Veille DevOps – Mars 2025

Synthèse du mois de mars 2025

Le mois de mars 2025 a été riche en annonces et évolutions pour l'écosystème DevOps. Les plateformes d'intégration continue (CI) et de déploiement continu (CD) ont introduit de nouvelles fonctionnalités significatives, notamment l'adoption accrue de l'**IA** pour accélérer les revues de code et diagnostiquer les pipelines. **GitLab** a livré sa version 17.10 avec plus de 120 améliorations, dont un système de revue de code assisté par IA (Duo Code Review) et une analyse automatisée des causes d'échecs de pipelines (GitLab 17.10 released with Duo Code Review & Root Cause Analysis | GitLab (https://about.gitlab.com/releases/2025/03/20/gitlab-17-10-released/#:%7E:text=GitLab%2017,DORA%20Metrics%20and%20much%20more)). **Jenkins**, l'outil CI historique, a engagé une refonte de son interface pour rattraper son retard technologique, tout en maintenant sa stabilité légendaire. Dans la sphère **GitHub Actions**, la fin de vie de l'environnement Ubuntu 20.04 a été préparée par des coupures programmées en mars, forçant les équipes à mettre à jour leurs workflows (Notice of upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=Ubuntu%2020%20image%20brownouts)). Parallèlement, un incident majeur de **sécurité supply chain** a secoué la communauté : un composant tiers populaire de GitHub Actions a été compromis, exposant la nécessité de renforcer les pratiques DevSecOps dans les pipelines CI/CD (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Repositories%20widely%20used%20the%20tj,trust%20and%20consume%20GitHub%20Actions)).

En **conteneurisation** et **orchestration**, aucune sortie majeure de Kubernetes n'a eu lieu en mars, mais la communauté s'est préparée à la version 1.33 prévue en avril, avec notamment la généralisation des *Sidecar Containers* pour simplifier certains déploiements (Kubernetes Sidecar Containers Explained: Benefits, Use Cases ... (https://www.percona.com/blog/kubernetes-sidecar-containers-explained-benefits-use-cases-and-whats-new/#:%7E:text=Kubernetes%20Sidecar%20Containers%20Explained%3A%20Benefits%2C,33%20release%2C%20to%20implement)). **Docker**, de son côté, a apporté des améliorations pratiques à son écosystème : *Docker Bake*, un nouvel outil déclaratif pour orchestrer les builds multi-images, est passé en disponibilité générale dans Docker Desktop 4.38 (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=Docker%20Bake%20is%20an%20orchestration,to%20speed%20up%20build%20times)), tandis que Docker Engine v28 a renforcé la sécurité réseau en isolant mieux les conteneurs par défaut (Docker Navigator: New CEO, Docker Hub updates & AI-powered dev Docker (https://www.docker.com/resources/2025-03-10-new-ceo-docker-hub-updates/#:%7E:text=Docker%20Engine%20v28%3A%20Hardening%20container,networking%20by%20default)). L'infrastructure as code (IaC) a également connu des avancées notables. **Pulumi** a annoncé des fonctionnalités orientées DevSecOps (rotation automatique des secrets, intégration plus sûre avec GitHub Actions, RBAC granulaire) pour améliorer la gouvernance du cloud (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=Pulumi%20has%20introduced%20new%20features,and%20compliance%20at%20large%20scale)). **HashiCorp Terraform**, toujours leader malgré la concurrence émergente d'un fork OpenTofu, a poursuivi son rythme de sorties fréquentes (passant en version 1.11 en mars) avec des correctifs et rappelle l'importance de la qualité du code IaC via son framework de tests introduit depuis la v1.6 (New Terraform testing and UX features reduce toil, errors, and costs (https://www.hashicorp.com/en/blog/new-terraform-testing-and-ux-features-reduce-toil-errors-and-costs#:%7E:text=The%20Terraform%20test%20framework%2C%20introduced,post%20and%20Testing%20Terraform%20documentation)). **Ansible**, quant à lui, prépare la transition de sa distribution communautaire : la série 9.x arrive en fin de vie (EOL) en avril, ouvrant la voie à Ansible 10 et suscitant des discussions sur un éventuel support long terme pour la version 11 (Ansible Community, Ansible Core and RHEL 8 - Get Help - Ansible (https://forum.ansible.com/t/ansible-community-ansible-core-and-rhel-8/11198#:%7E:text=,13)). Enfin, les outils **Chef** (maintenant portés par Progress Software) continuent d'évoluer de manière incrémentale : en mars sont sortis Chef Infra Server 15.10.33 et Chef Infra Client 18.7.3, apportant des correctifs de sécurité et la prise en charge de plates-formes récentes (Chef Release Announcements - Chef Questions (https://discourse.chef.io/c/chef-release/9#:%7E:text=0%2075%20March%203%2C%202025,17)).

Le volet **observabilité et DevSecOps** a été marqué par un renforcement des bonnes pratiques et une adoption croissante des solutions open source. Selon le rapport annuel Grafana publié lors de KubeCon EU fin mars, **75 % des entreprises utilisent désormais des outils d'observabilité open source**, avec en tête **Prometheus** et **OpenTelemetry** dont 70 % des organisations se servent conjointement (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=Grafana%20Labs%20Shares%20Open%20Source,Using%20Open%20Source%20Observability%20Tools)) (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=,quarters%20of%20all)). OpenTelemetry a d'ailleurs publié la version 2.0 de son SDK JavaScript fin mars, introduisant des changements majeurs (abandon du support de Node.js 14/16, passage à TypeScript 5 et ES2022) afin d'optimiser les performances et la maintenabilité (Announcing the OpenTelemetry JavaScript SDK 2.0 | OpenTelemetry (https://opentelemetry.io/blog/2025/otel-js-sdk-2-0/#:%7E:text=,x%2C%20see%20the%20upgrade%20guide)). La complexité restant le défi principal en observabilité, les éditeurs misent sur l'**IA** pour automatiser la détection d'incidents et l'analyse de cause racine. De leur côté, les équipes SecOps et plateforme ont tiré les leçons de l'attaque sur GitHub Actions en mars en prônant des mesures concrètes : épingler précisément les versions des actions tierces, restreindre les permissions par défaut des runners, et intégrer des outils de sécurité supply chain (signatures, SBOM) dans les workflows (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Security%20researchers%20and%20open,the%20workflows%20they%20rely%20upon)) (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=The%20compromise%20echoes%20similar%20issues,trust%20enforcement%20on%20reusable%20Actions)). L'ensemble de ces tendances souligne une **maturation du DevOps vers plus de fiabilité et de sécurité**, tout en maintenant un rythme d'innovation soutenu.

Intégration et Déploiement Continu (CI/CD)

Jenkins modernise son interface sans sacrifier la stabilité

Jenkins demeure un pilier du CI/CD, et malgré son âge, la communauté investit pour le faire évoluer. Un billet de blog de mars (“Redesigning Jenkins (Part One)”) détaille l’initiative de **refonte de l’interface web de Jenkins**, un chantier nécessaire pour remplacer des technologies front-end obsolètes tout en conservant la compatibilité ascendante (Redesigning Jenkins (Part One) (https://www.jenkins.io/blog/2025/03/26/design-post/#:%7E:text=We%E2%80%99ve%20carried%20forward%20legacy%20technologies,a%20real%20barrier%20for%20contributors)) (Redesigning Jenkins (Part One) (https://www.jenkins.io/blog/2025/03/26/design-post/#:%7E:text=The%20first%20significant%20milestone%20in,but%20also%20enabled%20the%20Jenkins)). Les développeurs Jenkins ont ainsi retiré progressivement des bibliothèques vieillissantes (Prototype.js, YUI 2, etc.) qui compliquaient l’entretien du code, afin de pouvoir adopter des standards modernes (JavaScript ES6+, CSS récents). Cette modernisation se fait de manière **itérative et prudente** pour éviter toute régression dans les milliers de plugins de l’écosystème. Par exemple, la suppression de Prototype.js – un ancien framework JavaScript imbriqué dans le cœur de Jenkins – a levé un important frein technique et ouvert la voie à l’ajout de nouvelles fonctionnalités UI (Redesigning Jenkins (Part One) (https://www.jenkins.io/blog/2025/03/26/design-post/#:%7E:text=The%20first%20significant%20milestone%20in,but%20also%20enabled%20the%20Jenkins)). On en voit déjà les fruits : la communauté a introduit récemment une *palette de commande* (“Command Palette”) offrant une recherche unifiée dans Jenkins, ce qui améliore grandement l’ergonomie pour retrouver jobs, builds ou configurations (cette fonctionnalité est apparue dans la mise à jour 2.492.1 en février).

En parallèle, Jenkins continue ses sorties hebdomadaires et LTS régulières pour fournir corrections et améliorations. Au-delà du code, l’écosystème reste dynamique : l’organisation Jenkins a annoncé en mars sa participation au Google Summer of Code 2025 pour attirer de nouveaux contributeurs (The Jenkins Blog (https://www.jenkins.io/blog/#:%7E:text=,and%20guide%20GSoC%20contributors%2C%20we)), et les **Jenkins Contributor Awards 2025** ont ouvert leurs nominations sous l’égide de la Continuous Delivery Foundation (The Jenkins Blog (https://www.jenkins.io/blog/#:%7E:text=,Vote%20Voting%20begins%20on%20April)). Ces initiatives témoignent d’une communauté active. **Analyse de maturité :** Jenkins est un outil extrêmement éprouvé (plus de 15 ans d’existence) avec une communauté large, garantissant un haut niveau de stabilité. Cependant, son architecture ancienne le rend moins agile face aux outils plus récents. La refonte UI en cours est donc pertinente pour améliorer l’expérience utilisateur et l’attractivité du projet. Il faudra surveiller la feuille de route (disponible via la section “Ansible Roadmap” du site Jenkins) pour voir comment ces changements seront livrés dans les mois à venir. En attendant, Jenkins reste fiable en production, et les entreprises conservatrices continueront de s’appuyer sur ses LTS robustes, quitte à lui adjoindre des interfaces plus modernes (ex: Blue Ocean) en attendant la nouvelle UI native.

GitLab CI/CD : IA générative et analyse de performances DevOps

GitLab a poursuivi son cycle de releases mensuelles, avec la version **GitLab 17.10** déployée le 20 mars 2025. Cette édition met clairement l’accent sur l’aide à la productivité et la visibilité des processus DevOps. D’une part, GitLab enrichit son **offre d’IA intégrée** (baptisée “GitLab Duo”) : la v17.10 introduit en bêta le **Duo Code Review**, un outil d’assistance à la relecture de code piloté par l’IA, et un système de **Root Cause Analysis** automatique pour les pipelines CI/CD (disponible sur les instances self-managed équipées de GitLab Duo) (GitLab 17.10 released with Duo Code Review & Root Cause Analysis | GitLab (https://about.gitlab.com/releases/2025/03/20/gitlab-17-10-released/#:%7E:text=GitLab%2017,DORA%20Metrics%20and%20much%20more)). Concrètement, GitLab Duo peut analyser les logs d’un job de pipeline échoué afin d’identifier la cause première de l’échec et suggérer une piste de correction, ce qui promet de faire gagner un temps précieux aux développeurs. Ces fonctionnalités d’IA étant encore en bêta, leur **maturité** est limitée pour l’instant – GitLab les propose aux clients Ultimate et Duo dans une optique de feedback. D’autre part, GitLab 17.10 offre de nouveaux **outils d’observabilité interne** de la performance DevOps : un tableau de bord consolidé des *DORA Metrics* (Déploiement, Fréquence de déploiement, Lead time, MTTR) permet désormais aux managers de visualiser, au niveau groupe, les quatre indicateurs clés de performance des projets et de comparer les équipes (GitLab 17.10 released with Duo Code Review & Root Cause Analysis | GitLab (https://about.gitlab.com/releases/2025/03/20/gitlab-17-10-released/#:%7E:text=New%20visualization%20of%20DevOps%20performance,with%20DORA%20metrics%20across%20projects)) (GitLab 17.10 released with Duo Code Review & Root Cause Analysis | GitLab (https://about.gitlab.com/releases/2025/03/20/gitlab-17-10-released/#:%7E:text=The%20DORA%20metrics%20are%20available,DevOps%20health%20top%20to%20bottom)). Cette vue aide à repérer les goulots d’étranglement et à guider les efforts d’amélioration continue. GitLab a également livré en bêta un **langage de requête GitLab (GLQL)** pour interroger et filtrer les objets (issues, merge requests, etc.) plus finement, signe d’une tendance à fournir des capacités de *Reporting* avancées sur la plateforme.

