keyrus
make data matter

Tech Advisory Board

DevSecOps Spéciales

Sécurisez votre code comme un commando

www.keyrus.com

DevSecOps Spéciales

Sécurisez votre code comme un commado

Le DevSecOps est une approche essentielle pour les entreprises modernes qui cherchent à améliorer la qualité de leurs logiciels, accélérer les cycles de développement, renforcer la sécurité et optimiser les coûts. Cette méthodologie intégrée combine développement, opérations et sécurité, permettant ainsi une transformation numérique efficace et durable.

L'importance du DevSecOps réside principalement dans sa capacité à briser les silos traditionnels entre les équipes et à favoriser une collaboration fluide et continue. En utilisant des méthodologies agiles et des outils automatisés, les entreprises peuvent, en effet, réaliser une intégration et un déploiement continus, tout en garantissant une sécurité renforcée à chaque étape du processus de développement logiciel.

Les bénéfices stratégiques et opérationnels en sont nombreux, puisque cette approche permet d'améliorer l'efficacité du développement, de renforcer la sécurité des applications, d'optimiser l'utilisation des ressources et de promouvoir des pratiques durables.

Cependant, l'implémentation du DevSecOps pose également des défis, tels que la gouvernance, les conflits de priorités, le manque de compétences et les outils inadéquats.

C'est pour cette raison que cet ebook a pour intention de fournir une compréhension approfondie du DevSecOps, en détaillant ses principes, ses avantages, ses défis et les solutions pour une mise en œuvre réussie.

Image générée par **Midjourney** avec la consigne : *« Vintage illustration poster of a happy woman computer engineer, casual clothes, military face paint, in a futuristic software development environment, capturing the essence with dark eyes, bright daylight lighting , framed in a centered manner --style raw --v 6.0 --ar 53:89 »*

Image de couverture générée par **Midjourney** avec la consigne : *« Hyper-realistic portrait of a happy computer engineer with commando face paint in a software development environment, capturing the essence with dark eyes, bright daylight lighting , framed in a centered manner »*

Il était une fois le DevOps...

Le DevSecOps est une approche moderne et intégrée de la création de solutions logicielles qui combine le développement (Dev), les opérations (Ops) et la sécurité (Sec) en un processus homogène. Cette méthodologie est née de la nécessité d'améliorer continuellement la qualité des logiciels, de raccourcir les cycles de développement, de renforcer la sécurité à chaque étape du processus et de gérer efficacement les coûts tout en promouvant des pratiques informatiques durables.

Le DevSecOps se distingue de ses prédécesseurs par son approche holistique. Historiquement, le développement de logiciels et les opérations étaient des silos distincts, souvent en conflit. Le DevOps a émergé pour briser ces silos, en prônant la collaboration étroite entre les équipes de développement et d'opérations pour accélérer la livraison de logiciels de qualité. Cependant, la sécurité restait souvent une préoccupation de dernière minute, introduisant des vulnérabilités potentielles dans les systèmes déployés.

Le concept de DevSecOps est une évolution naturelle du DevOps, intégrant la sécurité dès le départ et tout au long du cycle de développement. Cette intégration précoce permet de détecter et de corriger les vulnérabilités dès les premières phases de développement, réduisant ainsi les risques et les coûts liés aux failles de sécurité découvertes en fin de cycle.

L'intégration du développement, des opérations et de la sécurité dans un processus unifié présente de nombreux avantages. Elle permet non seulement de livrer des logiciels de meilleure qualité plus rapidement, mais aussi de garantir que la sécurité est une composante fondamentale et non une réflexion après coup. Cette approche proactive permet de minimiser les vulnérabilités et d'assurer une résilience accrue face aux menaces de sécurité.

En intégrant ces trois disciplines, les équipes peuvent collaborer plus efficacement, partager des responsabilités et adopter des pratiques communes qui améliorent la qualité globale des logiciels. La communication entre les équipes est renforcée, les cycles de feedback sont raccourcis et les processus sont continuellement optimisés pour répondre aux exigences changeantes du marché.

Image générée par **Midjourney** avec la consigne : *« Modern painting of a happy woman computer engineer with camouflage paint on face. »*

Les objectifs du DevSecOps

Les principaux objectifs du DevSecOps sont multiples et visent à transformer radicalement la façon dont les logiciels sont développés et déployés :

1. **Amélioration de la qualité des logiciels** : en intégrant des tests continus et des contrôles de sécurité tout au long du cycle de développement, les logiciels produits sont de meilleure qualité et présentent moins de vulnérabilités
2. **Accélération des cycles de développement** : la collaboration et l'automatisation permettent de réduire les délais de livraison, rendant les entreprises plus agiles et réactives face aux besoins du marché.
3. **Renforcement de la sécurité** : la sécurité est intégrée dès le début du processus de développement, assurant une protection robuste contre les menaces tout au long du cycle de vie du logiciel.
4. **Optimisation des coûts** : en détectant les problèmes plus tôt et en automatisant les processus, les entreprises peuvent réduire les coûts liés aux corrections tardives et aux failles de sécurité.
5. **Promotion des pratiques informatiques durables** : en adoptant des pratiques Green IT, le DevSecOps contribue à réduire l'empreinte carbone des opérations informatiques, en optimisant l'utilisation des ressources.

Le DevSecOps n'est pas seulement une méthodologie technique, mais **un véritable changement culturel au sein des organisations**. Il requiert une collaboration étroite entre les équipes, une adoption de nouvelles technologies et outils, ainsi qu'un engagement à la formation continue et à l'amélioration des processus. En somme, il représente une avancée significative dans le domaine du développement logiciel, offrant une approche intégrée et sécurisée qui répond aux besoins croissants des entreprises modernes. On serait même tenté d'ajouter qu'il est essentiel pour les organisations souhaitant rester compétitives, innovantes et sécurisées dans un paysage numérique en constante évolution.

Afin de mieux comprendre comment cette approche se matérialise au sein des entreprises, il est essentiel d'explorer les fondements qui en assurent le succès.

> « Le DevSecOps n'est pas seulement une méthodologie technique, mais **un véritable changement culturel** au sein des organisations. »

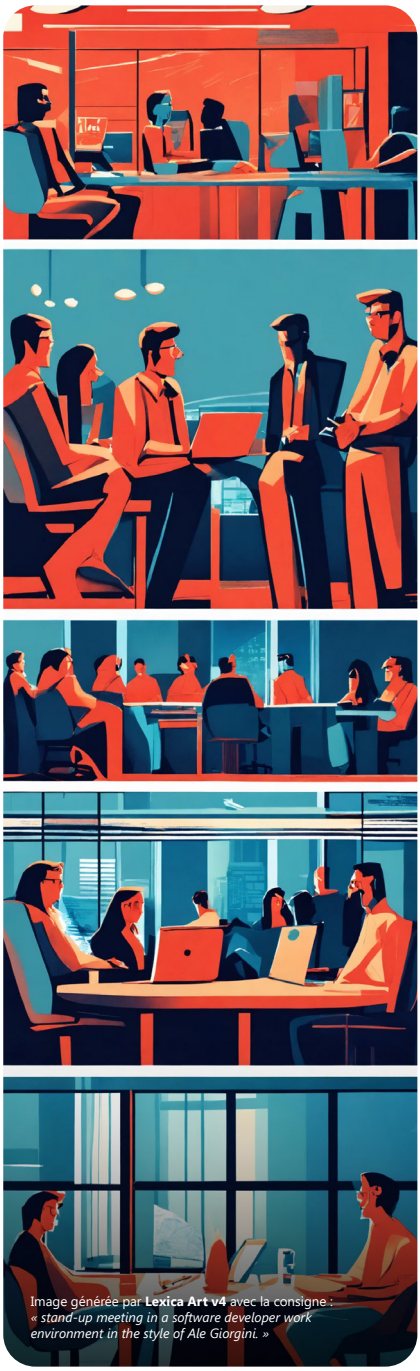

Image générée par **Lexica Art v4** avec la consigne : « *stand-up meeting in a software developer work environment in the style of Ale Giorgini.* »

Une combinaison de principes, de pratiques et d'outils

Le DevSecOps repose sur une combinaison de principes, de pratiques et d'outils qui permettent une collaboration efficace entre les équipes de développement, d'opérations et de sécurité. Mais quels sont les éléments clés qui constituent les fondements du DevSecOps ?

La collaboration inter-équipes est au cœur du DevSecOps. Les équipes de développement, d'opérations et de sécurité doivent travailler ensemble dès le début du cycle de vie du logiciel. Cela nécessite un changement culturel où chaque membre de l'équipe comprend et respecte les objectifs et les contraintes des autres départements. Les silos traditionnels sont brisés, permettant une communication fluide et une prise de décision collective.

Pour favoriser cette collaboration, des pratiques telles que les réunions quotidiennes de *stand-up* (pas celui des humoristes, hein, mais celui des équipes de développement), les revues de code partagées et les *post-mortems* sans blâme (ouf !) sont instaurées. Ces pratiques renforcent la transparence et l'engagement de chaque membre de l'équipe, créant ainsi un environnement propice à l'innovation et à la réactivité.

Le succès du DevSecOps dépend fortement de **l'adoption de méthodologies agiles** et de **l'utilisation d'outils automatisés**. Les méthodologies agiles, telles que Scrum et Kanban, permettent une planification flexible et une livraison itérative de fonctionnalités. Elles facilitent également l'intégration continue (CI *continuous integration*) et le déploiement continu (CD ou *continuous deployment*), qui sont des piliers du DevSecOps.

Les outils automatisés jouent également un rôle important en standardisant et en accélérant les processus. Par exemple, les pipelines CI/CD automatisent les tests, les builds et les déploiements, réduisant ainsi le risque d'erreurs humaines. Des outils comme ***Terraform***, ***Ansible*** ou ***Puppet***, permettent de maintenir la cohérence des environnements de développement et de production. Par ailleurs, des solutions de sécurité automatisées, comme les scanners de vulnérabilités et les tests de pénétration automatisés, sont intégrées dans le pipeline pour garantir une surveillance continue de la sécurité.

De la planification à la surveillance continue

Le cycle de vie du DevSecOps comprend plusieurs étapes clés, chacune intégrant des pratiques spécifiques pour assurer une livraison continue et sécurisée des logiciels :

1. **Planification** : les équipes collaborent pour définir les exigences, établir les priorités et planifier les sprints. Cette phase inclut la définition des politiques de sécurité et des exigences de conformité.
2. **Développement** : les développeurs écrivent le code en suivant des normes de codage sécurisées et en utilisant des outils d'analyse statique pour détecter les vulnérabilités dès le début.
3. **Intégration** : le code est intégré dans un dépôt central où il est automatiquement testé et validé. Des tests unitaires, des tests de sécurité et des revues de code sont effectués pour garantir la qualité et la sécurité.
4. **Déploiement** : les applications validées sont déployées automatiquement dans des environnements de test et de production. Les pratiques de déploiement continu permettent des mises à jour fréquentes et sans interruption.
5. **Surveillance** : une surveillance continue est mise en place pour détecter les anomalies, les performances dégradées et les tentatives d'intrusion. Des outils de *monitoring* et de *logging* fournissent des informations en temps réel, permettant une réaction rapide aux incidents.

Image générée par **Midjourney** avec la consigne :
« stand-up meeting in a software developer work environment --v 6.0 --ar 2:5 »

On l'aura compris, les fondements du DevSecOps reposent sur une collaboration étroite entre les équipes, l'adoption de méthodologies agiles et l'utilisation d'outils automatisés. Ces éléments permettent de créer un environnement où la qualité, la sécurité et la rapidité sont au cœur du processus de développement logiciel.

Si comprendre les fondements du DevSecOps permet d'apprécier pleinement son potentiel transformateur, il paraît également essentiel d'explorer les avantages stratégiques et opérationnels que cette approche apporte aux entreprises.

Des avantages qui renforcent la compétitivité

Le DevSecOps offre une multitude d'avantages qui renforcent la compétitivité et l'efficacité des entreprises. Ces bénéfices se manifestent tant sur le plan stratégique qu'opérationnel, contribuant à une meilleure performance globale.

L'un des principaux avantages du DevSecOps est l'augmentation de **la vélocité du développement**. En intégrant les équipes de développement, d'opérations et de sécurité, les processus deviennent plus fluides et les cycles de feedback plus courts. L'automatisation des tâches répétitives, telles que les tests et les déploiements, réduit considérablement le temps nécessaire pour livrer de nouvelles fonctionnalités. Les entreprises peuvent ainsi répondre plus rapidement aux besoins du marché et aux attentes des clients, renforçant leur agilité et leur capacité d'innovation.

Image générée par **Ideogram** avec laconsigne : *« collaborating operations teamwork; portrait of two software engineers man and woman brainstorming on Green IT opportunities.»*

En intégrant des pratiques de sécurité dès les premières phases, les vulnérabilités sont détectées et corrigées plus tôt, réduisant ainsi les risques de failles de sécurité en production. Cette approche proactive permet de **prévenir les incidents de sécurité coûteux** et de **protéger les données sensibles**. De plus, la surveillance continue assure une vigilance permanente, détectant les menaces en temps réel et permettant **une réponse rapide aux incidents**.

L'optimisation des ressources est un autre avantage clé du DevSecOps. En automatisant les processus et en utilisant des outils de gestion de configuration, les entreprises peuvent mieux gérer leurs infrastructures et éviter le gaspillage de ressources. Cela se traduit par une réduction des coûts opérationnels, notamment ceux liés à l'utilisation des ressources cloud. Par ailleurs, la détection précoce des erreurs et des vulnérabilités réduit les coûts associés aux correctifs tardifs et aux interruptions de service.

Le DevSecOps encourage **l'adoption de pratiques Green IT**, contribuant à une réduction de l'empreinte carbone des entreprises. En optimisant l'utilisation des ressources et en automatisant la gestion des infrastructures, il est possible de minimiser la consommation énergétique et les déchets électroniques. Cette approche soutient les objectifs de développement durable des entreprises, renforçant leur responsabilité environnementale.

Enfin, le DevSecOps favorise **une culture d'amélioration continue et d'innovation**. Les cycles de développement itératifs permettent d'expérimenter de nouvelles idées et de les mettre rapidement en production. Les feedbacks constants entre les équipes encouragent l'apprentissage et l'optimisation des processus. Cette dynamique d'innovation est essentielle pour rester compétitif dans un environnement technologique en constante évolution.

Les avantages stratégiques et opérationnels du DevSecOps sont indéniables. Cependant, la mise en œuvre de cette approche présente également des défis importants. Il est essentiel d'identifier ces obstacles et d'explorer les solutions pour les surmonter.

> « En automatisant les processus et en utilisant des outils de gestion de configuration, les entreprises peuvent **mieux gérer leurs infrastructures et éviter le gaspillage** de ressources. »

Image générée par **Lexica Aperture v4** avec la consigne :
« Tension at work in a software environment over different development priorities between people from different business units in the style of Ernie Nordli »

Défis et solutions pour l'implémentation du DevSecOps

L'implémentation du DevSecOps peut être complexe et nécessiter des ajustements significatifs dans les processus et la culture d'entreprise. Plusieurs défis doivent être relevés pour garantir une adoption réussie, et parmi lesquels on peut citer :

1. **La gouvernance et les barrières organisationnelles** : les structures organisationnelles traditionnelles peuvent poser des obstacles à l'intégration des équipes de développement, d'opérations et de sécurité. Les silos peuvent ralentir la communication et la collaboration, entraînant des retards et des inefficacités
2. **Les conflits de priorités et de service** : les équipes peuvent avoir des objectifs et des priorités différents, ce qui peut créer des tensions. Par exemple, les équipes de sécurité peuvent être perçues comme un frein à la vitesse de développement en imposant des contrôles supplémentaires.
3. **Le manque de compétences et de formation** : l'adoption du DevSecOps nécessite des compétences spécifiques en automatisation, en sécurité et en gestion de la configuration. Le manque de formation et de sensibilisation peut ralentir le processus de mise en œuvre.
4. **Les outils et les technologies inadéquats** : l'absence d'outils appropriés ou l'utilisation d'outils non intégrés peut compliquer l'automatisation des processus et la collaboration entre les équipes.
5. **Le soutien et l'engagement de la direction** : le succès du DevSecOps dépend du soutien actif de la direction. Sans un engagement fort de la part des dirigeants, il peut être difficile de surmonter les résistances au changement et de mobiliser les ressources nécessaires.

Image générée par **Midjourney** avec la consigne : *« Aligning objectives and priorities in the style of Bron Payne. »*

Fort heureusement, des solutions et bonnes pratiques existent, et assez logiquement, l'on recommandera de toujours :

- **Établir une gouvernance clairvoyante et souple** : la mise en place d'une gouvernance flexible qui favorise la collaboration inter-équipes est essentielle. Cela peut inclure la création de comités de gouvernance transversaux et la mise en œuvre de politiques de communication ouvertes et transparentes.
- **Aligner les objectifs et les priorités** : il est crucial de définir des objectifs communs pour toutes les équipes impliquées. L'organisation de workshops et de séances de planification collaborative peut aider à aligner les priorités et à comprendre les contraintes de chaque équipe.
- **Investir dans la formation et le développement des compétences** : offrir des programmes de formation et de certification en DevSecOps, en automatisation et en sécurité peut aider à combler les lacunes en compétences. Encourager la participation à des conférences et à des communautés professionnelles peut également favoriser le partage des connaissances.
- **Choisir et intégrer les bons outils** : sélectionner des outils compatibles et interopérables pour l'intégration continue, le déploiement continu, la gestion de configuration et la sécurité. L'automatisation des tests de sécurité et l'utilisation de pipelines CI/CD intégrés sont des pratiques essentielles.
- **Obtenir le soutien de la direction** : impliquer la direction dès le début du processus de mise en œuvre. Présenter des études de cas et des exemples concrets de succès peut aider à démontrer les bénéfices du DevSecOps et à obtenir un engagement fort. La direction doit jouer un rôle actif en soutenant les initiatives et en allouant les ressources nécessaires.

De plus, la mise en œuvre du DevSecOps doit être progressive, en suivant des étapes bien définies :

- **Commencer par une évaluation de la maturité** DevSecOps de l'organisation pour identifier les forces et les faiblesses.
- **Lancer des projets pilotes pour tester** les pratiques et les outils DevSecOps. Ces projets servent de modèle pour les déploiements futurs à plus grande échelle.
- **Étendre progressivement les pratiques** DevSecOps à d'autres équipes et projets, en ajustant les processus en fonction des retours d'expérience.
- **Mettre en place un processus d'amélioration continue** pour affiner les pratiques, les outils et la collaboration entre les équipes.

Surmonter les défis de l'implémentation du DevSecOps est donc essentiel pour réussir sa transformation numérique. Une approche progressive et soutenue par une gouvernance flexible, des objectifs alignés, une formation adéquate, des outils appropriés et le soutien de la direction se révèlera indispensable pour garantir une adoption réussie du DevSecOps.

Mais tout ceci reste très théorique... L'application pratique de cette méthodologie peut être mieux comprise à travers des études de cas concrètes et des exemples réels.

Quelques études de cas et applications pratiques

Voici quelques exemples concrets d'implémentation du DevSecOp, qui illustrent comment cette approche peut transformer les processus de développement et de déploiement des logiciels.

Déploiement de pratiques DevSecOps dans un projet d'IA

Pour une entreprise de renom dans l'industrie manufacturière, Keyrus a intégré les briques d'IA présentes dans le projet dans le processus global DevSecOps du client.

L'essor des projets autour de l'IA confirme la nécessité absolue des les intégrer dans les processus d'automatisation, sécurisation et testing. La sécurisation et l'isolement des données est une contrainte majeure sur ce type de projet.

Les pipelines CI/CD ont été enrichis pour prendre en compte l'outillage d'IA de bout en bout. Cette intégration a non seulement accéléré le cycle de développement, mais a également renforcé la sécurité et la fiabilité des produits livrés, tout en optimisant les coûts de production.

Optimisation des coûts et de la sécurité d'infrastructures cloud

Une enseigne multinationale de produits de grande consommation a adopté le DevSecOps pour optimiser ses coûts et améliorer la sécurité de ses infrastructures cloud.

L'entreprise a mis en place des processus d'automatisation pilotés par API pour gérer les ressources cloud de manière efficace. Cela a permis de réduire considérablement les coûts en identifiant et en désactivant les instances inutilisées et en optimisant l'utilisation des ressources.

Par ailleurs, cette multinationale a intégré des outils de surveillance continue et de gestion des vulnérabilités, assurant une protection constante contre les menaces de sécurité. Cette approche proactive a permis à l'entreprise de maintenir un haut niveau de sécurité tout en réduisant les coûts opérationnels, démontrant ainsi les avantages tangibles du DevSecOps.

Automatisation du processus de livraison

Une société technologique majeure a réussi à automatiser l'ensemble de son processus de livraison, de la mise en place de l'infrastructure au déploiement en production, grâce au DevSecOps. En utilisant ***Kubernetes*** (orchestration de conteneurs docker) et des pipelines CI/CD robustes, l'entreprise a pu déployer des applications de manière continue sans interruption de service.

Cette automatisation a non seulement amélioré l'agilité et l'efficacité des équipes de développement, mais a également réduit les risques d'erreurs humaines et augmenté la fiabilité des déploiements. La surveillance continue et les tests automatisés ont garanti que chaque nouvelle version était sécurisée et performante, assurant une expérience utilisateur optimale.

Les études de cas démontrent l'impact positif du DevSecOps sur les entreprises. Pour maximiser ces bénéfices, il est recommandé d'être bien accompagné dans ce changement.

Un accompagnement Keyrus fondé sur l'expérience

Keyrus s'appuie sur une vaste expérience et des études de cas réussies pour guider les entreprises dans leur démarche DevSecOps, et à motiver les équipes. Notre approche pragmatique et fondée sur l'expérience garantit une transition en douceur et efficace vers le DevSecOps.

Plusieurs aspects clés caractérisent l'accompagnement proposé par Keyrus.

Keyrus commence par **une évaluation détaillée de la maturité DevSecOps de l'entreprise**. Cette étape permet d'identifier les forces et les faiblesses actuelles, ainsi que les opportunités d'amélioration. Grâce à une méthodologie éprouvée, un diagnostic précis est établi, fournissant une feuille de route claire et personnalisée pour l'implémentation du DevSecOps.

La formation est au cœur de l'accompagnement proposé par Keyrus. Des programmes de formation sur mesure sont conçus pour renforcer les compétences des équipes en matière de DevSecOps, d'automatisation et de sécurité. En partenariat avec des organismes de certification reconnus, Keyrus assure que les équipes disposent des connaissances et des compétences nécessaires pour adopter efficacement les pratiques DevSecOps.

Keyrus aide aussi les entreprises à intégrer et automatiser leurs processus en utilisant les meilleurs outils disponibles. Cela inclut la mise en place de pipelines CI/CD, l'automatisation des tests de sécurité et l'optimisation des ressources cloud. L'objectif est de créer des processus robustes, efficaces et sécurisés, qui soutiennent les objectifs stratégiques de l'entreprise.

Image générée par **Midjourney** avec la consigne : *« Meeting with consultants, developers and clients in a software developer work environment. »*

L'accompagnement ne s'arrête pas à la mise en œuvre initiale. **Keyrus offre un support continu** pour assurer le succès à long terme de l'adoption du DevSecOps. Des cycles d'amélioration continue sont établis, permettant d'ajuster et d'optimiser les pratiques en fonction des retours d'expérience et des évolutions technologiques. Ce support inclut des audits réguliers, des ateliers de révision et des sessions de coaching.

Adopter le DevSecOps avec l'accompagnement de Keyrus permet aux entreprises de naviguer efficacement dans l'ère numérique, en combinant sécurité, rapidité et innovation pour garantir une performance durable et compétitive.

Article co-écrit par keyrus, Chat-GPT[4] , Claude, Mistral et Perplexity

Vous avez trouvé cette lecture utile ?

Vous voudrez sûrement lire aussi :

IAnalyse pour tous

Augmenter les capacités des analystes métier avec l'IA générative

IAnalyse pour tous explore l'amélioration des capacités des analystes métier par l'intégration de l'intelligence artificielle générative au sein de la plateforme Alteryx. Il aborde comment cette technologie transforme les étapes d'analyse de données, de la préparation à la visualisation, pour accroître l'agilité et la productivité des entreprises. L'ouvrage met en lumière les défis culturels et organisationnels de cette intégration tout en détaillant le rôle d'accompagnement de Keyrus, et illustre ses applications pratiques, notamment la génération de jeux de données fictives et l'automatisation des processus métiers.

