2025

État de l'observabilité

Un nouveau moteur de valeur

splunk>
a CISCO company

Sommaire

Avant-propos

Lorsque j'ai fait mes premiers pas dans le domaine de l'observabilité il y a plus de dix ans, notre mission était simple : maintenir les services et les systèmes en état de marche. Comprendre ce qui se passe et qui est touché, isoler le problème et le résoudre. Aujourd'hui, le logiciel n'est plus seulement un rouage de l'entreprise : il *est* l'entreprise.

Depuis que les expériences numériques sont devenues le principal vecteur d'engagement client, l'impact des pratiques d'observabilité dépasse largement les limites des salles de serveurs et des NOC. En corrélant les données de télémétrie et les résultats métiers, il devient possible de prendre des décisions majeures pour améliorer la satisfaction des clients ou même de déterminer quels produits développer. Aujourd'hui, l'IA déclenche un nouveau séisme, et les pratiques d'observabilité doivent assumer des responsabilités plus lourdes encore : superviser les workloads complexes et dynamiques de l'IA pour en garantir la performance et la fiabilité. Cette évolution fait de l'observabilité non seulement un véritable fondement de l'expérience client, mais aussi un facteur clé d'innovation et de croissance dans les entreprises axées sur l'IA.

Pour rédiger le rapport *État de l'observabilité en 2025*, nous avons interrogé 1 855 professionnels ITOps et de l'ingénierie, dans le but de mieux comprendre cette transformation et d'identifier ce qui distingue les équipes les plus performantes. Un groupe de participants se démarque en contribuant davantage que leurs pairs au résultat net. Comment ? Ils collaborent davantage avec les équipes de sécurité, abordent la gestion des incidents de manière plus stratégique et investissent dans des technologies et des pratiques visionnaires.

Les professionnels de l'observabilité sont désormais intégrés à la planification et à la prise de décisions stratégiques. Ils mettent leur expertise (et leurs données) au service des stratégies d'engagement client, des feuilles de route des produits et du comité de direction. Ils ont voix au chapitre et ils sont bien déterminés à la faire entendre.

Patrick Lin,
SVP et directeur général de l'Observabilité chez Splunk.

Chapitre1

L’observabilité s’impose comme un moteur de valeur

Derrière chaque initiative métier et chaque innovation audacieuse se cache une étincelle essentielle : un moteur qui donne une direction et motive à agir. Parfois, c’est une étude de marché qui surprend en révélant qu’un groupe démographique différent utilise votre produit de manière inattendue, et ouvre ainsi les portes d’un nouveau marché. Dans d’autres cas, c’est une fonctionnalité mineure et négligée qui s’avère être la clé de l’engagement client, bouleversant du même coup toute la feuille de route du produit.

Ces moments de révélation ne se produisent pas par hasard. Ils sont le fruit de pratiques parfois silencieuses, mais toujours essentielles. Aujourd’hui, l’observabilité s’impose comme cette force motrice. Et même si l’observabilité et les informations qu’elle peut révéler ne prennent pas elles-mêmes les décisions finales, sans elles, rien n’avance assez vite pour avoir un impact.

Les données renforcent le lien entre l'observabilité et les fonctions métiers

Les entreprises savent mieux que jamais que les décisions liées aux logiciels entraînent des répercussions considérables sur l'expérience client, l'image de la marque et bien plus encore. Lorsqu'elles exploitent les données d'observabilité, c'est pour poser la question : « Comment utiliser les données de nos applications pour prendre des décisions métiers ? », et non « Où est le problème ? ».

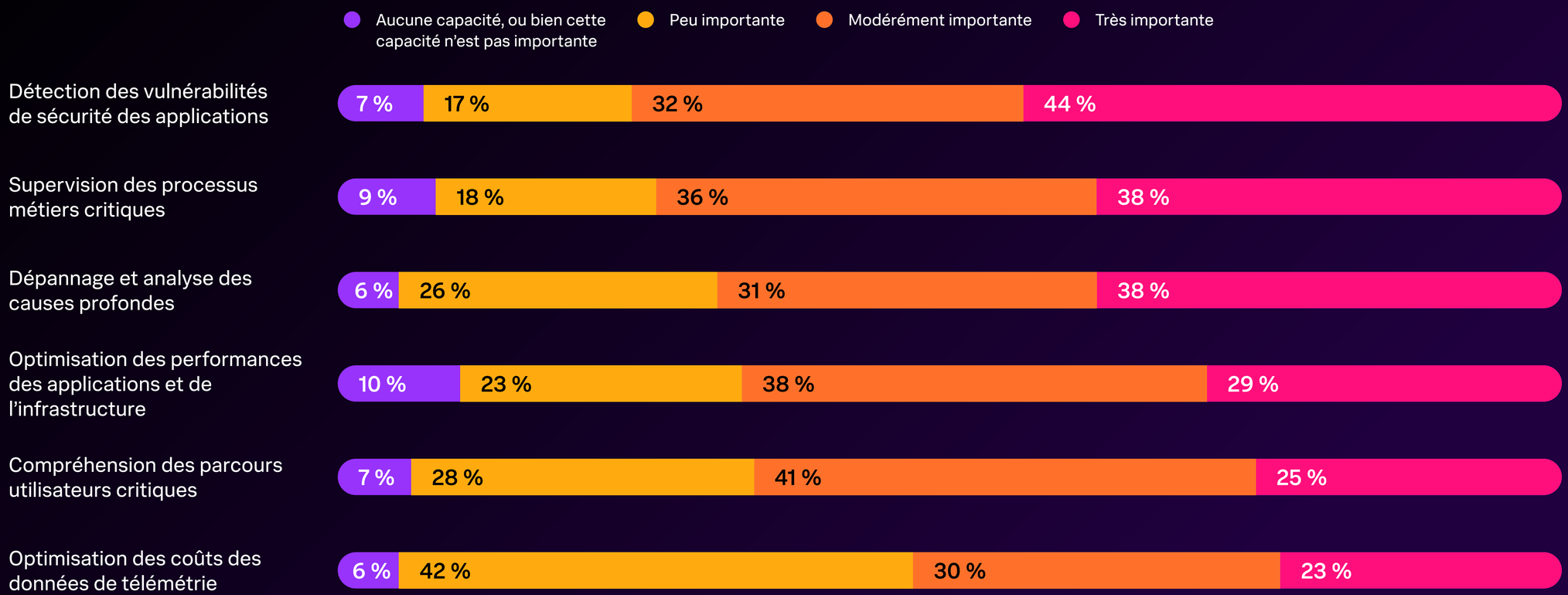
Pour éclairer ces décisions, les équipes d'observabilité ont fait de la capture des métriques métiers une priorité absolue. Pour près des trois quarts (74 %) des personnes interrogées, la supervision des processus métiers critiques est *modérément* à *très* importante. Celles qui enregistrent d'importants retours sur investissement avec leurs solutions d'observabilité sont particulièrement catégoriques sur ce point : les processus métiers critiques sont plus souvent mentionnés dans leurs préoccupations que toute autre option.

Est-ce que l'augmentation des revenus de l'entreprise est due à l'introduction d'une nouvelle fonctionnalité ou à une campagne particulièrement performante de l'équipe marketing ? Il fut un temps où il fallait aux professionnels beaucoup de temps, d'esprit d'analyse et de patience pour répondre à cette question. Aujourd'hui, l'observabilité est le catalyseur qui convertit la télémétrie des applications en action métier. Grâce aux données d'observabilité, les spécialistes vous diront *pourquoi* les revenus ont chuté, *où* se produisent les frictions clients et *comment* les performances des produits affectent la croissance de l'entreprise.

Les équipes produit doivent travailler en étroite collaboration avec l'ingénierie pour éclairer les décisions relatives à la feuille de route et déterminer les fonctionnalités à traiter en priorité, sur la base des informations issues de la télémétrie. Démocratiser ces données métiers est le meilleur moyen de faire en sorte que cette magie opère. Si les équipes doivent attendre qu'un analyste métier extraie des données de trois tableaux de bord différents, l'instant est passé.

– Greg Leffler, Directeur de l'évangélisation des développeurs, Splunk

L’importance des capacités d’observabilité pour l’entreprise

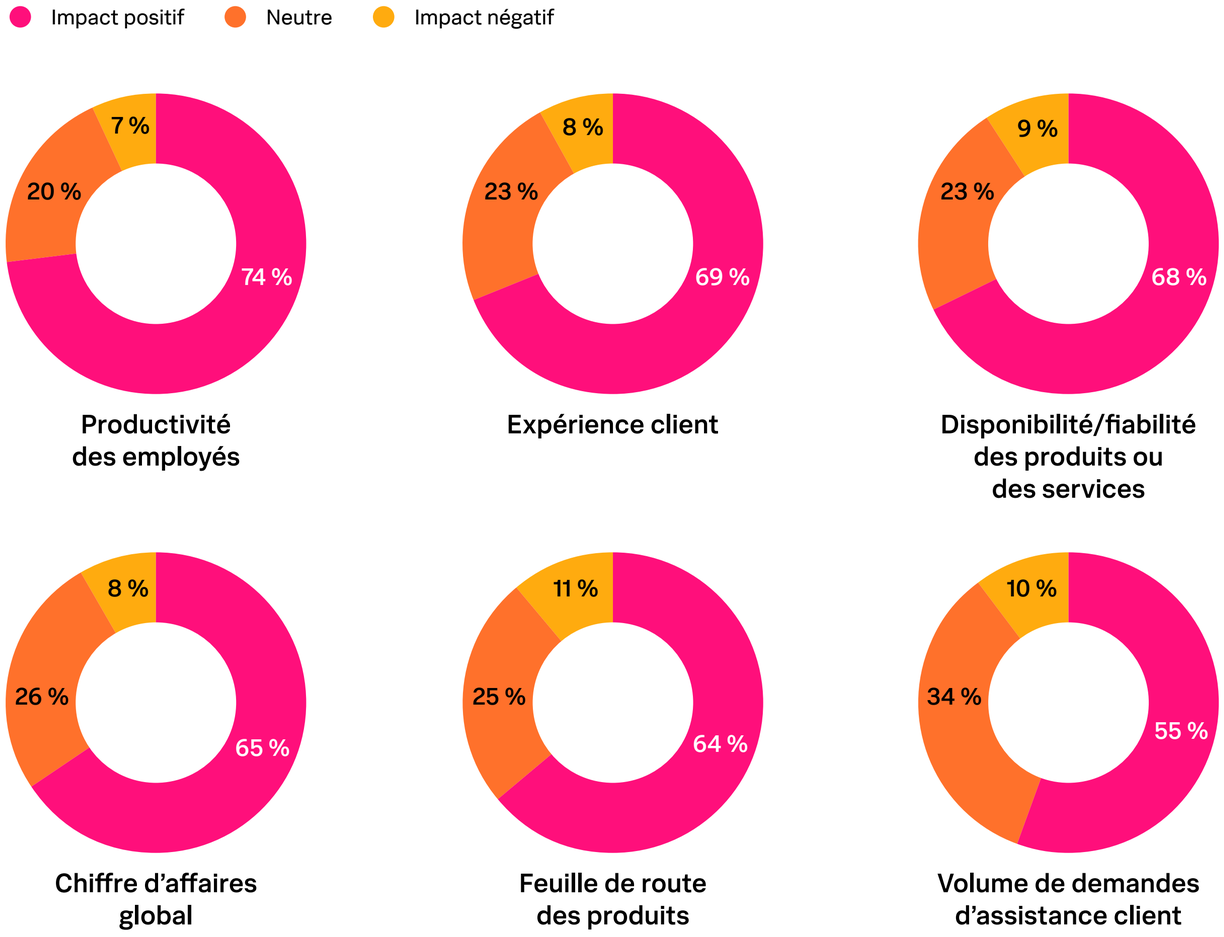


Les pourcentages ne totalisent pas toujours 100 % en raison des arrondis.

La pratique d'observabilité ne doit pas seulement avoir une connaissance détaillée des indicateurs métiers, elle doit aussi contribuer aux résultats en améliorant les performances, l'expérience des utilisateurs et les revenus de l'entreprise. Lorsqu'elles disposent de mesures fiables, les équipes d'ingénierie et ITOps peuvent se consacrer à des tâches qui ont un impact direct sur l'entreprise : comprendre les parcours utilisateurs critiques, créer des tableaux de bord détaillés en temps réel pour informer à la fois les stratégies technologiques et métiers, et associer les problèmes de performance des applications en opportunités de revenus. Une entreprise d'e-commerce, par exemple, utilisera l'observabilité pour visualiser l'ensemble du parcours client, de la visite du site web au traitement de la commande, et éviter des pertes de revenus en assurant la disponibilité des principaux systèmes métiers. Il est donc logique que 65 % des participants considèrent *modérément* à *très* importante la capacité de leur solution d'observabilité à comprendre les parcours utilisateurs critiques.

Les organisations sont à la hauteur de l'enjeu : 65 % des personnes interrogées affirment que leur pratique d'observabilité influence positivement les revenus. Elle sont également 64 % à affirmer que cette pratique exerce un impact positif sur la feuille de route des produits. Les équipes produit s'appuient sur les données de supervision des utilisateurs réels (RUM) pour savoir combien de temps il faut à une page pour s'afficher complètement et dans quels délais les utilisateurs peuvent interagir avec elle, puis corréler ces données avec les indicateurs de performance des applications pour tirer des conclusions. L'ajout d'une nouvelle fonctionnalité à un site web pourrait, par exemple, ralentir les performances et faire grimper le taux d'abandons de panier. Pour prendre un autre exemple, une mise à jour intégrant une fonction de protection contre la fraude plus agressive pourrait entraîner une baisse des revenus.

L'impact de l'observabilité sur l'entreprise



Les pourcentages ne totalisent pas toujours 100 % en raison des arrondis.

Chapitre 2

Soulager les points de tension de l'observabilité

Si vous travaillez dans l'ITOps ou l'ingénierie, vous avez déjà vécu ce genre de journées. Elle commence par la pire alerte que vous puissiez imaginer et empire avec une vague de notifications. Cette spirale continue jusqu'au moment où vous devez réveiller votre responsable pour lui annoncer de mauvaises nouvelles. Pendant ce temps, une petite voix dans votre tête murmure : « *Tu es fichu* ». Quand la journée se termine, avec un peu de chance, vous avez arrêté le déluge. Vous avez le doigt sur la fuite et votre taux d'adrénaline est toujours bien trop haut.

