MICRO FOCUS

WWW.MICROFOCUS.COM

L'Observatoire **DevSecOps** pour la DSI 2019

SOMMAIRE

Micro Focus a mandaté Timspirit, cabinet de conseil indépendant spécialisé dans la transformation des DSI, pour analyser les résultats de l'enquête.
Remerciements particuliers à Nathan Srour et Alice Aroulanda.

INTRODUCTION

Face aux attaques de sécurité, rançongiciels et fuites de données massives, préjudiciables à l'image des entreprises, les DSI doivent désormais élaborer une stratégie de sécurité informatique proactive basée sur le « Security by Design » et la gestion des risques.

Les chiffres du rapport « Cybercrime Report 2017 : A Tear in Review », publié par ThreatMetrix, en témoignent : les cyberattaques visant les entreprises ont augmenté de 170% en 2017 et le phénomène ne cesse de s'amplifier.

Ce qui explique en grand partie la progression des dépenses IT sur le marché des solutions de sécurité informatique. Selon le cabinet d'études Gartner, elle serait de + 20 % sur la période 2018-2019, et le total des dépenses devrait dépasser 124 milliards de dollars à l'échelle mondiale. La croissance marquée de ce marché est assurée par les évolutions fréquentes de régulation ainsi que par le déficit chronique de compétences dans ce domaine.

Pour les organisations informatiques engagées dans l'adoption des pratiques DevOps, le schéma est aujourd'hui modifié : on évoque désormais une évolution vers des pratiques « DevSecOps » : l'enjeu est désormais d'intégrer la sécurité de façon continue sur l'ensemble du cycle de vie des applications. Avec la montée en puissance des méthodes agiles, la sécurité informatique est désormais une responsabilité partagée notamment avec les équipes informatiques qui gèrent le cycle de vie des produits. Concrètement, cela se traduit par des démarches de conduite du changement, qui se matérialisent sous la forme de sensibilisation, coaching et communications internes auprès des collaborateurs de la DSI. L'accent est porté sur la nécessité de pousser l'automatisation de ces tâches au maximum.

Pour mieux appréhender l'émergence de ces nouvelles pratiques, Micro Focus a lancé le Premier Observatoire des Directeurs et Responsables Informatiques sur l'adoption de la sécurité dans leurs initiatives DevOps. L'étude a été menée au premier trimestre 2019, en France, auprès des décideurs informatiques de grandes entreprises principalement. 18 questions clés ont été posées pour mesurer l'état d'adoption de l'initiative DevSecOps à plus de 2000 professionnels.

ETAT DES LIEUX ET ENJEUX IT

• Premier observatoire des Directeurs et Responsables Informatiques sur l'adoption de la sécurité dans leurs initiatives DevOps.

• Étude menée en janvier et février 2019 en France auprès de décideurs Informatiques de grandes entreprises principalement.

• 18 questions clés pour mesurer l'état d'adoption de l'initiative DevSecOps.

• Plus de 2 000 professionnels ont participé au sondage, dont plus de 130 ont répondu à l'intégralité des questions.

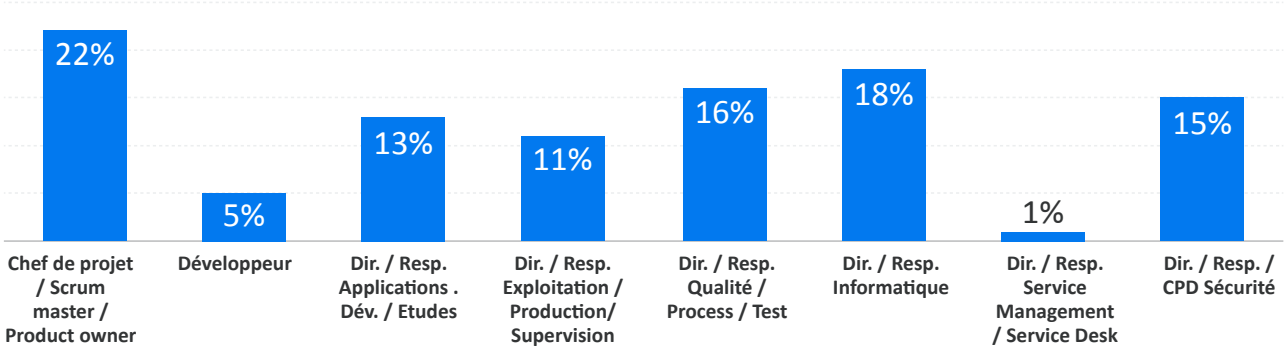
• 69% des répondants ont connu des incidents de sécurité et 41% vont investir prochainement dans une initiative DevSecOps.

VOTRE ENTREPRISE ET VOUS

La diversité des répondants à cette enquête, que ce soit en termes de secteurs d'activités, de tailles d'entreprises, ou encore de fonctions montre clairement que la protection des actifs informatiques de l'entreprise est une préoccupation partagée par tous les collaborateurs.