En plus de ces nouveautés, GitLab continue d’affiner son socle CI/CD : citons l’arrivée des **Pipeline Inputs** (en version 17.11) qui permettront de paramétrer interactivement l’exécution d’un pipeline, ou l’amélioration de l’éditeur de pipelines. La communauté ne ralentit pas – GitLab 17.10 compte plus de 205 contributions externes (GitLab 17.10 released with Duo Code Review & Root Cause Analysis | GitLab (https://about.gitlab.com/releases/2025/03/20/gitlab-17-10-released/#:%7E:text=These%20are%20just%20a%20few,of%20the%20great%20updates%20below)) – et GitLab suit sa *roadmap* transparente vers la version **18.0 prévue pour mai 2025** (Releases | GitLab (https://about.gitlab.com/releases/categories/releases/#:%7E:text=Apr%2017%2C%202025)) (Releases | GitLab (https://about.gitlab.com/releases/categories/releases/#:%7E:text=GitLab%2017)). À noter, GitLab a déjà publié la liste des évolutions attendues pour 18.0 sur sa page “Upcoming Releases”, promettant une intégration encore plus poussée de l’IA dans toutes les étapes du cycle DevOps. **Analyse de maturité :** La plateforme GitLab est considérée comme très **mature et complète**, occupant à la fois le rôle de gestion de code, d’outil CI/CD, de registry, etc. Ses nouvelles fonctions d’IA (résumés de code ou suggestions de tests) sont innovantes mais devront faire leurs preuves en conditions réelles (précision des suggestions, acceptation par les développeurs). L’appétence de GitLab pour l’IA s’aligne avec le marché (GitHub ayant Copilot et Actions, Azure DevOps intégrant OpenAI...), et la communauté semble réceptive tout en restant vigilante sur les questions de confidentialité des données analytiques. Sur le plan stabilité, GitLab 17.10 est une version mineure relativement sûre, tandis que la 18.0 sera un **saut majeur** où il conviendra d’attendre quelques patchs avant déploiement en production. GitLab reste bien soutenu (entreprise solide, large communauté) – l’adoption de ses nouveautés devrait donc être accompagnée d’une documentation abondante et de retours d’expérience rapides.

GitHub Actions : nettoyage des environnements et leçons de sécurité

Dans l’univers **GitHub**, le mois de mars n’a pas apporté de nouvelle version (GitHub Actions évolue en continu dans le cloud GitHub), mais plusieurs changements importants ont impacté les pipelines CI des développeurs :

- **Fin de vie d’Ubuntu 20.04 dans les runners** : GitHub a annoncé que l’image `ubuntu-20.04` ne serait plus supportée à partir de fin avril 2025. Pour s’assurer que les utilisateurs migrent vers Ubuntu 22.04 ou plus récent, GitHub Actions a procédé à des **brownouts** chaque mardi de mars (coupures temporaires de disponibilité de l’image 20.04) (Notice of upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=Ubuntu%2020%20image%20brownouts)). Concrètement, pendant quelques heures aux dates indiquées (4, 11, 18, 25 mars), tous les jobs Actions demandant `runs-on: ubuntu-20.04` ont systématiquement échoué, affichant un message d’avertissement. Cette stratégie incitative a poussé les équipes DevOps à mettre à jour leurs fichiers workflow vers `ubuntu-22.04` afin d’éviter des interruptions. Une mesure similaire de *brownout* a concerné les actions de cache (`actions/cache`) en versions v1 et v2, dont la dépréciation a été annoncée (GitHub souhaitant que les pipelines adoptent la v3) (Notice of

upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=match%20at%20L555%20actions%2Fcache%20v1,and%20actions%2Ftoolkit%20cache%20package%20brownouts)). **Impact :** Ces changements montrent la nécessité pour les organisations de maintenir leurs pipelines CI à jour, en suivant la *roadmap* de GitHub (disponible sur le changelog GitHub Actions). Le support de l'infrastructure CI cloud évolue vite, et une veille attentive est requise pour éviter les surprises. Du côté positif, GitHub fournit à l'avance les dates d'obsolescence et la documentation de migration, ce qui témoigne d'une certaine maturité du service.

- **Attaque supply chain sur un écosystème Actions** : un événement marquant de mars 2025 a été la compromission d'une action tierce très utilisée, **tj-actions/changed-files**, par un acteur malveillant. Mi-mars, un nouveau mainteneur de ce projet a publié la version v44 de l'action contenant un code shell obscurci, capable d'exécuter du code à distance sur les runners GitHub (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Repositories%20widely%20used%20the%20tj,a%20blind%20spot%20in%20how)). Des milliers de dépôts utilisant cette action ont ainsi, à leur insu, fait tourner du code potentiellement malveillant lors de leurs workflows. L'attaque, heureusement détectée et neutralisée rapidement (le code malicieux a été supprimé et le projet repris en main), a servi d'**électrochoc** pour la communauté. Elle a révélé la **vulnérabilité de la chaîne d'approvisionnement logicielle** dans le contexte CI : beaucoup d'équipes intègrent des actions open-source sans vérification approfondie, en leur accordant une confiance aveugle, alors que ces actions s'exécutent avec de hautes permissions (accès aux dépôts, aux secrets, etc.). Suite à l'incident, les experts sécurité ont émis plusieurs recommandations fortes : épingler les actions tierces sur un commit SHA exact plutôt que de suivre `@master` ou une version mutable (pour éviter de tirer une mise à jour piégée) (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Security%20researchers%20and%20open,the%20workflows%20they%20rely%20upon)), limiter les droits des GitHub Tokens et secrets exposés aux workflows, auditer régulièrement la liste des actions utilisées, et tirer parti des outils comme **Dependabot** ou **Scorecards** pour surveiller la fiabilité des dépendances CI/CD. **Analyse de maturité :** GitHub Actions en tant que plateforme est très stable et riche (elle est d'ailleurs l'outil CI/CD cloud le plus utilisé selon le CNCF (CNCF Readies Next Major Update to Argo CD Platform - Cloud Native Now (https://cloudnativenow.com/news/cncf-readies-next-major-update-to-argo-cd-platform/#:%7E:text=Argo%20CD%2C%20thanks%20to%20the,be%20running%20disparate%20DevOps%20tools))). Néanmoins, cet épisode met en lumière un point faible de l'écosystème : l'absence de mécanismes natifs de signature ou de vérification d'intégrité pour les Actions communautaires. Des initiatives émergent (par ex. le projet *Sigstore* pour signer les composants, ou du côté de GitHub, le concept d'"Immutable Actions" actuellement en preview (Notice of upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=In%20preparation%20for%20the%20public,actions%20resolution%20where%20none%20exist))), mais leur adoption est encore embryonnaire. Les organisations ayant des exigences de sécurité élevées commencent à formaliser des politiques internes (*trusted Actions*, miroirs privés, etc.) pour maîtriser ce risque (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=lack%20first,trust%20enforcement%20on%20reusable%20Actions)). En somme, GitHub Actions reste un choix de premier plan pour l'automatisation CI/CD, mais en 2025 la **gouvernance des actions tierces** doit être renforcée pour atteindre une maturité DevSecOps satisfaisante.

- **Améliorations diverses et roadmap** : GitHub a également généralisé en mars certaines fonctions utiles comme les **métriques de performance des workflows** (temps d'exécution par job, parallélisme, etc.) disponibles pour les référentiels afin d'optimiser les pipelines (actions - GitHub Changelog (https://github.blog/changelog/label/actions/#:%7E:text=Performance%20Metrics%20for%20GitHub%20Actions,workflow%20and%20job%20performance)). Côté gouvernance, GitHub Enterprise Cloud a rendu GA les *rulesets* et propriétés personnalisées pour uniformiser les règles de compliance à l'échelle de l'entreprise (actions - GitHub Changelog (https://github.blog/changelog/label/actions/#:%7E:text=Octocat)). Enfin, le *changelog* signale que CodeQL (analyse statique de code) supporte désormais l'analyse des fichiers de workflow Actions, améliorant la couverture sécurité du code d'infrastructure (Notice of upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=CodeQL%20is%20the%20static%20analysis,bug%20fixes%20and%20small%20improvements)) (Notice of upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=,3%20%E2%80%93%2024%20January%202025)). Pour les mois à venir, GitHub a inscrit à sa feuille de route l'intégration de fonctionnalités d'**IA générative** (via GitHub Copilot) encore plus poussées dans les actions (pilotage automatique de certaines étapes) et la fin programmée de Windows Server 2019 pour les runners hébergés (mi-2025). Les équipes DevOps doivent donc anticiper ces changements et tester les versions bêta en avance lorsque possible.

Argo CD et le déploiement en mode GitOps

En matière de *Continuous Delivery* et de **GitOps**, le projet **Argo CD** a fait parler de lui à l'occasion de la KubeCon + CloudNativeCon Europe 2025 (début avril à Londres). Le *Cloud Native Computing Foundation (CNCF)* y a dévoilé la prochaine version majeure **Argo CD 3.0**, dont la sortie générale est prévue pour mai 2025 (CNCF Readies Next Major Update to Argo CD Platform - Cloud Native Now (https://cloudnativenow.com/news/cncf-readies-next-major-update-to-argo-cd-platform/#:%7E:text=CloudNativeCon%20Europe%202025%20events,become%20generally%20available%20next%20month)). Si l'annonce a eu lieu en avril, elle fait suite aux travaux du mois de mars et mérite d'être intégrée dans la veille :

- **Performances et sécurité en hausse** : Argo CD 3.0 apporte une base de code allégée et optimisée, réduisant significativement la consommation mémoire de l'application (CNCF Readies Next Major Update to Argo CD Platform - Cloud Native Now (https://cloudnativenow.com/news/cncf-readies-next-major-update-to-argo-cd-platform/#:%7E:text=Michael%20Crenshaw%2C%20a%20staff%20software,based%20access%20controls%20%28RBAC)). Ceci permettra de gérer davantage de clusters et d'applications GitOps par instance Argo, ou simplement d'économiser les ressources cloud. En parallèle, la version intègre nativement la gestion fine des permissions via **RBAC** (Role-Based Access Control), un point crucial pour les entreprises. Jusqu'alors, Argo CD nécessitait des configurations RBAC assez manuelles ; la 3.0 promet un modèle plus robuste et intégré pour contrôler qui peut synchroniser ou modifier quelles applications, renforçant ainsi la **sécurité** des déploiements automatisés.

- **Streamlining du processus GitOps** : Les développeurs d'Argo (Intuit en tête) cherchent à **simplifier l'expérience utilisateur** et le débit de livraison. Argo CD s'impose déjà comme une référence pour découpler CI et CD – laissant à CI (Jenkins, GitLab, etc.) le soin de construire les artefacts, tandis qu'Argo CD déploie en continu les modifications de configuration vers Kubernetes. La v3.0 va plus loin dans cette philosophie en éliminant certains cas de latence ou de décalage. D'après les retours de la CNCF, Argo CD 3.0 améliore encore la fréquence de conciliation des états désirés, ce qui signifie que les écarts entre le code Git (manifests Kubernetes souhaités) et l'état du cluster réel seront détectés et corrigés plus rapidement et plus efficacement qu'avant. Cela conforte Argo comme l'outil GitOps par excellence pour Kubernetes.

- **Adoption grandissante et interopérabilité** : Un chiffre marquant, communiqué lors de KubeCon EU, est qu'Argo CD est désormais utilisé par 45 % des organisations interrogées pour gérer les workflows DevOps Kubernetes, juste derrière GitHub Actions (51 %) et à égalité technique avec Jenkins (44 %) (CNCF Readies Next Major Update to Argo CD Platform - Cloud Native Now (https://cloudnativenow.com/news/cncf-readies-next-major-update-to-argo-cd-

platform/#:%7E:text=Argo%20CD%2C%20thanks%20to%20the,be%20running%20disparate%20DevOps%20tools)). Cette popularité repose sur la montée en puissance du *platform engineering* – de plus en plus d'équipes plateforme outillent leurs clusters Kubernetes avec Argo pour fournir un "**service de CD**" centralisé aux développeurs, plutôt que de les laisser écrire du scripting. Argo s'intègre d'ailleurs avec d'autres solutions (notifications, templating Helm/Kustomize, gestion secrets avec Vault, etc.) et l'écosystème Argo s'étend (projets Argo Rollouts, Argo Workflows, Argo Events). **Maturité :** Argo CD est un projet relativement jeune (open-source depuis 2018) mais déjà **gradué** au sein de la CNCF, gage de stabilité. La 3.0 sera un jalon important – on peut s'attendre à quelques *breaking changes* nécessitant des adaptations mineures de configuration lors de la mise à niveau. Cependant, l'équipe Argo a l'habitude de documenter clairement ces changements (la *roadmap* officielle et les notes de version sont publiées sur le site CNCF et GitHub). La base utilisateurs active (>4 500 contributeurs sur GitHub) fera remonter rapidement les éventuels bugs. Il est donc conseillé de tester Argo CD 3.0 sur un environnement de staging dès sa sortie, mais on peut anticiper un passage en production d'ici l'été 2025 pour profiter de ses avantages. Notons enfin que d'autres solutions GitOps émergent (FluxCD, Rancher Fleet), mais Argo CD conserve une longueur d'avance en fonctionnalités et en communauté.