Impossible de ne pas ressentir de stress dans une telle situation. Nous ne sommes pas des machines. Lorsqu'il faut prendre en charge un incident, les instants de panique devraient être rares et sporadiques. Pourtant, 21 % des personnes interrogées déclarent paniquer *parfois*, *souvent* ou *toujours* lorsque survient un incident qui touche les clients. Et même si ce n'est que *parfois*, c'est encore trop. Ces interventions dans l'urgence épuisent les équipes et sont le signe clair qu'elles ne disposent pas de tous les éléments de contexte pour résoudre l'incident.

Seuls des plans solides permettent de tenir la panique à distance

Lorsque l'on travaille dans l'ITOps ou l'ingénierie, la pression fait partie du quotidien. La performance d'une pratique d'observabilité se mesure à la manière dont elle réagit aux incidents et empêche que d'autres ne se produisent. Il est donc essentiel que les équipes gardent leur calme et leur maîtrise lorsque les alertes fusent et que l'incendie semble se propager.

Les cahiers de procédures, les plans de réponse et les bilans post-incident sont autant d'approches méthodiques et stratégiques qui permettent d'éviter la panique. Plus de la moitié (54 %) des participants à l'étude élaborent *souvent* ou *systématiquement* un plan de réponse détaillé, et 71 % déclarent effectuer *souvent* ou *systématiquement* un bilan post-incident approfondi.

N'oublions pas non plus que l'union fait la force : il est parfois réconfortant de se tourner vers un collègue qui est au front avec vous. Mais il faut faire la différence entre ce qui relève de la collaboration stratégique et de la mobilisation générale en urgence. Les cellules de crise peuvent facilement dégénérer et chacun finit par se marcher dessus. Ce type de scénario disperse les ressources et épuise les collaborateurs les plus précieux en les absorbant dans des investigations sans fin. Pourtant, 20 % des personnes interrogées affirment former *souvent* ou *systématiquement* une cellule de crise pour réunir les membres de plusieurs équipes jusqu'à ce que le problème soit résolu. C'est le signe que l'approche réactive est encore courante et que les problèmes en cascade sèment encore la confusion.

Patrick Lin, Vice-président senior et Directeur général de l'observabilité chez Splunk, explique : « Les cellules de crise prolifèrent lorsque les outils d'une organisation ne sont pas suffisamment efficaces pour aider les équipes à isoler le problème. Les logiciels d'observabilité ont tellement évolué qu'aujourd'hui, les équipes devraient pouvoir rétablir les services sans réunir 50 personnes dans la même pièce. »

Une approche plus intelligente consiste à circonscrire l'incident à une équipe spécifique qui sera chargée de le résoudre, ce que seulement 22 % des participants à l'étude déclarent faire *souvent* ou *systématiquement*. Cette approche est typique des pratiques d'observabilité matures qui ont beaucoup développé la collaboration (nous y reviendrons plus tard).

73 %

des interruptions subies sont dues à des alertes ignorées ou supprimées

Les évaluations post-incident permettent de tourner la page, et cela peut être un véritable soulagement. Savoir qu'un incident ne se reproduira plus, aussi anxiogène soit-il au départ, fait des merveilles sur la santé mentale de chacun.

– Caitlin Halla, Développeuse évangéliste, Splunk

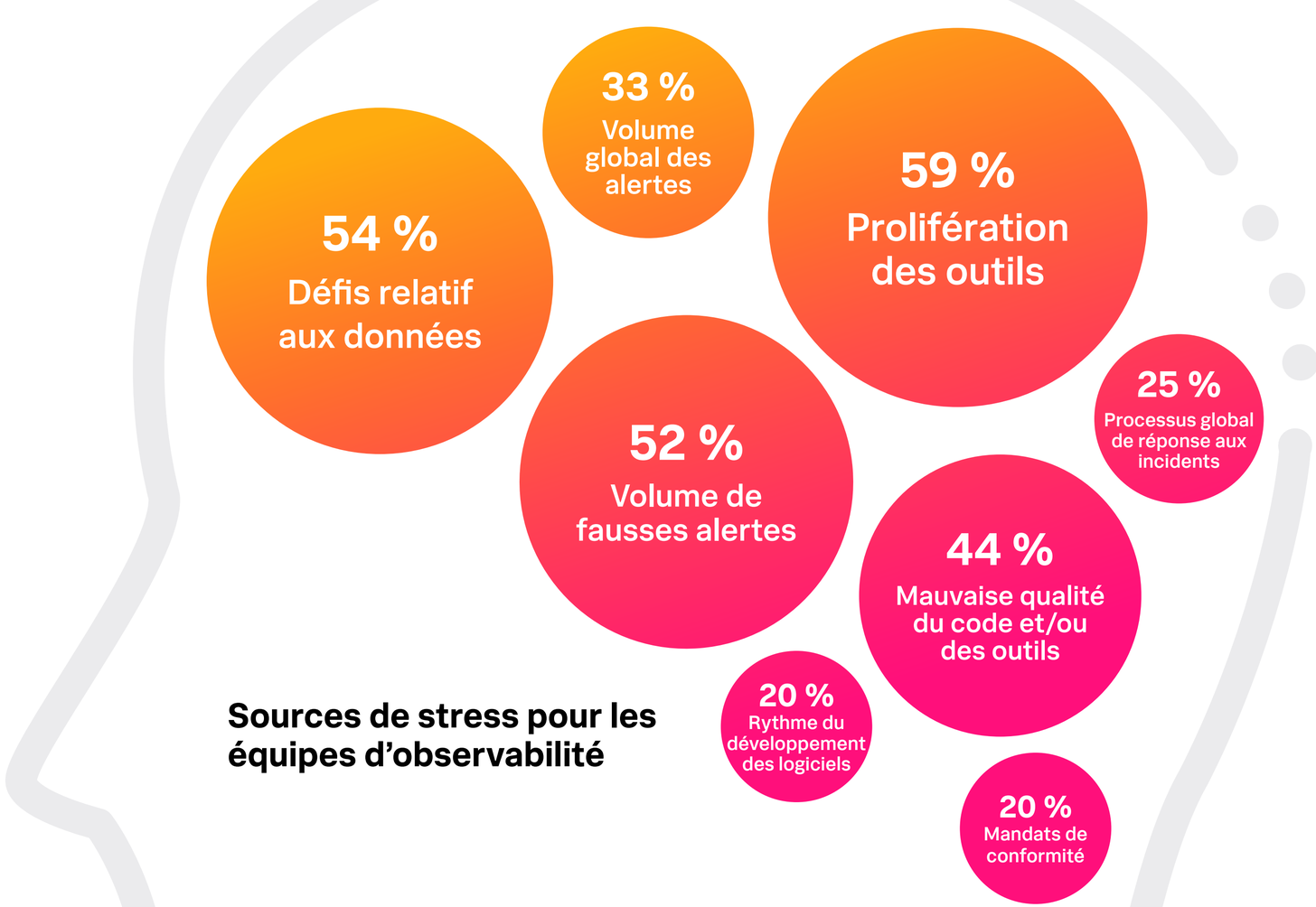
Les fausses alertes et les outils mal gérés sapent le moral des équipes autant que le retour sur investissement

C'est indéniable, les incidents sont source de stress, mais ils ne sont pas le plus grand ennemi de la santé mentale des équipes si on les compare à d'autres facteurs. Seuls 25 % des participants considèrent que la réponse aux incidents a un impact négatif sur le moral. En revanche, ils sont 59 % à voir dans la prolifération des outils une source d'anxiété.

Vient ensuite un problème qui accable les équipes d'ingénierie et ITOps depuis des années : le volume de fausses alertes. Les deux problèmes sont inextricablement liés. Plus une organisation accumule d'outils, plus la probabilité qu'ils génèrent de fausses alertes augmente, en particulier si les équipes sont tellement sollicitées qu'elles n'ont pas le temps d'affiner les règles qui les déclenchent, de corréler les signaux entre les systèmes ou d'évaluer ce qui compte vraiment.

La prolifération des outils est un véritable défi, mais ce qui nuit réellement au retour sur investissement est la mauvaise qualité des détections qu'ils génèrent. Lorsque les alertes sont bruyantes, redondantes ou dépourvues de contexte, même les ensembles d'outils les plus avancés ne peuvent apporter une valeur concrète.

– Stephanie Elsesser, Directrice des stratèges d'observabilité, Splunk



Sources de stress pour les équipes d'observabilité

Les participants pouvaient sélectionner toutes les réponses valables.

Les fausses alertes ne se contentent pas de stresser les équipes. Elles entraînent des conséquences à grande échelle, notamment sur les résultats financiers. Plus de la moitié (54 %) des participants affirment que la qualité de leurs détections est l'un des principaux facteurs du ROI de l'observabilité, et 47 % affirment que les alertes influencent *significativement* les décisions de sécurité au sein de leur organisation.

Pour tenter d'échapper au déluge de fausses alertes, certaines équipes ont recours à des méthodes risquées. En effet, 13 % avouent ignorer ou supprimer *souvent* ou *systématiquement* les alertes. Plus alarmant encore (sans mauvais jeu de mots), 73 % des personnes interrogées disent avoir connu des interruptions dues à des alertes ignorées ou supprimées.

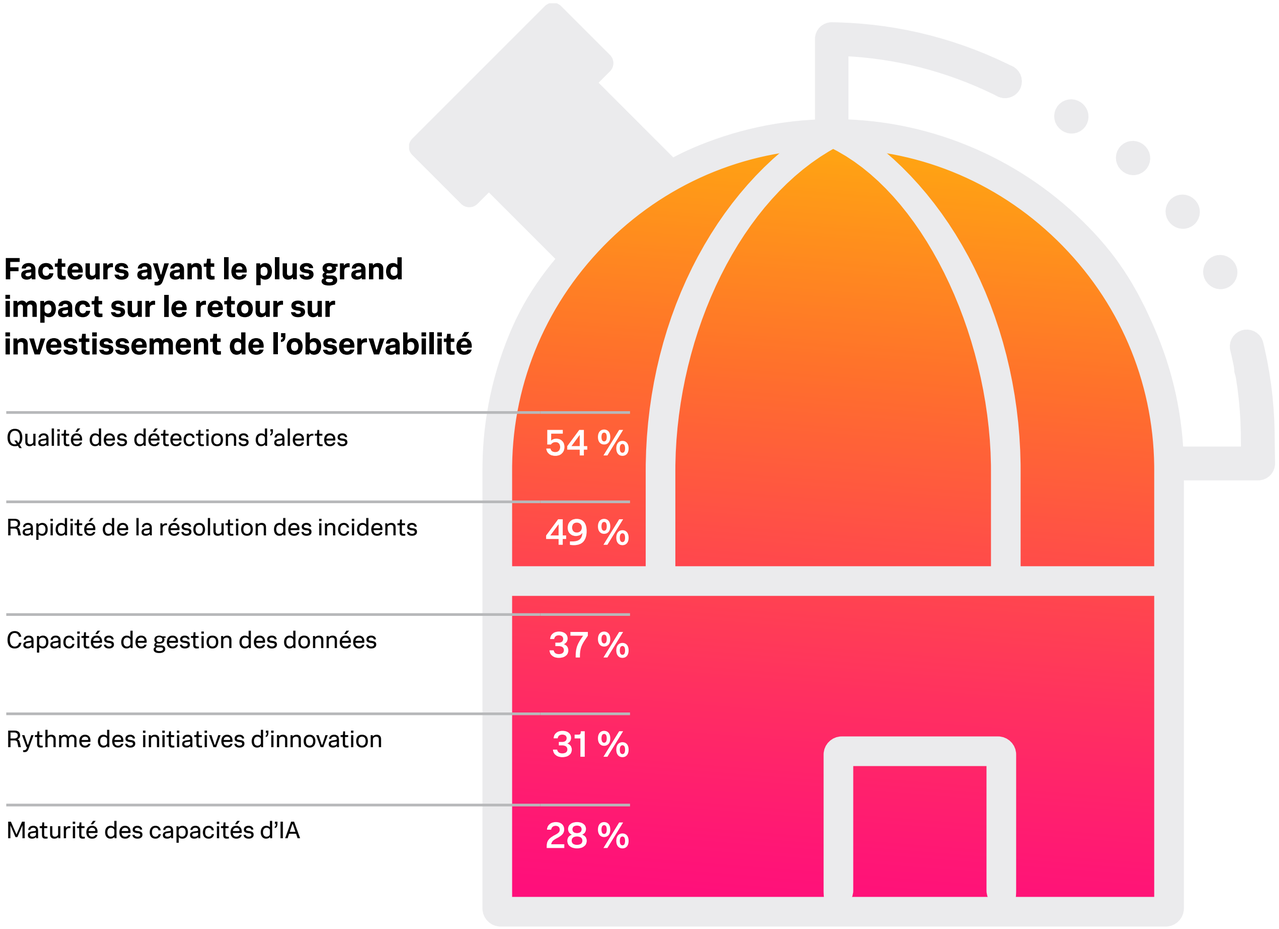
Greg Leffler, Directeur de l'Évangélisation des développeurs chez Splunk, déclare : « Une pratique d'observabilité performante ne devrait supprimer aucune alerte, point final. Idéalement, les alertes ne devraient signaler qu'un problème immédiat ayant un impact métier. »

Que les équipes traquent les fausses alarmes, fassent le tri dans une avalanche d'alertes, investiguent un incident obscur ou reconfigurent des seuils à la volée, une chose est claire : les alertes occupent trop de cycles de productivité, sans parler du nombre d'arrêts maladie pour épuisement qu'elles provoquent. 43 % des participants admettent passer « plus de temps qu'ils ne le devraient » à répondre aux alertes.

Si vous passez devant un tableau de bord d'alerte, vous verrez certainement en bas une multitude d'alertes non lues et non traitées. C'est la réalité, mais c'est loin d'être idéal. Les alertes sont censées mobiliser immédiatement l'attention et contenir suffisamment de contexte pour permettre une action rapide. Elles ne devraient pas être un bruit de fond.