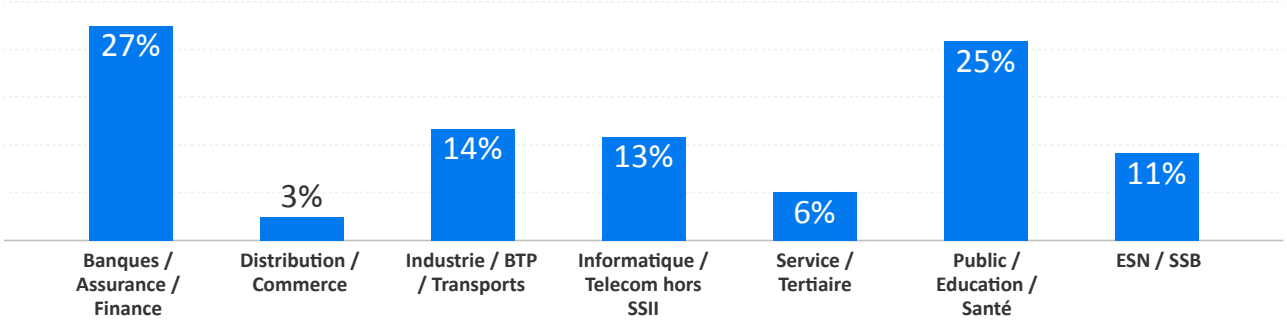
POUVEZ-VOUS NOUS PRÉCISER VOTRE FONCTION ?

LES RÉPONDANTS OCCUPENT PRINCIPALEMENT DES POSTES DE **RESPONSABLES INFORMATIQUES** AVEC UNE PART SIGNIFICATIVE DE **CHEFS DE PROJETS**

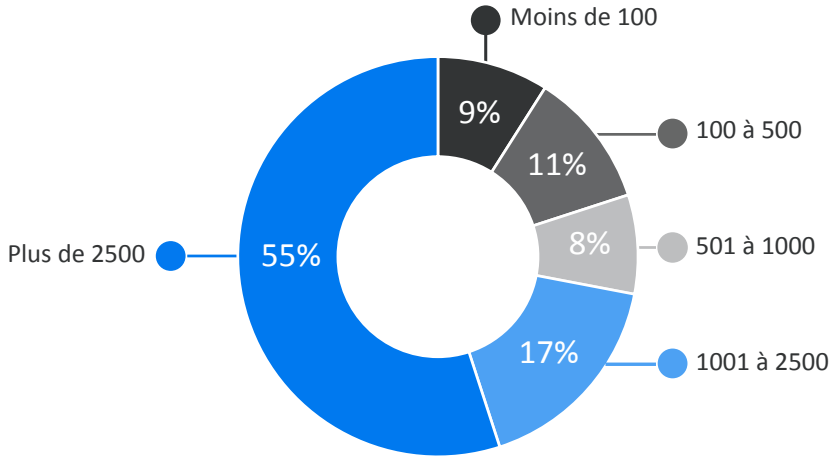


QUEL EST VOTRE SECTEUR D'ACTIVITÉ ?

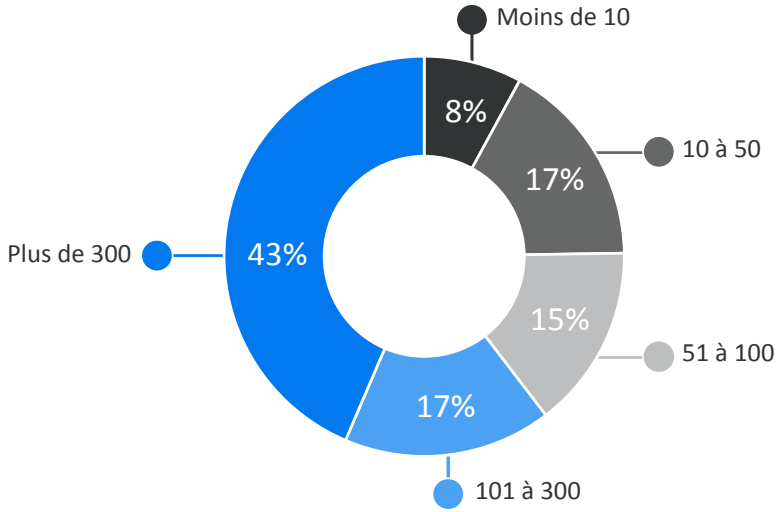
LES RÉPONDANTS TRAVAILLENT MAJORITAIREMENT DANS LE SECTEUR DE LA **BANQUE** / **ASSURANCE** / **FINANCE** ET DU **PUBLIC** / **ÉDUCATION** / **SANTÉ**.



QUEL EST VOTRE EFFECTIF ?



QUEL EST L'EFFECTIF DU DÉPARTEMENT INFORMATIQUE ?



72%

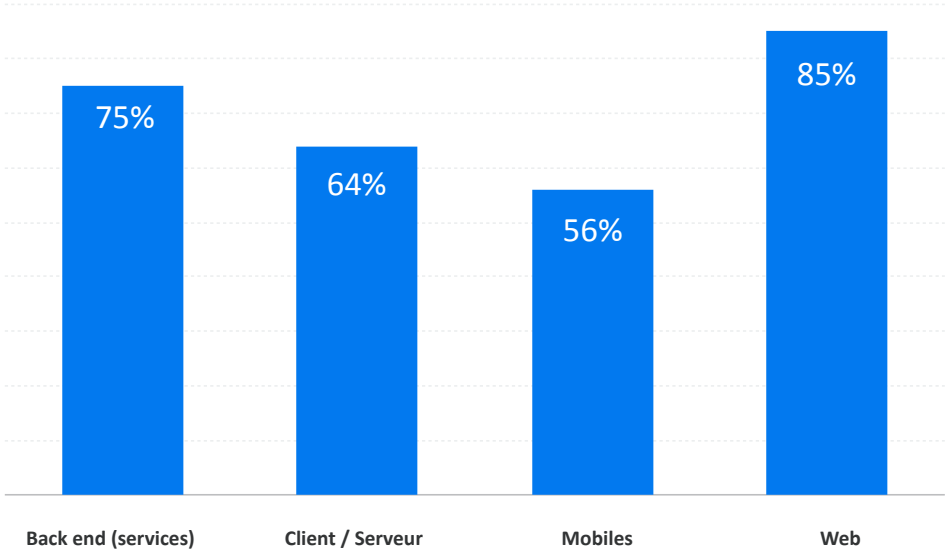
DES RÉPONDANTS TRAVAILLENT AVANT TOUT DANS DE GRANDES ENTREPRISES À EFFECTIF DE PLUS DE 1000