En résumé, le CD "classique" via pipelines scriptés tend à s'effacer au profit du **CD déclaratif** à la Argo CD, surtout dans les environnements Kubernetes. Les annonces de mars-avril 2025 confortent cette trajectoire en rendant Argo plus performant, plus sécurisé et en renforçant la confiance des entreprises dans ce modèle GitOps. Pour les prochains mois, il faudra suivre l'adoption d'Argo CD 3.0 et son impact : permettra-t-il de réduire la charge des clusters en production ? Simplifiera-t-il suffisamment la vie des développeurs pour que ceux restés sur des déploiements manuels ou Jenkins X envisagent la migration ? Ce sont des points à surveiller dans les retours d'expérience à venir.

Conteneurisation et Orchestration

Docker & écosystème conteneurs : BuildKit à l'honneur, Docker Hub assoupli

Docker, acteur historique de la conteneurisation, a concentré en mars 2025 ses efforts sur l'expérience développeur et la rationalisation des builds d'images :

- **Docker Bake (build orchestration)** : Le 9 mars, Docker Inc. a annoncé la disponibilité générale de **Docker Bake** dans Docker Desktop 4.38 (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=Published%20Mar%209%2C%202025)). Docker Bake est un nouvel outil en ligne de commande (extension de `docker buildx`) qui permet de décrire les processus de construction d'images Docker de façon **déclarative**, via un fichier de recette (format HCL, similaire à Terraform). L'idée est de simplifier les builds complexes impliquant plusieurs images, de la même manière que Docker Compose simplifie le déploiement multi-conteneurs. Plutôt que d'enchaîner manuellement plusieurs commandes `docker build` avec moult options et contextes, on peut définir avec Bake des *targets* (cibles de build) qui incluent chacune les chemins Dockerfile, variables et étapes associées, puis lancer `docker buildx bake` pour tout construire en une passe (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=Docker%20Bake%20is%20an%20orchestration,to%20speed%20up%20build%20times)) (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=Bake%20changes%20the%20game%20by,faster%20and%20more%20efficient%20builds)). Bake exploite sous le capot **BuildKit**, le moteur de build concurrent de Docker, afin d'exécuter en parallèle les étapes indépendantes et de réutiliser les couches en cache au maximum. Les gains en performances sont significatifs pour les projets monorepos ou microservices : Docker cite des réductions de temps de build pouvant atteindre 30-40 %. En pratique, un fichier Bake (`docker-bake.hcl`) permet par exemple de définir un service backend et un frontend qui partagent une base d'image commune, et Bake s'assurera de ne compiler la partie commune qu'une seule fois. **Maturité :** Docker Bake était auparavant expérimental – son passage en GA indique qu'il a été testé et amélioré grâce aux retours de la communauté. Désormais, Bake est inclus par défaut dans Docker Desktop et a vocation à devenir le standard pour les pipelines CI nécessitant la construction de multiples images. Les premiers retours sont positifs, soulignant la *simplicité* qu'apporte Bake (on conserve des fichiers de configuration versionnés plutôt que des scripts shell complexes) et la *flexibilité* (prise en charge de matrices de build, de la cross-compilation multi-arch, etc. nativement) (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=Docker%20Bake%20tackles%20these%20challenges,with%20a%20simple%2C%20declarative%20approach)) (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=,image%20workflows)). Les équipes CI/CD peuvent d'ores et déjà intégrer Bake dans leurs workflows (par ex. via l'action GitHub `docker/build-push-action` qui supporte Bake). On notera que Bake utilise un DSL en HCL – cela pourrait dérouter au début les habitués du format YAML de Compose, mais la courbe d'apprentissage reste modérée et Docker fournit des guides de migration Compose -> Bake. À terme, on peut s'attendre à ce que Docker Bake devienne un atout pour implémenter des *politiques de build* uniformes dans les grandes organisations, en standardisant la manière dont les images sont produites.

- **Sécurité et networking** : Fin mars, Docker a livré (via son newsletter *Docker Navigator*) un aperçu de **Docker Engine v28**, focalisé sur la sécurité par défaut. En particulier, Docker Engine 28 **durcit la configuration réseau** en isolant mieux les conteneurs : désormais, un conteneur sans mapping de port explicite ne sera plus accessible sur le réseau hôte involontairement (Docker Navigator: New CEO, Docker Hub updates & AI-powered dev | Docker (https://www.docker.com/resources/2025-03-10-new-ceo-docker-hub-updates/#:%7E:text=Docker%20Engine%20v28%3A%20Hardening%20container,networking%20by%20default)). Historiquement, Docker ouvrait parfois des ports aux interfaces réseau via le *userland proxy*, ce qui pouvait exposer des services localement sans que l'utilisateur en ait conscience. Ce changement réduit la surface d'exposition des conteneurs "par accident", ce qui est bienvenu pour les déploiements sur postes de travail ou serveurs multi-tenant. Docker renforce ainsi son image de fiabilité en comblant des failles de configuration, montrant que même sur des composants matures, il reste attentif aux retours (cette modification répond à une vieille préoccupation de la communauté DevSecOps). On constate également que Docker multiplie les *certifications* sécurité : en mars, Docker a obtenu l'attestation **SOC 2 Type 2 et la certification ISO 27001** pour son infrastructure cloud, rassurant les clients entreprise sur la conformité de Docker Hub et Docker Desktop (Docker Navigator: New CEO, Docker Hub updates & AI-powered dev | Docker (https://www.docker.com/resources/2025-03-10-new-ceo-docker-hub-updates/#:%7E:text=Docker%20Announces%20SOC%202%20Type,Attestation%20%26%20ISO%2027001%20Certification)).

- **Docker Hub et licences** : Après avoir suscité de vives réactions en 2023 pour des restrictions (comme les limites de pulls anonymes ou la purge d'images inactives des comptes gratuits), Docker a infléchi sa politique en faveur des développeurs. En mars 2025, de **nouvelles politiques Docker Hub** sont entrées en vigueur pour **assouplir les quotas de pulls et de stockage** (Docker Navigator: New CEO, Docker Hub updates & AI-powered dev | Docker (https://www.docker.com/resources/2025-03-10-new-ceo-docker-hub-updates/#:%7E:text=Revisiting%20Docker%20Hub%20policies%3A%20Prioritizing,developer%20experience)). D'après Docker, ces ajustements visent à faire de Docker Hub "une ressource puissante et précieuse pour les développeurs" et privilégient l'expérience. Concrètement, les comptes *Personal* conservent la gratuité sans expiration d'images, et les comptes *Pro/Team* gagnent des volumes de pulls et de stockage supplémentaires sans surcoût (Announcing Upgraded Docker Plans: Simpler, More Value, Better Development and Productivity | Docker (https://www.docker.com/blog/november-2024-updated-plans-

announcement/#:%7E:text=These%20changes%20increase%20access%20to,applications%20faster%20and%20more%20efficiently)) (Announcing Upgraded Docker Plans: Simpler, More Value, Better Development and Productivity | Docker (https://www.docker.com/blog/november-2024-updated-plans-announcement/#:%7E:text=Areas%20we%E2%80%99ve%20invested%20in%20during,the%20past%20year%20include)). Le 1er mars 2025 a marqué en particulier le début du nouveau modèle de **consommation Docker Hub** : plus de flexibilité pour acheter à la demande du quota de pulls ou de la rétention d'images au-delà des offres standard (Announcing Upgraded Docker Plans: Simpler, More Value, Better Development and Productivity | Docker (https://www.docker.com/blog/november-2024-updated-plans-announcement/#:%7E:text=will%20take%20effect%20on%20March,on%20or%20after%20December%2010)). **Analyse de maturité :** Ces changements montrent que Docker a écouté sa communauté et trouvé un équilibre entre viabilité économique et bienveillance envers l'open-source. Les projets OSS et les petites équipes devraient souffler un peu quant à la pérennité de leurs images sur Hub. Couplé aux investissements de Docker dans **Scout (analyse de vulnérabilités)** et l'acquisition de **Atomist/Testcontainers** en 2023 (Announcing Upgraded Docker Plans: Simpler, More Value, Better Development and Productivity | Docker (https://www.docker.com/blog/november-2024-updated-plans-announcement/#:%7E:text=,offers%20enterprise%20features%20and%20a)), cela renforce l'attractivité de l'écosystème Docker en 2025. Sur un plan plus général, Docker reste la référence en conteneurisation, mais voit la concurrence de **Podman** (CNCF) se structurer : Podman a atteint sa version 5.4 début avril 2025 (Podman - Wikipedia (https://en.wikipedia.org/wiki/Podman#:%7E:text=Podman%20,and%20its%20companion%20tools)), proposant une expérience sans daemon et rootless très prisée en milieu Linux. Cependant, Docker conserve l'avantage de l'intégration multiplateforme (Windows/Mac) via Desktop, un écosystème d'extensions et la familiarité pour des millions de développeurs. On suivra tout de même la progression de Podman, notamment son outil Podman Desktop (v1.18 en mars) qui cherche à offrir une alternative open-source à Docker Desktop, ou encore **Containerd** qui continue d'évoluer en sous-marin (Docker Engine repose dessus).

En résumé, pour mars 2025, Docker consolide sa position en facilitant la vie des développeurs (builds plus simples, moins de contraintes d'utilisation), tout en comblant certaines faiblesses sur la sécurité by default. La communauté DevOps bénéficie directement de ces améliorations : on peut s'attendre à ce que Docker Bake devienne un standard dans les configurations CI/CD complexes, et que les pipelines DevSecOps s'appuient sur Docker Scout et les nouvelles garanties de Hub pour renforcer la confiance dans la chaîne des conteneurs. Il conviendra de garder un œil sur la compatibilité ascendante de Bake (quelques différences par rapport aux builds traditionnels peuvent nécessiter des ajustements mineurs de Dockerfile) et sur l'évolution des offres Docker en matière d'IA – un *Docker AI* a été évoqué dans Docker Desktop pour fournir de l'aide contextuelle aux développeurs (Docker Navigator: New CEO, Docker Hub updates & AI-powered dev | Docker (https://www.docker.com/resources/2025-03-10-new-ceo-docker-hub-updates/#:%7E:text=Docker%20Desktop%204,platform%20image%20management%2C%20and%20more)), s'inscrivant dans la vague globale d'assistants intelligents.

Kubernetes : entre versions stables et élan communautaire

Le cœur de l'orchestration de conteneurs, **Kubernetes**, n'a pas publié de nouvelle version stable en mars 2025, conformément à son cycle de release d'environ 3 par an. La version **Kubernetes 1.32**, sortie fin 2024, reste la plus déployée à ce jour, et la communauté préparait activement la version **1.33** prévue pour fin avril 2025 (1.33 Kubernetes Release Sneak Peek (https://groups.google.com/a/kubernetes.io/g/dev/c/ofJFFfOBhdc#:%7E:text=I%E2%80%99m%20excited%20to%20kick%20off,Release%20Lead%20for%20this%20cycle)). Néanmoins, plusieurs informations et tendances autour de Kubernetes méritent l'attention dans la veille de mars :

- **Sneak Peek de Kubernetes 1.33** : Les notes préliminaires laissent entrevoir des évolutions notables en 1.33, axées sur la qualité de vie des opérateurs. Une des fonctionnalités phares attendues est la promotion en **GA des *Sidecar containers*** (Kubernetes Sidecar Containers Explained: Benefits, Use Cases ... (https://www.percona.com/blog/kubernetes-sidecar-containers-explained-benefits-use-cases-and-whats-new/#:%7E:text=Kubernetes%20Sidecar%20Containers%20Explained%3A%20Benefits%2C,33%20release%2C%20to%20implement)). Introduits en alpha dans une version précédente, les Sidecars natifs permettront de définir dans un Pod Kubernetes quels conteneurs sont des sidecars (par ex. un agent de logging ou de mise à jour) afin que le scheduler gère différemment leur cycle de vie. Cela évite les hacks actuels (comme des initContainers ou des scripts d'attente) pour synchroniser l'arrêt des sidecars avec l'application principale. Leur arrivée en stable améliorera la fiabilité des déploiements de Pod complexes. Autre point en vue : l'auto-instrumentation de Kubernetes avec OpenTelemetry, qui devrait voir une meilleure intégration (profiling et traces du control-plane plus aisés). Enfin, on parle d'améliorations sur la **scalabilité du plan de contrôle** (pouvoir supporter encore plus de nœuds par cluster via des optimisations etc.), sujet crucial pour les opérateurs cloud publics.