Mike Simon, Développeur évangéliste chez Splunk, déclare : « Les alertes seront toujours un élément central de l'observabilité. Mais pour qu'elles soient exploitables à grande échelle, il ne faut pas seulement réduire le bruit, il faut aussi améliorer le signal. Établissez une corrélation entre les éléments essentiels, comprenez leur impact sur l'entreprise et mettez en évidence ce qui mérite vraiment l'attention pour que les équipes approfondissent leurs recherches lorsque cela est nécessaire. Les ingénieurs vont gagner du temps qui pourra être consacré à la véritable priorité : créer de meilleurs logiciels. »

Facteurs ayant le plus grand impact sur le retour sur investissement de l'observabilité



Les participants pouvaient sélectionner toutes les réponses valables.

Chapitre 3

Collaborer avec la sécurité étend l'influence de l'observabilité

Vous supervisez la plateforme d'e-commerce de votre entreprise, et vous remarquez que la latence de connexion augmente et que les services back-end sont sous tension. Les abandons de panier se multiplient, des alertes se déclenchent à tous les niveaux et, pour couronner le tout, les revenus sont en chute libre. L'ITOps transmet le problème à l'ingénierie, qui rétablit la version précédente du code… mais rien n'y fait. Pendant ce temps, l'équipe de sécurité investigue discrètement du trafic provenant potentiellement de robots, mais elle ne considère pas encore ce problème comme urgent.

Chaque équipe pourrait ainsi s'engager sur sa propre voie et y perdre beaucoup de temps et d'énergie. Mais toutes ces équipes pourraient aussi utiliser des données, des tableaux de bord, des navigateurs et du contexte partagés au sein d'une plateforme d'observabilité afin de résoudre les problèmes en parallèle. En travaillant ensemble, elles découvriraient bientôt la cause profonde du problème (une attaque par injection d'identifiants qui submerge les ressources du back-end) et le résoudraient rapidement pour atténuer l'impact sur le client.

La collaboration entre l'observabilité et les équipes de sécurité s'avère hautement fructueuse. Près des deux tiers (64 %) des personnes interrogées rencontrent moins de problèmes de performances des applications et de l'infrastructure, 54 % améliorent la qualité des données et 54 % affirment perdre moins de temps à localiser les problèmes. Résultat : une nette réduction du MTTD et du MTTR.

Ces avantages s'étendent également à l'ensemble de l'entreprise. Pour 64 % des personnes interrogées, la collaboration avec les équipes de sécurité s'est traduite par une réduction du nombre d'incidents affectant les clients. Il devient clair que la valeur des données d'observabilité ne s'arrête pas aux équipes ITOps et d'ingénierie. Plus des trois quarts (76 %) des participants considèrent que la capacité de leur solution d'observabilité à détecter les vulnérabilités et les menaces de sécurité des applications est *modérément* à *très* importante pour l'activité globale de leur entreprise.

La collaboration avec les équipes de sécurité porte ses fruits

Les participants attribuent de nombreux avantages à la collaboration

64 %
Moins d'incidents affectant les clients

64 %
Diminution des problèmes de performances des applications et de l'infrastructure

54 %
Amélioration de la qualité des données

54 %
Moins de temps perdu à traquer les problèmes

Les participants pouvaient sélectionner toutes les réponses valables.

Les équipes de sécurité et d'observabilité moins avancées utilisent des outils différents, elles n'ont pas les mêmes priorités et ne communiquent souvent que lorsque c'est absolument nécessaire, généralement lors d'un incident. Mais aujourd'hui, ces cloisons qui enferment les données et les outils et bloquent la communication s'effondrent. Les pratiques d'observabilité qui n'ont pas encore pris de mesures pour faciliter cette collaboration ne parviendront pas à progresser, en particulier dans le contexte de l'utilisation croissante de l'IA.

– Patrick Lin, SVP et Directeur général de l'observabilité chez Splunk.

Le partenariat accélère la résolution

Collaboration, synergie, synchronicité ou simplement travail d'équipe… Quel que soit le nom que vous lui donnez, le partenariat avec les équipes de sécurité est un processus réfléchi et structuré. Il ne suffit pas de distribuer des données d'observabilité au hasard en espérant qu'elles servent à quelque chose.

Parmi les participants, 74 % indiquent que leurs équipes d'observabilité et de sécurité partagent et réutilisent les données, une première étape décisive vers la collaboration. Parallèlement à cela, 68 % des personnes interrogées nous disent que les deux équipes utilisent le même ensemble d'outils.

Ces pratiques devraient être des enjeux majeurs dans l'entreprise. La collaboration en temps réel donne accès à des éléments de contexte que les tableaux de bord ne suffisent pas à fournir. Imaginons que l'ingénierie ait renouvelé la clé API d'un service back-end, mais qu'elle n'ait pas mis à jour un service qui l'utilise en amont. La nouvelle version est déployée, les requêtes des utilisateurs se mettent à échouer les unes après les autres, les nouvelles tentatives se multiplient et la latence augmente. Il faut souvent rapprocher les données de pic de latence des logs de sécurité pour détecter ce problème, et ce niveau de corrélation est rarement accessible dans la plupart des tableaux de bord d'observabilité.

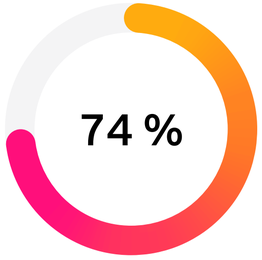
L'échange bidirectionnel des données constitue un bon point de départ, mais pour un véritable travail d'équipe, il faut que les équipes d'observabilité et de sécurité soient ensemble sur le front dès le début, sans attendre que les problèmes émergent lentement à travers des workflows cloisonnés.

Mark Maslach, Vice-président des ventes techniques mondiales, Splunk Observability chez Cisco, explique : « Lorsque les logiciels d'observabilité et de sécurité sont cloisonnés, il n'existe pas de lien profond entre les outils et la collaboration devient un exercice manuel pénible. C'est souvent le signe de problèmes au sein de l'organisation. »

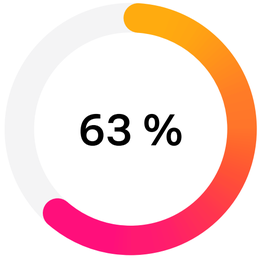
Les formes de collaboration plus sophistiquées sont le signe d'une véritable maturité organisationnelle : il faut en effet que les équipes aient activement éliminé les silos et se coordonnent étroitement. Par exemple, 62 % des participants déclarent que leur équipe dépanne et résout les problèmes en tandem avec l'équipe de sécurité, et ils sont 63 % à pouvoir distinguer rapidement les problèmes de performances des applications et de l'infrastructure dont l'origine est liée à la sécurité.

Craig Robin, Directeur technique de terrain chez Splunk, affirme : « Il faudra sans doute toujours maintenir une certaine séparation entre les équipes de sécurité, d'ingénierie et ITOps, tout simplement parce que leurs compétences et leurs motivations sont trop différentes. Mais nous voyons bien que les pratiques d'observabilité matures permettent de trier les incidents et de les envoyer à l'équipe spécialisée appropriée le plus rapidement possible, en lui fournissant toutes les données utiles pour les résoudre efficacement. C'est la meilleure manière de gérer les problèmes qui ont un impact métier. »

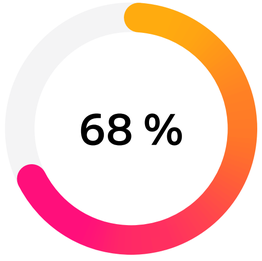
Les meilleures approches de collaboration des équipes d'observabilité et de sécurité



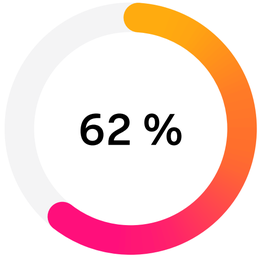
Partager et réutiliser les données



Possibilité de faire rapidement la distinction entre les incidents liés aux applications ou l'infrastructure et ceux qui ont trait à la sécurité



Consulter et utiliser le même ensemble d'outils



Dépanner et résoudre les problèmes ensemble

Le manque de compétences et les silos nuisent à la collaboration

La collaboration des équipes d'observabilité et de sécurité lors de la réponse aux incidents est certainement le signe d'une pratique d'observabilité mature, mais elle est loin d'être généralisée. Le principal obstacle à l'amélioration de la collaboration dans le domaine de la sécurité est la résistance au changement, comme l'évoquent 59 % des participants.

Les organisations de sécurité et d'observabilité adoptent des approches fondamentalement différentes face aux incidents. Alors que les équipes de sécurité prouvent leur valeur en fermant des tickets (« Nous avons trouvé 2 000 possibilités d'attaque et les avons atténuées ! »), les équipes ITOps et d'ingénierie visent à maintenir le nombre d'incidents au plus bas niveau. Leurs visions de ce qu'est ou non un incident peuvent même être très contradictoires. La résistance peut également se manifester par des conflits de responsabilité : on cherche des coupables et on se dispute pour savoir qui héritera du ticket.

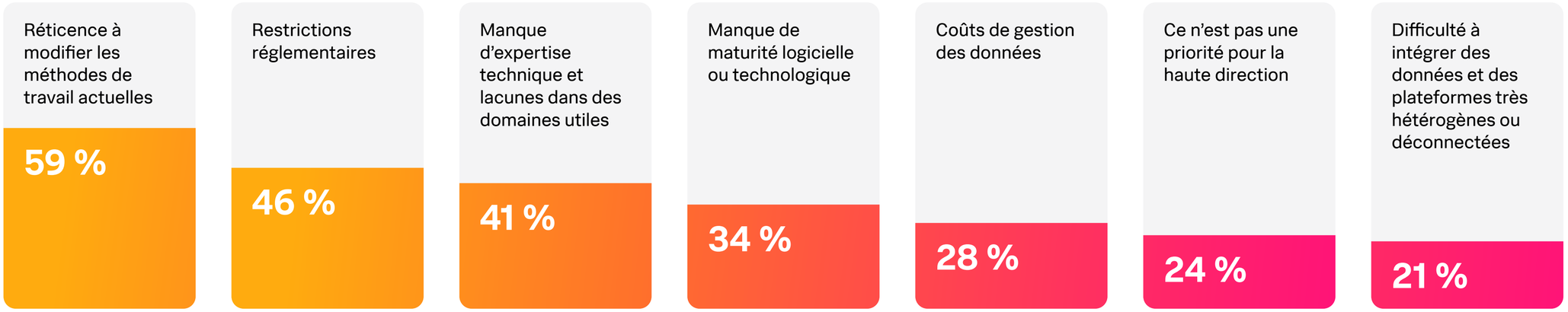
Le manque de connaissances est un autre obstacle majeur à la collaboration efficace des équipes de sécurité et d'observabilité : 41 % des équipes ITOps et d'ingénierie mentionnent le manque d'expertise technique et de compétences pertinentes comme un défi.

M. Leffler explique : « Les ingénieurs SRE et NOC ont très peu d'informations sur les problèmes de sécurité car ils n'ont jamais été formés sur ce sujet. Pendant ce temps, les équipes de sécurité se soucient peu des performances des applications tant que personne ne les pirate. »

Un tiers (34 %) des personnes interrogées désignent leurs logiciels ou leur manque de maturité technologique comme un obstacle à leurs efforts de collaboration. De nombreuses organisations utilisent encore des plateformes de sécurité et d'observabilité cloisonnées qui empêchent de corréler les signaux des équipes et des systèmes en temps réel. Par exemple, lorsqu'une plateforme de gestion des incidents et des événements de sécurité (SIEM) déclenche une alerte DDoS concernant une application client, certains logiciels d'observabilité affichent uniquement les problèmes de performances qui découlent de l'attaque : augmentation de la latence, des taux d'erreur ou de l'utilisation des ressources. Cette représentation conduit les équipes ITOps et d'ingénierie à envisager l'incident comme un problème de performances.

« Les organisations les plus avancées ont compris que les données d'observabilité sont aussi des données de sécurité, et elles adoptent une approche unifiée qui permet à la technologie de faire l'essentiel du travail d'identification des impacts de sécurité », explique M. Robin.

Les obstacles à la collaboration les plus importants



Les participants pouvaient sélectionner toutes les réponses valables.

Chapitre 4

L’observabilité à l’ère de l’IA

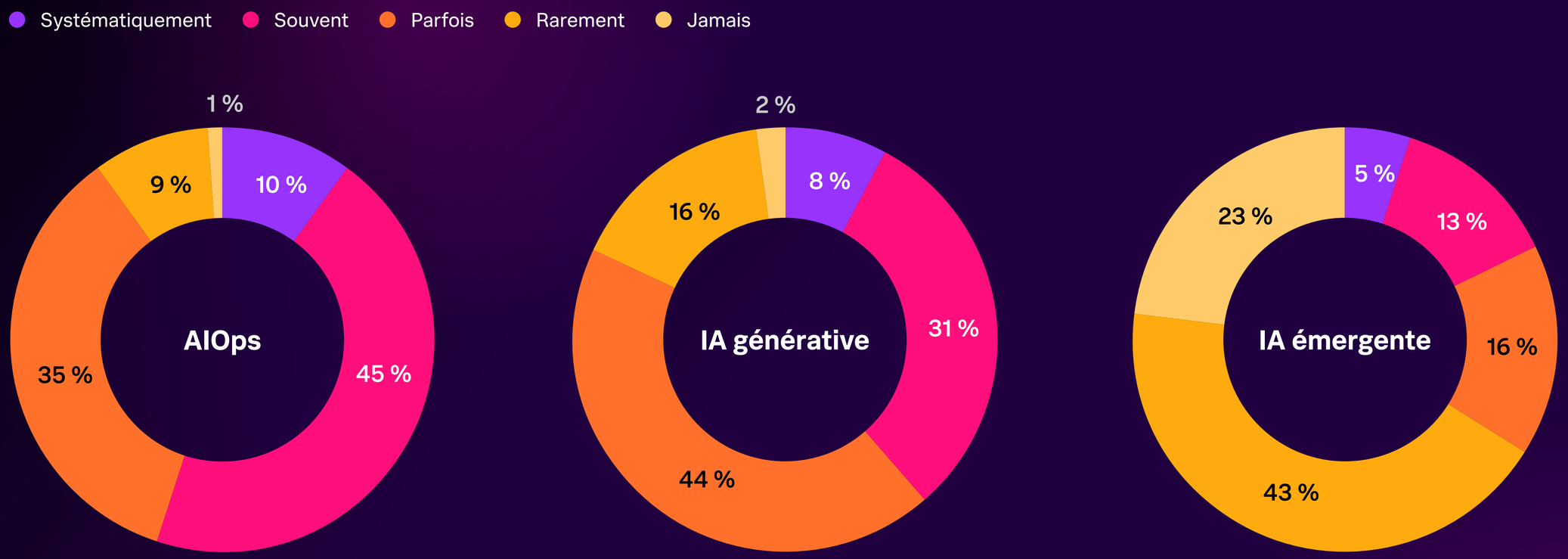
L’IA a piqué la curiosité des sceptiques les plus endurcis : les professionnels de l’observabilité prennent conscience de son immense intérêt lorsqu’elle est correctement mise en œuvre (le mot-clé étant *correctement*).