61%

DES DÉPARTEMENTS INFORMATIQUES ONT UNE TAILLE DE PLUS DE 100 PERSONNES

ETAT DES LIEUX ET ENJEUX IT

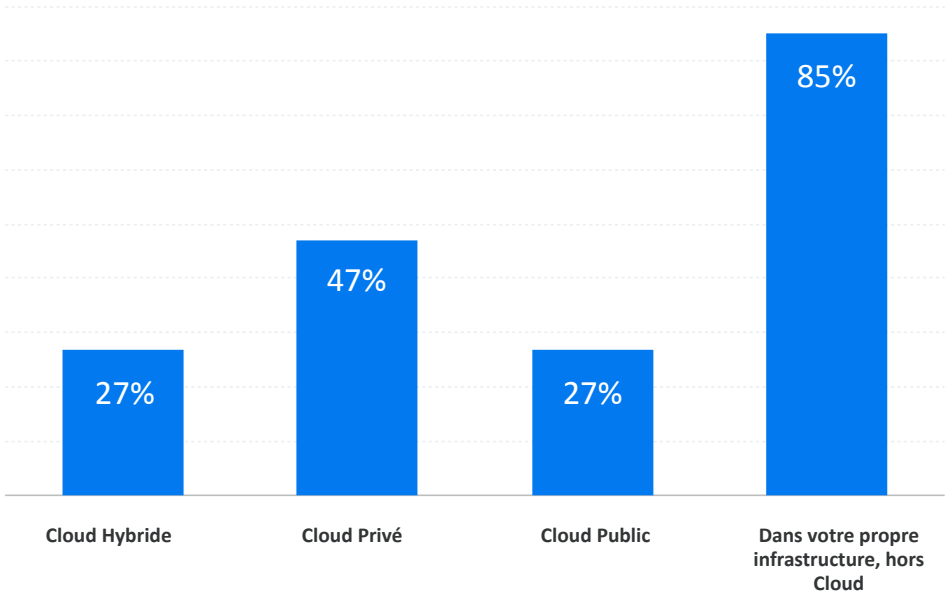
Le résultat est significatif : la démarche croissante de digitalisation des processus métiers et offres digitales est nettement orientée vers le client final. Les risques de sécurité sur le web et le mobile ne sont pas encore bien maîtrisés par les entreprises, notamment par manque de formation des administrateurs systèmes, réseaux ou encore de la plupart des développeurs web. Parmi les failles les plus fréquentes, nous retrouvons celles qui portent sur la conception applicative, le code mal sécurisé, la configuration des infrastructures ou encore le manque de chiffrement des informations permettant à l'utilisateur de s'authentifier. Nous recommandons à nos clients de réaliser des tests d'intrusions fréquents ainsi que des scans du code afin de déceler les potentielles vulnérabilités et les corriger de façon proactive. Dans la mesure du possible, sachant que ces tâches s'avèrent répétitives dans un cycle de développement Agile, il est également fortement recommandé de les automatiser.



QUELS TYPES D'APPLICATIONS DÉVELOPPEZ-VOUS ?

(plusieurs réponses possibles)

LES RÉPONDANTS DÉVELOPPENT TOUT TYPE D'APPLICATIONS, ET SURTOUT DES APPLIS WEB ET BACK END.



COMMENT DÉPLOYEZ-VOUS VOS APPLICATIONS ?

(plusieurs réponses possibles)

LES RÉPONDANTS DÉPLOIENT AUSSI BIEN LEURS APPLICATIONS SUR LEURS INFRASTRUCTURES (**85%**) QUE DANS LE CLOUD ET PLUTÔT EN CLOUD PRIVÉ (**47%**).

