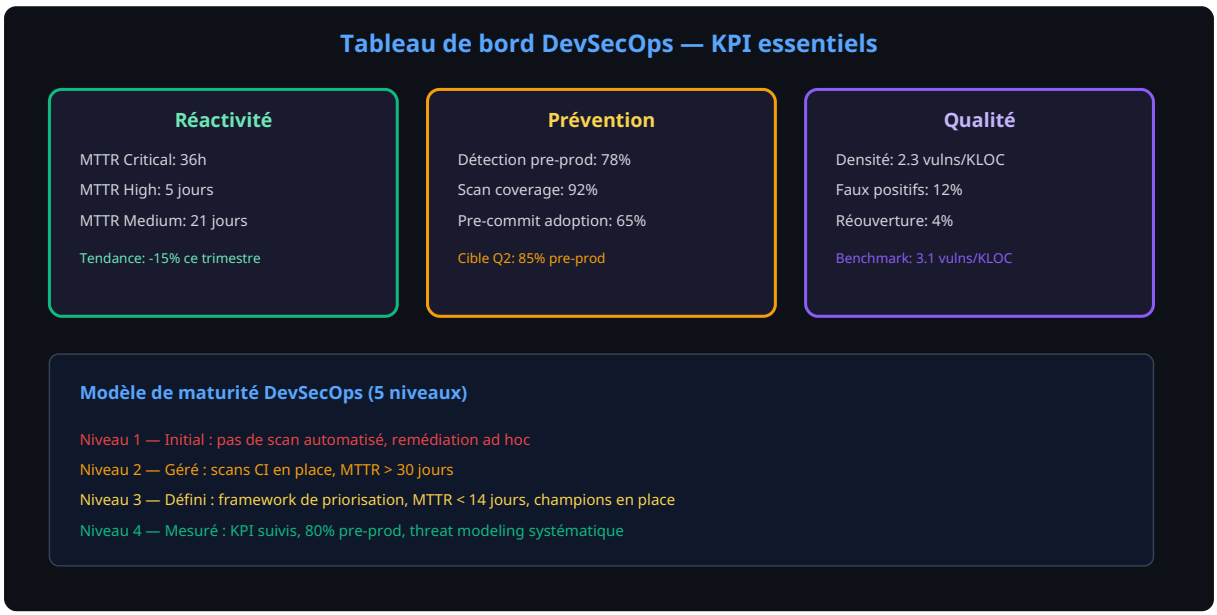
Catégorie : DevSecOps Lecture : 5 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Mesurez la maturité de votre programme DevSecOps avec les bons KPI : MTTR, couverture de scan, density de vulnérabilités et taux de détection.

Votre RSSI vous demande un rapport sur l'état de la sécurité applicative. Vous n'avez que deux chiffres : le nombre de vulnérabilités ouvertes (827) et le nombre d'incidents de sécurité cette année (2). Ces chiffres ne racontent rien. 827 vulnérabilités, c'est beaucoup ou peu ? Par rapport à quoi ? Est-ce en hausse ou en baisse ? Quelles équipes progressent et lesquelles stagnent ? Sans métriques structurées, votre programme DevSecOps fonctionne à l'aveugle. Vous investissez dans des outils, des formations, des processus — mais vous ne savez pas si cet investissement produit des résultats. Les métriques DevSecOps transforment cette intuition en données. Le MTTR (Mean Time To Remediate) mesure la réactivité de vos équipes. Le taux de détection pre-prod évalue l'efficacité de votre shift-left. La densité de vulnérabilités par ligne de code ou par composant identifie les points chauds. Ce guide vous fournit le framework complet pour bâtir un tableau de bord DevSecOps actionnable, avec les formules de calcul, les cibles réalistes et les pièges à éviter.

Points clés à retenir

- Le **MTTR** (Mean Time To Remediate) par sévérité est le KPI le plus actionnable — cible : CRITICAL < 48h, HIGH < 7j
- Le **taux de détection pre-prod** mesure l'efficacité du shift-left — cible : 80%+ des vulnérabilités trouvées avant la mise en production
- La **densité de vulnérabilités** (vulns par KLOC) permet de comparer les équipes et les composants entre eux
- Mesurez l'**adoption des outils** (% de repos scannés, % de devs avec pre-commit hooks) pour suivre la transformation culturelle



Les 5 KPI essentiels du DevSecOps

Trop de métriques tue la métrique. Commencez par ces cinq indicateurs qui couvrent les trois dimensions de la sécurité applicative (prévention, détection, réponse) :

MTTR : la métrique reine de la réactivité

Le **Mean Time To Remediate** mesure le temps moyen entre la détection d'une vulnérabilité et sa correction en production. C'est le KPI le plus révélateur de la maturité DevSecOps. Calculez-le par sévérité :

```
MTTR_critical = somme(date_fix - date_detection) / nombre_vulns_critiques
```

Les benchmarks sectoriels (données **Veracode State of Software Security 2024**) :

Sévérité	MTTR médian (industrie)	Cible mature	Top 10%
CRITICAL	60 jours	48 heures	24 heures
HIGH	90 jours	7 jours	3 jours
MEDIUM	180 jours	30 jours	14 jours
LOW	> 365 jours	90 jours	30 jours

Si votre MTTR critique est supérieur à 30 jours, concentrez-vous sur ce KPI avant tous les autres. Les leviers : automatisation du triage (cf. notre guide sur la gestion des vulnérabilités), SLA clairs par sévérité, et responsabilisation des équipes de développement.