La majorité des équipes d’ingénierie et ITOps ont adopté l’IA : 76 % des personnes interrogées l’utilisent régulièrement dans leurs workflows quotidiens. En revanche, les taux d’adoption varient selon la nature de l’IA. L’AIOps, composant essentiel de l’ITOps depuis près de dix ans, est *souvent* ou *systématiquement* utilisée chez 54 % des participants. Quant à l’IA générative, 39 % l’utilisent *souvent* ou *systématiquement*.

En revanche, ils ne sont que 18 % à utiliser *souvent* ou *systématiquement* des technologies d’IA émergentes et prometteuses comme l’IA agentique. Capables d’apprendre, de raisonner, de s’adapter et d’agir de manière autonome, les agents peuvent réaliser des workflows complets comme le codage et le débogage de logiciels. Tout porte à croire, cependant, que l’adoption de l’IA agentique augmentera fortement au cours des prochaines années.

Les pratiques d’observabilité s’appuient sur l’IA

À quelle fréquence les participants utilisent-ils les différents types d’IA ?



L’IA encourage l’innovation et accélère la résolution des problèmes

Les équipes d’ingénierie et ITOps savent bien que l’IA peut accroître la productivité ; 78 % d’entre elles affirment que l’IA leur a permis de consacrer plus de temps à l’innovation qu’à la maintenance, et donc à produire de meilleurs résultats métiers. Grâce à ces gains de temps, les équipes peuvent se concentrer sur des initiatives à fort impact, comme la mise en œuvre de microservices et de technologies serverless ou le développement de nouveaux produits numériques.

Toutes ces promesses devraient parler aux équipes qui ont du mal à équilibrer leurs priorités : 42 % d’entre elles admettent passer plus de temps qu’elles ne le devraient aux activités de maintenance des applications telles que l’édition de code et l’activation d’indicateurs de fonctionnalités. Près de la moitié (45 %) des personnes interrogées déclarent passer moins de temps qu’elles ne devraient à créer de nouveaux logiciels. Pour 12 % d’entre elles, c’est même *considérablement* moins, ce qui fait de cette tâche la plus négligée parmi toutes celles que nous avons abordées.

Capable de répondre à des questions sur les applications et l’infrastructure, un assistant d’IA générative peut s’avérer très utile pour les membres d’équipe moins expérimentés qui risquent autrement de perdre beaucoup de temps à effectuer des tâches de maintenance. Un ingénieur junior peut ainsi demander à un assistant d’IA générative d’analyser un identifiant de trace lors d’une interruption de service pour obtenir des recommandations de correction, voire un rapport d’incident complet.

Cory Minton, Directeur technique de terrain chez Splunk, affirme : « Donnez à vos analystes juniors des outils capables d’analyser les logs, les métriques et les traces avec précision, et laissez l’IA générative faire le gros du travail d’identification du contexte et des modèles. De cette façon, vos ingénieurs d’élite – vos ninjas – pourront se concentrer sur les tâches stratégiques, comme le développement de systèmes d’automatisation et d’ingénierie évolutifs. »

Les personnes interrogées s’attendent à ce que l’IA apporte une valeur ajoutée dans les domaines les plus critiques pour l’entreprise. Questionnées sur les capacités d’observabilité les plus utiles, elles citent majoritairement la détection des vulnérabilités et des menaces de sécurité des applications : pour 58 % d’entre elles, l’IA va exercer un impact positif dans ce domaine.

De même, pour 69 % des personnes interrogées, la capacité de dépannage et d’analyse des causes profondes de l’observabilité est *modérément* à *très* importante pour l’entreprise. Elles s’attendent d’ailleurs à ce que ce soit dans ce domaine que l’IA soit la plus utile : 60 % pensent en effet qu’elle aura un impact positif. L’AIOps a notamment le pouvoir d’accélérer l’analyse des causes profondes en découvrant les signaux faibles qui contribuent à la dégradation des services et en identifiant les problèmes sous-jacents au niveau du code.

La croissance rapide de l’IA générative a ouvert la voie à l’IA agentique qui assume aujourd’hui des rôles encore plus complexes et autonomes en matière d’observabilité. Nous nous dirigeons vers un avenir où les agents d’IA pourront gérer l’intégralité des workflows de réponse aux incidents.

– Julie Gibbs, Vice-présidente du marketing produit Splunk IA et intégrations, Splunk

78 %

des personnes interrogées consacrent plus de temps à l’innovation qu’à la maintenance avec l’aide de l’IA

La qualité des données a un impact sur la préparation à l'IA

Pour tirer profit des avantages de l'IA, il ne suffit pas d'installer un système et de le laisser travailler. Pour réussir l'adoption de l'IA, ou même simplement pour être en mesure de l'utiliser, il faut l'intégrer dans les opérations quotidiennes de l'équipe, comprendre ses résultats, mesurer sa valeur, en faire un usage durable et évaluer ses bienfaits en fin de compte.

La qualité et la quantité des données sont tout aussi essentielles pour réussir avec l'IA. La médiocrité des données constitue le principal obstacle à la préparation à l'IA : c'est l'un des plus grands défis pour 48 % des personnes interrogées.

M. Leffler explique : « Il arrive souvent que personne ne soit explicitement désigné comme responsable du maintien de la qualité des données. En général, une équipe de développement ou de SRE se contentera de collecter les principaux signaux – latence, erreurs, saturation et trafic – et s'imaginera que la qualité des données suffit pour les activités de dépannage. »

Mais qui est responsable ? Ceux qui se soucient profondément de l'observabilité peuvent mettre sur pied un centre d'excellence pratique pour définir et appliquer des normes de qualité des données dans toute l'organisation. Il faudra collaborer avec les principales parties prenantes, équipe de conformité en tête, pour garantir que les données répondent aux besoins de chacun.

Principaux obstacles à la préparation à l'IA

1. Manque de qualité des données
2. Coût de l'infrastructure de l'IA
3. Manque d'expertise ou de compréhension au sein des équipes
4. Réticence à modifier les méthodes de travail actuelles
5. Faible visibilité sur les données

Les équipes d’observabilité s’adaptent à la nouvelle dynamique de l’IA

L’IA est une arme à double tranchant pour les professionnels de l’observabilité : elle permet d’en faire plus, mais il faut aussi passer plus de temps à superviser les workloads qu’elle produit. Près de la moitié (47 %) des personnes interrogées affirment que la supervision des workloads de l’IA a rendu leur travail plus difficile.

Il est pourtant crucial de comprendre et de capturer les données des LLM, d’autant plus que l’impact de l’IA se fait sentir dans l’ensemble de l’entreprise.

Les charges d’IA sont hautement dynamiques et changent souvent lorsque les modèles sont réentraînés ou mis à jour. De plus, des modifications subtiles dans les données (un phénomène qu’on appelle aussi « dérive ») peuvent dégrader les performances du modèle sans déclencher d’alertes traditionnelles.

Rappelons également que l’IA n’est pas un workload classique ; elle implique une infrastructure spécialisée qui se situe souvent en dehors des piles d’applications typiques. Les équipes doivent saisir les subtilités associées à une workload d’IA. Par exemple, les GPU sont-ils utilisés au maximum ? À quelle vitesse les tokens sont-ils générés et utilisés ? Quel est le temps de réponse du modèle ? Le comportement du modèle a-t-il soudainement dérivé après un réentraînement ? Et surtout, combien est-ce que tout cela va coûter ?

Une équipe ITOps ou d’ingénierie ne saura pas nécessairement répondre à toutes ces questions. Le manque d’expertise ou de compréhension reste un obstacle majeur. Pour 40 % des personnes interrogées, c’est même un défi majeur dans les efforts de préparation à l’IA.

Annette Sheppard, Directrice du marketing produit pour l’observabilité chez Splunk, explique : « Il est important qu’une seule équipe dispose de tout le contexte nécessaire pour superviser les performances de l’ensemble de l’application, IA incluse. Autrement dit, les équipes d’observabilité doivent perfectionner les compétences de leurs professionnels et les former aux nuances qui nécessitent leur attention. »

Si vos systèmes d’IA ne sont pas observables, ils représentent déjà un risque. Quand un modèle dérive, les choses peuvent aller très vite sans pour autant que cela se voie. L’observabilité est un impératif pour l’IA, plus encore que pour la plupart de vos systèmes numériques, parce qu’elle évolue de manière inattendue.

– Cory Minton, Directeur technique de terrain, Splunk

47 %

des personnes interrogées affirment que la supervision des workloads de l’IA a rendu leur travail plus difficile

OpenTelemetry évolue : la norme devient stratégie

Avec son format cohérent et intuitif, OpenTelemetry s'est imposé comme la référence du secteur pour la collecte de données d'observabilité au cours des dernières années. En effet, tous les fournisseurs d'observabilité ou presque (ils sont plus de 40) prennent en charge OpenTelemetry, et de nombreuses autres applications offrant une prise en charge intégrée sont publiées aujourd'hui.

Les avantages techniques d'OpenTelemetry sont bien connus. Notre rapport *État de l'observabilité en 2024 : construire sa réussite* a révélé qu'OpenTelemetry permet aux organisations d'accéder à un vaste écosystème technologique, de répondre aux exigences liées à la résidence des données et d'adopter plus facilement des cadres cloud modernes. Mais cette année, ses avantages dépassent largement le cadre de la pratique de l'observabilité. La grande majorité de ceux qui utilisent OpenTelemetry au moins *parfois* affirme que ce standard influe positivement sur la croissance des revenus (72 %), les marges d'exploitation (71 %) et la perception de la marque (71 %).

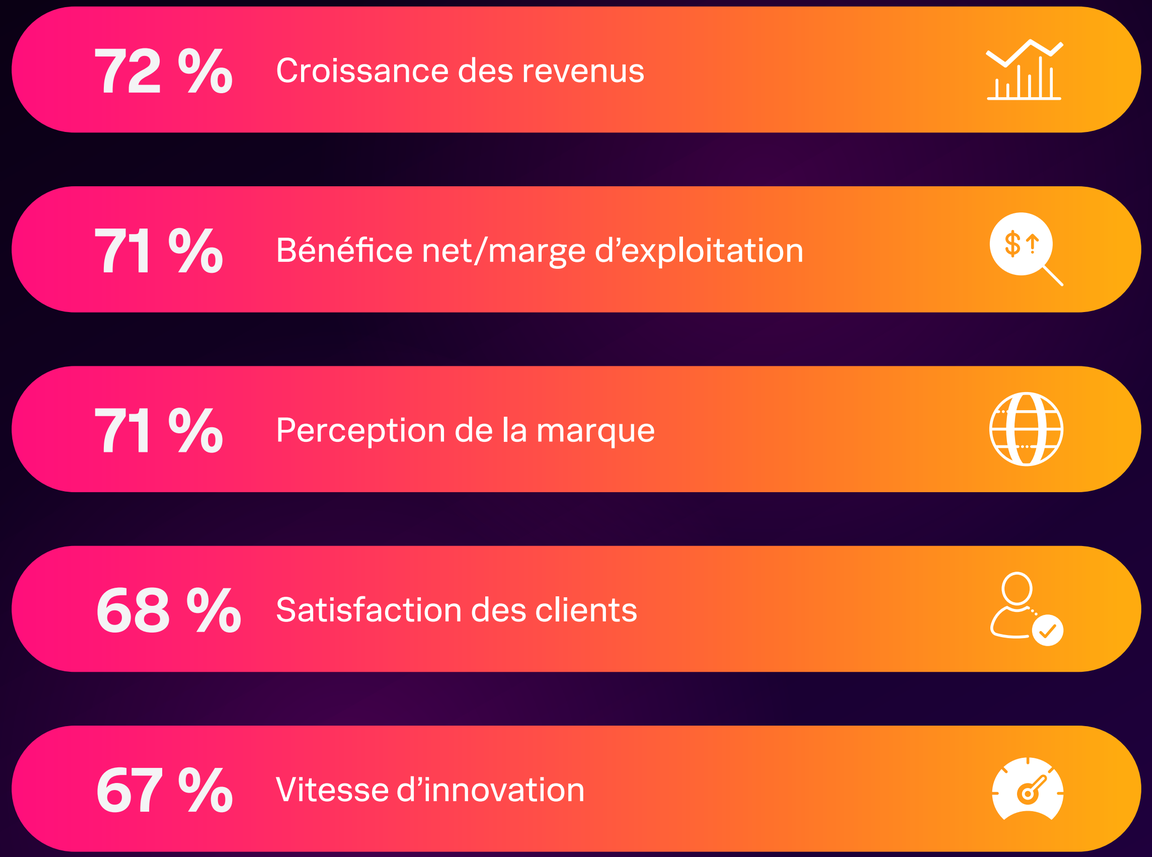
Les utilisateurs expérimentés d'OpenTelemetry obtiennent des informations plus précises

Quelle est exactement l'envergure de l'impact d'OpenTelemetry ? OpenTelemetry enregistre sans effort les traces, les métriques, les logs et les profils distribués, puis les enrichit de métadonnées standardisées. Ce processus simplifie l'unification des données dont les environnements, langues et plateformes d'origine varient. OpenTelemetry facilite également la capture de données personnalisées supplémentaires qui traduisent des aspects stratégiques de vos activités, ainsi que la modification des données qui lui sont envoyées. Lorsqu'elles sont en possession de toutes ces données de télémétrie enrichies, les équipes parviennent à résoudre des problèmes uniques qui passeraient autrement inaperçus ou, pire encore, resteraient indétectables jusqu'à ce que les clients s'en plaignent.

Imaginons qu'une organisation gère un site avec un volume de trafic très élevé, mais qu'une partie des visiteurs, parce qu'ils utilisent un navigateur spécifique, rencontrent des erreurs de connexion. Sans certaines métadonnées, l'organisation n'aurait aucune idée du problème.