Quelles sont les 3 idées principales ?

1. **Augmentation des capacités analytiques via l'IA**: l'utilisation de l'intelligence artificielle générative au sein de la plateforme Alteryx permet d'augmenter significativement les capacités analytiques des entreprises, en rendant l'analyse de données plus intuitive et accessible aux analystes métier, tout en améliorant la rapidité et la précision des décisions d'affaires.

2. **Intégration holistique de l'IA**: l'eBook souligne l'importance d'intégrer l'IA générative de manière holistique dans les processus métiers, permettant non seulement d'automatiser les tâches, mais aussi de stimuler l'innovation par des nouvelles méthodes d'analyse et de visualisation des données.

3. **Gestion des défis et accompagnement** : il met en relief les défis culturels et organisationnels associés à l'adoption de ces technologies avancées et le rôle primordial de Keyrus en tant que partenaire pour aider les entreprises à entreprendre ces transformations, en assurant une intégration réussie de l'IA dans leurs opérations.

SCAN ME

keyrus

make data matter

Acteur international du conseil et des technologies, Keyrus a pour mission de donner du sens aux données, en révélant toute leur portée, notamment sous un angle humain.

Parce que ce ne sont pas tant les données elles-mêmes qui importent, mais les opportunités que nous pouvons développer en les apprivoisant vraiment, nous nous efforçons constamment de comprendre les objectifs que nos clients souhaitent atteindre. Nous explorons et mesurons les comportements, nous les comprenons et les traduisons en un résultat concret. Nous donnons un sens aux réalités que les données portent afin d'aider nos clients à prendre des décisions plus efficaces.

Les données, qu'elles soient grandes, petites, humaines, complexes, historiques ou prospectives, n'ont de sens que lorsqu'elles sont utilisées pour développer les expériences, affiner la compréhension du quotidien et prendre les meilleures décisions.

Notre proposition de valeur est fondée sur cinq grands groupes de services, chacun comprenant des offres multiples :

- **Automatisation et intelligence artificielle** : nous fournissons à nos clients les moyens d'améliorer leur productivité et leur précision sur l'ensemble de leurs processus, afin de se concentrer sur le travail à plus forte valeur ajoutée.
- **Expérience numérique centrée sur l'humain** : la relation avec les clients et l'engagement des collaborateurs constituent deux des plus grands contributeurs au succès global des entreprises. Nous aidons les entreprises à imaginer et à créer des expériences numériques multimodales et fluides pour atteindre leurs objectifs.
- **Mise en œuvre des données et des analyses** : les données sont une clé incontestable du succès pour les entreprises. Lorsqu'elles sont utilisées intelligemment, elles ouvrent des opportunités uniques pour faire face aux défis actuels et futurs. Nous permettons aux organisations de déployer tout le potentiel de leurs données : nous mettons la science des données au profit du développement de l'entreprise.
- **Cloud et sécurité** : le Cloud et les plateformes numériques ont le potentiel de révolutionner la façon dont les données sont transformées en valeur, tout en portant l'extensibilité et la flexibilité à un niveau supérieur. Nous sécurisons l'ensemble de vos données et veillons à ce qu'elles soient protégées et confidentielles.
- **Transformation et innovation** : pour prospérer dans l'écosystème actuel, chaque entreprise doit non seulement accélérer sa transformation numérique, mais aussi acquérir des compétences pour stimuler son adaptabilité, sa résilience et sa compétitivité. Nous aidons nos clients à se transformer avec succès pour développer un meilleur futur.

S'appuyant sur l'expérience cumulée de plus de 3 500 collaborateurs et présent dans 27 pays sur 4 continents, Keyrus est l'un des principaux experts internationaux en matière de données, de conseil et de technologie.

Pour en savoir plus : **www.keyrus.fr**

Jean-Philippe CLAIR
Directeur Marketing, Communication & Expérience client
jean-philippe.clair@keyrus.com