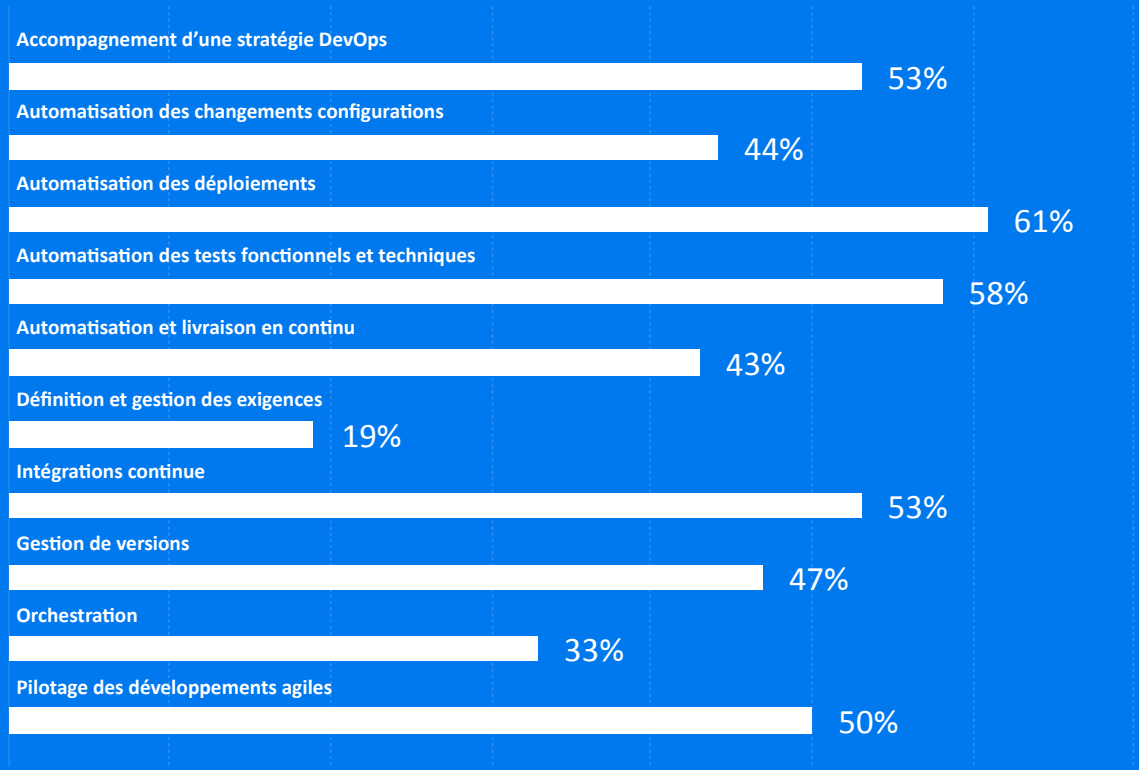
Malgré une prépondérance du déploiement applicatif On-premise, l'usage croissant du Cloud hybride & public induit de nouveaux challenges pour sécuriser les données sensibles.

Les problèmes de configuration sur les infrastructures On-premise rencontrés par les DSI existent également dans le cas des infrastructures Cloud. Selon le rapport de **RedLock** *(Redlock Cloud Threat Defense, Mai 2018)* plus de la moitié des entreprises n'ont pas sécurisé efficacement leurs services Cloud de stockage en 2017, et ont subi en conséquence une fuite ou un vol de données stockées. Ce ne sont pas les opérateurs Cloud qui sont responsables de cette situation, mais bien l'aptitude des DSI à maîtriser la sécurisation des services Cloud. Un autre exemple frappant concerne les patchs critiques à mettre à jour pour combler des failles de sécurité dans le Cloud public : environ un quart des entreprises ne les téléchargent pas à ce jour !

Les besoins de montée en compétences des équipes de la DSI pour assoir la maîtrise des services en Cloud sont très significatifs.

QUELLES INITIATIVES DEVOPS AVEZ-VOUS EN COURS OU SOUHAITEZ-VOUS METTRE EN PLACE ?

(plusieurs réponses possibles)



DANS LE TOP 5 DES INITIATIVES DEVOPS, ON RETROUVE : L'AUTOMATISATION DES DÉPLOIEMENTS, L'AUTOMATISATION DES TESTS FONCTIONNELS/TECHNIQUES, L'INTÉGRATION CONTINUE, L'ACCOMPAGNEMENT D'UNE STRATÉGIE DEVOPS ET LE PILOTAGE DES DÉVELOPPEMENTS AGILES.

DEVOPS ET SÉCURITÉ DANS LE CYCLE APPLICATIF

Dans cette étude, les initiatives d'automatisation du cycle de vie applicatif sont considérées prédominantes pour les répondants. De nombreuses entreprises voient l'automatisation comme un moyen d'accroître la productivité, la rapidité d'exécution, mais également de réduire les tâches répétitives - également sources d'erreurs humaines.

Sur le terrain, nous constatons que nos clients les plus avancés mettent en place des centres de compétences dédiés à l'automatisation des taches.

Par ailleurs, l'agilité et la transformation numérique semblent également être au centre des débats pour l'adoption de l'automatisation, dû au cycle itératif de développement induit.

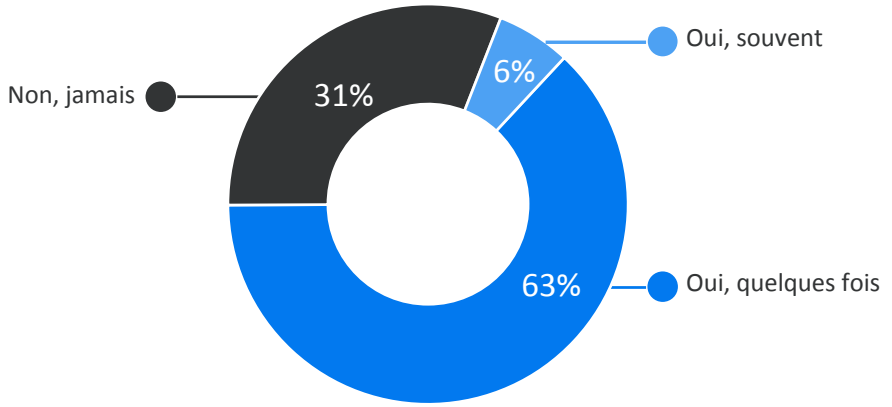
Au-delà des démarches d'automatisation, nos clients insufflent un changement de culture auprès de l'ensemble de la DSI en termes de pratiques de sécurité. On le constate depuis l'avènement de nouvelles législations comme la RGPD, qui contraint les entreprises à gérer plus efficacement la protection et la confidentialité des données de leurs clients.

