CESIN

Synthèse des instantanés de S1 2026

*Les instantanés du CESIN du premier semestre de 2026 s'appuient sur 21 mini-sondages hebdomadaires effectués auprès de ses membres. Les panels varient entre 84 et 160 répondants avec une moyenne se situant à **116** répondants pour ce semestre.*

Les questions posées chaque semaine sont hétérogènes. Nous les avons regroupées pour ce semestre selon 4 catégories : Nouvelles technologies / Mesures de sécurité / Gouvernance / Les sujets qui ont fait l'actualité.

Synthèse exécutive de S1 2026

Les résultats du premier semestre 2026 mettent en évidence une fonction cyber en pleine transformation, tirée simultanément par l'intensification des menaces, la pression réglementaire et l'émergence rapide de nouveaux usages technologiques. Les 21 mini-sondages CESIN montrent que la cybersécurité n'est plus seulement un sujet de protection technique : elle devient un enjeu de gouvernance, de résilience, de conformité et de capacité d'arbitrage au niveau de la direction. Les répondants partagent une même préoccupation : prioriser les investissements et les dispositifs dans un contexte où les risques se renouvellent plus vite que les ressources disponibles.

La première tendance forte est la montée en puissance de l'IA, à la fois comme levier d'efficacité et comme facteur de risque. Les politiques d'usage de l'IA générative progressent, mais restent incomplètes, notamment pour les IDE (Integrated Development Environment) enrichis à l'IA et les outils de transcription ou de synthèse de réunions. La cyberdéfense par l'IA suscite un intérêt marqué, mais les niveaux de maturité demeurent très hétérogènes : les organisations avancent entre expérimentation, POC, premiers cas d'usage et prudence face aux enjeux de confidentialité, de fiabilité et de souveraineté.

La deuxième tendance est l'accélération des risques liés aux nouvelles technologies. A titre d'illustration, nous avons interrogé nos membres au sujet des lunettes connectées : les risques liés à leur usage restent peu adressés à ce stade, avec seulement 17% des répondants ayant pris des mesures, alors que les enjeux de captation d'images, de sons et de données sensibles pourraient rapidement devenir significatifs.

La troisième tendance concerne la préparation encore insuffisante à certains chantiers structurants. Ces résultats montrent que les démarches de résilience stratégique, d'anticipation technologique et de mesure des dépendances numériques restent moins matures que les dispositifs de protection plus classiques.

Sur les mesures de sécurité, les résultats traduisent une recherche d'équilibre entre efficacité opérationnelle, soutenabilité et maîtrise du risque. Les chiffres exposés ci-après rappellent que la

surface d'exposition liée aux usages des collaborateurs reste importante, malgré la généralisation d'outils de filtrage et de sensibilisation.

La cybersécurité écoresponsable apparaît comme un thème émergent mais déjà pris en compte par une partie du panel. Les leviers les plus cités relèvent de pratiques utiles à la fois pour la sobriété et pour la sécurité : réduction de la surface d'attaque, sécurité dès la conception, sensibilisation des utilisateurs, rationalisation des outils, optimisation des logs et dimensionnement des dispositifs à l'usage réel. Les grandes entreprises sont naturellement davantage engagées sur une approche structurée, tandis que les TPE/PME privilégient plus fortement la sensibilisation et les leviers directement actionnables.

Les sujets d'actualité confirment enfin la sensibilité accrue de la chaîne logicielle et de l'écosystème fournisseurs. La gestion des vulnérabilités est largement pilotée selon la criticité, avec des SLA différenciés, mais les pratiques restent variables selon la maturité des tests, la capacité d'automatisation et le niveau d'acceptation du risque.

Au total, les enquêtes du semestre dessinent trois axes d'action prioritaires pour les RSSI :

- consolider la gouvernance des usages émergents, en particulier l'IA et les données issues des outils collaboratifs ;
- renforcer la résilience face aux dépendances technologiques, au risque fournisseurs et à la pression réglementaire ;
- accélérer l'industrialisation des pratiques de sécurité, du patching à la communication de crise, en passant par la gestion des accès, des postes de travail et des clauses contractuelles.

Le message central est clair : la maturité cyber ne se mesure plus seulement à la capacité de déployer des outils, mais à la capacité de piloter des arbitrages rapides, documentés et alignés avec les risques métiers.

Synthèse des tendances cyber de S1 2026

Cette synthèse met en regard les réponses des grandes entreprises, des ETI et des TPE/PME pour dégager les points de convergence et les écarts de maturité entre ces trois profils d'organisations ainsi que l'analyse des tendances pour ce semestre.

Les grandes entreprises : une maturité qui va de pair avec une exposition plus forte

Durant ce semestre, les grandes entreprises se distinguent d'abord par leur niveau d'exposition aux menaces les plus actuelles : **54%** d'entre elles déclarent avoir déjà été victimes d'une attaque de type deepfake, contre 19% des ETI et seulement 5% des TPE/PME. Cette exposition plus forte s'accompagne toutefois d'une préparation plus structurée sur plusieurs fronts. En matière de communication de crise, **67%** des grandes entreprises se situent aux niveaux 4 ou 5 (dispositif structuré, voire complet et opérationnel), loin devant les ETI et les TPE/PME . Sur le patching applicatif, **81%** priorisent leurs correctifs selon la criticité avec des SLA différenciés, contre 74% pour les ETI et 54% pour les TPE/PME.