Les avantages d'OpenTelemetry dépassent le cadre de la pratique de l'observabilité

Personnes interrogées faisant part d'un impact positif sur les résultats de l'entreprise



Morgan McLean, Directeur principal de la gestion des produits chez Splunk, explique : « Lorsque les équipes adoptent OpenTelemetry, cela signifie généralement qu'elles ont atteint un tournant. Elles ne se contentent plus de collecter des signaux : elles investissent pour comprendre le fonctionnement réel de leurs systèmes. Ce changement de mentalité est précisément un signe de maturité dans l'ingénierie moderne. »

Plus les équipes utilisent OpenTelemetry, plus elles en tirent de bénéfices ; les utilisateurs fréquents (les participants qui disent utiliser OpenTelemetry *souvent* ou *systématiquement*) gèrent en effet les incidents avec davantage de calme et de méthode. Ils sont même 47 % à affirmer qu'ils ne paniquent *jamais* lors d'incidents affectant les clients, contre seulement 32 % de ceux qui utilisent *rarement* ou *jamais* OpenTelemetry.

Ces utilisateurs expérimentés sont trois fois plus nombreux que les retardataires à dire que leur pratique d'observabilité exerce un impact *significatif* sur la productivité des employés. Ils disent également deux fois plus souvent que leur pratique d'observabilité a une influence *significative* sur l'expérience client.

Les utilisateurs d'OpenTelemetry ont également tendance à être plus avant-gardistes vis-à-vis d'autres technologies, sans doute parce qu'ils ont développé une culture qui encourage la curiosité intellectuelle et l'utilisation d'outils modernes. Les utilisateurs expérimentés d'OpenTelemetry sont beaucoup plus nombreux à utiliser l'IA générative, le ChatOps, l'observabilité en tant que code et la correction automatique. Pour prendre un exemple, la majorité (57 %) des utilisateurs fréquents d'OpenTelemetry *utilisent souvent* ou *systématiquement* l'observabilité en tant que code, contre seulement 10 % de ceux qui tardent à adopter pleinement le framework.

Lorsque les équipes utilisent OpenTelemetry comme base de normalisation, elles collectent des données plus riches qui forment le socle indispensable à de meilleurs résultats d'IA générative. Avec un pipeline de télémétrie unifié, associé à des balises métiers comme l'ID client ou le groupe de campagnes marketing, les modèles d'IA reçoivent des données plus riches et plus cohérentes. Ils peuvent alors fournir des informations mieux contextualisées et de meilleures recommandations, et ils ont moins d'angles morts.

Chez les utilisateurs expérimentés, OpenTelemetry améliore plus encore les résultats de l'entreprise

3 fois

plus d'impact sur la productivité des employés

2 fois

plus d'impact sur l'expérience client

OpenTelemetry est le fondement incontournable de toute solution d'observabilité. Il s'agit de la norme la plus performante, la plus extensible et la plus évolutive pour la télémétrie.

– Morgan McLean, Directeur senior, Gestion des produits chez Splunk et cofondateur d'OpenTelemetry

Chapitre 6

Les bonnes pratiques d’observabilité améliorent les revenus et le ROI

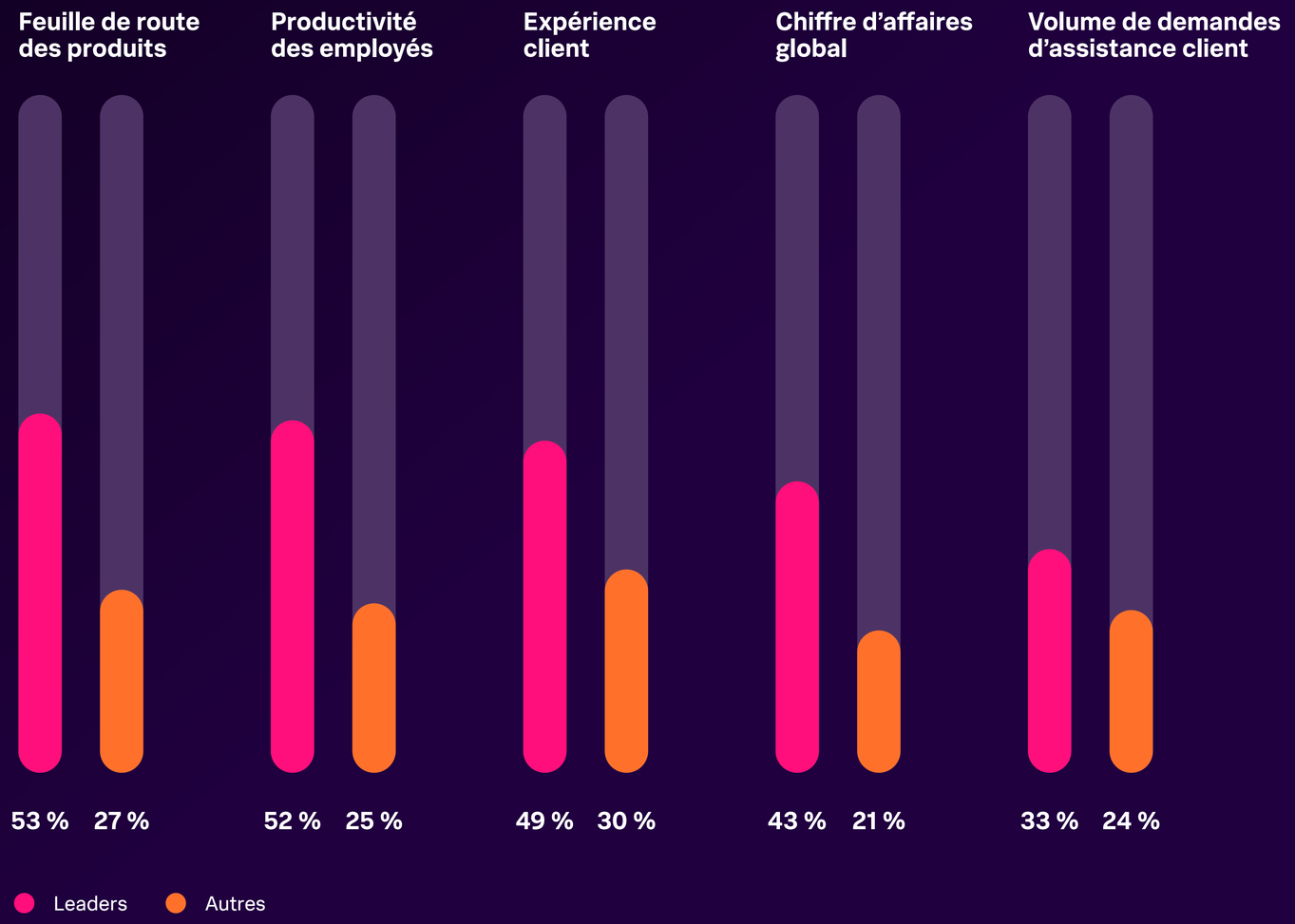
L’observabilité ne se contente plus de maintenir les systèmes en état de marche. Elle joue un rôle décisif dans l’avenir de l’entreprise. Les professionnels de l’ITOps et de l’ingénierie influencent désormais des métriques aux enjeux élevés, comme les revenus et l’expérience client, et les équipes qui exercent le plus grand impact deviennent des moteurs de valeur qui accélèrent les performances de l’ensemble de l’organisation.

Notre recherche a mis en évidence un groupe unique de participants qui se démarquent des autres et obtiennent systématiquement de meilleurs résultats que leurs homologues. Ces leaders de l'observabilité étendent leur influence à l'ensemble de l'organisation. Ils sont presque deux fois plus nombreux que les autres participants à affirmer que leur pratique d'observabilité améliore de manière *significative* le chiffre d'affaires global, la productivité des employés et la feuille de route des produits. Leur pratique génère également un retour sur investissement annuel de 125 %, soit 53 points de plus que leurs homologues.

Leur point commun ? Une base technologique de premier ordre : ces participants utilisent *souvent* ou *systématiquement* des technologies de pointe, à savoir OpenTelemetry, le profilage de code et l'observabilité en tant que code.

Les leaders élargissent leur cercle d'influence

Les pratiques d'observabilité ont un impact positif *significatif* sur l'entreprise



Le profilage du code et l'observabilité en tant que code ouvrent la voie à de meilleurs résultats

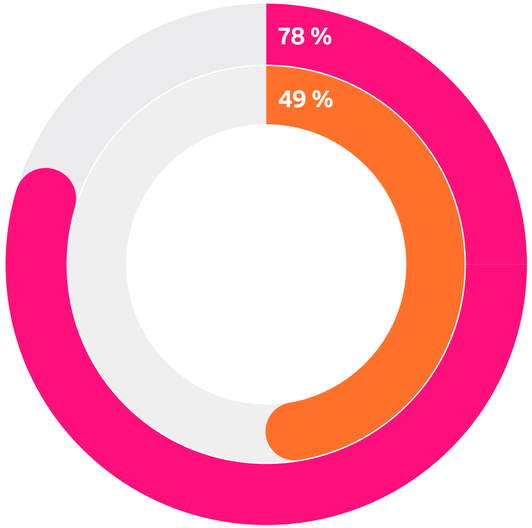
Nous avons longuement parlé d'OpenTelemetry au chapitre 5 ; nous savons que près des trois quarts des personnes interrogées (72 %) affirment que ce framework affecte positivement la croissance des revenus, et sa valeur est indéniable. Intéressons-nous maintenant au profilage du code et à l'observabilité en tant que code.

Le profilage de code donne accès à un niveau de détail supérieur lors du dépannage ; il permet aux équipes d'identifier le fichier de code source problématique (jusqu'à localiser l'appel problématique et la ligne de code associée), et donc de savoir quel ingénieur contacter et comment résoudre le problème. Pour une grande majorité de leaders (78 %), le profilage de code accélère l'identification des causes profondes de manière *significative* ou *transformatrice*.

Chaque minute de retard est un client qui s'en va et des revenus perdus, d'où l'importance cruciale d'obtenir des informations spécifiques. M. Leffler explique : « Lorsqu'il n'est pas possible d'analyser en profondeur les problèmes de performance du code, cela revient à vouloir éteindre un incendie dans le quartier sans savoir dans quelle maison il a pris. Le profilage de code apporte cette limpidité : il localise avec précision la maison, l'étage exact et même la pièce d'où est parti l'incendie. »

L'observabilité en tant que code est une approche DevOps qui traite les configurations d'observabilité comme du code. De ce fait, les équipes peuvent suivre leurs modifications, collaborer et restaurer ces configurations à l'aide de systèmes de contrôle de version. Cette approche permet également de créer des tableaux de bord, des alertes et d'autres composants à l'aide du langage et des méthodes déjà utilisés pour créer les applications elles-mêmes. Dans cette configuration, les équipes d'ingénierie logicielle considèrent l'observabilité comme un élément essentiel du processus de développement, et non comme un ajout après coup. Résultat : une pratique cohérente, normalisée et évolutive.

M. Lin affirme : « L'observabilité en tant que code est l'un des signes les plus clairs de la maturité d'une pratique d'observabilité. Elle est la preuve que l'observabilité est intégrée au processus de développement ; la collecte et l'interprétation de la télémétrie sont traitées avec la même discipline que le reste du code, et l'observabilité devient versionnée, automatisée et cohérente. »



Les leaders ont un raccourci vers les causes profondes grâce au profilage de code

L'accélération est *significative* ou *transformatrice*

Leaders Autres

Lorsqu'il n'est pas possible d'analyser en profondeur les problèmes de performance du code, cela revient à vouloir éteindre un incendie dans le quartier sans savoir dans quelle maison il a pris. Le profilage de code apporte cette limpidité : il localise avec précision la maison, l'étage exact et même la pièce d'où est parti l'incendie.

– Greg Leffler, Directeur de l'évangélisation des développeurs, Splunk

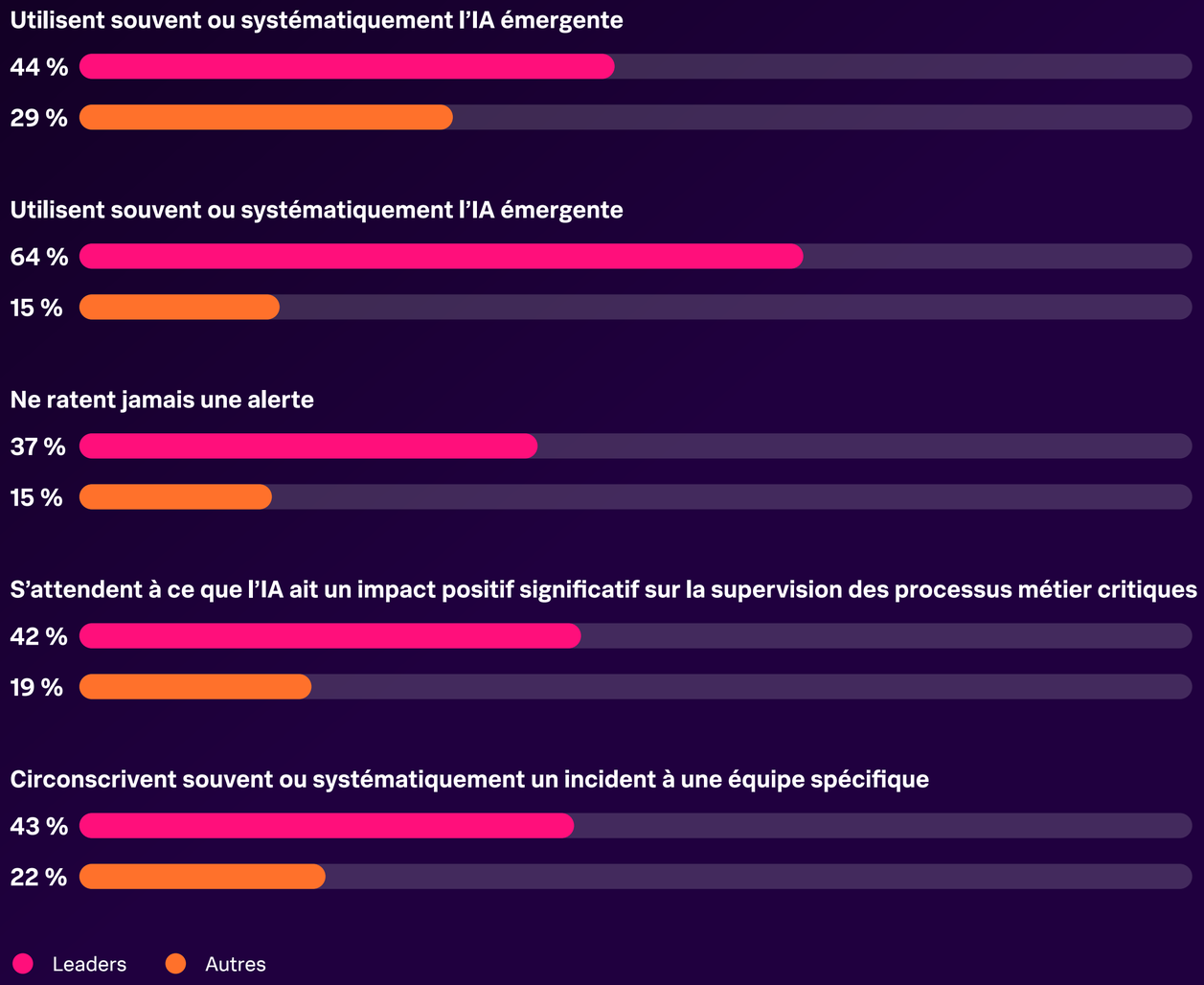
Encourager une culture qui fait avancer l'entreprise

Toute cette technologie – profilage du code, observabilité en tant que code et OpenTelemetry – est indubitablement très utile, mais soyons honnêtes : son adoption est un *symptôme* de maturité, et non sa cause. Ce sont avant tout des personnes qui décident d'investir dans des technologies d'avenir. Et cette décision met en évidence des qualités progressistes : un goût pour l'innovation, un engagement pour l'excellence des expériences numériques, un effort concerté d'adaptation au paysage de l'observabilité et la ténacité indispensable pour acquérir et actualiser ses compétences.