Parmi les causes explicatives :

- Le manque de sensibilisation de l'organisation IT,
- Les bonnes pratiques de gestion des problèmes sont peu adoptées par les DSI, ce qui n'encouragent pas la définition et la mise en oeuvre de plans de prévention,
- Le manque de formalisme des retours d'expérience, ne permettant pas de capitaliser en transverse de la DSI,
- Les boucles de rétroaction des Ops vers les équipes de Dev Agiles trop rares, ne permettant pas d'enrichir en continu le relevé des besoins en terme de sécurité applicative.

Il est également à noter qu'1/3 des répondants estiment n'avoir jamais rencontré d'incidents de sécurité. Cette réponse pourrait traduire le fait que, pour certains répondants, il y a une incapacité partielle de la DSI à détecter les vulnérabilités. Très probablement, ces répondants ne réalisent peu voire pas de tests d'intrusions.

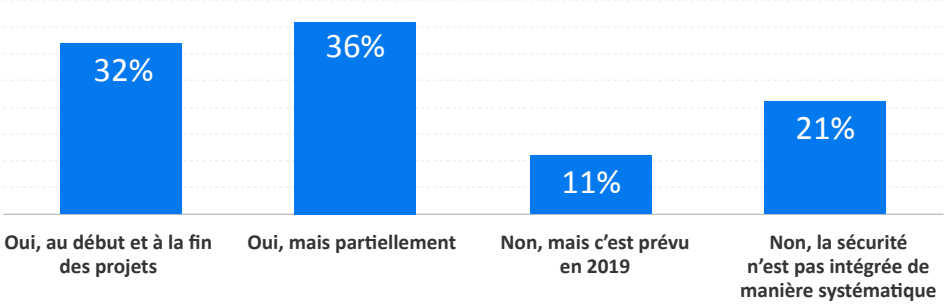
AVEZ-VOUS DÉJÀ RENCONTRÉ DES INCIDENTS DE SÉCURITÉ À LA MISE EN PRODUCTION APPLICATIVE ?



69%

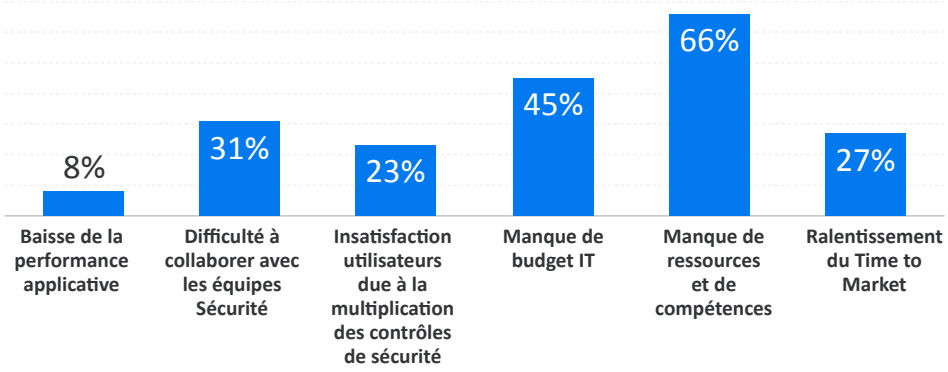
DES RÉPONDANTS ADMETTENT AVOIR DÉJÀ SUBI DES INCIDENTS DE SÉCURITÉ.

INTÉGREZ-VOUS DÉJÀ LA PRÉVENTION DES RISQUES ET LA SÉCURITÉ DANS VOS PROJETS DEVOPS ?



11% DES RÉPONDANTS N'INTÈGRENT PAS ENCORE LA SÉCURITÉ LORS DE LEURS DÉVELOPPEMENTS ET **21%** PAS SYSTÉMATIQUEMENT.

QUELS SONT LES FREINS À UNE DÉMARCHE 100% DEVSECOPS ?



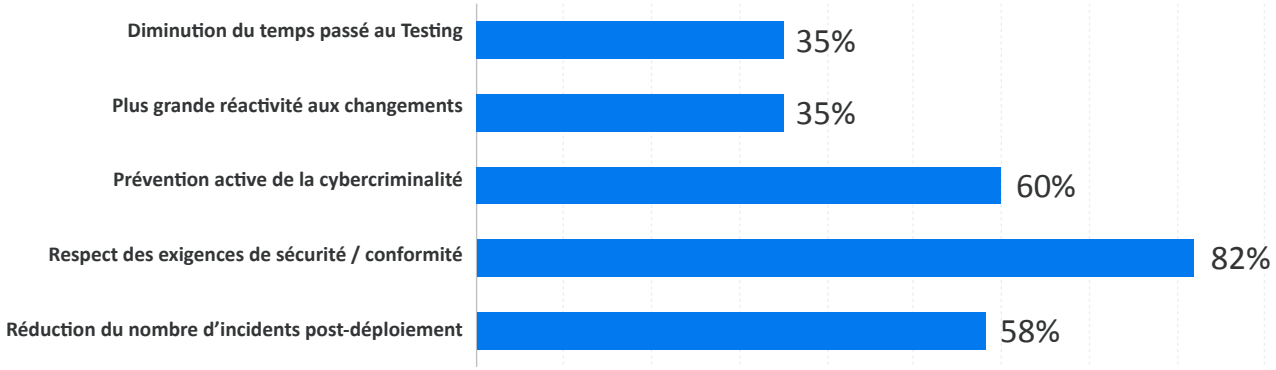
LE MANQUE DE RESSOURCES ET DE COMPÉTENCES RESTE DE LOIN LE PRINCIPAL FREIN (**66%**) SUIVI DU MANQUE DE BUDGET (**45%**).