Les grandes entreprises sont aussi celles qui ont le plus largement mis en place des RSSI locaux (**74%**, contre 37% pour les ETI et 25% pour les TPE/PME), reflet de structures multi-sites plus fréquentes. Concernant leurs chantiers prioritaires pour 2026, elles se démarquent par une répartition plus équilibrée entre conformité réglementaire, sécurité de l'IA, gestion des tiers et gouvernance, quand les organisations plus petites concentrent davantage leurs efforts sur la seule conformité.

Sur le budget, **66%** s'appuient sur une collaboration rapprochée avec la direction pour arbitrer leurs investissements, la proportion la plus élevée des trois segments.

L'exposition aux deepfake s'inscrit dans une tendance nationale marquée : selon les chiffres cités par la DGSI, le volume de deepfakes en circulation a été multiplié par plus de dix en France entre 2023 et 2025, pour un préjudice cumulé dépassant 1,3 milliard d'euros sur la même période.

Sur le Cyber resilience Act (CRA), l'échéance du 11 septembre 2026 - qui imposera la notification sous 24 heures de toute vulnérabilité activement exploitée à l'ENISA - rapproche sensiblement le calendrier et rend d'autant plus stratégique une mise en conformité.

Enfin, sur le sujet naissant de Claude Mythos et Project Glasswing, la taille de l'organisation ne garantit pas à elle seule la vigilance sur les ruptures technologiques les plus récentes.

Les ETI : le maillon le plus dépendant de ses tiers

Le point saillant mesuré pour les ETI ce semestre est leur forte dépendance aux fournisseurs et prestataires. Sur le Cyber Resilience Act, **52%** d'entre elles indiquent ne pas être directement concernées mais être clientes de fournisseurs qui le sont, la proportion la plus élevée des trois

segments. En ce qui concerne la question sur les rachats du secteur : **74%** ont observé une explosion des coûts consécutive à une opération de rachat chez un de leurs fournisseurs (contre 69% pour les grandes entreprises et 38% pour les TPE/PME), et **41%** évoquent un enfermement technologique, également la proportion la plus haute des trois profils.

Leurs chantiers prioritaires pour 2026 restent dominés par la conformité réglementaire (61%), la gestion des tiers (43%) et la réponse aux incidents (36%), avec une préparation à la communication de crise intermédiaire (36% au niveau 4, 15% au niveau 5). Cette dépendance aux tiers résonne avec l'actualité récente de la chaîne d'approvisionnement logicielle : les compromissions à répétition de l'écosystème npm (Shai-Hulud, puis sa variante de novembre 2025 ayant touché plus de 700 paquets et 487 organisations) illustrent concrètement le risque que des ETI, souvent moins outillées pour auditer leurs dépendances, subissent les conséquences d'un incident chez un fournisseur sans y être elles-mêmes directement exposées.

Sur l'Indice de Résilience Numérique, ce retard d'adoption tranche avec la dynamique du marché : porté par la Caisse des Dépôts, RTE et Docaposte, puis rejoint début 2026 par de grands groupes comme la SNCF, Orange ou CMA CGM - tous très au-delà du seuil des 5 000 salariés qui définit une ETI -, l'indice reste pour l'instant l'affaire des plus grandes structures, ce qui pourrait accentuer l'écart de maturité si les ETI ne s'en emparent pas à leur tour.

Les TPE/PME : la conformité avant tout, la sobriété comme réflexe

Pour les TPE/PME, la conformité réglementaire s'impose comme la priorité numéro un de très loin : **72%** la citent parmi leurs trois chantiers pour 2026, devant les usages de l'IA (56%) et la gouvernance de la cybersécurité (34%), une concentration plus marquée que chez les ETI (61%) et surtout que chez les grandes entreprises (46%), qui, signe de maturité, répartissent davantage leurs efforts entre plusieurs fronts. Cette pression concentrée sur la conformité reflète une réalité de marché documentée au niveau national : la transposition de la directive NIS2 en droit français, attendue via la loi Résilience au second semestre 2026, va mécaniquement élargir le périmètre des entités concernées, alors que les plus petites structures disposent rarement d'une fonction juridique ou conformité dédiée pour absorber cette charge - ce qui explique sans doute pourquoi la conformité écrase à ce point leurs autres priorités, contrairement aux grandes entreprises qui peuvent répartir l'effort sur plusieurs fronts.

Ce segment se distingue également par son engagement sur la sobriété numérique : 61% des TPE/PME citent la sensibilisation des utilisateurs comme levier prioritaire pour concilier sécurité et sobriété numérique (contre 45% pour les grandes entreprises, qui misent davantage sur la sécurité dès la conception). Sur le sujet de Claude Mythos et Project Glasswing, elles affichent également la plus forte vigilance : 77% déclarent en suivre l'actualité de près, la proportion la plus élevée des trois segments.