M. Robin déclare : « Pour moi, c'est la preuve que des personnes se soucient profondément de l'art de l'observabilité dans l'entreprise et s'efforcent de mettre en place la bonne culture. Ces équipes sont prêtes à fournir les efforts nécessaires pour intégrer l'observabilité à l'ADN culturel de l'organisation en adoptant de nouvelles technologies, en faisant des recherches et en se formant, en encourageant les équipes internes et en justifiant l'investissement consenti en temps et en argent. »

En dehors des investissements dans les outils, voyons de plus près comment ces moteurs de valeur améliorent concrètement les résultats.

Avec leurs pratiques d'observabilité de pointe, les leaders surpassent leurs homologues.



Un alignement étroit sur la sécurité

Les leaders ont tendance à collaborer plus efficacement avec les équipes de sécurité de leur organisation sur les aspects décisifs. Ils partagent et réutilisent davantage de données que leurs homologues (59 % contre 45 %), mais ce n'est que le point de départ de la collaboration. Près de la moitié d'entre eux (44 %) sont *tout à fait* d'accord pour dire que leurs équipes ITOps et d'ingénierie dépannent et résolvent les problèmes en coordination avec les équipes de sécurité, contre 29 % des autres participants.

Cette collaboration est probablement facilitée par les outils qu'ils ont mis en place. OpenTelemetry, par exemple, offre aux équipes d'observabilité et de sécurité un langage commun ainsi que des signaux et un contexte partagés qui fluidifient le travail d'équipe. Seuls 16 % des leaders estiment que les logiciels immatures constituent un obstacle à la collaboration, contre 35 % des autres personnes interrogées. Seuls 7 % des leaders affirment rencontrer des difficultés à intégrer des plateformes informatiques, d'ingénierie et de sécurité dispersées ou déconnectées – c'est trois fois moins que leurs pairs.

Cette collaboration plus étroite permet aux données de télémétrie des leaders d'avoir davantage de valeur au sein des équipes. Toutes les catégories de données d'observabilité que nous avons abordées (métriques, événements, traces et logs) jouent un rôle plus important pour leurs équipes de sécurité que chez les autres participants. Pour prendre un exemple précis, les dirigeants sont 2,6 fois plus nombreux à dire que les traces influencent de manière *significative* les décisions de sécurité.

C'est la preuve tangible que les leaders brisent les frontières qui séparent les équipes. Le fait que les équipes de sécurité utilisent activement les traces n'est pas seulement le signe que les données sont partagées : cela implique qu'elles sont comprises et adoptées par des équipes au-delà de l'ingénierie.

Libérez le potentiel de l'IA

Peut-on avoir une pratique d'observabilité de pointe sans IA ? Probablement pas. Les leaders surfent sur la vague des innovations IA tandis que leurs pairs pagaient péniblement derrière eux. Ils sont 64 % à utiliser *systématiquement* ou *souvent* des technologies d'IA émergentes comme l'IA agentique, contre seulement 15 % de leurs homologues. Ils affichent également des taux supérieurs d'adoption de l'IA générative et de l'AIOps.

Les leaders rencontrent moins d'obstacles sur la voie de l'innovation en matière d'IA. La qualité des données ne représente pas pour eux un obstacle majeur à la préparation à l'IA. Environ un tiers (34 %) des personnes interrogées estiment que la médiocrité des données constitue un défi, contre près de la moitié (49 %) des autres. Les manques de connaissances sont également moins criants : le manque d'expertise est considéré comme un frein à la préparation à l'IA chez 25 % des leaders, mais c'est le cas chez 41 % de leurs homologues.

Les leaders pensent également que l'IA va améliorer les opérations essentielles. Pour 42 % d'entre eux, l'IA exercera un impact positif *significatif* sur la supervision des processus métiers critiques, contre 19 % des autres personnes interrogées.

Gérez les alertes et les incidents avec davantage de précision

Les alertes sont une source d'angoisse pour la plupart des organisations, mais c'est moins le cas de leaders. Plus de la moitié (52 %) des autres participants affirment que le volume de fausses alertes a un impact négatif sur le moral de leur équipe, alors que seulement 35 % des leaders s'en plaignent.

Cela est probablement dû au fait que les leaders ont généralement de meilleurs processus pour la gestion des alertes et la réponse aux incidents. Ils sont en effet 37 % à affirmer qu'ils ne ratent *jamais* une alerte, contre seulement 15 % des autres participants. Ils sont 2,3 fois plus nombreux que leurs pairs à dire qu'ils élaborent *systématiquement* un plan de réponse détaillé lorsqu'un incident affecte les clients. Ils sont aussi plus susceptibles d'associer *souvent* ou *systématiquement* un incident à une équipe spécifique et de compter sur elle pour sa résolution (43 % contre 22 % des autres participant), au lieu d'impliquer inutilement plusieurs équipes et d'épuiser le personnel.

Comment devenir un moteur de valeur

Les pratiques d'observabilité de pointe sont des moteurs qui augmentent les revenus, améliorent les expériences client et font progresser une multitude d'autres objectifs essentiels. La valeur de leurs données se répercute dans toute l'entreprise, bien au-delà du cadre de l'observabilité.

En gardant à l'esprit les résultats de l'étude, voici quelques conseils pour bien utiliser votre pratique d'observabilité afin de générer de meilleurs résultats.

1 Limitez les cellules de crise et les approches réactives

La panique est rarement la meilleure façon de réagir à un incident qui touche les clients. Pourtant, 21 % des personnes interrogées disent que cela se produit *parfois*, *souvent* ou *systématiquement*. Et 20 % disent créer *souvent* ou *systématiquement* une cellule de crise impliquant des membres de nombreuses équipes jusqu'à ce que le problème soit résolu, alors que cette pratique freine la productivité et met les ressources de l'entreprise sous tension. Évitez ces situations en vous inspirant des leaders :

- **Circonscrivez l'incident à une équipe spécifique.** Lorsque l'on peut déterminer rapidement si un problème est lié à la sécurité ou à l'observabilité, on évite que plusieurs équipes ne s'engagent dans des voies différentes. Idéalement, les équipes ITOps, d'ingénierie et de sécurité doivent résoudre les problèmes en parallèle et partager le contexte et les informations nécessaires à l'identification de la cause première, puis transmettre l'incident à l'équipe appropriée.
- **Faites des évaluations post-incident une routine.** Non seulement les évaluations post-incident aident les équipes à tirer les leçons des victoires et des erreurs du passé, mais elles remontent le moral des équipes en leur rappelant que l'histoire ne se répétera pas. Intégrez des évaluations post-incident au processus de réponse pour qu'elles deviennent la norme et traitez-les comme des documents dynamiques, capables de s'adapter aux changements de politique, d'outils ou de plan à venir.

2 Maîtrisez les alertes

Les fausses alertes sont l'une des principales sources de stress des équipes ITOps et d'ingénierie. Et 54 % des personnes interrogées affirment que la qualité des alertes est le plus grand facteur d'impact sur le ROI de l'observabilité. La maîtrise des alertes sera donc nécessairement rentable.

- **Passez au niveau supérieur de finesse avec les seuils adaptatifs.** Ajustez les seuils en fonction de la nature critique du système ou du service que vous supervisez en filtrant les faux positifs bruyants et en veillant à ce que chaque alerte soit valide. Les seuils adaptatifs permettent de passer au niveau supérieur en ajustant dynamiquement les lignes de base en fonction des données historiques.
- **Ne supprimez les alertes que pour de *très* bonnes raisons.** Utilisez la suppression des alertes avec la plus grande parcimonie. Idéalement, laissez votre système de déploiement continu (CD) s'en charger à votre place. Réfléchissez bien avant de supprimer des alertes : vous devez avoir une raison spécifique de le faire, dans le cadre d'un déploiement à venir ou d'une maintenance planifiée, par exemple, et non parce que vous faites face à un pic de trafic.

3 Fixez des normes de qualité des données pour profiter de tous les avantages de l'IA

La grande majorité des personnes interrogées (78 %) affirme que l'IA permet de consacrer plus de temps à l'innovation qu'à la maintenance ; pourtant, elles sont près de la moitié (48 %) à affirmer que la mauvaise qualité des données les empêche d'être prêtes pour l'IA.

- **Clarifiez les responsabilités concernant la qualité des données.** Dans de nombreuses organisations, il est difficile de savoir qui est responsable de la qualité de la télémétrie des applications. Souvent, la responsabilité revient par défaut à l'ingénierie de plateforme, quelle que soit la capacité ou l'expertise de l'équipe. Identifiez un groupe de personnes passionnées par l'art de l'observabilité et donnez-leur les moyens de développer et d'expérimenter un ensemble de normes de qualité des données applicables à toute l'organisation, en impliquant des parties prenantes comme l'équipe de conformité, pour répondre aux besoins de chacun. En articulant cette démarche avec les possibilités sophistiquées offertes par des données de meilleure qualité, vous motiverez certainement les équipes à s'engager dans cette pratique.
- **Injectez du contexte métier et des balises.** Une excellente manière d'enrichir les informations que l'IA (et vos ingénieurs) peuvent extraire consiste à étiqueter les données métiers pertinentes. Vous pouvez ajouter des balises indiquant l'application qui a émis la donnée, le numéro de version, l'environnement ou l'utilisateur connecté. Grâce à ce complément de contexte, les équipes découvriront plus facilement des tendances ayant un impact sur l'entreprise (lorsqu'un problème affecte des clients VIP, par exemple) et pourront hiérarchiser les alertes et les interventions en conséquence.

4 Faites l'expérience des technologies d'avenir

Au sein de la cohorte de participants que nous appelons « moteurs de valeur », ils sont deux fois plus susceptibles que leurs homologues de dire que leur pratique d'observabilité améliore de manière *significative* le chiffre d'affaires global. Qu'ont-ils en commun ? Un engagement envers les technologies d'avenir. Ils utilisent tous *souvent* ou *systématiquement* OpenTelemetry, le profilage de code et l'observabilité en tant que code.

- **Commencez par votre plus gros bottleneck.** Adopter ces trois technologies simultanément représenterait une charge bien trop lourde. Identifiez vos priorités, puis prenez des décisions. Votre pratique d'observabilité n'identifie pas les problèmes assez rapidement ? Le profilage de code peut être un bon point de départ. Votre équipe a du mal à collecter des données dans un format cohérent ? Cette fois, OpenTelemetry sera sans doute la meilleure piste.
- **Organisez régulièrement des séances de partage des connaissances.** Une fois que vos ambassadeurs internes auront eu l'occasion de se former, organisez des forums techniques mensuels ou trimestriels pour qu'ils puissent faire le point sur les outils d'observabilité, les cadres et les avancées avec le reste de l'équipe. Ces sessions sont des espaces privilégiés pour discuter de nouveaux outils et relever les défis de mise en œuvre afin d'encourager une adoption généralisée.

Poursuivez votre parcours pour devenir un leader de l’observabilité

Les Résilients : le podcast des super-héros du numérique

Notre podcast met en scène des super-héros du numérique qui œuvrent au quotidien pour protéger leurs organisations. Qu’ils soient RSSI, DSI ou CTO, leur valeur commune est la résilience d’entreprise.

Écouter le podcast

Les nouvelles règles de la gestion des données : redéfinir leur valeur à l’ère de l’IA

Maîtrisez le volume et la complexité des données et améliorez vos résultats de cybersécurité et d’observabilité en suivant les nouvelles règles de la gestion des données.

Lire le rapport

Éclairages par secteur

Nous avons fait des observations intéressantes dans quatre secteurs d'activité internationaux.

Services financiers

Les organisations de services financiers observent des liens puissants entre leur pratique d'observabilité et leur impact métier. Plus des trois quarts (77 %) des personnes interrogées affirment que l'observabilité a un impact positif sur les revenus, ce qui est bien au-dessus de la moyenne de 65 %, et elles sont presque autant (75 %) à affirmer qu'elle influence la feuille de route des produits. Ces réponses sont en phase avec leurs priorités en matière d'observabilité, puisque 40 % d'entre elles affirment que la supervision des processus métiers critiques est *très* importante pour l'entreprise dans sa globalité.

Dans l'ensemble, le secteur est enthousiaste à l'égard de l'IA : 46 % des participants se disent enthousiasmés par le potentiel de l'IA (contre 36 % au total), mais ils sont également conscients des défis que cela va introduire. Plus de la moitié (54 %) déplorent que la supervision des workloads de l'IA ait rendu leur travail plus difficile, contre 47 % en moyenne.