Plusieurs raisons possibles peuvent expliquer ces réponses :

- **Le ralentissement du cycle de livraison continue**. Les équipes de développement peuvent ressentir une certaine frustration concernant le temps nécessaire à la bonne construction d'un code sécurisé. Ce ressenti peut aussi être lié au fait que les équipes de développement sont confrontées à la rigidité de processus imposés par la sécurité.
- **L'exécution manuelle des tests de sécurité**, lorsqu'ils existent. Le manque d'automatisation peut aussi être un élément important.
- **Le manque de temps alloué aux exigences de sécurité**. Il parait assez évident que les équipes ne consacrent pas le temps nécessaire à la définition des exigences de sécurité, tout comme aux tests permettant d'assurer le respect des exigences par l'application.
- **Une mauvaise priorisation**. Parfois, pour des enjeux de « Time-to-Market », la sécurité n'est pas considérée comme prioritaire dans les organisations.
- **Une absence de considération en amont de la phase de développement**. Enfin, il semblerait que pour 2/3 des répondants, la sécurité n'est pas intégrée dès le début de la phase de développement.
- **Un manque de compétences des équipes**. D'après les répondants de cette enquête, les équipes agiles ne sont pas assez sensibilisées aux bonnes pratiques de sécurité informatique. Ces dernières sous-estiment même leurs compétences en matière de cybersécurité.

QUELS SONT LES AVANTAGES D'UNE DÉMARCHE 100% DEVSECOPS ?

(plusieurs réponses possibles)



LE RESPECT DES EXIGENCES DE SÉCURITÉ ET DE CONFORMITÉ EST L'AVANTAGE LE PLUS CITÉ.

LES RÉPONDANTS PERÇOIVENT TRÈS BIEN LES AVANTAGES D'UNE INITIATIVE DEVSECOPS, MAJORITAIREMENT EN CE QUI CONCERNE LE RESPECT DES EXIGENCES DE SÉCURITÉ ET DE CONFORMITÉ **82%**.

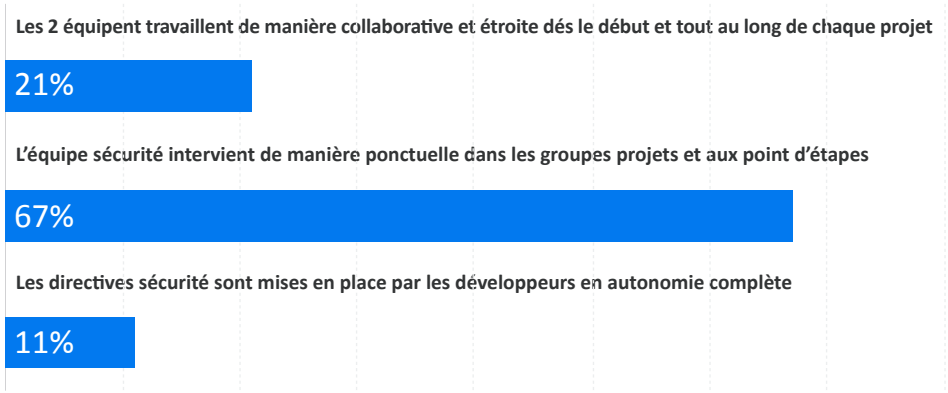
En effet, les entreprises qui ne seraient pas conformes aux nouvelles réglementations comme la RGPD se verraient infliger des pénalités pouvant aller jusqu'à 4% de leur chiffre d'affaires annuel. Les premières sanctions en France sont déjà tombées ! Par exemple, la CNIL a infligé une sanction record de 50 M€ à Google pour manquement à ses obligations au règlement général européen de protection des données.

On peut également citer la protection des données clients, préoccupation majeure des DSI. L'atteinte à l'image de l'entreprise en cas de fuite de données avérée lui est très préjudiciable. **La confiance des clients est très difficile à gagner, mais très facile à perdre.**

L'automatisation permet aussi aux équipes de développeurs de pouvoir revenir à des versions antérieures rapidement en cas de failles de sécurité liées au code.

Enfin, plus un bug est détecté tardivement dans le cycle de vie, plus son coût de résolution est élevé. En effet, un bug de sécurité repéré en production coûte 100 fois plus cher à résoudre que lorsqu'il a été détecté dans la phase de spécification. En automatisant les tests de sécurité sur l'ensemble du cycle de vie applicatif, le coût potentiel de non qualité pour l'entreprise sera infiniment moindre (sans évoquer son image de marque). De plus, le traitement des vulnérabilités de façon intégrée permet de ne pas ralentir le rythme de livraison.

COMMENT QUALIFIEZ-VOUS LA COLLABORATION ENTRE LES ÉQUIPES DE DÉVELOPPEMENT ET CELLES D'AUDIT / SÉCURITÉ ?