- **Communauté et Bugfixes** : En mars, divers patchs de sécurité ont été backportés sur les branches supportées (1.31 et 1.32) – notamment des correctifs concernant *CRD* et *Ingress* – rappelant qu'il est important pour les ops de maintenir à jour les clusters (les distributions managées comme GKE, EKS l'ont fait automatiquement). La communauté Kubernetes reste hyper-active, comme en témoigne la **KubeCon EU 2025** (1-4 avril à Londres) qui a fait salle comble. Durant cette conférence, de nombreux projets gravitant autour de Kubernetes ont annoncé des mises à jour en mars : par exemple, Grafana Labs a présenté un système de **Fleet Management** pour centraliser la gestion des collecteurs de métriques sur des milliers de clusters (Grafana Labs Extends Observability Reach Deeper into Kubernetes (https://cloudnativenow.com/news/grafana-labs-extends-observability-reach-deeper-into-kubernetes/#:%7E:text=Kubernetes%20cloudnativenow,management%20of%20telemetry%20data%20collectors)), et la CNCF a accueilli de nouveaux projets en sandbox (notamment autour de l'optimisation du coût des clusters, signant une tendance FinOps). Les retours d'expérience de grandes entreprises lors de KubeCon ont souligné l'importance croissante du **Platform Engineering** : mettre en place une plateforme interne sur Kubernetes pour que les devs puissent déployer facilement (via des *services templates*, du *GitOps*, etc.). Kubernetes sert désormais de base standardisée pour ces plateformes, avec des abstractions plus haut niveau par-dessus (exemple : Backstage Kubernetes plugins, Crossplane pour offrir des *services managés* on-cluster, etc.).

- **Écosystème CNCF** : Mars a vu des progrès dans des projets connexes importants. **Prometheus** (monitoring) a continué ses releases 2.4x et on note l'intégration grandissante avec OpenTelemetry (exposition mutuelle des métriques). **Istio** (maillage de services) a livré en mars la version 1.18, améliorant la VM Mesh et supportant les sidecars distants. **Knative** (serverless sur K8s) a été officiellement adopté par la CNCF ce trimestre, ce qui peut accroître son développement. Par ailleurs, l'offre de **certifications Kubernetes** a évolué : la CNCF a annoncé en mars la mise à jour prochaine des examens CKA/CKAD pour couvrir les nouveautés des versions 1.32 et 1.33, encourageant les professionnels à se certifier ou re-certifier sur les dernières pratiques (comme l'utilisation de *ephemeral containers* pour le debug, ou les sidecars natifs). Enfin, on a vu émerger en mars des **outils K8s orientés IA** – par exemple, un plugin expérimental "Kubectl AI" permettant de formuler des requêtes en langage naturel pour générer des commandes kubectl, ou encore l'intégration de **Kubernetes GPT** dans Lens pour expliquer les objets cluster. Ce sont des gadgets pour l'instant, mais ils illustrent l'omniprésence de l'IA y compris dans l'admin système.

Analyse de maturité : Kubernetes en lui-même est un projet très **mature et stable** (plus de 8 ans d'existence, soutenu par tous les grands cloud providers). La version 1.33 à venir ne devrait pas déroger à la règle des évolutions incrémentales maîtrisées. Cependant, le fait qu'aucune sortie majeure n'ait eu lieu en Q1 2025 a permis aux organisations de **consolider** leurs déploiements sur 1.32 et d'adopter massivement les features GA récentes (par exemple les *StatefulSets avec Pod Ordinal* ou la *CSIMigration* achevée). On constate que la communauté adopte un rythme un peu moins effréné qu'il y a quelques années, ce qui est bon signe : Kubernetes devient un **standard industriel stable** plutôt qu'une source de changements incessants. Cela dit, son écosystème continue d'évoluer rapidement sur les couches supérieures : GitOps, Service Mesh, Serverless, etc. Pour les mois prochains, la vigilance portera sur la compatibilité des addons lors du passage à 1.33 (les fournisseurs de CNI, CSI, Ingress Controller vont publier des mises à jour alignées).

Les entreprises doivent prévoir de tester 1.33 sur des clusters de dev dès que possible (sortie prévue fin avril) afin de planifier les upgrades production dans le courant du T2 2025. Globalement, Kubernetes reste **très pérenne** : les compétences K8s sont toujours recherchées, et l'accent se déplace vers l'efficacité opérationnelle (monitoring, optimisation des coûts, simplification pour les devs via des *Internal Developer Platforms*). La maturité se voit aussi dans la robustesse du support commercial (Red Hat OpenShift, VMware Tanzu, etc. sont en versions stables alignées) et la qualité des outils périphériques. Kubernetes est donc dans une phase de **consolidation** en 2025, où l'on s'attend à moins de révolutions mais à un polissage constant – exactement ce dont les équipes Ops ont besoin pour fiabiliser leurs infrastructures conteneurisées à grande échelle.

Infrastructure as Code (Terraform, Ansible, Pulumi, Chef…)

Terraform et alternatives : évolution sous licence et tests IaC

Terraform, la solution IaC de HashiCorp, a continué d'être un choix de référence en mars 2025, avec toutefois un contexte communautaire particulier depuis le changement de licence de 2023. Côté technique, HashiCorp a publié la version **Terraform 1.11** fin février puis plusieurs correctifs 1.11.x en mars (Releases · hashicorp/terraform - GitHub (https://github.com/hashicorp/terraform/releases#:%7E:text=Releases%20%C2%B7%20hashicorp%2Fterraform%20,0%20%28February%2027%2C%202025)). Cette version n'a pas introduit de rupture majeure (Terraform est en v1.x depuis fin 2021, garantissant la stabilité), mais elle a incorporé de petites améliorations du langage HCL et du moteur d'exécution. Par exemple, Terraform 1.11 a optimisé le traitement des dépendances implicites, ce qui peut accélérer légèrement l'application de plans sur de gros modules. L'essentiel de la nouveauté Terraform de ce début d'année était en fait arrivé avec **Terraform 1.10** et **1.6** (sorties en 2024) qui avaient apporté un **framework de test** intégré pour les modules (New Terraform testing and UX features reduce toil, errors, and costs (https://www.hashicorp.com/en/blog/new-terraform-testing-and-ux-features-reduce-toil-errors-and-costs#:%7E:text=The%20Terraform%20test%20framework%2C%20introduced,post%20and%20Testing%20Terraform%20documentation)). Même si cette fonctionnalité a quelques mois, il convient de la rappeler car son adoption commence réellement à décoller en mars 2025 : les équipes IaC intègrent désormais des tests unitaires de leurs configurations Terraform (via le mot-clé `terraform test` en HCL) afin de valider des modules sans devoir déployer pour de vrai. Les articles de blog de HashiCorp insistent sur l'importance de tester les modules partagés pour éviter des bugs aux conséquences potentiellement graves (vu que l'IaC touche à l'infra critique) (New Terraform testing and UX features reduce toil, errors, and costs (https://www.hashicorp.com/en/blog/new-terraform-testing-and-ux-features-reduce-toil-errors-and-costs#:%7E:text=Modules%20are%20a%20primary%20way,sometimes%20testing%20is%20skipped%20altogether)) (New Terraform testing and UX features reduce toil, errors, and costs (https://www.hashicorp.com/en/blog/new-terraform-testing-and-ux-features-reduce-toil-errors-and-costs#:%7E:text=The%20Terraform%20test%20framework%2C%20introduced,post%20and%20Testing%20Terraform%20documentation)). **Maturité :** Terraform est un outil stable et éprouvé, son écosystème est énorme (des centaines de providers officiels ou communautaires). La maturité technique est excellente, comme en témoigne la stabilité de l'interface sur toute la v1.x. En revanche, sur le plan **communautaire**, une scission s'est opérée : le passage de Terraform sous licence BSL (propriétaire après un certain usage) en 2023 a conduit à la naissance du fork open-source **OpenTofu**. En mars 2025, OpenTofu (soutenu par une fondation distincte) en est à sa version 1.4 environ et vise la compatibilité avec Terraform 1.5/1.6 (Comparing OpenTofu and Terraform | Ned In The Cloud (https://nedinthecloud.com/2024/01/22/comparing-opentofu-and-terraform/#:%7E:text=Comparing%20OpenTofu%20and%20Terraform%20,that%20share%20a%20common%20ancestry)). Pour l'instant, la plupart des grands acteurs cloud continuent de fournir des providers Terraform officiels, mais on note qu'OpenTofu gagne en contributions. Il faudra surveiller dans les mois à venir si une divergence de fonctionnalités apparaît entre Terraform et OpenTofu – ce dernier se voulant 100% open-source pourrait attirer les contributeurs open qui hésitent maintenant à proposer du code à HashiCorp. Au niveau entreprise, cependant, Terraform Cloud/Enterprise reste très implanté, et HashiCorp a prolongé le support de **Terraform Enterprise en mode "installé" jusqu'en mars 2025** avant de pousser tout le monde vers Terraform Cloud SaaS (Terraform Enterprise Releases - 2025 - HashiCorp Developer (https://developer.hashicorp.com/terraform/enterprise/releases/2025#:%7E:text=Developer%20developer,release%20until%20April%201%2C%202026)). Cela marque la fin d'une ère (beaucoup d'entreprises auto-hébergeaient Terraform Enterprise) au profit du cloud managé par HashiCorp. Les utilisateurs devront donc planifier une migration ou accepter d'utiliser l'offre SaaS pour continuer à avoir les dernières versions.

Conseils : Pour les équipes IaC, Terraform 1.11 peut être adopté sans crainte, en profitant des tests HCL natifs pour renforcer la qualité infra. Il convient aussi de suivre l'actualité d'OpenTofu – même si vous restez sur Terraform, la compatibilité est assurée pour le moment, mais toute extension de Terraform (outils tiers, modules registry) pourrait envisager un double support Terraform/Tofu. Enfin, HashiCorp ayant décidé de sorties plus fréquentes (mineures mensuelles), il est important de tester régulièrement les nouvelles versions sur les pipelines CI (HashiCorp publie un *Changelog* et une documentation de migration pour chaque version mineure). À horizon 2025, on peut anticiper une version Terraform 1.12 ou 1.13 intégrant davantage d'automatisation (peut-être de l'IA – HashiCorp a montré un concept de **Terraform Copilot** en beta, similaire à Pulumi, pour suggérer du code IaC).

Ansible : transition de versions et pratiques multi-plateforme

Ansible, l'outil d'automatisation agentless de Red Hat (et de la communauté), se trouve en mars 2025 à un tournant important de son cycle de vie. D'un côté, la **communauté Ansible** maintient un rythme de releases soutenu : la série **Ansible 9.x** approche de sa fin de vie. En effet, il a été confirmé qu'**Ansible 9.13 serait la dernière version** de la série et qu'aucune extension de support n'est prévue au-delà (Ansible Community, Ansible Core and RHEL 8 - Get Help - Ansible (https://forum.ansible.com/t/ansible-community-ansible-core-and-rhel-8/11198#:%7E:text=,13)). Cela signifie que la communauté se prépare à la sortie de **Ansible 10.0** (probablement en avril/mai 2025) puis à passer relativement vite à Ansible 11 fin 2025. Cette cadence rapide est due au fait qu'Ansible (le package "batteries included") embarque énormément de collections de modules qui évoluent sans cesse, et à la volonté de coller aux versions d'**ansible-core** (le moteur ex-Base) qui suit son propre chemin (actuellement ansible-core 2.16 LTS, avec 2.17 qui devrait accompagner Ansible 10). En parallèle, du côté **Red Hat Ansible Automation Platform (AAP)** – la distribution entreprise payante – on est sur la version **AAP 2.4** depuis 2024, et des correctifs ponctuels sont publiés. En mars, Red Hat a livré *AAP 2.4 – patch 8* (12 mars) et *patch 10* (26 mars), corrigeant des CVE (ex: faille Jinja2 sandbox) et mettant à jour Automation Controller en 4.5.20 (Red Hat Ansible Automation Platform release notes | Red Hat Product Documentation (https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.4/html-single/red_hat_ansible_automation_platform_release_notes/index#:%7E:text=8,March%2026%2C%202025)) (Red Hat Ansible Automation Platform release notes | Red Hat Product Documentation (https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.4/html-single/red_hat_ansible_automation_platform_release_notes/index#:%7E:text=)). Ces patchs soulignent l'importance de maintenir Ansible à jour pour la sécurité, en particulier pour ceux utilisant l'Event-Driven Ansible (qui était en tech preview en 2024 et commence à être stable en 2025).

Nouvelles fonctionnalités : Bien que mars n'ait pas introduit de fonctionnalité révolutionnaire dans Ansible, on observe plusieurs *tendances/bonnes pratiques* mises en avant dans les blogs et conférences : l'usage des **collections** devient la norme pour organiser les playbooks et rôles, le **modèle événementiel** (découle du projet *Lightspeed* et *Event-Driven Ansible*) se concrétise – on a vu des démos d'Ansible réagissant à des événements (via RabbitMQ ou Kafka) pour déclencher des automatisations en quasi temps-réel. Par exemple, un capteur qui envoie un message peut provoquer l'exécution d'un playbook ciblé sans intervention humaine. Cela rapproche Ansible d'un outil d'orchestration d'auto-remédiation.

Aussi, **Ansible sur d'autres OS** : Microsoft a annoncé en mars que la prise en charge d'Ansible sous Windows via WSL était améliorée, et l'intégration avec **Azure** continue (les *Azure Preview Modules* pour Ansible ont été renouvelés pour supporter les derniers services cloud). **Lightspeed** (l'IA de rédaction de playbooks en partenariat avec IBM Watson) a reçu des mises à jour de modèle en début d'année, ce qui encourage son test pour accélérer l'écriture de tâches Ansible basiques via l'IDE VSCode.

Maturité : Le moteur d'Ansible-core est stable (beaucoup d'entreprises utilisent encore Ansible 2.9 ou 2.12 sans souci). Cependant, la **dualité entre la version communauté rapide et la version Red Hat lente** peut prêter à confusion. En 2025, Red Hat positionne Ansible Automation Platform comme la solution pour entreprises (avec support long, stabilité, modules certifiés), tandis que la communauté pousse des versions plus *edge*. Ce modèle est similaire à Fedora/RHEL dans Linux. Par conséquent, pour un usage critique, beaucoup restent sur Ansible 8 ou 9 community, ou directement sur AAP 2.3/2.4, qui sont bien éprouvés. L'arrivée d'Ansible 10 va apporter l'**ansible-core 2.17** et potentiellement marquer la fin du support Python 3.8 (allant vers 3.9+ uniquement). Il faudra alors vérifier la compatibilité des anciens playbooks et rôles (le portage de Python 2 est heureusement derrière nous depuis longtemps). En termes de communauté, Ansible est toujours très vivant (des milliers de modules couvrant toute la sphère IT), mais il fait face à la concurrence de Terraform sur l'IaC *déclaratif* et de nouveaux outils "API-driven". Red Hat tente de répondre à cela en combinant Ansible et **Event-Driven/Advanced Automation**, mais cela reste un marché de niche pour l'instant. L'adoption d'Ansible est stable, avec une base d'utilisateurs fidèle, notamment pour la configuration système, les déploiements on-prem et l'automatisation ad-hoc. La tendance *Infrastructure as Code* pure (déclarative) a cependant fait migrer certaines tâches vers Terraform/Pulumi, limitant Ansible aux configurations post-provisionnement. À surveiller : la proposition en cours de faire de **Ansible 11 une LTS prolongée** ([vote open until 2025-04-16] Make Ansible 11 a "LTS" (similar to ... (https://forum.ansible.com/t/vote-open-until-2025-04-16-make-ansible-11-a-lts-similar-to-ansible-9/40851#:%7E:text=%5Bvote%20open%20until%202025,the)), qui pourrait satisfaire ceux voulant un cycle plus lent. Si acceptée, cela signifierait qu'Ansible 11 (fin 2025) pourrait être maintenu 2 ans, offrant une alternative aux mises à jour annuelles obligatoires.

En somme, pour mars 2025, **la recommandation** est de planifier la transition vers Ansible 10.x d'ici fin d'année, de tester les playbooks avec ansible-core 2.17 (dès qu'il sera dispo en release candidate), et pour les utilisateurs AAP 2.4, d'appliquer les derniers patchs de sécurité. Penser aussi à modulariser via des collections, car Red Hat et la communauté poussent ce modèle (Galaxy Hub). Ansible demeure **mature pour la config automatisée**, et son intégration à de nombreux écosystèmes (VMware, AWS, etc. via des modules officiels) en fait encore un atout dans la toolbox DevOps.

Pulumi : IaC orienté développeur et intégration DevSecOps

Pulumi, l'outil d'IaC en langage de programmation général (TypeScript, Python, Go, etc.), continue de tracer son chemin en misant sur l'expérience développeur et la sécurité. Fin mars 2025, Pulumi a annoncé une série d'améliorations de son service cloud (Pulumi Cloud) et de sa plateforme, avec un accent marqué sur la **gestion des secrets et la gouvernance** (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=Infrastructure,greater%20control%20over%20cloud%20resources)) :

- **Automatisation de la rotation des secrets** : Pulumi propose un composant nommé *ESC* (Embedded Secrets Configuration) pour stocker et injecter les secrets dans les stacks IaC. En mars, une nouvelle fonctionnalité de **Rotated Secrets** a été introduite. Dorénavant, Pulumi peut automatiquement faire tourner (rotate) les secrets stockés de façon programmée, en adoptant une stratégie "dual-secret" où à tout instant deux secrets – l'ancien et le nouveau – sont valides, assurant une transition en douceur lors du roulement (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=The%20first%20announcement%20is%20the,while%20integrating%20with%20existing%20workflows)). Par exemple, si une base de données utilise un mot de passe géré par Pulumi, celui-ci peut être renouvelé périodiquement et Pulumi orchestrera la mise à jour de l'infra (rotation du secret dans le cloud provider, mise à jour du secret Kubernetes, etc.) sans interruption de service. Cette automatisation du cycle de vie des secrets est une **bonne pratique DevSecOps** pour éviter les secrets statiques à long terme qui augmentent le risque en cas de fuite. Pulumi facilite ainsi l'implémentation du principe de "secret zéro-jour" (rotation fréquente).

- **Intégration sécurisée à GitHub Actions** : Conscient de la popularité de GitHub Actions, Pulumi a sorti en mars une **Pulumi ESC GitHub Action** officielle (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=history%20of%20credentials%2C%20when%20they,rotated%20and%20who%20accessed%20them)). Celle-ci permet à un workflow GitHub d'obtenir des secrets depuis Pulumi de manière éphémère, **sans les stocker comme variables GitHub**. En d'autres termes, plutôt que de conserver un secret sensible (clé cloud, etc.) dans les *GitHub Secrets* (où il pourrait être extrait si un Action malveillant est exécuté, cf. l'incident mentionné plus haut), le workflow fait appel à Pulumi qui injecte le secret au moment voulu puis le révoque. Cela réduit énormément la fenêtre d'exposition et évite de multiplier les copies de secrets. Ce mécanisme s'inscrit dans la tendance **"Zero Trust CI"** où on ne fait plus confiance aveuglément à l'environnement d'exécution CI et on minimise ce qui y réside en clair.

- **Nouveau système de RBAC** : Pulumi Cloud se dote d'un **RBAC unifié et granulaire**. Les administrateurs peuvent définir des rôles personnalisés avec des permissions fines (ex : qui peut déployer sur tel stack, qui peut consulter les logs, etc.) (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=Up%20next%2C%20Pulumi%20has%20launched,ESC%20environments%20and%20Insights%20accounts)). Cela répond à la demande des grandes organisations qui veulent segmenter l'accès à l'infrastructure-as-code de la même façon qu'elles le font pour l'infrastructure elle-même. Avec ce RBAC, Pulumi se positionne clairement pour un usage **multi-équipes / multi-projets** en entreprise, rivalisant ainsi avec Terraform Cloud sur ce terrain de la gouvernance centralisée.

- **Policy as Code étendue** : Pulumi Insights, le module de gouvernance et d'observabilité des déploiements, étend son champ d'action. Désormais, Pulumi peut appliquer des **politiques de conformité** non seulement aux ressources gérées par Pulumi, mais également aux ressources externes découvertes sur le cloud (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=organization,ESC%20environments%20and%20Insights%20accounts)). En clair, Pulumi peut auditer l'état du compte cloud et signaler des écarts de conformité même sur des ressources créées en dehors de Pulumi (par exemple, une VM créée manuellement ou via un autre outil). Cette vision globale aide à détecter les *shadow IT* ou les dérives par rapport aux standards (ex: un bucket S3 non chiffré) et de les ramener dans le giron de l'IaC ou de les corriger. Couplé à la fonctionnalité *Drift Detection* déjà présente, Pulumi se dote donc d'outils pour assurer l'**alignement constant** de l'infrastructure réelle sur les politiques souhaitées.

Maturité et perspectives : Pulumi en est à sa 5e année d'existence et gagne en fonctionnalités d'entreprise tout en conservant sa philosophie *"Infrastructure pour développeurs"*. L'intégration d'un Copilot IA (en beta depuis 2024) et ces nouveautés de mars 2025 montrent que Pulumi cherche à combler les lacunes perçues de Terraform : écriture du code plus assistée, et meilleure intégration dans les workflows CI/CD modernes. Pulumi reste cependant **moins répandu** que Terraform dans la base installée, mais on observe une adoption

croissante, notamment dans les organisations déjà orientées “tout-dev” (qui aiment écrire l’infra en TypeScript pour bénéficier du typage et de l’IDE, par exemple). En mars, un cas d’usage marquant a été publié : une grande fintech a partagé son retour sur la migration de 3000 ressources AWS de CloudFormation vers Pulumi, avec des pipelines GitHub Actions orchestrés par Pulumi (mettant en avant justement l’intérêt des secrets dynamiques). Ce type de retour crédibilise Pulumi pour du large scale.

En termes de support, Pulumi a aligné ses providers sur les nouveautés cloud très rapidement (par ex, le provider AWS a supporté quelques nouveautés annoncées à AWS re:Invent 2024 dès février). La **roadmap** Pulumi pour 2025 inclut possiblement la prise en charge du langage Java (encore en preview) pour séduire le monde enterprise Java, et l’amélioration des temps d’exécution (`pulumi preview` plus rapide sur gros states). Pulumi a aussi mentionné travailler sur la réduction de la taille de ses SDKs, ce qui a été accompli pour Azure (taille réduite de 75% (Pulumi Blog (https://www.pulumi.com/blog/#:%7E:text=Pulumi%20Blog%20This%20release%20delivers,Azure%20Native%20provides%20direct))) – cela facilite la vie des développeurs en allégeant les dépendances.

Conseil : Pour les équipes attirées par Pulumi, mars 2025 apporte un signal positif : l’outil est suffisamment mature pour être utilisé en environnement complexe en toute sécurité (les features RBAC, secrets mgmt en attestent) et l’éditeur semble réactif aux préoccupations DevSecOps. La coexistence Terraform/Pulumi est possible (des passerelles existent pour importer un state Terraform dans Pulumi, etc.), mais demande de la rigueur pour ne pas gérer la même ressource avec deux outils. Sur la question de la licence, Pulumi est 100% open-source (licence Apache 2.0) pour son CLI, avec un modèle SaaS optionnel : cela peut rassurer ceux échaudés par le cas HashiCorp. En synthèse, Pulumi se positionne en **outsider sérieux** qu’il faudra continuer de surveiller, notamment si l’IA Copilot de Pulumi (annoncé en 2024) devient un argument clé – la promesse étant qu’un dev pourrait demander en langage naturel “Crée-moi un VPC avec 3 subnets privés et un NAT” et que Pulumi génère le code IaC correspondant. Ce genre de fonctionnalités pourrait rebattre les cartes de l’adoption IaC dans les années à venir.

Chef, Puppet et co. : maintenance continue et intégration au DevOps moderne

Les outils d’Infrastructure as Code plus anciens comme **Chef** et **Puppet** ont poursuivi leur vie en mars 2025 dans une relative discrétion, se concentrant sur des mises à jour de maintenance. **Chef**, désormais sous l’égide de Progress Software, a diffusé en mars plusieurs versions correctives : *Chef Infra Server 15.10.33* (3 mars 2025) et *Chef Infra Client 18.7.3* (31 mars 2025) (Chef Release Announcements - Chef Questions (https://discourse.chef.io/c/chef-release/9#:%7E:text=0%2075%20March%203%2C%202025,17)), ainsi que des mises à jour de Chef InSpec (5.22.72) et Chef Automate. Ces versions n’apportent pas de nouvelles fonctionnalités marquantes, mais intègrent les derniers correctifs de sécurité (par ex. mise à jour des dépendances Ruby, correction d’une vulnérabilité dans InSpec) et le support des plateformes récentes (compatibilité de l’Agent avec RHEL 9.3, Debian 12, etc.). **Analyse maturité :** Chef Infra est un outil de configuration système très stable et éprouvé, utilisé dans de grandes entreprises (notamment dans le retail, la finance) pour gérer des milliers de serveurs. Cependant, il est souvent perçu comme appartenant à la “génération précédente” d’outils par rapport aux approches déclaratives/cloud-native. En 2025, Chef est principalement utilisé pour la gestion de configurations *post-déploiement* (installer des logiciels sur des VM, appliquer des politiques de sécurité sur des OS, etc.), et on voit fréquemment Chef cohabiter avec Terraform (Terraform crée la VM, Chef la configure). Progress tente de moderniser l’offre via le *Chef Enterprise Automation Stack*, en y intégrant Habitat (packaging applicatif) et InSpec (scans de compliance). En mars 2025, Progress a d’ailleurs été nommé dans une étude (*Constellation ShortList*) comme l’une des plateformes DevOps reconnues pour la gestion de configurations (Progress Chef Platform Named to Constellation ShortList™ (https://www.globenewswire.com/news-release/2025/03/11/3040667/0/en/Progress-Chef-Platform-Named-to-Constellation-ShortList-for-DevOps.html#:%7E:text=Progress%20Chef%20Platform%20Named%20to,Source%3A%20Progress%20Software%20Corporation)), preuve que l’outil reste pertinent. **Puppet**, de son côté (maintenant chez Perforce), a concentré en début 2025 ses efforts sur Puppet Comply (audits) et la simplification de Puppetize pour Kubernetes. Il n’y a pas eu d’annonce spécifique en mars, mais Puppet Enterprise suit aussi un rythme de patch trimestriel. Ces outils, bien qu’en “fonds de tableau” de l’actualité, continuent d’évoluer discrètement pour s’adapter à l’infrastructure hybride (par ex. Chef Inspec intègre de plus en plus de profils de sécurité cloud, Puppet a des modules pour gérer du GCP/Azure).

Conseil : Les équipes utilisant Chef/Puppet peuvent continuer de le faire en confiance si cela répond à leurs besoins, mais elles doivent être conscientes que l’industrie se dirige vers d’autres paradigmes (conteneurs immuables, GitOps…). Il peut être judicieux de surveiller comment **Ansible** ou d’autres solutions plus cloud-friendly peuvent parfois remplacer ou compléter Chef/Puppet sur certaines tâches (par exemple, des entreprises remplacent leur cookbook Chef de déploiement d’app sur VM par un pipeline CI + image Docker + orchestrateur). Néanmoins, pour la gestion fine d’OS, Chef reste très puissant (système de recettes mature, testable via Test Kitchen, etc.). La sortie de *Chef Infra Client 19* est attendue plus tard en 2025, possiblement avec un passage à Ruby 3 natif et l’intégration de features de Chef Habitat. L’un des challenges sera de voir comment **Chef et Puppet s’intègrent dans les flux DevOps globalisés** : Progress travaille à rendre Chef utilisable via des pipelines GitHub Actions/Azure DevOps (il existe des actions GitHub officielles pour lancer des cookbooks), ce qui facilite son utilisation dans des environnements *GitOps* (on stocke les cookbooks en Git, pipeline les applique). Donc, bien que moins en lumière, Chef et consorts continuent d’être maintenus pour ne pas freiner les organisations qui les ont adoptés à large échelle. L’annonce de mars d’un support prolongé jusqu’en 2026 pour Chef 18.x (Chef Release Announcements (https://discourse.chef.io/c/chef-release/9#:%7E:text=Chef%20Release%20Announcements%20%3B%20Chef,0%2C%2094%2C%20March%203%2C%202025)) assure une **stabilité à long terme** pour les clients.

Observabilité et DevSecOps

Observabilité open source : l’ère de Prometheus+OpenTelemetry et de l’IA Ops

Les pratiques d’**observabilité** (monitoring, logs, traces, etc.) ont clairement atteint une nouvelle étape de maturité en 2025, comme le révèle l’**Observability Survey 2025** de Grafana Labs dévoilé le 25 mars. Cette enquête (1255 répondants) souligne la domination des outils open source : **75 % des entreprises utilisent des solutions d’observabilité en open source** et 70 % combinent spécifiquement **Prometheus** et **OpenTelemetry** dans leur stack (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=Grafana%20Labs%20Shares%20Open%20Source,Using%20Open%20Source%20Observability%20Tools)) (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=,quarters%20of%20all)). Cela confirme que le duo *Prometheus (métriques) + OpenTelemetry (traces, logs, métriques)* est en train de s’imposer comme standard de facto, éclipsant progressivement des solutions propriétaires ou fermées.

Plusieurs tendances fortes ressortent pour l’année 2025 en observabilité :

- **Convergence des signaux** : On observe une intégration accrue entre les différents types de données. OpenTelemetry, projet unificateur, a atteint des jalons importants – par exemple la **stabilisation du signal de profiling** (analyse de performance fine des applications) qui vient s’ajouter aux traces, métriques et logs déjà supportés (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-

2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=advancements%20from%20the%20past%20year%2C,Spring%20Boot%20starter%2C%20and%20helping)). Désormais, une seule instrumentation OpenTelemetry peut couvrir la collecte de traces distribuées et de profils CPU/mémoire, ce qui enrichit considérablement le diagnostic de performance. De plus, OpenTelemetry a amélioré le support des dernières **conventions sémantiques** pour uniformiser les métriques d'infrastructure, rendant plus facile la corrélation entre métriques Prometheus et traces OTel (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=advancements%20from%20the%20past%20year%2C,Spring%20Boot%20starter%2C%20and%20helping)). Grafana Labs a annoncé contribuer à cette interopérabilité en développant des passerelles entre **Prometheus et OpenTelemetry** (par ex. des exporters Prometheus vers OTel) (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=,quarters%20of%20all)). Tout cela vise à fournir aux équipes une **vue unifiée** de la santé des systèmes – un aspect crucial alors que la complexité des environnements microservices reste le souci #1 exprimé dans l'enquête Grafana. En effet, la moitié des répondants ont augmenté leurs investissements en Prometheus et OTel sur 2 années consécutives, montrant une confiance dans ces outils pour maîtriser la complexité croissante (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=,quarters%20of%20all)).

- **Focus sur l'AI Ops** : Avec la pléthore de données télémétriques à disposition, l'intérêt se porte sur l'**intelligence artificielle appliquée à l'observabilité**. Les deux besoins les plus cités par les utilisateurs sont *la réduction de la fatigue d'alertes* et *l'accélération de l'analyse de cause racine*, et beaucoup voient dans l'IA/ML un moyen de les adresser (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=,focused%20on%20getting%20value%20from)). En mars, on a ainsi vu plusieurs annonces. Datadog et New Relic (éditeurs SaaS) ont communiqué sur des fonctionnalités de détection d'anomalies pilotées par ML plus automatisées. Côté open source, Grafana intègre déjà depuis v9 des suggestions basiques, et promet via son module Mimir d'explorer du machine learning pour détecter des motifs inhabituels dans les métriques. Un article notable d'OpenTelemetry de mars examine les *"AI Agent Observability"*, c'est-à-dire comment tracer et monitorer des agents IA (comme ChatGPT ou autres) qui prennent des décisions – un sujet de niche mais révélateur que l'IA devient à la fois l'outil et l'objet de l'observabilité (AI Agent Observability - Evolving Standards and Best Practices | OpenTelemetry (https://opentelemetry.io/blog/2025/ai-agent-observability/#:%7E:text=,Instrumentation%20Beta)) (AI Agent Observability - Evolving Standards and Best Practices | OpenTelemetry (https://opentelemetry.io/blog/2025/ai-agent-observability/#:%7E:text=AI%20Agents%20are%20becoming%20the,especially%20when%20scaling%20these%20agents)). **Concrètement**, on peut s'attendre à l'arrivée de fonctionnalités telles que : des alertes plus intelligentes (par ex. qui regroupent plusieurs symptômes en une seule alerte multi-signal pour éviter le spam), des systèmes d'**auto-explanation** (un assistant qui commente un tableau de bord Grafana pour expliquer une anomalie), et des *correlators* qui proposent automatiquement une cause probable en croisant logs et métriques.

- **Profiling et amélioration continue** : L'observabilité ne sert pas que pendant les incidents, elle devient un outil d'optimisation continue. Par exemple, l'intégration d'**outils de profiling** (Pyroscope, Parca, etc.) dans les suites existantes se généralise. Grafana a annoncé durant KubeCon que son outil de profiling (Pyroscope) a atteint la v1.13 et s'intègre étroitement avec Tempo (tracing) pour lier un trace à un profil sur un intervalle de temps (Download Grafana | Grafana Labs (https://grafana.com/grafana/download#:%7E:text=March%2025%2C%202025,50GB%20traces%2C%2050GB%20profiles)). Ceci aide les développeurs à identifier les *goulets d'étranglement* de performance directement depuis leurs traces de requêtes. De plus, la part belle est donnée aux **SLOs (Service Level Objectives)** : l'enquête Grafana note que les orga dont la direction considère l'observabilité comme critique sont plus enclines à mettre en place des SLO, du tracing et de l'Otel (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=OpenTelemetry%20and%20Prometheus%20during%20the,The%20number%20one%20observability%20concern)). On voit ainsi les SLO (et leur suivi via Grafana ou SquaredUp) devenir un standard pour communiquer de la fiabilité de service jusqu'au niveau exécutif.

Maturité : L'écosystème open source d'observabilité est désormais très mature. Prometheus est en version 2.x stable depuis plusieurs années, Grafana est en v11.x avec une interface aboutie. OpenTelemetry a atteint ou approche la **version 1.0** pour la majorité de ses composants (traces et metrics déjà 1.0, logs en cours de stabilisation). Le fait que 75% des entreprises s'appuient sur l'open source signifie qu'il existe un large support (communautaire et commercial) pour ces outils. Des distributions commerciales *supportées* d'OpenTelemetry apparaissent (Elastic a lancé en mars une distribution OpenTelemetry supportée sur sa suite (Elastic Launches Enterprise-Grade OpenTelemetry Distribution with ... (https://www.stocktitan.net/news/ESTC/elastic-announces-general-availability-of-elastic-distributions-of-5z6t3dz9axh6.html#:%7E:text=Elastic%20Launches%20Enterprise,grade%20support))). On assiste peut-être à ce qu'on a connu pour Linux : un noyau open source utilisé partout, avec différentes entreprises offrant du support autour (Datadog, Dynatrace et consorts étant aux "Red Hat" du monde obs).

Pour les ingénieurs en observabilité, mars 2025 confirme qu'il faut maîtriser OpenTelemetry car il devient la pierre angulaire pour instrumenter les applis. De même, apprendre à gérer la **scalabilité des data** (Stockage longue durée via Mimir pour métriques, Loki pour logs, Tempo pour traces) est crucial. Une annonce de Grafana Labs en mars sur le **Fleet Management** de collecteurs montre qu'on outille maintenant la gestion à large échelle des pipelines de collecte (centraliser la config de centaines d'agents promtail, etc.) (Grafana Labs Extends Observability Reach Deeper into Kubernetes (https://cloudnativenow.com/news/grafana-labs-extends-observability-reach-deeper-into-kubernetes/#:%7E:text=Kubernetes%20cloudnativenow,management%20of%20telemetry%20data%20collectors)). Ceci améliore la fiabilité et réduit la charge Ops liée à l'observabilité elle-même.

Enfin, la dimension **coût** n'est pas oubliée : si 75% des orga disent que le coût compte, moins d'un tiers s'en inquiètent excessivement (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=obstacle%20to%20faster%20incident%20response%2C,just%20selecting%20the%20cheapest%20option)), ce qui indique qu'elles privilégient la valeur apportée. Néanmoins, on voit une montée du **FinOps** pour l'observabilité : compression des données, filtrage à la source pour n'ingérer que le pertinent, etc. Des projets comme **Parca** promettent un profiling continu à moindre coût, Loki permet de ne pas tout indexer pour réduire la facture. Autant de techniques à appliquer pour garder l'observabilité soutenable financièrement.

Sécurité du cycle DevOps : vers le "everything as code" sécurisé et la supply chain protégée

En mars 2025, la sécurité dans le cycle DevOps (DevSecOps) a été mise sur le devant de la scène notamment par l'incident GitHub Actions déjà relaté. Les organisations ont pris conscience que la **supply chain logicielle** est aussi forte que son maillon le plus faible, qui peut être un script CI/CD. Au-delà de cet incident, plusieurs éléments clefs ont rythmé la veille DevSecOps du mois :

- **Nouvelles réglementations et standards** : Le mouvement autour des **SBOM (Software Bill of Materials)** continue de prendre de l'ampleur. Suite à l'Executive Order américain de 2024, de nombreux fournisseurs ont commencé à fournir des SBOM pour leurs produits. En mars 2025, on a vu des outils open source comme *Syft/Grype* ou *CycloneDX* devenir presque un passage obligé dans les pipelines de build, pour générer l'inventaire des composants logiciels. Certaines grandes entreprises établies (par ex. Siemens) ont partagé en conférences comment elles intègrent des SBOM dans leur gestion de risques. De plus, le standard **SLSA (Supply Chain Levels for Software Artifacts)** a été réévalué : plusieurs organisations visent un niveau SLSA 3 pour leurs projets internes (signatures attestant la provenance, etc.). Des projets comme Tekton Chains ou GitLab Integrity attestent cryptographiquement que le build CI n'a pas été altéré. Bien que cela reste technique, mars a vu la sortie de **SLSA v1.0** en tant que standard officiel, clarifiant les exigences de chaque niveau.

- **Secrets Management et Zero Trust** : Outre l'exemple Pulumi mentionné précédemment, d'autres outils ont cherché à améliorer la gestion des secrets en CI. HashiCorp Vault, la référence en la matière, a sorti en mars la v1.14 avec des performances accrues et un meilleur intégration aux *Kubernetes Secret Store CSI drivers*. Microsoft a annoncé la preview d'**Azure Managed HSM integration** pour GitHub Actions (stockage de secrets Actions dans un HSM cloud plutôt que dans GitHub). On tend globalement vers un modèle où **les secrets ne résident plus en clair** dans les plateformes DevOps, mais sont appelés à la demande, un peu comme Pulumi l'a fait. Ce principe Zero Trust s'étend également aux environnements d'exécution : par exemple GitHub a renforcé l'isolation de ses runners hébergés pour éviter les cross-job token leak. De son côté, GitLab a introduit (17.9) un *Vault*, alternative à HashiCorp Vault, pour stocker les secrets CI/CD de manière chiffrée, traduisant la demande des clients.

- **Collaboration Dev-Sec-Ops** : La culture DevSecOps se reflète aussi dans l'organisation. En mars 2025, plusieurs conférences (telles que *DevSecCon* virtuel) ont mis en avant le concept d'**équipes fusionnées** ou *Purple Teams*. Les *Security Champions* (développeurs sensibilisés sécurité) dans les squads agiles sont de plus en plus courants. On a vu également l'essor de l'**Infrastructure as Code Scanning** : les mêmes outils qui scannent du code applicatif (SAST) sont maintenant appliqués aux fichiers Terraform, Kubernetes YAML, Dockerfiles pour détecter des erreurs de config ou des mauvaises pratiques. Par exemple, *Checkov*, *kics*, *Tfsec* ont eu des mises à jour en mars pour couvrir de nouveaux types de règles de compliance (NIST, ISO27001 sur l'infra). Cela permet aux devs infra de recevoir des retours sécurité en PR, bien en amont du déploiement.

- **Retour d'expérience Log4Shell++** : Bien que l'affaire Log4Shell date de fin 2021, elle a eu un impact durable. En mars 2025, un rapport de l'ENISA a fait état que 50% des entreprises européennes interrogées ont mis en place un plan de réponse aux vulnérabilités de la supply chain post-Log4Shell. Cela inclut une **meilleure inventory des dépendances**, le déploiement de scanners de vulnérabilités (SCA – Software Composition Analysis). On a vu des projets comme *Dependabot* ou *Renovate* utilisés plus strictement : par ex, certaines orga imposent que toute dépendance out-datée soit mise à jour dans le mois.

- **CI/CD et conformité** : Les pipelines eux-mêmes entrent dans le scope d'audit. En mars, **Azure DevOps** a implémenté la possibilité d'attacher des attestations de build (e.g. via in-toto) pour prouver qu'un artifact provient d'un pipeline donné. De plus, la **norme ISO/IEC 27001:2025** qui doit paraître plus tard cette année devrait inclure une section sur la sécurité des pipelines CI/CD, officialisant l'idée que les systèmes de build doivent avoir des contrôles (accès restreint, logs conservés, etc.). Ainsi, les responsables sécurité commencent à demander des comptes non seulement sur les applis en prod, mais aussi sur les jobs Jenkins ou GitLab qui les fabriquent.

Événements et communauté DevSecOps : En mars se sont tenus plusieurs meetups et webinaires sur ces sujets. Citons *"DevOps Connect: DevSecOps at RSA Conference"* (en préparation de RSAConf avril), ou le sommet *TechStrong Con: DevSecOps* où des experts ont échangé sur l'état de l'art. Il en ressort un message clair : la **sécurité doit être traitée au même titre que le code** dans le pipeline. Les outils se multiplient pour aider (beaucoup d'open source, mais aussi des solutions comme Palo Alto Prisma Cloud, Aquasec, Sysdig Secure, etc.). Toutefois, il reste un **travail humain** important de formation et d'intégration entre équipes. DevSecOps ne peut réussir que si les silos tombent : c'est encourageant de voir des *SecOps* participer à des sprints Dev ou des *Chaos Days* inclure des scénarios d'attaque interne.

En résumé, mars 2025 nous montre un paysage DevSecOps en consolidation : les grandes lignes directrices (supply chain sécurisée, automatisation des contrôles, zero trust dans CI, culture collaboratives) sont connues, et on passe à l'**outillage concret** et la généralisation. La maturité est encore variable selon les organisations – certaines très avancées signent tout de bout en bout, d'autres démarrent à peine le scanning de conteneurs – mais la tendance est irréversible vers davantage de sécurité intégrée. Les nouveautés techniques (ex: rotation automatique de secrets Pulumi, pinned actions GitHub, etc.) sont autant de briques qui viennent faciliter l'adoption de ces bonnes pratiques en les rendant plus automatiques et moins contraignantes pour les développeurs.

Événements DevOps marquants en mars 2025

Le mois de mars a également été ponctué de plusieurs **événements, conférences et initiatives communautaires** dans le domaine DevOps :

- **The DEVOPS Conference – Global** : Le 26 mars 2025 a eu lieu à Londres (et en ligne) "The DEVOPS Conference", un événement international gratuit axé sur les dernières tendances DevOps (DevOps Conferences & Events 2025: Complete Guide | Splunk (https://www.splunk.com/en_us/blog/learn/devops-conferences-events.html#:%7E:text=Cost%3A%C2%A0Starting%20at%20%C2%A3270)). Cette conférence, organisée par Eficode, a rassemblé plus de 9000 participants virtuels et 200 en présentiel. Les thèmes phares ont été la montée de l'**IA dans le développement logiciel** et la maîtrise du **platform engineering**. Des intervenants de grands groupes (Google, Spotify…) ont partagé des conseils pratiques pour adopter l'IA de manière responsable dans les pipelines CI/CD ou pour mettre en place des plateformes internes auto-servies. Par exemple, on a beaucoup parlé de l'usage de ChatGPT comme assistant aux opérations (pour générer des scripts Terraform basiques, etc.) – tout en rappelant les risques (les solutions AI ne doivent pas être utilisées sans validation humaine). Le sujet du platform engineering a été traité via des retours d'expérience : comment des entreprises ont construit des "portails développeurs" offrant base de code, pipeline CI/CD prêt à l'emploi, environnement Kubernetes managé, afin de réduire la charge cognitive sur les équipes produit. Un leitmotiv a été *"Developer Experience"* (DX) qui est devenu aussi important que l'expérience utilisateur finale. On a également noté, durant les panels, l'accent mis sur la **culture DevOps** : ce n'est pas qu'outiller, c'est aussi encourager la prise de responsabilité de bout en bout par les équipes produits. La conférence a délivré un *certificate* aux participants, soulignant son aspect éducatif. Pour ceux qui souhaitent approfondir, les sessions sont souvent disponibles en replay sur YouTube (DevOps Conference 2025).

- **Meetups et événements locaux** : En mars, le circuit des **DevOpsDays** s'est poursuivi dans plusieurs villes. Par exemple, **DevOpsDays Atlanta 2025** s'est tenu mi-mars en format présentiel, traitant de l'observabilité et du leadership DevOps. En France, on a eu un meetup **"Paris Kubernetes"** fin mars où des speakers de Datadog et OVHcloud ont abordé la gestion multi-clusters et le WebAssembly dans Kubernetes. Aussi, les **Communautés Ansible francophones** ont organisé un webinar le 19 mars pour discuter

de la fin de vie d'Ansible 9 et des meilleures pratiques de migration vers Ansible 10 (ce qui a permis aux utilisateurs de poser des questions directes aux mainteneurs de la communauté). Ce type d'événement local est précieux pour glaner des conseils concrets et networker.

- **Conférence Cloud & Kubernetes (KubeCon EU 2025)** : Bien que se déroulant officiellement début avril (1-4 avril), KubeCon EU a concentré beaucoup d'annonces déjà en mars (puisque les entreprises publient souvent leurs communiqués juste avant ou pendant la conférence). KubeCon EU 2025 à Londres fut un événement majeur (plus de 10 000 participants). On peut citer la **Keynote de la CNCF** le 25 mars, qui a mis en lumière les projets CNCF émergents – par exemple, la **promotion d'Apache APISIX (API Gateway)** et de **OpenFeature (feature flags)** au stade incubating. De nombreuses annonces éditeurs ont eu lieu à l'occasion : **AWS** a présenté des améliorations de son service EKS (aperçu d'EKS v1.32, support des sidecars), **Google Cloud** a teasé des fonctionnalités Autopilot avancées (scheduling optimisé par AI), et **Azure** a annoncé l'aperçu de **Azure Kubernetes Fleet Manager** pour gérer plusieurs clusters AKS de façon cohérente. On a également parlé *Green IT* avec des sessions sur l'efficacité énergétique de Kubernetes (scheduler orienté économies d'énergie). Ce foisonnement d'informations a évidemment de l'impact sur la veille DevOps d'avril, mais dès mars il fallait avoir un œil dessus.

- **Certifications et formations** : Mars a vu quelques nouveautés en termes de certifications professionnelles. La **Linux Foundation** a lancé la certification **DFCAR (DevOps For Container Adoption Role)**, visant à valider les compétences DevOps spécifiques à l'adoption de conteneurs et Kubernetes en entreprise (un mix de CKAD + CKA + notion de CI/CD). C'est assez ciblé, mais reflète la demande des entreprises pour des talents capables de mener la transformation conteneurs. Par ailleurs, **GitHub** a actualisé en mars son examen de certification *GitHub Actions* (disponible sur la plateforme de formation de GitHub), pour y inclure les dernières features (cache v3, etc.) (GitHub Actions Certification Exams - UPDATED March 2025 | Udemy (https://www.udemy.com/course/github-actions-certification-practice-exams-march-2025/?srsltid=AfmBOorxi0y7lSlzWpPGBiRyf4wOA2h89Lvlnej1s_tnMcLoPCabPLMT#:%7E:text=GitHub%20Actions%20Certification%20Exams%20,with%20our%20meticulously%20). Ce genre de micro-certification atteste qu'un ingénieur maîtrise bien l'outil CI de GitHub – potentiellement utile sur un CV quand l'outil est très utilisé chez un employeur. Enfin, du côté des formations gratuites, l'initiative de l'**AWS DevOps Professional Challenge** a eu lieu en mars : un bootcamp en ligne de 4 semaines pour préparer la certif AWS DevOps Engineer – beaucoup y ont participé et les retours mentionnent une bonne mise à jour sur les services AWS CodePipeline, CodeBuild, etc.

- **Communautés open-source** : Le mois de mars a aussi été rythmé par des sorties de nouvelles versions dans de nombreux projets open-source DevOps. Par exemple, la version 2.0 de **FluxCD** (outil GitOps alternatif) a été publiée en RC avec une refonte de son kustomize controller. **Backstage** (plateforme développeur open source) a sorti un plugin pour visualiser les pipelines Jenkins et GitHub Actions directement dans son UI, facilitant l'adoption de la philosophie "DevOps self-service". Ce bouillonnement de la communauté signifie qu'il est toujours utile de consulter les newsletters spécialisées (ex: *DevOps Weekly*, *KubeWeekly*) pour ne rien manquer.

Perspectives pour les mois à venir

Le paysage DevOps évolue sans cesse, et à l'issue de ce mois de mars 2025, on peut dégager quelques perspectives sur ce qui va compter dans les prochains mois :

- **Montée en version des outils majeurs** : Le trimestre à venir verra plusieurs sorties importantes. **GitLab 18.0** est planifié pour mai 2025 (Releases | GitLab (https://about.gitlab.com/releases/categories/releases/#:%7E:text=Apr%2017%2C%202025)) et apportera assurément son lot de nouveautés (on s'attend à encore plus d'intégration AI dans toutes les features DevOps de la plateforme et peut-être des changements d'architecture pour la scaler). **Kubernetes 1.33** en avril concrétisera les évolutions anticipées : les équipes SRE devront vite se positionner pour l'adopter ou non (sachant que les distributions Cloud le pousseront quelques mois plus tard). **Jenkins** pourrait publier la seconde partie de sa refonte UI (Part 2 du blog) avec possiblement un aperçu d'un nouveau thème ou d'une console modernisée – si cela se confirme, ce serait un tournant pour les utilisateurs Jenkins qui depuis longtemps adaptent l'outil via des plugins.

- **Outils émergents à surveiller** : Dans le domaine CI/CD, on garde un œil sur **Tekton** (pipeline Kubernetes natif) qui sort version après version et s'intègre bien avec Argo; Tekton commence à être utilisé dans des offres cloud CI (OpenShift Pipelines, etc.). Sur l'infra as code, **CDKTF (Cloud Development Kit for Terraform)** de HashiCorp pourrait combler le vide vis-à-vis de Pulumi en permettant d'écrire du Terraform en Python/TypeScript – s'il devient stable courant 2025, cela offrira une alternative aux fans de Terraform qui veulent du langage haut niveau. Côté conteneurs, **Wasm** (WebAssembly) comme alternative légère à Docker se concrétise : Docker a une preview de runWasm, Kubernetes via les projets like runwasi – peut-être verrons-nous d'ici fin 2025 des premiers usages en prod de WebAssembly pour des microservices (cas d'usage typique : fonctions serverless ultra-rapides). Sur l'observabilité, un projet comme **GraphQL for Prometheus** (Perses) ou des nouveautés **OpenTelemetry** (comme l'expansion vers l'observabilité de pipelines CI/CD (AI Agent Observability - Evolving Standards and Best Practices | OpenTelemetry (https://opentelemetry.io/blog/2025/ai-agent-observability/#:%7E:text=,Instrumentation%20Beta)) (AI Agent Observability - Evolving Standards and Best Practices OpenTelemetry (https://opentelemetry.io/blog/2025/ai-agent-observability/#:%7E:text=,18))) peuvent changer la donne sur comment on interroge et utilise les données. Enfin en DevSecOps, le standard **OCI v1.1** devrait être finalisé – il permettra de signer les images conteneurs de façon plus native (notation, cosign) et de stocker des attestations SBOM dans les registries; ceci deviendra un must-have pour toute chaîne CI produisant des conteneurs.

- **Impacts organisationnels** : Le ralentissement des sorties massives (on l'a vu ce mois-ci, pas de K8s nouveau etc.) peut aider les organisations à **consolider leurs pratiques**. On anticipe une **standardisation accrue** : ex, GitOps se normalise comme approche de CD, FinOps se structure pour le pilotage coûts, etc. Les rôles en entreprise continuent d'évoluer : on voit apparaître des postes de *Platform Engineers*, des *Site Reliability Engineers* plus nombreux, alors que le rôle classique *"Build & Release Engineer"* se transforme pour maîtriser les plateformes CI/CD as-a-Service. La collaboration inter-équipes va rester un enjeu central – les entreprises qui réussissent à créer des *communautés internes DevOps* (chapters, guildes) pour partager outils et connaissances seront celles qui tireront le meilleur parti de l'innovation technique.

- **Adoption du Cloud & Edge** : Sur un plan plus large, l'adoption du cloud public et des architectures hybrides continue de façonner la roadmap DevOps. Les entreprises qui migrent sur cloud investissent massivement dans la containerisation et l'automatisation IaC. En 2025, on commence aussi à parler du **DevOps à l'Edge** (déployer des workloads dans des mini-datacenters ou sur le terrain, avec GitOps + K3s par ex.). On peut donc s'attendre à voir d'ici fin 2025 des outils orientés edge (Rancher k3s, Fleet, etc.) gagner en popularité pour gérer des centaines de clusters edge. Ce sera un domaine où les pratiques DevOps devront s'adapter (par ex, CI/CD avec connectivité intermittente, observabilité edge centralisée).

- **Incertitudes et innovations** : La vitesse d'évolution reste élevée, et certaines innovations actuelles pourraient être disruptives si elles tiennent leurs promesses. Par exemple, l'**AI pair programming** est déjà là pour le code, mais quid de l'**AI pair ops** ? On voit des débuts (Copilots pour YAML, etc.) – peut-être qu'en fin d'année on aura des bots capables d'ouvrir une pull request sur un repo Terraform pour corriger une config non conforme détectée automatiquement. Ce scénario de *"self-healing infrastructure as code"* est ambitieux mais des briques sont là (Policiers as Code + AI). De même, l'**observabilité prédictive** grâce à l'IA (prévoir une panne avant qu'elle n'arrive) est le Graal recherché – on surveillera si les annonces marketing se concrétisent en produits utilisables.

Pour conclure, la veille de mars 2025 montre un écosystème DevOps très **actif et en maturation simultanée**. Les bases outillées solides posées ces dernières années (CI/CD généralisé, conteneurs, infra as code, monitoring unifié) servent maintenant de socle à des améliorations continues en performance, sécurité et fiabilité. Les équipes DevOps ont aujourd'hui accès à un éventail d'outils incroyablement puissant et sont confrontées non plus à un manque de solutions, mais parfois à un **trop plein** – d'où l'importance de cette veille pour identifier les tendances durables et les outils qui valent l'investissement. Les prochains mois devraient voir se confirmer l'intégration de l'IA dans tous les volets du cycle DevOps, l'adoption de GitOps et de l'automatisation avancée comme nouvelle norme, et un accent toujours plus prononcé sur la collaboration et la qualité (X-as-Code) pour accompagner la complexité croissante des systèmes. Rendez-vous en fin de Q2 2025 pour constater comment ces perspectives se seront réalisées, et quels nouveaux défis auront émergé entre-temps dans l'univers passionnant du DevOps.

Sources :

- GitLab 17.10 – *Release blog (mars 2025)* (GitLab 17.10 released with Duo Code Review & Root Cause Analysis | GitLab (https://about.gitlab.com/releases/2025/03/20/gitlab-17-10-released/#:%7E:text=GitLab%2017,DORA%20Metrics%20and%20much%20more))
- GitHub Actions – *Changelog & blog (févr.-mars 2025)* (Notice of upcoming deprecations and breaking changes for GitHub Actions - GitHub Changelog (https://github.blog/changelog/2025-02-12-notice-of-upcoming-deprecations-and-breaking-changes-for-github-actions/#:%7E:text=Ubuntu%2020%20image%20brownouts)) (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Repositories%20widely%20used%20the%20tj,trust%20and%20consume%20GitHub%20Actions))
- Jenkins.io – *Blog "Redesigning Jenkins" (mars 2025)* (Redesigning Jenkins (Part One) (https://www.jenkins.io/blog/2025/03/26/design-post/#:%7E:text=We%E2%80%99ve%20carried%20forward%20legacy%20technologies,a%20real%20barrier%20for%20contributors)) (Redesigning Jenkins (Part One) (https://www.jenkins.io/blog/2025/03/26/design-post/#:%7E:text=The%20first%20significant%20milestone%20in,but%20also%20enabled%20the%20Jenkins))
- CloudNativeNow – *Annonce Argo CD 3.0 (avril 2025, KubeCon EU)* (CNCF Readies Next Major Update to Argo CD Platform - Cloud Native Now (https://cloudnativenow.com/news/cncf-readies-next-major-update-to-argo-cd-platform/#:%7E:text=Michael%20Crenshaw%2C%20a%20staff%20software,based%20access%20controls%20%28RBAC))
- Docker Inc – *Docker Bake GA (LinkedIn, mars 2025)* (Docker Bake is Now Generally Available in Docker Desktop 4.38! (https://www.linkedin.com/pulse/docker-bake-now-generally-available-desktop-438-docker-xi6we#:%7E:text=Docker%20Bake%20is%20an%20orchestration,to%20speed%20up%20build%20times)); *Newsletter Docker Navigator* (Docker Navigator: New CEO, Docker Hub updates & AI-powered dev | Docker (https://www.docker.com/resources/2025-03-10-new-ceo-docker-hub-updates/#:%7E:text=Docker%20Engine%20v28%3A%20Hardening%20container,networking%20by%20default))
- Ansible Forum – *Discussion EOL Ansible 9* (Ansible Community, Ansible Core and RHEL 8 - Get Help - Ansible (https://forum.ansible.com/t/ansible-community-ansible-core-and-rhel-8/11198#:%7E:text=,13)); Red Hat – *Notes de version AAP 2.4 patch Mars* (Red Hat Ansible Automation Platform release notes | Red Hat Product Documentation (https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.4/html-single/red_hat_ansible_automation_platform_release_notes/index#:%7E:text=8,March%2026%2C%202025))
- SiliconAngle – *Pulumi sécurise IaC (mars 2025)* (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=Pulumi%20has%20introduced%20new%20features,and%20compliance%20at%20large%20scale)) (Pulumi enhances cloud security with automated secrets rotation and new GitHub integration - SiliconANGLE (https://siliconangle.com/2025/03/26/pulumi-enhances-cloud-security-automated-secrets-rotation-new-github-integration/#:%7E:text=The%20first%20announcement%20is%20the,while%20integrating%20with%20existing%20workflows))
- Grafana Labs – *Communiqué Observability Survey 2025* (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=Grafana%20Labs%20Shares%20Open%20Source,Using%20Open%20Source%20Observability%20Tools)) (Grafana Labs Unveils 2025 Observability Survey Findings and Open Source Updates at KubeCon Europe | Grafana Labs (https://grafana.com/about/press/2025/03/25/grafana-labs-unveils-2025-observability-survey-findings-and-open-source-updates-at-kubecon-europe/#:%7E:text=,quarters%20of%20all))
- InfoQ – *Article supply chain GitHub Action (avril 2025)* (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Repositories%20widely%20used%20the%20tj,a%20blind%20spot%20in%20how)) (Compromised GitHub Action Highlights Risks in CI/CD Supply Chains - InfoQ (https://www.infoq.com/news/2025/04/compromised-github-action/#:%7E:text=Security%20researchers%20and%20open,scanning%20their%20workflows%20for%20unpinned))
- Splunk Blog – *DevOps Events 2025* (DevOps Conferences & Events 2025: Complete Guide | Splunk (https://www.splunk.com/en_us/blog/learn/devops-conferences-events.html#:%7E:text=Cost%3A%C2%A0Starting%20at%20%C2%A3270)), etc. (et autres sources mentionnées inline)