Du côté des outils, le secteur connaît une forte adoption d'OpenTelemetry : 36 % des personnes interrogées déclarent l'utiliser *souvent* ou *systématiquement* (contre une moyenne de 26 %), et sont plus nombreuses à en récolter les fruits. Les trois quarts (75 %) de ceux qui utilisent OpenTelemetry au moins *parfois* affirment que la technologie a eu un impact positif sur les revenus.

Pourtant, il existe des limites à une véritable collaboration entre les équipes d'observabilité et de sécurité dans les services financiers. Seulement 59 % des participants de ce secteur déclarent que les équipes ITOps, d'ingénierie et de sécurité partagent les mêmes outils (contre 68 % au total), et seulement 61 % disent partager des données entre les équipes (contre 74 %). Dans ce secteur axé sur la conformité, il est logique que 60 % des entreprises considèrent les restrictions réglementaires comme le principal obstacle.

Ces silos expliquent peut-être en partie le haut niveau de stress subi par les équipes des services financiers lors des incidents : 12 % déclarent paniquer *souvent* ou *systématiquement* lors d'événements ayant un impact sur les clients, contre 9 % au total.

Lire le guide d'action pour les services financiers (en anglais).

Fabrication

Dans les organisations manufacturières, les pratiques d'observabilité exercent une forte influence sur l'entreprise, et plus particulièrement sur la productivité des employés ; 86 % des participants déclarent qu'elles améliorent cet aspect, contre 74 % dans l'ensemble des secteurs.

Les équipes ITOps, d'ingénierie et de sécurité travaillent bien plus fréquemment ensemble dans le secteur manufacturier. Pas moins de 97 % des participants de ce secteur déclarent partager et réutiliser des données, et ils sont 81 % à dépanner et résoudre les problèmes avec leurs équipes de sécurité.

L'IA joue un rôle important dans les pratiques d'observabilité des entreprises manufacturières. Près de la moitié (48 %) manifestent de l'enthousiasme pour les avantages qu'apporte l'IA à leur équipe. Les personnes interrogées dans le secteur manufacturier rencontrent généralement moins de difficultés dans la préparation à l'IA : 35 % mentionnent le manque de qualité des données comme un obstacle, contre 48 % dans l'ensemble.

Les fabricants ne se contentent pas d'être optimistes à propos de l'IA, ils l'utilisent également dans ses formes les plus avancées. En effet, près de la moitié (45 %) des personnes interrogées déclarent utiliser *souvent* ou *systématiquement* l'IA émergente, contre seulement 18 % en moyenne. Tous les participants ou presque (94 %) affirment que l'IA leur permet de consacrer plus de temps à l'innovation plutôt qu'à la maintenance des systèmes. Il est possible que ce temps d'innovation soit consacré au développement logiciel, car 39 % seulement des entreprises de fabrication disent consacrer moins de temps qu'elles ne le devraient à la création de nouveaux logiciels, contre 45 % au total.

Les équipes de fabrication s'appuient sur des outils d'observabilité sophistiqués. Elles sont en tête dans l'adoption de nombreuses technologies : elles utilisent *souvent* ou *systématiquement* la correction automatisée (43 %), le profilage de code (41 %) et l'observabilité en tant que code (39 %). Ces investissements, associés à une collaboration étroite et à une maturité dans l'utilisation de l'IA, positionnent le secteur manufacturier comme un leader avant-gardiste en matière d'observabilité.

Lire le guide d'action pour la fabrication (en anglais).

Secteur public

Les agences du secteur public étudient actuellement des approches pour que les pratiques d'observabilité influencent plus directement les résultats de leur mission. Comparés à d'autres secteurs, les participants du secteur public sont nettement moins nombreux à affirmer que leur pratique d'observabilité a une influence positive sur le budget (30 % contre 65 %), la feuille de route des produits (30 % contre 64 %) et la productivité des employés (36 % contre 74 %).

Pour les participants du secteur public, le retour sur investissement est étroitement lié à l'efficacité opérationnelle, et en particulier aux alertes : 69 % mentionnent la qualité des détections d'alertes comme l'un des principaux moteurs de retour sur investissement, un chiffre très supérieur à la moyenne de 54 %. Cette réponse fait écho à leur principale source de stress : le volume élevé de fausses alertes, cité par 61 % des personnes interrogées.

La collaboration reste un domaine essentiel à développer au sein du secteur public. Seulement 46 % des équipes du secteur public déclarent réutiliser et partager les données d'observabilité, et elles ne sont que 35 % à résoudre les problèmes en partenariat avec la sécurité, soit le taux le plus bas de tous les secteurs. À cela s'ajoutent d'importantes lacunes en matière de talents et d'infrastructure : le manque de compétences (62 % des réponses) et la faiblesse de la maturité technologique (60 %) sont cités comme des obstacles majeurs, et ces deux chiffres sont nettement supérieurs à la moyenne.

Les pratiques d'observabilité du secteur public sont encore en phase de développement : il est donc logique qu'elles ne parviennent pas à exploiter les technologies d'avenir. Seuls 35 % des participants déclarent utiliser l'AIOps *souvent* ou *systématiquement* (contre 54 % en moyenne), et ils ne sont que 10 % à utiliser l'IA générative *souvent* ou *systématiquement*, contre 39 % au total. Seuls 8 % d'entre eux utilisent *souvent* ou *systématiquement* l'observabilité en tant que code (contre 29 %), le profilage de code (2 % contre 21 %) et OpenTelemetry (2 % contre 26 %).

Lire le guide d'action pour le secteur public (en anglais).

Communication et médias

Les organisations du secteur de la communication et des médias sont parmi les plus avancées dans leur pratique d'observabilité, et elles en tirent des avantages métiers considérables. Une très grande majorité des personnes interrogées (88 %) affirment que leur pratique d'observabilité exerce un impact positif sur leur chiffre d'affaires global, contre 65 % de moyenne tous secteurs confondus, et 81 % disent que cela influence positivement la feuille de route des produits (contre 64 %).

La rapidité est primordiale pour ce secteur. Les participants du secteur de la communication et des médias sont les plus nombreux à citer la vitesse de résolution des incidents comme l'un des principaux moteurs du retour sur investissement de l'observabilité (68 % contre 49 % au total). Ils accordent également une grande importance à l'IA : pour 51 % d'entre eux, la maturité des capacités d'IA a un impact majeur sur le ROI de l'observabilité.

Les équipes du secteur des communications et des médias sont des leaders dans l'adoption de l'IA : 79 % utilisent *souvent* ou *systématiquement* l'AIOps, et 68 % utilisent *souvent* ou *systématiquement* l'IA générative – deux chiffres bien au-dessus de la moyenne. Les données, en revanche, restent un obstacle : 56 % des membres de ce secteur évoquent la qualité des données comme un obstacle à la préparation à l'IA, et 69 % désignent les défis liés aux données (accessibilité, qualité et fragmentation) comme leur principale source de stress.

Malgré cela, les équipes de ce secteur parviennent à rester concentrées. Elles ne sont que 27 % à se plaindre de passer trop de temps à répondre aux alertes (contre 43 % au total) et 73 % ne manquent que *rarement* voire *jamais* les alertes, bien au-dessus de la moyenne de 60 %. Pourtant, 69 % des participants de ce secteur affirment également passer moins de temps qu'ils ne le souhaiteraient à créer de nouveaux logiciels, ce qui suggère la présence de conflits de priorités persistants.

Les organisations du secteur des communications et des médias sont en tête de l'utilisation d'OpenTelemetry : 67 % d'entre elles l'utilisent *souvent* ou *systématiquement*, soit plus du double de la moyenne tous secteurs confondus. Et cela porte ses fruits : 86 % des personnes interrogées affirment qu'OpenTelemetry contribue à la croissance des revenus et 83 % observent aussi un impact positif sur la satisfaction des clients.

Lire le guide d'action pour le secteur de la communication et des médias (en anglais).

Éclairages par pays

Aperçu de neuf pays du monde.

Australie

L'Australie se distingue comme un leader de l'adoption de l'IA et des pratiques avancées d'observabilité. Des signes forts indiquent que ces investissements produisent déjà des effets métiers mesurables. 45 % des participants australiens se disent enthousiasmés par les avantages que l'IA peut apporter à leurs équipes, un chiffre nettement supérieur à la moyenne mondiale de 36 %. Et cet optimisme se traduit en actes : les organisations australiennes affichent une adoption supérieure dans les trois catégories de technologies d'IA ; 21 % d'entre elles déclarent qu'elles utilisent *souvent* ou *systématiquement* l'IA émergente (comme l'IA agentique), contre seulement 18 % de moyenne mondiale.

Cette approche avant-gardiste porte ses fruits. Une majorité impressionnante de participants australiens (87 %) affirment que l'IA leur a permis de consacrer plus de temps à l'innovation qu'à la maintenance (contre 78 % à l'échelle mondiale). Cela peut expliquer pourquoi seulement 37 % des personnes interrogées déclarent passer moins de temps qu'elles ne le souhaiteraient à créer de nouveaux logiciels. Ce chiffre très inférieur à la moyenne de 45 % indique que les ingénieurs australiens sont plus susceptibles d'avoir le temps nécessaire pour se consacrer à des tâches à forte valeur ajoutée.

Les participants australiens ont des attentes plus élevées quant à l'impact de l'IA sur l'observabilité. Pour 72 % des personnes interrogées, l'IA doit améliorer le dépannage et l'analyse des causes profondes – c'est 12 points de plus que la moyenne mondiale.

Les organisations australiennes sont également plus nombreuses à utiliser OpenTelemetry : 36 % d'entre elles déclarant l'utiliser *souvent* ou *systématiquement* (contre 26 % à l'échelle mondiale). Il est important de noter que cette utilisation se traduit par des résultats métiers tangibles : 79 % de ceux qui utilisent OpenTelemetry au moins *parfois* affirment que cela influence positivement la croissance des revenus, contre 71 % de moyenne dans l'ensemble des régions.

France

En France, les défis liés aux données sont considérables : elles sont à la fois un obstacle à la préparation à l'IA et une source de stress quotidien pour les équipes d'observabilité. 58 % des participants français voient dans les problèmes de données (accessibilité et qualité, notamment) le principal facteur de dégradation du niveau de stress de leur équipe. Il n'est donc pas surprenant que 51 % des personnes interrogées désignent également la mauvaise qualité des données comme le principal frein à l'adoption de l'IA.

Malgré ces difficultés, les organisations françaises montrent des signes de discipline opérationnelle, notamment dans la gestion des alertes et la réponse aux incidents. Seuls 8 % déclarent manquer *souvent* ou *systématiquement* les alertes, un chiffre bien en dessous de la moyenne mondiale de 13 %, ce qui suggère de solides pratiques de gestion des alertes. Cela contribue probablement à réduire le stress lié aux incidents : 4 % seulement des personnes interrogées en France déclarent paniquer *souvent* ou *systématiquement* lors d'incidents affectant les clients, contre une moyenne mondiale de 9 %.

L'importance accordée à la vitesse de résolution des incidents renforce encore cette tendance. En effet, 55 % des participants français considèrent la rapidité de résolution des incidents comme le plus grand facteur de ROI de l'observabilité, faisant de la rapidité et de l'efficacité de la réponse des priorités absolues.

Pour atteindre cette rapidité, les organisations françaises adoptent des outils d'avenir. On remarque notamment que le profilage de code est plus largement adopté en France que dans bien d'autres pays : 30 % des personnes interrogées déclarent l'utiliser *souvent* ou *systématiquement*, contre seulement 21 % à l'échelle mondiale. Et cet investissement a une importance stratégique ; 43 % de ceux qui utilisent au moins *parfois* le profilage de code pensent qu'il améliore l'efficacité de leurs capacités d'IA.

Allemagne

Les pratiques d'observabilité allemandes génèrent de solides résultats métiers : 74 % des participants font part d'un impact positif sur le chiffre d'affaires global, soit un chiffre nettement supérieur à la moyenne mondiale de 65 %. Cette performance reflète non seulement un haut niveau de maturité technique, mais aussi une approche collaborative de la résolution de problèmes qui rassemble les équipes. Les personnes interrogées en Allemagne déclarent à 62 % que leurs équipes d'observabilité et de sécurité résolvent les problèmes ensemble.

Les pratiques de réponse aux incidents révèlent toutefois une image plus nuancée. D'un côté, 74 % des équipes allemandes effectuent *souvent* ou *systématiquement* des évaluations post-incident détaillées, soit un chiffre légèrement supérieur à la moyenne mondiale de 71 %, ce qui reflète un engagement envers la formation et l'amélioration continues. En revanche, 28 % disent créer *souvent* ou *systématiquement* une cellule de crise lorsqu'un incident affecte les clients, un taux nettement supérieur à la moyenne mondiale de 20 %.

Les équipes allemandes sont également de grandes utilisatrices d'OpenTelemetry : 32 % d'entre elles déclarant l'utiliser *souvent* ou *systématiquement*. Les effets sont nets : 79 % de ceux qui utilisent OpenTelemetry au moins *parfois* affirment que cela influence positivement la croissance des revenus, contre 72 % de moyenne dans le monde.

Inde

En Inde, les équipes collaborent étroitement avec leurs collègues de la sécurité : 81 % d'entre elles disent partager et réutiliser des données avec les équipes de sécurité, contre 74 % à l'échelle mondiale. Plus important encore, 74 % déclarent pouvoir tracer avec précision l'origine des problèmes de performances des applications et de l'infrastructure jusqu'aux causes profondes de sécurité, bien au-dessus de la moyenne mondiale de 65 %. C'est le signe que cette collaboration n'est pas seulement superficielle : il existe un véritable alignement technique entre les fonctions.

Cependant, la collaboration n'est pas exempte de difficultés. Plus de la moitié (53 %) des participants indiens mentionnent les restrictions réglementaires comme le principal obstacle à l'amélioration de la collaboration ; c'est même l'obstacle numéro un dans le pays.

Autre point fort : l'adoption de l'IA. 82 % des participants indiens affirment que l'IA leur a permis de consacrer plus de temps à l'innovation qu'à la maintenance, un peu plus que la moyenne mondiale de 78 %. Ils ne sont que 36 % à se plaindre de passer plus de temps qu'ils ne devraient à répondre aux alertes, contre une moyenne mondiale de 43 %, ce qui peut indiquer que l'IA commence à alléger une partie de la charge opérationnelle.