67%

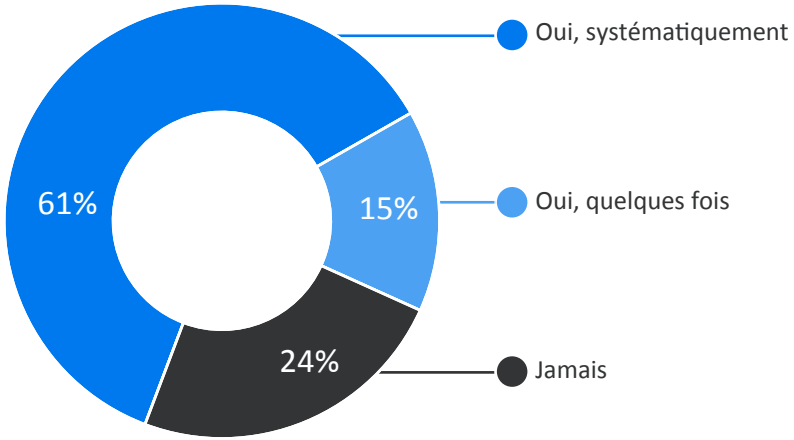
DES ÉQUIPES SÉCURITÉ N'INTERVIENNENT QUE PONCTUELLEMENT DANS LE CYCLE APPLICATIF

Un spécialiste de la sécurité IT ou un propriétaire de produit ne seront pas forcément en mesure de rédiger correctement des « stories » en lien avec la sécurité, qui plus car elles ne sont pas vraiment des « users stories » mais plutôt des cas d'usage exprimés exclusivement par des développeurs et des architectes pour prévenir des vulnérabilités. Ces « stories » sont plus perçues comme des contraintes supplémentaires, et donc la tentation de les mettre de côté est grande tant est que le propriétaire de produit n'en exprime pas le besoin de façon explicite.

Il faut être en mesure de créer des stories illustrant des usages déviants des applications et réfléchir en se mettant dans la peau d'un Hacker informatique. On part souvent du postulat que nos systèmes informatiques évoluent dans un domaine de confiance ce qui nous empêche de réfléchir librement aux comportements potentiellement malveillants.

On va parler « d'abuse case » pour comprendre le comportement du système face aux attaques et aux défaillances, répertorier les vulnérabilités à combler.

FAITES-VOUS PRATIQUER DES AUDITS SÉCURITÉ APPLICATIVE PAR DES SOCIÉTÉS EXTERNES ET INDÉPENDANTES ?



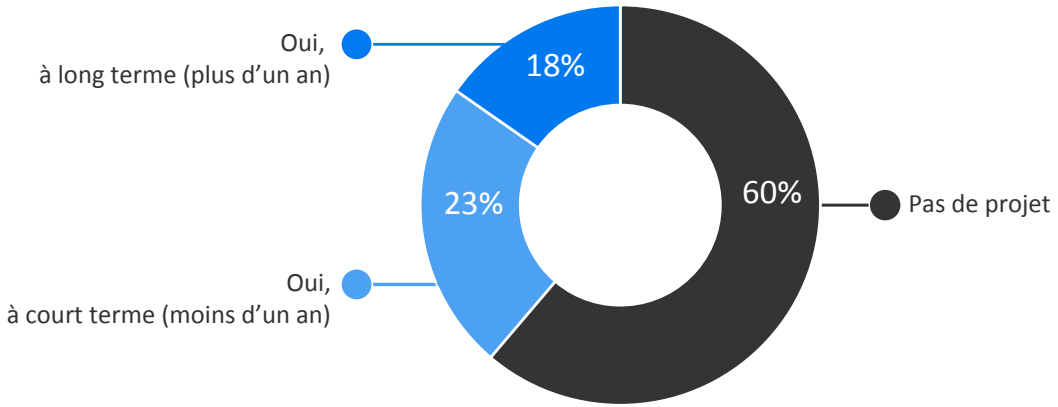
85%

DES RÉPONDANTS NE PRATIQUENT JAMAIS OU TRÈS PEU
DES AUDITS DE SÉCURITÉ.

Il apparait dans cette étude que la majorité des répondants n'adoptent pas de mesures de sécurité proactives en cherchant à combler de façon efficace et préventive les failles applicatives. La sécurité informatique est le problème de tous, pas uniquement du RSSI ! Le manque de visibilité sur les menaces n'incite pas à la prévention.

Les initiatives DevSecOps semblent s'installer progressivement dans les entreprises. En effet, près de la moitié des répondants ont déclaré qu'ils allaient investir dans cette voie à court et moyen terme, ce qui atteste d'une nouvelle prise en considération et de sa légitimité pour la mise en conformité.

AVEZ-VOUS UN PROJET D'INVESTISSEMENT DEVSECOPS ?



41%

DES RÉPONDANTS ONT UN PROJET DEVSECOPS,
CE QUI MONTRE LE DYNAMISME DE CETTE NOUVELLE TENDANCE.