Taux de détection pre-production

Ce KPI mesure le pourcentage de vulnérabilités trouvées avant le déploiement en production par rapport au total des vulnérabilités (pre-prod + production). C'est l'indicateur direct de l'efficacité de votre **shift-left**.

```
taux_preprod = vulns_trouvées_en_CI / (vulns_trouvées_en_CI + vulns_trouvées_en_prod) *
100
```

Un taux de 30% est typique d'une organisation qui démarre le DevSecOps. La cible à 12 mois : 80%. Le moyen d'y arriver : scanner plus tôt (SAST en pre-commit), scanner plus large (SCA sur toutes les dépendances), et scanner plus souvent (DAST hebdomadaire sur staging). Notre article sur le shift-left et la culture sécurité détaille les leviers humains et organisationnels pour atteindre cet objectif.

Densité de vulnérabilités et couverture de scan

La **densité de vulnérabilités** (nombre de vulns par millier de lignes de code, ou vulns/KLOC) permet de comparer la qualité sécurité entre les composants et entre les équipes. C'est une métrique normalisée qui ne pénalise pas les grands projets.

La **couverture de scan** mesure le pourcentage de vos applications et dépôts qui sont couverts par au moins un scanner de sécurité dans le pipeline CI. Un scan qui ne couvre que 40% de vos applications laisse 60% dans l'ombre. Cible : 95% en 6 mois.

Deux autres métriques complètent ce tableau :

- **Taux de faux positifs** — % des findings fermés comme "faux positif" ou "non applicable". Au-dessus de 30%, vos outils sont mal configurés. Cible : moins de 15%. Consultez notre comparatif des outils de test pour optimiser la configuration.
- **Taux de réouverture** — % des vulnérabilités corrigées puis réintroduites. Au-dessus de 10%, le problème est systémique (absence de tests de régression sécurité).

Modèle de maturité DevSecOps en 5 niveaux

Les métriques prennent leur sens dans un modèle de maturité qui définit les jalons de progression :

Niveau	Caractéristiques	KPI typiques
1 — Initial	Pas de scan automatisé, sécurité réactive uniquement	MTTR > 90j, preprod < 10%
2 — Géré	Scans CI en place, processus de triage basique	MTTR 30-60j, preprod 30-50%
3 — Défini	Framework de priorisation, security champions actifs	MTTR 7-14j, preprod 50-70%
4 — Mesuré	KPI suivis, threat modeling systématique, formation continue	MTTR < 7j, preprod 70-85%
5 — Optimisé	Amélioration continue, automatisation avancée, culture intégrée	MTTR < 48h, preprod > 85%

Chaque niveau prend 6-12 mois à atteindre. Visez une progression d'un niveau par an. Le passage du niveau 2 au niveau 3 est le plus difficile car il nécessite le changement culturel décrit dans notre article sur le shift-left security. Pour la conformité réglementaire associée, consultez notre guide NIS2 et ISO 27017.

Construire le tableau de bord

L'outil n'a pas d'importance — Grafana, Datadog, un Google Sheet, peu importe. Ce qui compte : la fréquence de mise à jour (hebdomadaire minimum), l'audience (partagé avec les tech leads et le management), et l'actionnabilité (chaque KPI dégradé déclenche une action identifiée).

Les sources de données typiques :

- **DefectDojo / Dependency-Track** — MTTR, densité, volume par sévérité
- **Pipeline CI** — Couverture de scan, taux d'échec des gates sécurité
- **Git** — Taux d'adoption des pre-commit hooks, nombre de secrets détectés
- **LMS / plateforme de formation** — Taux de complétion des formations sécurité

Automatisez l'extraction avec des scripts qui interrogent les APIs. Le rapport Veracode State of Software Security et le NIST Cybersecurity Framework fournissent les benchmarks pour contextualiser vos chiffres.

Sources et références : OWASP DevSecOps · NIST

Questions fréquentes sur les métriques DevSecOps

Combien de KPI faut-il suivre au démarrage ?

Trois suffisent au démarrage : MTTR critique, taux de détection pre-prod et couverture de scan. Ajoutez les autres progressivement quand les premiers sont stabilisés et que vos sources de données sont fiables. Un tableau de bord avec 20 KPI dont la moitié sont approximatifs ne sert personne.

Comment éviter que les métriques deviennent un outil de pression toxique ?

Trois règles : ne comparez jamais les développeurs individuellement (comparez les équipes ou les composants), valorisez la progression plutôt que la valeur absolue, et utilisez les métriques pour identifier les besoins de support — pas pour sanctionner. Un MTTR élevé dans une équipe signifie peut-être qu'elle manque de formation, pas qu'elle est incompétente.

Quel est le ROI attendu d'un programme DevSecOps mesuré ?

Le ROI se mesure en réduction des incidents de sécurité et en coûts de remédiation. Selon les données IBM Cost of a Data Breach 2024, les organisations avec un programme DevSecOps mature réduisent le coût moyen d'une brèche de 1.68 million de dollars. Le coût d'un programme DevSecOps pour 50 développeurs est d'environ 150K euros par an (outils + temps). Le ROI est largement positif dès la première année.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr