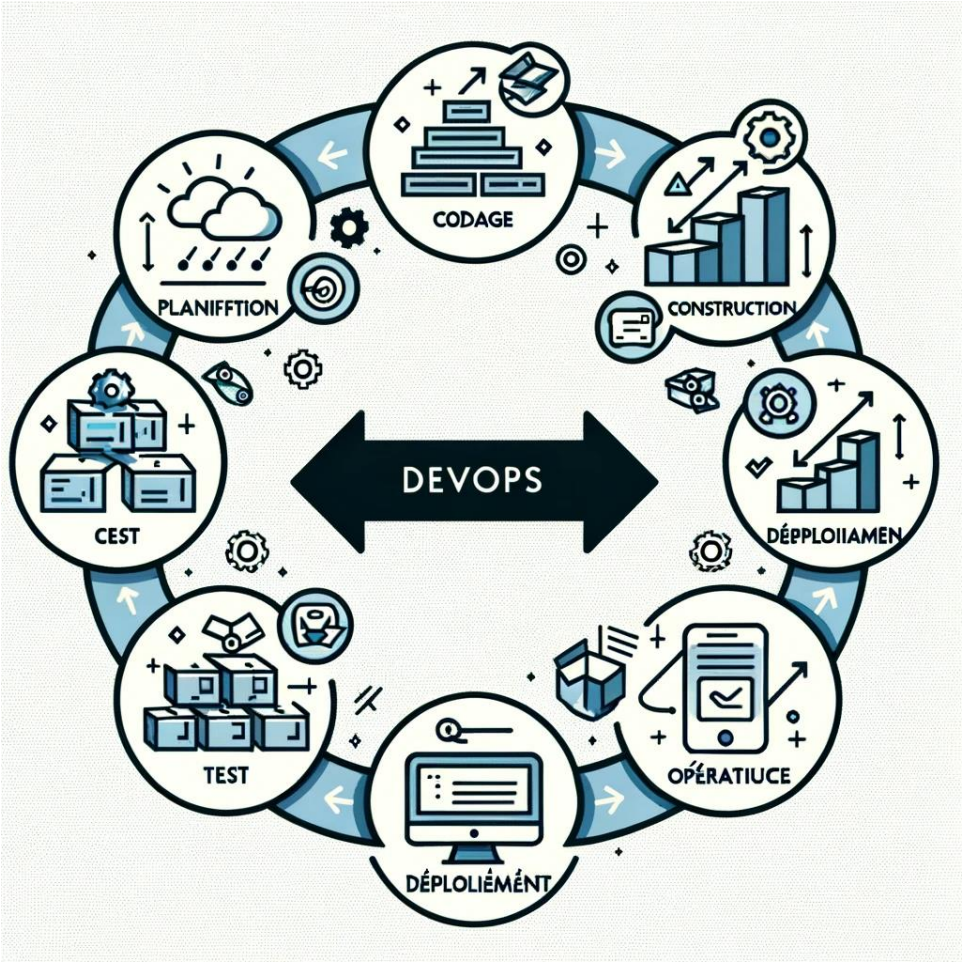
Veille Technologique : L'évolution de DevSecOps en 2023

Dans quelle mesure le métier et le méthodes DevSecOps vont devenir primordiaux dans le futur ? Pourquoi je pense que le métier de développeur va devenir un DevOps et comment l'IA va être un allié de choix

Introduction

Qu'est-ce que DevOps ?



(Parler de l'importance croissante de la sécurité)

L'univers technologique actuel, dynamique et en rapide mutation, impose aux organisations une adaptation constante pour maintenir leur compétitivité et leur efficience. Dans ce contexte, les pratiques DevOps émergent comme un pivot central permettant d'assurer une

livraison rapide et fiable des applications logicielles, tout en maintenant une haute qualité et une sécurité optimale. DevOps, contraction des termes "Développement" et "Opérations", est une philosophie, un ensemble de pratiques et une culture visant à réduire le cloisonnement entre les développeurs (Dev) et les équipes d'exploitation (Ops), facilitant ainsi un cycle de développement plus rapide, plus fiable et plus sécurisé.