Les TPE/PME restent en revanche les moins avancées sur plusieurs sujets structurants : seules **12%** disposent d'un dispositif de communication de crise complet et testé (niveau 5), **54%** priorisent leur patching selon la criticité (le taux le plus bas des trois profils), et **34%** des organisations directement concernées par le CRA n'ont pas encore engagé leurs travaux de mise en conformité. Sur les rachats du secteur, 46% ne se disent pas concernées, signe d'un écosystème de fournisseurs plus restreint et sans doute moins consolidé que celui des grandes entreprises et des ETI.

Elles se distinguent également par leur vigilance sur le sujet naissant de Claude Mythos et Project Glasswing, qu'elles suivent de près à 77%, la proportion la plus élevée des trois segments - alors même qu'elles sont structurellement les moins armées pour absorber une éventuelle accélération des cycles de découverte de vulnérabilités.

Tendances transversales

Au-delà des écarts entre profils, plusieurs constats traversent l'ensemble du panel ce semestre. La conformité réglementaire (NIS2, CRA, DORA) s'impose comme la priorité commune à tous les segments pour 2026, avec une intensité d'autant plus marquée que l'organisation est petite.

La gouvernance de l'IA générative reste, elle, largement à construire : plus d'un quart des répondants n'ont mis en place aucune politique sur le sujet, et la migration post-quantique n'en est encore, pour l'écrasante majorité des organisations tous profils confondus, qu'au stade de la réflexion (69% n'ont pas encore commencé à s'en préoccuper).

Enfin, la sobriété numérique appliquée à la cybersécurité, sujet encore émergent en 2025, a suffisamment mobilisé la communauté pour faire l'objet de deux mini-sondages consécutifs ce semestre, signe d'un intérêt croissant pour l'articulation entre performance de protection et impact environnemental.

Ce calendrier réglementaire chargé - DORA déjà applicable depuis janvier 2025 dans le secteur financier, NIS2 attendue au second semestre 2026, puis le CRA dès septembre 2026 - accélère une transformation plus profonde de la fonction RSSI, de plus en plus positionnée comme un pilotage du risque rattaché à la direction et exposé juridiquement en cas de manquement, plutôt que comme une fonction strictement technique.

Le retard sur la migration post-quantique observé dans ce panel fait par ailleurs écho à un constat plus large : malgré la finalisation des standards NIST dès août 2024, et du référentiel ReCyf publié par l’ANSSI dans sa dernière version de juin 2026, l'adoption réelle reste très en retrait de la prise de conscience du risque à l'échelle mondiale, la grande majorité des organisations reconnaissant la menace qu'un ordinateur quantique ferait un jour peser sur leurs échanges actuels sans avoir encore engagé de déploiement concret.

Nouvelles technologies

Cette catégorie regroupe les sujets liés à l'adoption de nouvelles technologies, au premier rang desquelles l'intelligence artificielle sous toutes ses formes, et aux risques qu'elles font peser sur la fonction cyber. Un même constat traverse l'ensemble des questions posées ce semestre : les usages progressent plus vite que la gouvernance censée les encadrer. Le risque deepfake, s'est suffisamment concrétisé pour justifier une réactualisation de l'enquête menée fin 2024, tandis que l'IA générative appliquée à la cyberdéfense s'installe progressivement comme un levier d'accélération pour les équipes, mais reste elle aussi à un stade encore largement exploratoire.

Politique IA générative et IDE enrichis à l'IA

L'IA générative s'installe durablement dans les usages professionnels, y compris dans les environnements de développement où des outils comme GitHub Copilot, Cursor ou Claude s'imposent progressivement aux côtés des IDE traditionnels. Pour les RSSI, ce mouvement pose un double défi de gouvernance : encadrer l'usage de l'IA générative pour l'ensemble des collaborateurs, tout en adaptant des règles spécifiques pour les équipes techniques dont les pratiques de développement évoluent rapidement.

Entre autorisation encadrée, interdiction ciblée et absence de politique formalisée, les organisations avancent à des rythmes très différents sur ce sujet encore jeune. La question de l'installation des IDE enrichis à l'IA cristallise particulièrement ces tensions, entre productivité recherchée par les développeurs et risques liés à la fuite de code source ou de données sensibles vers des services tiers.

118 membres ont répondu à la question [Q190] concernant la politique mise en place sur l'utilisation de l'IA générative et des IDE enrichis à l'IA, ainsi que les modalités d'autorisation de leur installation. Les résultats font apparaître un sujet encore largement à construire : une majorité des organisations n'a pas encore de politique intégrant les IDE enrichis à l'IA, et une part significative n'a mis en place aucune politique sur l'IA générative, l'approche différenciée pour les développeurs restant minoritaire. Sur l'installation de ces IDE, les pratiques se répartissent de façon assez équilibrée entre autorisation générale, autorisation par exception et absence d'usage, l'interdiction pure et simple restant marginale.