Les alertes jouent un rôle essentiel dans l'élaboration de la stratégie de sécurité : 58 % des participants indiens déclarant qu'elles influencent de manière *significative* les décisions de sécurité, contre seulement 47 % à l'échelle mondiale. Soulignons également que 62 % des personnes interrogées affirment que la qualité des détections d'alertes est l'un des plus importants facteurs de retour sur investissement de l'observabilité. Cependant, les alertes posent encore certains problèmes. Pour 55 % des personnes interrogées, le volume de fausses alertes dégrade le moral de l'équipe.

Japon

Au Japon, les pratiques d'observabilité adoptent une approche prudente, mais optimiste à l'égard des technologies émergentes, et en particulier l'IA. L'adoption de l'IA reste légèrement inférieure à la moyenne mondiale : 48 % des participants disent utiliser *souvent* ou *systématiquement* l'AIOps (contre 54 % à l'échelle mondiale), et ce chiffre tombe à 9 % lorsqu'il s'agit d'IA émergente telle que l'IA agentique (contre 18 % à l'échelle mondiale).

Le principal frein à l'adoption semble être la qualité des données ; 47 % des participants japonais la voient comme le plus grand obstacle à la préparation à l'IA. Autre problème, plus de la moitié (53 %) déplorent que la supervision des workloads de l'IA ait rendu leur travail plus difficile, contre 47 % en moyenne. Malgré ces obstacles, les équipes japonaises voient nettement le potentiel de l'IA. Elles pensent à 62 % que l'IA aura un impact positif sur la supervision des processus métier critiques, un chiffre légèrement supérieur à la moyenne mondiale.

En revanche, les équipes d'observabilité japonaises souffrent de la prolifération des outils. Pour 65 % des personnes interrogées, la multiplication d'outils déconnectés a un impact négatif sur le moral des équipes ; c'est le facteur de nuisance le plus fréquemment cité dans le pays, devant la moyenne mondiale de 59 %. Cette fragmentation peut également contribuer à l'insensibilisation aux alertes et aux lacunes de visibilité : 15 % des participants avouent en effet manquer *souvent* ou *systématiquement* des alertes.

Nouvelle-Zélande

Les pratiques d'observabilité de Nouvelle-Zélande se distinguent par leur impact clair et mesurable sur l'expérience client et l'alignement métier. Une majorité impressionnante de participants (82 %) affirme que les efforts d'observabilité ont un impact positif sur l'expérience client, soit un chiffre nettement supérieur à la moyenne mondiale de 69 %. Ce succès découle probablement du fait que le parcours client est une grande priorité pour les organisations. Près de la moitié (48 %) déclarent que la compréhension des parcours utilisateurs critiques est *très* importante pour leur stratégie métier globale, contre seulement 25 % à l'échelle mondiale.

La collaboration entre les équipes de sécurité et d'observabilité est un autre point fort de la Nouvelle-Zélande. 90 % des personnes interrogées déclarent pouvoir relier avec précision les problèmes de performances des applications ou de l'infrastructure aux causes profondes liées à la sécurité, loin devant la moyenne mondiale de 65 %. Et cette collaboration semble porter ses fruits : 74 % des personnes interrogées affirment que le travail d'équipe interfonctionnel fait baisser le nombre d'incidents affectant les clients, contre 64 % à l'échelle mondiale.

Les participants néo-zélandais misent également sur l'IA. 44 % d'entre eux manifestent leur enthousiasme à l'égard des avantages que l'IA apporte à leurs équipes, et 38 % disent utiliser *souvent* ou *systématiquement* des technologies d'IA émergentes comme l'IA agentique, soit plus du double de la moyenne mondiale. Cependant, le plus grand obstacle à l'expansion de la préparation à l'IA n'est pas la qualité des données, mais les compétences : 50 % citent le manque d'expertise ou de compréhension au sein des équipes comme le principal obstacle, contre 40 % à l'échelle mondiale.

Malgré ces atouts, la fatigue induite par les alertes reste un écueil important. 52 % des personnes interrogées déclarent passer plus de temps qu'elles ne le devraient à répondre aux alertes, ce qui laisse penser que les équipes avancées ne sont pas à l'abri de frictions dans ce domaine.

Singapour

À Singapour, les pratiques d'observabilité évoluent rapidement, et les équipes mettent clairement l'accent sur la rapidité et l'efficacité. 64 % des participants singapouriens affirment que la rapidité de résolution des incidents est l'un des principaux moteurs de retour sur investissement de l'observabilité, contre seulement 49 % à l'échelle mondiale. Cette approche est le signe d'une culture informatique d'un grand dynamisme où la rapidité de la réponse est cruciale.

Les participants singapouriens investissent massivement dans des solutions basées sur l'IA, probablement pour répondre à cet impératif de rapidité. Ils sont 61 %, soit plus que la moyenne, à utiliser *souvent* ou *systématiquement* l'AIOps dans leurs workflows d'observabilité. Ils sont même 85 %, un chiffre record, à utiliser régulièrement l'IA dans leur travail quotidien, soit près de 10 points devant la moyenne mondiale. Ces chiffres suggèrent que l'IA n'est pas seulement un objet d'étude, mais un outil activement intégré dans les pratiques opérationnelles.

Mais la voie de l'efficacité opérationnelle reste semée d'embûches. La prolifération des outils reste une source majeure de difficultés à Singapour : pour 65 % des personnes interrogées, elle a un impact négatif sur le bien-être des équipes. Pourtant, ce n'est pas le nombre d'outils qui nuit le plus au moral des troupes, mais le volume de fausses alertes. La moitié des personnes interrogées (50 %) se plaignent de passer plus de temps qu'elles ne le devraient à répondre aux alertes. Autrement dit, les équipes ont du mal à distinguer le signal du bruit, même lorsqu'elles adoptent des technologies sophistiquées.

Royaume-Uni

Au Royaume-Uni, l'observabilité est un puissant moteur de productivité : 75 % des personnes interrogées considèrent que leur pratique d'observabilité exerce un impact positif sur l'efficacité des employés. On peut en déduire que les équipes britanniques savent exploiter les données d'observabilité pour réduire les frictions, rationaliser les workflows et permettre aux équipes de se consacrer à des tâches à plus forte valeur ajoutée.

Le Royaume-Uni se distingue également par sa position prudemment optimiste vis-à-vis de l'IA. 39 % des personnes interrogées manifestent leur enthousiasme à l'égard des avantages de l'IA – quelques points devant la moyenne mondiale de 36 % – et près de la moitié d'entre elles (48 %) se disent optimistes tout en attendant d'avoir obtenu davantage d'informations avant d'adopter pleinement l'IA. Le dépannage et l'analyse des causes profondes sont vus comme des domaines d'impact prioritaire de l'IA ; 60 % des personnes interrogées s'attendent à ce que cette technologie exerce un impact positif sur ces processus.

Il reste néanmoins des défis à relever, notamment en matière de gestion des alertes. Plus de la moitié (54 %) déplorent que le volume de fausses alertes nuise au niveau de stress de leur équipe. Et lorsqu'on leur demande d'identifier le défi qui affecte le plus leur moral, les fausses alertes arrivent en tête de liste. Ce bruit dégrade les pratiques de gestion des alertes : 15 % avouent ignorer ou supprimer *souvent* ou *systématiquement* les alertes, un niveau légèrement supérieur à la moyenne mondiale.

Bien que l'adoption d'OpenTelemetry au Royaume-Uni soit conforme à la moyenne mondiale (26 % l'utilisent *souvent* ou *systématiquement* aujourd'hui), c'est sur l'image de marque que son impact est le plus prononcé. Plus des trois quarts (76 %) de ceux qui utilisent OpenTelemetry au moins *parfois* affirment que le standard a amélioré la façon dont leur marque est perçue, soulignant la valeur stratégique des outils d'observabilité modernes au-delà des résultats techniques.

États-Unis

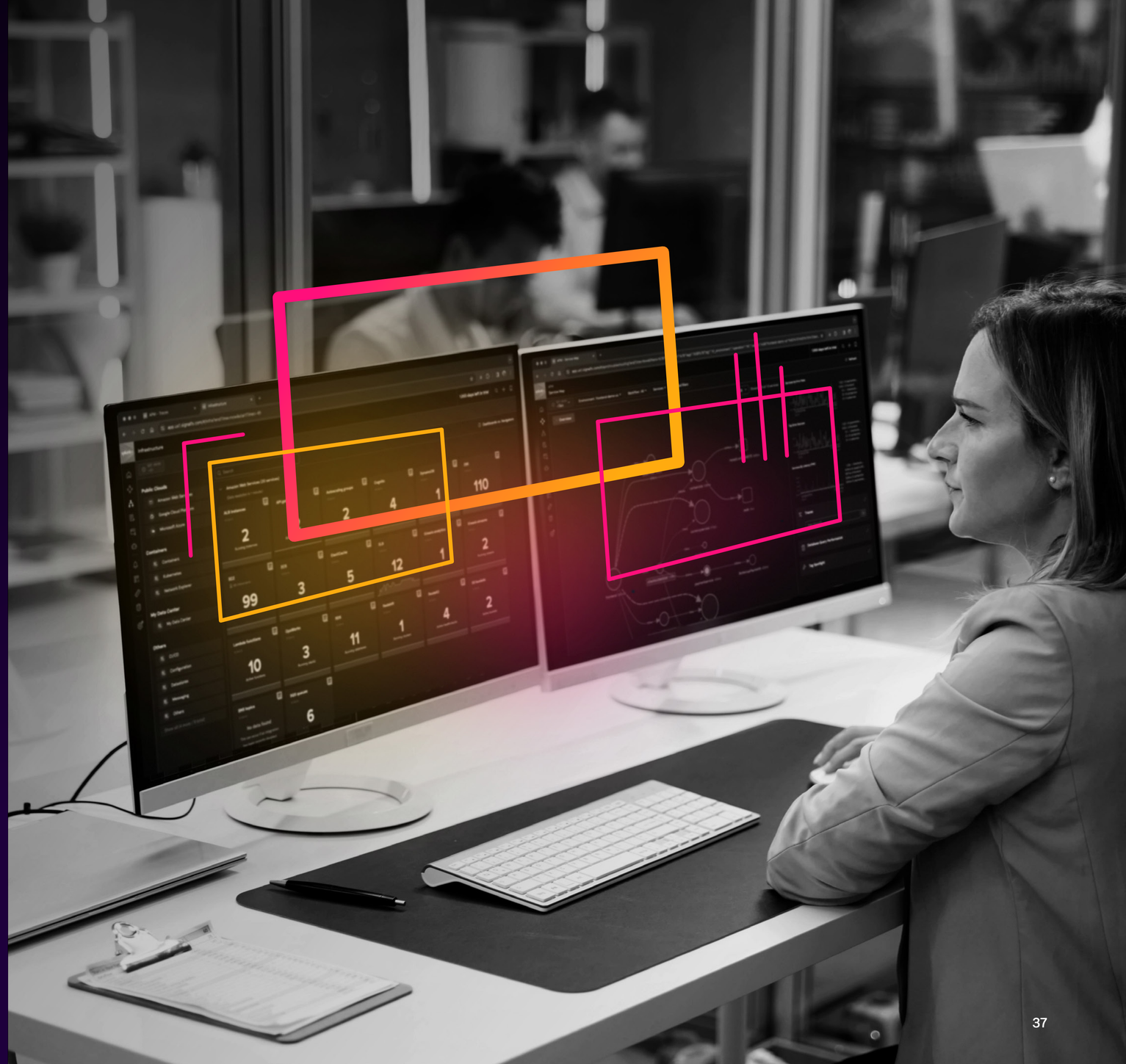
Aux États-Unis, les pratiques d'observabilité s'alignent largement sur les moyennes mondiales dans la plupart des indicateurs clés, mais elles se distinguent dans plusieurs domaines, à commencer par la manière dont les données d'observabilité soutiennent les équipes de sécurité et celle dont les organisations gèrent la réponse aux incidents.

La sécurité semble fortement bénéficier des données d'observabilité aux États-Unis : 54 % des participants affirment que les alertes influent *significativement* sur les décisions de sécurité, loin devant la moyenne mondiale de 47 %. Ils se montrent également optimistes quant au potentiel de l'IA dans ce domaine, et pensent à 65 % que cette technologie aura un impact positif sur la détection des vulnérabilités des applications et des menaces, contre 58 % à l'échelle mondiale. Ces chiffres suggèrent un alignement croissant des fonctions d'observabilité, d'IA et de cybersécurité.

En revanche, la gestion des alertes représente toujours un défi aux États-Unis. 15 % des participants américains avouent manquer *souvent* ou *systématiquement* des alertes (contre 13 % à l'échelle mondiale) et 16 % disent subir *souvent* ou *systématiquement* des interruptions dues à des alertes manquées, un chiffre supérieur à la moyenne mondiale de 11 %. Ces difficultés expliquent peut-être que la panique s'empare plus souvent des équipes lors de la prise en charge des incidents : 12 % des participants américains admettent qu'ils paniquent *souvent* ou *systématiquement* face à des incidents qui touchent les clients, contre seulement 9 % à l'échelle mondiale.

Méthodologie

Les chercheurs d'Oxford Economics ont interrogé 1 855 professionnels de l'ITOps et de l'ingénierie, des praticiens aux cadres supérieurs (développeurs, SRE, ingénieurs système, professionnels des opérations d'infrastructure, CTO et DSI) de février à mars 2025. Les participants résidaient en Australie, en France, en Allemagne, en Inde, au Japon, en Nouvelle-Zélande, à Singapour, au Royaume-Uni et aux États-Unis. Ils représentaient également 16 secteurs d'activité : services aux entreprises, construction et ingénierie, biens de consommation emballés, éducation, services financiers, gouvernement (fédéral/national, étatique et local), soins de santé, sciences de la vie, fabrication, technologie, médias, pétrole/gaz, vente au détail/vente en gros, télécommunications, transport/logistique et services publics.



À propos de Splunk

Splunk, une entreprise de Cisco, contribue à renforcer la résilience numérique des entreprises. Les plus grandes entreprises utilisent notre plateforme unifiée de sécurité et d'observabilité pour garantir la sécurité et la fiabilité de leurs systèmes numériques. Les organisations misent sur Splunk pour éviter que les incidents d'infrastructure, d'application et de sécurité ne deviennent des problèmes majeurs, se remettre plus rapidement des perturbations des systèmes numériques et saisir les nouvelles opportunités.

Poursuivez la conversation avec Splunk.

splunk> a CISCO company

25_CMP_report_state-of-observability-2025_v15_FR