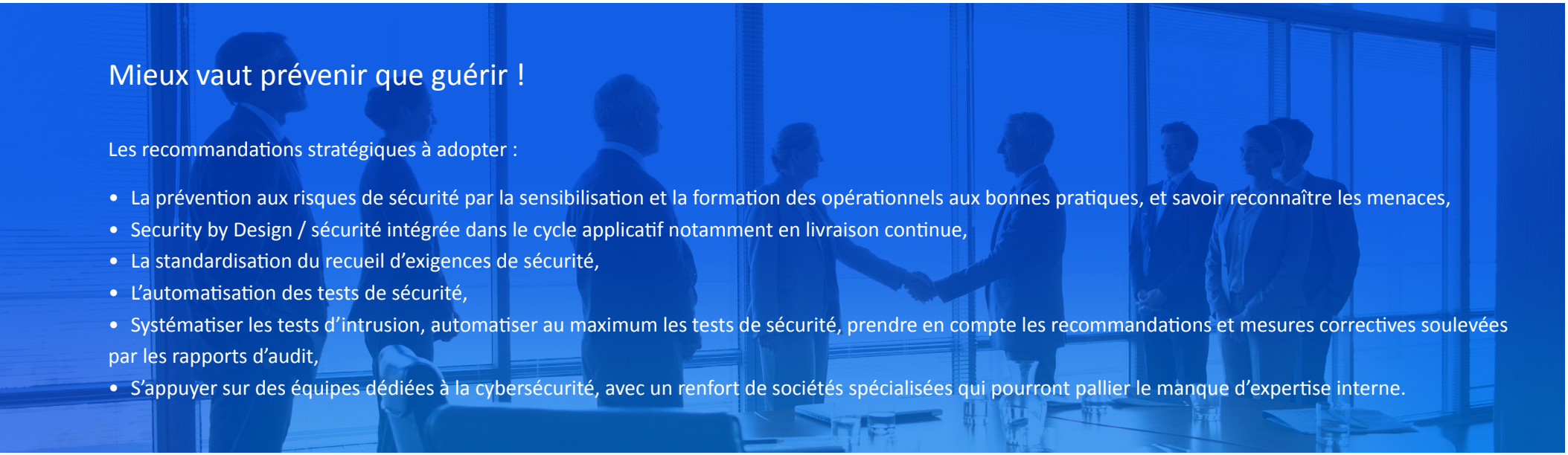
CONCLUSION

Bien que 69% des répondants rencontrent des incidents de sécurité, ils ne sont que 32% à l'intégrer du début à la fin de leurs projets. Le manque de ressources, de compétences et de budget sont les principaux freins à une démarche 100% DevSecOps.

Ce qui est confirmé par le fait que plus de 85% des répondants ne pratiquent jamais ou très peu d'audits de sécurité en externe.

Les répondants perçoivent très bien les avantages d'une initiative DevSecOps, surtout en ce qui concerne le respect des exigences de sécurité et de conformité (82%).

Près de la moitié des répondants vont investir dans cette initiative à court et moyen terme, ce qui atteste d'une nouvelle prise en considération et de sa légitimité pour la mise en conformité et le retour sur investissement des développements applicatifs.



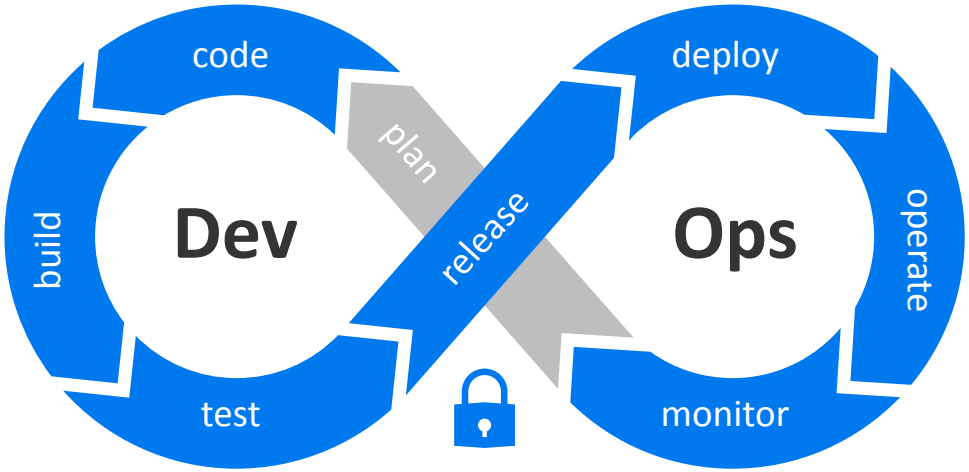
Mieux vaut prévenir que guérir !

Les recommandations stratégiques à adopter :

- La prévention aux risques de sécurité par la sensibilisation et la formation des opérationnels aux bonnes pratiques, et savoir reconnaître les menaces,
- Security by Design / sécurité intégrée dans le cycle applicatif notamment en livraison continue,
- La standardisation du recueil d'exigences de sécurité,
- L'automatisation des tests de sécurité,
- Systématiser les tests d'intrusion, automatiser au maximum les tests de sécurité, prendre en compte les recommandations et mesures correctives soulevées par les rapports d'audit,
- S'appuyer sur des équipes dédiées à la cybersécurité, avec un renfort de sociétés spécialisées qui pourront pallier le manque d'expertise interne.

LA VISION DEVSECOPS MICRO FOCUS

Micro Focus favorise une approche **DevSecOps** à l'échelle de l'entreprise.
Livrer, Exploiter et Sécuriser des applications de qualité plus rapidement.



PLAN/GOVERN

Optimiser la chaîne de valeur

DEVELOP/TEST

Qualité & Sécurité en **Continu**

DEPLOY/RELEASE

Accélérer les livraisons

OPERATE/MONITOR

Fiabilité accrue des services

Bâtir sur ce qui fonctionne

en connectant les anciennes et les nouvelles technologies au fil des changements

Réduire les frictions opérationnelles

en améliorant la visibilité et la collaboration ainsi qu'en automatisant

Gagner la confiance des métiers

en garantissant la qualité et la sécurité de chaque application

Améliorer les résultats

de manière continue en analysant l'ensemble des données et des retours de la chaîne DevSecOps

MICRO FOCUS

Chez Micro Focus, nous vous aidons à gérer votre entreprise et à la transformer. Notre offre logicielle fournit les outils essentiels dont vous avez besoin pour construire, exploiter, sécuriser et analyser votre entreprise. De par leur conception, nos solutions comblent le fossé entre les technologies existantes et émergentes, vous pouvez ainsi innover plus rapidement et à moindres risques, dans la course à la transformation digitale.

EN SAVOIR PLUS
HTTPS://WWW.MICROFOCUS.COM/EN-US/TREND/ENTERPRISE-DEVOPS