Migration vers la PQC

La cryptographie asymétrique, qui sécurise aujourd'hui l'essentiel des échanges numériques, sera un jour vulnérable face à la puissance de calcul des ordinateurs quantiques. Si l'échéance exacte de cette rupture reste débattue, l'ampleur du chantier de migration vers la cryptographie post-quantique (PQC) justifie d'anticiper dès maintenant : inventaire des usages cryptographiques, dépendance aux algorithmes vulnérables, feuille de route de transition.

Entre les organisations qui n'ont pas encore ouvert le sujet et celles qui ont déjà lancé un projet dédié, l'écart de maturité reflète autant la perception du risque que la disponibilité des ressources à y consacrer.

104 membres ont répondu à la question [Q193] concernant le lancement ou non d'un projet de migration PQC au sein de leur organisation. Le chantier reste embryonnaire pour l'écrasante majorité des organisations, qui n'ont pas encore commencé à s'en préoccuper. Les initiatives concrètes, qu'il s'agisse de pilotes ou de migrations déjà engagées, restent rares.

Une fois le projet de migration post-quantique engagé, se pose rapidement la question de sa gouvernance : qui doit être impliqué, et à quel titre ? Au-delà de l'aspect technique (inventaire des usages cryptographiques, mise à jour des infrastructures), la migration PQC engage aussi les métiers, qui doivent identifier les données critiques à protéger en priorité, et la direction, qui pilote les arbitrages de risques et d'investissements.

Cette question s'intéresse à la taille et à la composition des équipes projet PQC déjà constituées ou envisagées : équipes sécurité, IT, top management, risques, métiers, ou encore équipe cryptographie dédiée.

85 membres ont répondu à la question [Q205] concernant la taille de l'équipe projet PQC et les fonctions qui y sont associées. Le renoncement à constituer une équipe dédiée domine largement, en particulier chez les ETI et les TPE/PME, les grandes entreprises étant comparativement mieux loties. Quand une équipe existe, elle reste très majoritairement rattachée aux équipes sécurité et IT, la migration post-quantique demeurant à ce stade un sujet porté par la technique plus que par la gouvernance transverse.

Gestion du risque Deep fake (Mise à jour 2026)

En décembre 2024, le CESIN interrogeait déjà sa communauté sur le risque deepfake. Depuis, les usages malveillants de l'intelligence artificielle se sont accélérés, rendant les contenus falsifiés toujours plus crédibles et accessibles, qu'il s'agisse d'ingénierie sociale, d'usurpation d'identité ou de fraude financière.

Cette actualisation permet de mesurer l'évolution du niveau de préparation des organisations depuis la précédente enquête, à travers les incidents effectivement rencontrés et les dispositifs de prévention, détection et réponse mis en place ou envisagés.

98 membres ont répondu à la question [Q201] concernant les attaques de type deepfake déjà subies et les solutions organisationnelles ou technologiques mises en œuvre pour mieux prévenir, détecter et répondre à ce risque. L'exposition suit nettement la taille de l'organisation, les grandes entreprises étant très largement les plus touchées, loin devant les ETI et surtout les TPE/PME.

Lunettes connectées : nouvelle technologie, nouveau risque ?

Les lunettes connectées commencent à apparaître dans les environnements professionnels. Le risque cyber direct reste aujourd'hui limité, ces équipements n'étant pas encore massivement connectés au système d'information, mais les enjeux liés à la captation d'images, de vidéos et de sons deviennent bien réels : confidentialité, secrets industriels, droit à l'image, sécurité des locaux.

Avec l'essor des usages mobiles et des connexions via smartphone, ce sujet pourrait rapidement devenir un enjeu de gouvernance à part entière, comme l'ont été en leur temps les smartphones personnels ou les objets connectés.

121 membres ont répondu à la question [Q203] concernant la prise en compte de ce risque et les mesures éventuellement mises en place. Le sujet reste très largement non traité, avec toutefois un écart selon la taille de l'organisation. Parmi celles qui s'en sont saisies, la réponse passe d'abord par la sensibilisation, puis par des restrictions ciblées, une part notable traitant simplement le sujet comme celui d'un smartphone classique.

Réunions : transcriptions et synthèses IA ?

Les fonctionnalités de transcription automatique et de synthèse par IA sont désormais intégrées nativement dans la plupart des outils de visioconférence. Leur adoption progresse rapidement pour des raisons de productivité, mais leur usage lors de réunions sensibles (CODIR, incidents cyber, sujets RH, propriété intellectuelle, négociations stratégiques) soulève des questions concrètes de confidentialité, de souveraineté des données et de responsabilité.

Où ces données sont-elles stockées ? Qui y a accès ? Selon quelles règles de rétention et de consentement ? Les approches des organisations sur ce sujet encore récent semblent aujourd'hui très hétérogènes, entre interdiction explicite, autorisation conditionnelle et absence totale d'encadrement.