Le mouvement DevOps encourage une collaboration étroite et continue entre ces équipes tout au long du cycle de vie du développement logiciel, de la conception à la production. Cette collaboration permet une livraison continue, une intégration continue, ainsi qu'un monitoring et une rétroaction continus, formant un pipeline DevOps fluide qui augmente l'efficacité opérationnelle.

(96% des répondants trouvant DevSecOps bénéfique selon un rapport d'Infosec))

Cependant, l'incorporation de la sécurité et de l'innovation technologique dans les pratiques DevOps s'avère cruciale face à des cyber-menaces croissantes et des exigences de marché en constante évolution. C'est ici qu'intervient DevSecOps, une extension de DevOps, qui intègre la sécurité dès le début du cycle de développement, et l'IA/ML (Intelligence Artificielle / Machine Learning) qui offre des opportunités d'automatisation et d'optimisation avancées.

Ce document propose d'explorer ??? témoignant de l'évolution de DevOps / DevSecOps en 2023 :

Les tendances et sujets importants identifiés à partir des articles fournis concernent le DevSecOps, l'intégration de l'Intelligence Artificielle (IA) dans le DevOps, et l'évolution future du DevOps.

Plan du sujet:

(Il faut encore inclure les outils devOps et a quel point ils sont importants)

1. DevSecOps :

- Intégration précoce de la sécurité : Le passage du DevOps au DevSecOps, qui intègre la sécurité dès le début du cycle de développement, est une tendance majeure pour réduire les vulnérabilités et améliorer la robustesse des systèmes.

- Outils DevSecOps : L'adoption d'outils spécifiques comme SonarQube, ThreatModeler, ou Aqua Security pour automatiser et renforcer la sécurité tout au long du processus de développement et d'exploitation est crucial.

- collaboration entre les équipes de sécurité et de développement : Une collaboration étroite entre les équipes de sécurité et de développement est encouragée, notamment par la pratique de la modélisation des menaces et l'intégration d'outils de sécurité dans les pipelines d'intégration continue.

- Pourquoi un devsecops est-il important?

- ShiftLeft

2. Automatisation dans DevOps

- Automatisation Pervasive : L'automatisation des processus de déploiement, de gestion des applications et de réponse aux incidents de sécurité est une tendance dominante pour augmenter l'efficacité et la rapidité des opérations DevOps. Ici on peu inclure des outils devOps (terraform / ansible) / infrastructure as code

3. Interaction entre DevOps et IA :

- Automatisation intelligente : L'IA et le Machine Learning permettent une automatisation plus intelligente des tâches, notamment dans la détection précoce des problèmes et l'optimisation des ressources, réduisant ainsi la charge de travail manuelle et les erreurs humaines.

- Amélioration de la sécurité grâce à l'IA : L'IA contribue à renforcer la sécurité en identifiant rapidement les menaces potentielles et en aidant à mettre en place des défenses proactives.

- discuter des défis associés à l'adoption de DevSecOps et de l'IA dans DevOps, et comment ces défis pourraient être surmontés.

- automatisant la détection des vulnérabilités ou en aidant à la gestion des vulnérabilités, ce qui est mentionné dans votre sixième source.

4. Évolution Future du DevOps :

- *Évolution vers l'AIOps* : L'intégration de l'IA dans le DevOps, menant vers l'AIOps, est une tendance future qui promet d'améliorer l'efficacité, la qualité, et la sécurité des développements logiciels.

- *Adaptation et Évolution*: Les organisations et les praticiens du DevOps doivent s'adapter aux changements technologiques et méthodologiques, comme l'IA et le DevSecOps, pour rester pertinents et efficaces.

- La **mouvement GitOps**

5. Éducation et Formation Continues : ???

- Responsabilités des experts DevSecOps : La formation et l'éducation continues sur les responsabilités et les meilleures pratiques en matière de DevSecOps sont essentielles pour les professionnels du domaine.

Conclusion :

Les tendances majeures révèlent une convergence entre DevOps, sécurité, et IA, suggérant une évolution vers des pratiques plus intégrées et automatisées pour améliorer l'efficacité, la sécurité, et la gestion des opérations de développement et d'exploitation.

Sources et resumé bref de chaque articles:

Sources:

1. https://geekflare.com/fr/devops-latest-trends/

2. https://geekflare.com/devsecops-introduction/
3. https://www.techrepublic.com/article/best-devsecops-tools/#:~:text=,Browser%2Fload
4. https://www.devopsdigest.com/2023-devsecops-security-predictions-1#:~:text=%23%20%E3%80%9015%E2%80%A02023%20DevSecOps%20Predictions%20,bolted%20on%20as%20an%20afterthought
5. https://www.devopsdigest.com/2023-devsecops-security-predictions-2
6. https://about.gitlab.com/blog/2023/01/26/whats-next-for-devsecops/#:~:text=,the%20increased%20threats%20throughout
7. https://www.redhat.com/fr/topics/devops
8. https://www.techtarget.com/searchitoperations/feature/Is-DevOps-dead-What-the-future-of-DevOps-could-look-like
9. https://scalastic.io/future-devops-with-ai//

https://geekflare.com/fr/devops-latest-trends/

L'article de John Walter discute des tendances récentes en DevOps en 2023, en mettant l'accent sur l'amélioration de la rapidité et de l'efficacité dans le développement et le déploiement de logiciels. Voici un résumé des tendances et des statistiques essentielles mentionnées dans l'article :

DevSecOps : Intégration de la sécurité dès la conceptualisation du logiciel, réduisant ainsi les vulnérabilités. 96% des répondants dans un rapport d'Infosec ont trouvé DevSecOps bénéfique pour leur entreprise.

Informatique sans serveur : Accélération du développement et de l'exécution des applications sans gestion de serveurs, avec un marché de 9 milliards de dollars en 2022, et une croissance prévue de 25% de 2023 à 2032.

Architecture de microservices : Simplification du développement, du test et du déploiement des logiciels en divisant les applications en petits éléments gérables.

AIOPs/MLOPs : Utilisation de l'IA pour automatiser et rationaliser les flux de travail, avec une adoption prévue de 30% d'ici la fin de l'année.

Applications à faible code: Développement rapide avec moins d'efforts de codage, réduisant le temps de développement de 90%.

GitOps : Approche nouvelle combinant Git et l'orchestration de conteneurs pour automatiser l'infrastructure.

Kubernetes (K8s): Plateforme d'orchestration de conteneurs permettant un déploiement, une mise à l'échelle et une gestion automatisés des applications.

Infrastructure en tant que code (IaC) : Gestion et provisionnement de l'infrastructure via des fichiers de configuration, améliorant la précision et la cohérence.

Ingénierie de la fiabilité des sites (SRE): Collaboration entre l'ingénierie logicielle et les opérations pour construire des produits et des services logiciels de haute qualité.

Gestion des vulnérabilités: Processus continu et proactif pour gérer et atténuer les vulnérabilités de sécurité.

Ingénierie des plateformes : Création et exploitation d'applications sur des plateformes natives du cloud.

Déploiement hybride : Combinaison de ressources sur site et dans le cloud pour un développement et un déploiement agiles et flexibles.

Observabilité des données : Techniques permettant d'analyser en profondeur les performances des applications pour améliorer la fiabilité et la disponibilité.

Docker : Plateforme pour créer, tester et déployer des applications dans des conteneurs, simplifiant le développement et le déploiement.

Ansible : Logiciel d'automatisation pour le déploiement d'applications, la gestion de la configuration, et l'exécution de tâches d'administration système.

Terraform: Infrastructure as code permettant de définir des ressources sur site et en nuage dans des fichiers de configuration.

L'article conclut en soulignant l'intérêt du domaine DevOps pour les professionnels de l'ingénierie logicielle et recommande l'acquisition de ressources éducatives pour ceux qui cherchent à renforcer leurs compétences dans ce domaine.

2)

https://geekflare.com/devsecops-introduction/

Cet article d'Avi présente DevSecOps comme une extension de la pratique réussie de DevOps, abordant les défis de sécurité pressants dans le développement logiciel moderne. La motivation derrière DevSecOps provient de statistiques alarmantes sur les violations de données et les vulnérabilités logicielles, incitant à un changement de culture et de pratiques pour intégrer la sécurité dans le cycle de vie de DevOps. DevSecOps promeut une implication précoce de la sécurité, connue sous le nom d'approche shift-left, et une collaboration continue entre les équipes de développement, de sécurité et d'exploitation.

Les pratiques clés pour mettre en œuvre DevSecOps incluent la collaboration sur les modèles de menaces, l'intégration d'outils de sécurité dans le pipeline de développement, la priorisation des exigences de sécurité, la révision des politiques de sécurité de l'infrastructure avant déploiement, et les évaluations de sécurité automatisées par des experts. Des outils tels que SonarQube, ThreatModeler, et Aqua Security entre autres, sont mis en avant pour leur rôle dans la promotion des inspections de sécurité continues, la modélisation des menaces, et la sécurisation du cycle de vie des applications respectivement.

L'article offre un aperçu de l'écosystème DevSecOps, expliquant comment l'analyse de sécurité devient une partie intégrale de chaque phase, du développement à la production, assurant une approche holistique de la sécurité. Il met l'accent sur l'importance des innovations technologiques modernes telles que la Sécurité en tant que Code, la Conformité en tant que Code, et l'Infrastructure en tant que Code dans l'élimination des activités de sécurité manuelles et l'amélioration de l'efficacité.

En conclusion, il exhorte ceux qui travaillent dans DevOps à adopter et promouvoir la culture DevSecOps dans leurs organisations, suggérant une exploration plus large des responsabilités d'un expert DevSecOps.

3)

https://www.techrepublic.com/article/best-devsecops-tools/#:~:text=,Browser%2Fload

DevSecOps, intégrant la sécurité dans le cycle de vie du développement logiciel, met l'accent sur l'automatisation, la collaboration et l'adoption d'outils spécifiques pour garantir la sécurité tout en conservant l'efficacité. Des outils tels que GitLab, OWASP ZAP et SonarQube sont recommandés pour leur capacité à améliorer la qualité du code, détecter les vulnérabilités et faciliter la collaboration entre les équipes de développement et de sécurité

4)

https://www.devopsdigest.com/2023-devsecops-security-predictions-1#:~:text=%23%20%E3%80%9015%E2%80%A02023%20DevSecOps%20Predictions%20,bolted%20on%20as%20an%20afterthought

DevSecOps, mélangeant DevOps et sécurité, vise à intégrer la sécurité dès le début du cycle de développement, réduisant ainsi les vulnérabilités logicielles. Cette culture encourage la collaboration entre les équipes de développement et de sécurité, et incorpore des outils spécifiques pour automatiser et améliorer la sécurité. L'adoption de DevSecOps est en croissance, avec une attention particulière sur l'intégration de la sécurité dès les premières phases du développement. Des outils comme SonarQube et ThreatModeler facilitent cette intégration, permettant une inspection continue et une modélisation des menaces efficaces

5)

https://www.devopsdigest.com/2023-devsecops-security-predictions-2

Les prédictions pour 2023 soulignent une prise de conscience accrue de la sécurité dans le domaine DevSecOps. L'accent est mis sur la sécurisation de la chaîne d'approvisionnement logicielle, en réponse aux récentes attaques de chaîne d'approvisionnement. On note

également une tendance vers l'investissement dans des plateformes et des outils spécifiques pour améliorer la sécurité des applications. Les défis posés par l'adoption des services SaaS et des API en matière de cybersécurité sont mis en avant, tout comme l'importance de l'automatisation pour intégrer les pratiques de sécurité dès le début du cycle de développement logiciel

6)

https://about.gitlab.com/blog/2023/01/26/whats-next-for-devsecops/#:~:text=,the%20increased%20threats%20throughout

En 2023, le domaine DevSecOps continuera d'évoluer avec une attention accrue sur la sécurité dès les premières étapes du cycle de développement (shift-left), notamment dans la sécurité de la chaîne d'approvisionnement logiciel. L'intégration de l'IA et du ML tout au long du cycle de développement sera essentielle pour améliorer la productivité et la sécurité. L'éducation sur la sécurité sera intégrée dans la formation DevOps. La gestion des vulnérabilités et l'automatisation seront primordiales pour faire face aux défis de sécurité, avec des outils comme SonarQube, Aqua Security et CheckMarx facilitant ce processus

7)

https://www.redhat.com/fr/topics/devops

La page de Red Hat détaille DevSecOps comme une méthode proactive intégrant la sécurité dès le début du cycle de développement. Elle promeut la collaboration entre les équipes de développement, d'exploitation, et de sécurité, contribuant ainsi à une culture de sécurité renforcée. DevSecOps favorise une réponse rapide aux menaces, réduit les risques, et accélère la livraison des applications en intégrant des outils et des pratiques de sécurité dans le processus DevOps. Plusieurs ressources et solutions sont mentionnées pour aider à la mise en œuvre de DevSecOps.

8)

https://www.techtarget.com/searchitoperations/feature/Is-DevOps-dead-What-the-future-of-DevOps-could-look-like

https://scalastic.io/future-devops-with-ai//

En rassemblant les informations des différents articles consultés, on peut brosser un tableau des tendances actuelles et futures en matière de DevSecOps, et de l'interaction entre DevOps et l'Intelligence Artificielle (IA).

DevSecOps:

Intégration de la Sécurité: Le DevSecOps incarne une fusion entre le développement (Dev), l'exploitation (Ops) et la sécurité (Sec), cherchant à intégrer la sécurité dès le début du cycle de vie du développement logiciel, plutôt que de la rajouter à la fin

Outils: Certains outils tels que SonarQube, ThreatModeler, Aqua Security, et CheckMarx sont utilisés pour automatiser et renforcer la sécurité tout au long du processus de développement et d'exploitation

Approche Shift-Left Cette approche vise à intégrer les processus de sécurité dès les premières étapes du développement, favorisant ainsi une prise en compte plus efficace des problématiques de sécurité

Automatisation de la Sécurité: L'automatisation joue un rôle crucial dans le DevSecOps, notamment pour effectuer des analyses de sécurité continues et pour répondre rapidement aux incidents de sécurité

DevOps et IA:

Automatisation Améliorée: L'IA permet d'automatiser davantage de tâches au sein du pipeline DevOps, réduisant ainsi la charge de travail manuelle et accélérant les processus de déploiement et de gestion des applications.

Prédiction et Détection Précoce des Problèmes: L'utilisation de l'IA pour analyser les données en temps réel permet de prédire les problèmes potentiels avant qu'ils ne deviennent critiques, minimisant ainsi les temps d'arrêt.

Amélioration de la Sécurité: L'IA renforce la sécurité en identifiant rapidement les menaces potentielles et en aidant à mettre en place des défenses proactives

Optimisation des Ressources: L'IA permet une utilisation plus efficace des ressources informatiques, contribuant ainsi à réduire les coûts opérationnels

Tendances Futures:

1. Adoption Croissante du DevSecOps: Avec la prise de conscience croissante des risques de sécurité, la transition vers DevSecOps est susceptible de s'accélérer, faisant de la sécurité une préoccupation intégrée et non plus une réflexion après coup

2. Automatisation Pervasive: L'automatisation continuera d'être un pilier central du DevOps, avec une adoption accrue d'outils d'automatisation pour améliorer l'efficacité opérationnelle et la réponse aux menaces de sécurité

3. IA et Machine Learning: L'IA et le Machine Learning continueront d'avoir un impact sur le DevOps, en automatisant davantage de processus, en améliorant la détection des anomalies et en optimisant les performances des systèmes

Avoir une hierachie de document
- quels sont les plus importants par exemple