125 membres ont répondu à la question [Q204] concernant la gestion des enregistrements, transcriptions et synthèses IA des réunions au sein de leur organisation. Les grandes entreprises apparaissent les plus structurées sur ce sujet, quand les ETI affichent la plus forte proportion d'organisations sans aucun encadrement, alors même qu'elles se situent habituellement entre les deux autres profils sur la gouvernance de l'IA.

IA générative en cyberdéfense

Pour ce sujet, la question habituelle a été remplacée par un questionnaire en dix volets proposés par le groupe de travail (LAB) Cyber & IA du CESIN, portant sur le profil des répondants, leur niveau de maturité sur l'IA générative appliquée à la cyberdéfense, les usages déjà expérimentés, les bénéfices constatés ou recherchés, ainsi que les freins rencontrés. L'IA générative s'impose en effet progressivement comme un levier d'accélération pour les équipes cyber : triage des alertes, renseignement sur la menace, analyse de vulnérabilités, réponse à incident, génération de playbooks ou production de rapports.

Son adoption soulève aussi des questions structurantes de fiabilité, de confidentialité, de souveraineté et de gouvernance interne, des enjeux que ce mini-sondage anonyme, mené par le GT CyberIA, permet d'objectiver à travers l'expérience concrète des répondants, très majoritairement RSSI, qu'ils en soient encore au stade du POC ou déjà en production partielle. Les réponses alimenteront directement les travaux du livre blanc commun du CESIN et de l'IMA (Innovation Makers Alliance).

92 membres ont répondu au questionnaire [Q206] concernant l'usage de l'IA générative pour renforcer les capacités cyber de leur organisation. Les répondants sont très majoritairement des RSSI, et la maturité reste émergente, la majorité des organisations se situant encore au stade du pilote ou de l'expérimentation. Le bénéfice le plus recherché, un gain de vitesse sur la détection, n'est pour l'instant constaté que par une minorité, et les freins les plus cités touchent à la fiabilité, à la confidentialité et à la souveraineté.

Mesures de sécurité

Cette catégorie rassemble les dispositifs concrets que les organisations mettent - ou non - en œuvre pour se protéger et se préparer aux incidents. Elle illustre une recherche d'équilibre permanente entre efficacité opérationnelle, ressources disponibles et soutenabilité : les honeypots séduisent mais restent coûteux à maintenir, le blocage des usages non maîtrisés sur les postes de travail demeure partiel, et la sobriété numérique s'impose progressivement comme un critère à part entière dans le choix des mesures de sécurité.

Honey Pots : des « clochettes » indispensables

Dans un paysage cyber où les attaques deviennent de plus en plus furtives, les organisations cherchent des moyens innovants pour détecter les intrusions avant qu'elles n'impactent leurs systèmes critiques. Les honeypots, en simulant des cibles vulnérables, attirent les attaquants et déclenchent des alertes précoces, un peu comme des clochettes posées sur le système d'information.

Leur déploiement reste toutefois loin d'être anodin : coût de maintenance, risques juridiques liés à la collecte de données sur les attaquants, ou complexité technique peuvent freiner leur adoption, malgré l'intérêt qu'ils suscitent.

122 membres ont répondu à la question [Q189] concernant la mise en place de cette stratégie au sein de leur organisation. L'adoption progresse avec la taille de l'organisation, les grandes entreprises étant les plus nombreuses à avoir déployé des honeypots, seuls ou combinés à d'autres outils, quand les TPE/PME restent très en retrait, freinées avant tout par le manque de ressources internes pour les maintenir. Dans les trois segments, on note une préférence pour d'autres solutions jugées plus adaptées.

Usage d'applications de messagerie sur les postes de travail

Le filtrage de contenus malveillants sur les messageries professionnelles est désormais largement répandu. Mais les messageries professionnelles ne sont pas les seuls canaux d'échange de données : messageries instantanées personnelles, webmails, espaces de stockage en ligne restent accessibles depuis les postes de travail sans nécessairement être gérés ou approuvés par l'organisation.

Cette question s'est intéressée au niveau de blocage effectivement appliqué sur ces trois familles d'usages (messagerie instantanée, e-mails personnels, stockage en ligne), qu'il soit total, sélectif ou remplacé par une simple page de sensibilisation.

131 membres ont répondu aux questions [Q191] concernant les services de messagerie, d'e-mail ou de stockage en ligne bloqués sur les postes de travail lorsqu'ils ne sont pas gérés ou approuvés par l'entreprise. Le niveau de blocage reste globalement modéré sur les trois familles d'usages, la majorité des organisations n'appliquant aucun blocage spécifique sur les e-mails personnels et le stockage en ligne. Quand un contrôle existe, il reste le plus souvent sélectif plutôt que total.

Cybersécurité écoresponsable

Face à l'essor conjoint des exigences de cybersécurité et de responsabilité sociétale, les organisations cherchent aujourd'hui à concilier performance de protection et sobriété numérique. Sécurisation proportionnée au risque, réduction de la surface d'attaque, optimisation des logs ou rationalisation des outils : plusieurs pratiques commencent à s'imposer sur le terrain.

Cette question a permis de dresser un état des lieux des leviers concrètement intégrés par les organisations pour articuler sécurité et sobriété, entre approches déjà déployées et sujets encore à l'étude.

84 membres ont répondu à la question [Q199] concernant les leviers déjà intégrés pour concilier sécurité et sobriété numérique. Les grandes entreprises misent avant tout sur des leviers structurels comme la sécurité dès la conception, quand les TPE/PME privilégient la sensibilisation, une approche plus accessible avec des moyens limités. Les ETI se distinguent par la plus forte proportion d'organisations n'ayant encore rien mis en place.

Claude Mythos & Project Glasswing

En avril 2026, Anthropic a annoncé Claude Mythos Preview, un nouveau modèle d'IA généraliste dont les capacités en cybersécurité ont été jugées trop puissantes pour une diffusion publique. En quelques semaines de tests internes, le modèle a détecté de manière autonome des milliers de vulnérabilités critiques, dont des zero-days présents dans l'ensemble des grands systèmes d'exploitation et navigateurs, ainsi qu'une faille vieille de 27 ans dans OpenBSD.

Pour encadrer cet accès, Anthropic a lancé en avril 2026 le Project Glasswing, une coalition défensive réunissant à son lancement une cinquantaine d'organisations fondatrices (AWS, Apple, Microsoft, Google, CrowdStrike, Palo Alto Networks, ainsi que des mainteneurs open source comme Mozilla, OpenBSD ou FreeBSD, entre autres). La coalition a été élargie en juin 2026 à près de 150 organisations supplémentaires réparties dans une quinzaine de pays, portant le total à environ 200 membres, pour un usage strictement défensif du modèle.

Pour la grande majorité des équipes sécurité, Mythos n'est donc pas encore accessible. Mais ses implications sont immédiates : accélération de la découverte de vulnérabilités, réduction de la fenêtre entre détection et exploitation, pression accrue sur les processus de patching, et remise en question des compétences attendues au sein des équipes.

141 membres ont répondu à la question [Q200] concernant leur niveau de suivi de ce sujet. Contrairement à une intuition qui associerait la veille technologique à la taille de l'organisation, ce sont les TPE/PME qui suivent ce sujet de plus près, devant les ETI et les grandes entreprises, ces dernières se situant davantage dans une posture d'attention sans approfondissement.

Préparation à la communication de crise cyber

Les récentes fuites de données et incidents cybers majeurs ont montré que l'impact d'une crise ne se limite pas aux systèmes d'information : il touche directement la réputation et la confiance des parties prenantes. Une communication de crise mal anticipée peut aggraver considérablement les dommages d'un incident déjà critique.

D'où l'importance d'une préparation en amont, structurée et testée, pour réagir rapidement et de manière cohérente le moment venu. Cette question propose une auto-évaluation du niveau de préparation, sur une échelle de 1 (aucune préparation spécifique) à 5 (dispositif complet, opérationnel et déjà testé en exercice).

148 membres ont répondu à la question [Q202] concernant leur niveau de préparation en matière de communication de crise en cas d'incident cyber. La maturité progresse nettement avec la taille de l'organisation, les grandes entreprises étant très majoritairement dotées d'un dispositif structuré voire complet, quand les TPE/PME se concentrent surtout sur un dispositif partiellement défini et encore non testé.

Gouvernance

Cette catégorie couvre la manière dont les RSSI structurent, priorisent et pilotent leur fonction. Le modèle d'organisation (RSSI locaux ou centralisés), les chantiers prioritaires pour 2026, les méthodes de justification budgétaire et le niveau de préparation aux nouvelles réglementations (CRA notamment) varient tous fortement selon la taille de l'organisation, la conformité réglementaire s'imposant toutefois comme la priorité commune et transversale à tous les segments.

RSSI locaux : atout ou complexité pour les organisations multi-sites ou entités ?

Dans les organisations réparties sur plusieurs sites ou entités, la gouvernance de la sécurité peut vite devenir un défi. Certaines structures choisissent de s'appuyer sur des RSSI locaux pour renforcer la proximité et la réactivité, tandis que d'autres préfèrent conserver une direction centralisée.

Entre meilleure réactivité terrain et risque de complexité organisationnelle ou de perte de cohérence de la politique sécurité, le choix d'un modèle local ou centralisé reflète autant la taille de l'organisation que sa culture de gouvernance.

160 membres ont répondu à la question [Q186] en deux volets : la mise en place ou non de RSSI locaux dans leur organisation, et selon les cas, les avantages perçus de cette approche ou les raisons de ne pas y avoir recours. Le recours aux RSSI locaux suit très directement la taille de l'organisation, largement majoritaire chez les grandes entreprises.

Chantiers prioritaires 2026

2026 s'ouvre avec son lot de défis pour les RSSI : réglementations renforcées (NIS2, CRA, DORA), menaces en évolution (IA, attaques sur les chaînes logistiques, tensions géopolitiques), et enjeux de souveraineté numérique. Face à cette accumulation de sujets, la capacité à prioriser devient elle-même un exercice stratégique.

Cette question invitait chaque RSSI à identifier les trois chantiers qu'il compte réellement prioriser cette année, parmi un large éventail couvrant la conformité, la gouvernance, la détection, la réponse à incident, la gestion des actifs, les usages de l'IA, la gestion des tiers, la souveraineté numérique, la sensibilisation, le cloud ou la protection des données.

160 membres ont répondu à la question [Q187] concernant les trois chantiers prioritaires retenus pour 2026 (choix de trois maximum). La conformité réglementaire arrive en tête pour les trois segments, avec une intensité d'autant plus marquée que l'organisation est petite : 46% pour les grandes entreprises, 61% pour les ETI et 72% pour les TPE/PME. Les grandes entreprises se distinguent par une répartition plus équilibrée de leurs priorités entre plusieurs fronts (conformité, usages de l'IA, gestion des tiers, gouvernance), quand les ETI et les TPE/PME concentrent davantage leurs efforts sur la seule conformité, les ETI la complétant par la gestion des tiers et la réponse aux incidents, et les TPE/PME par les usages de l'IA., de manière globale, ETI et les

Budget et ROI

Justifier les budgets cybersécurité n'a jamais été aussi nécessaire, dans un contexte de contraintes financières accrues. Pourtant, les enjeux de conformité (NIS2, CRA) et de résilience face à des attaques toujours plus ciblées rendent ces investissements plus indispensables que jamais.

Priorisation par les risques métiers, indicateurs clés de performance, benchmark sectoriel, valorisation des incidents évités ou chiffrage d'incidents connus : les RSSI disposent d'un éventail de méthodes pour construire et défendre leur budget auprès de la direction.

137 membres ont répondu à la question [Q188] concernant les méthodes utilisées pour justifier le budget cybersécurité et en mesurer le retour sur investissement (plusieurs réponses possibles). La priorisation par les risques métiers domine largement dans les trois segments, tout comme le recours à la collaboration avec la direction, ces deux pratiques étant toutefois plus répandues chez les grandes entreprises. Le benchmark sectoriel reste également l'apanage des plus grandes structures.

Préparation au Cyber Resilience Act (CRA)

Le Cyber Resilience Act va imposer de nouvelles exigences de sécurité aux produits et services numériques, en particulier aux éditeurs de solutions : sécurité des produits, processus de développement, gestion des vulnérabilités et organisation interne sont directement concernés. Les obligations de notification s'appliqueront dès le 11 septembre 2026, et les principales obligations à partir du 11 décembre 2027.

Plutôt que d'attendre son entrée en vigueur, de nombreuses organisations anticipent déjà ses impacts vis à vis de leurs fournisseurs, entre audit des produits concernés, révision des contrats, sensibilisation interne et veille réglementaire.

120 membres ont répondu à la question [Q192] concernant les actions déjà entreprises pour s'assurer que leurs fournisseurs concernés par le CRA soient en conformité avec cette réglementation. Les ETI apparaissent les plus dépendantes de leurs fournisseurs sur ce sujet, une majorité d'entre elles n'étant pas directement concernées par le CRA mais clientes d'organisations qui le sont. Parmi les organisations directement impactées, les grandes entreprises sont les mieux engagées dans leur mise en conformité pour l'échéance de septembre 2026.

Indice de Résilience Numérique (IRN)

Porté par un collectif d'acteurs économiques et d'experts européens, dont la Caisse des Dépôts, RTE et Docaposte, l'Indice de Résilience Numérique (IRN) permet aux entreprises et aux organisations publiques de mesurer, piloter et réduire leurs dépendances numériques critiques, dans un contexte marqué par l'intensification des risques géopolitiques, technologiques et réglementaires.

Cet outil propose une approche concrète pour identifier les risques liés aux infrastructures critiques, aux chaînes d'approvisionnement et aux technologies clés, et pour renforcer l'autonomie stratégique des organisations comme celle de l'Europe.

90 membres ont répondu à la question [Q195] concernant leur niveau de connaissance et d'adoption de l'IRN, ainsi que les usages envisagés ou déjà mis en œuvre. La notoriété de l'outil reste globalement limitée, mais nettement plus élevée chez les grandes entreprises. Fait notable, ce sont les TPE/PME qui affichent la seule adoption effective au sein du panel, quand aucune ETI ne l'a encore mis en œuvre.

Outils de collaboration sectorielle

La collaboration entre RSSI repose souvent sur des moyens dédiés : plateformes de renseignement sur la menace, CERT sectoriels, ISAC, groupes de travail associatifs ou espaces collaboratifs fermés. Ces solutions permettent de partager de l'information, d'échanger sur les bonnes pratiques ou de coordonner des actions communes.

Leur efficacité dépend toutefois de leur pertinence, de leur accessibilité et de leur adoption réelle par la communauté. Cette question interroge à la fois les moyens utilisés et les motivations qui poussent les RSSI à s'y investir : réactivité, confiance, enrichissement mutuel, conformité ou anticipation des menaces.

90 membres ont répondu à la question [Q197] concernant les moyens utilisés pour faciliter la collaboration sectorielle et les raisons qui motivent ce choix. Les groupes de travail sectoriels au sein de clubs et associations, au premier rang desquels le CESIN, restent le moyen le plus cité, devant les groupes privés sur messageries sécurisées et les CERT sectoriels. Les répondants citent d'abord l'enrichissement mutuel et la confiance comme motivations, loin devant la seule conformité réglementaire.

Les sujets qui ont fait l'actualité

Cette catégorie revient sur trois sujets qui ont concrètement marqué l'actualité du semestre. Les attaques Shai-Hulud puis React2Shell sur la chaîne logicielle open source ont remis sur le devant de la scène l'arbitrage entre réactivité de patching et maîtrise du risque. Les rachats spectaculaires qui continuent d'agiter le marché de la cybersécurité pèsent directement sur les organisations clientes, en premier lieu par une hausse des coûts. Enfin, une décision de justice irlandaise est venue rappeler que l'encadrement de l'usage personnel des équipements professionnels a des conséquences juridiques bien réelles sur la responsabilité de l'organisation en cas d'incident.

Patching applicatif : réactivité vs. risque

Les récentes attaques ciblant des librairies open source, à l'image de Shai-Hulud sur NPM, suivie de près par React2Shell, ont rappelé la difficulté à trouver le bon équilibre entre patcher rapidement pour corriger des vulnérabilités connues, et limiter l'exposition à d'autres risques : nouvelles vulnérabilités introduites, régressions, incidents de production.

Cette tension soulève des questions stratégiques sur la gestion des risques, la confiance accordée aux dépendances logicielles, et les processus de validation des mises à jour, entre application systématique des correctifs critiques, SLA différenciés selon la criticité, pipelines automatisés ou validation via registre proxy interne.

97 membres ont répondu à la question [Q194] concernant l'arbitrage opéré entre la nécessité de patcher rapidement les librairies applicatives et le risque d'introduire une nouvelle vulnérabilité. La priorisation par la criticité, avec des SLA différenciés, reste l'approche dominante dans les trois segments, mais décroît avec la taille de l'organisation, les TPE/PME recourant davantage à des approches combinées ou hétérogènes. Documenter chaque arbitrage d'acceptation du risque reste une pratique nettement plus répandue chez les grandes entreprises.

Rachat important dans la cyber

Ces dernières années, le secteur de la cybersécurité a été marqué par des rachats spectaculaires : Broadcom/Symantec pour 10,7 milliards de dollars, Google avec Mandiant (5,4 milliards) puis Wiz (32 milliards), Mastercard avec Recorded Future, ServiceNow avec Armis (7,7 milliards), pour ne citer que les opérations les plus emblématiques.

Ces rachats visent souvent à proposer des solutions plus complètes, mais ils produisent la plupart du temps des effets indésirables pour les organisations clientes : enfermement technologique, hausse des coûts, dilution de l'innovation ou perte d'agilité.

86 membres ont répondu à la question [Q196] concernant les impacts observés à la suite des rachats majeurs dans la cybersécurité et les actions mises en œuvre en conséquence. L'explosion des coûts consécutive à un rachat est l'impact le plus cité. Face à ces mouvements de marché, les grandes entreprises et les ETI réagissent en engageant une revue de leurs contrats

Responsabilité de l'organisation concernant les données privées sur équipements professionnels

En 2025, une entreprise irlandaise a été victime d'une attaque cyber ayant débouché sur un vol de données puis sur leur publication. Un employé avait déposé une plainte auprès du régulateur de confidentialité irlandais, estimant que l'entreprise n'avait pas protégé les données personnelles qu'il stockait sur son mobile professionnel. Le régulateur a débouté la plainte, au motif que le règlement intérieur de l'employeur interdisait l'usage personnel des équipements professionnels, écartant ainsi sa responsabilité de traitement.

Cette décision éclaire un enjeu très concret pour les RSSI : l'encadrement de l'usage personnel des équipements professionnels conditionne directement la responsabilité de l'organisation en cas de perte, de vol ou de cyberattaque touchant des données privées.

130 membres ont répondu à la question [Q198] concernant l'encadrement de l'usage personnel des équipements professionnels au sein de leur organisation, et la politique appliquée en cas d'incident touchant des données privées. Dans la majorité des organisations, l'usage personnel reste autorisé, l'interdiction pure et simple ne concernant qu'une minorité des répondants. Or, en cas de perte, de vol ou de cyberattaque touchant un équipement à usage mixte, très peu d'organisations ont défini des règles précisant les responsabilités de chacun, illustrant un angle mort persistant sur un sujet pourtant tranché par la jurisprudence récente.

ANNEXES

QUESTION DE LA SEMAINE : DETAIL DES RESULTATS (graphiques)

[Q186] RSSI locaux : atout ou complexité pour les organisations multi-sites ou entités ? Dans le cas d'une organisation multi-sites ou entités, avez-vous mis en place des RSSI locaux ?

Parmi les **Grandes entreprises** :

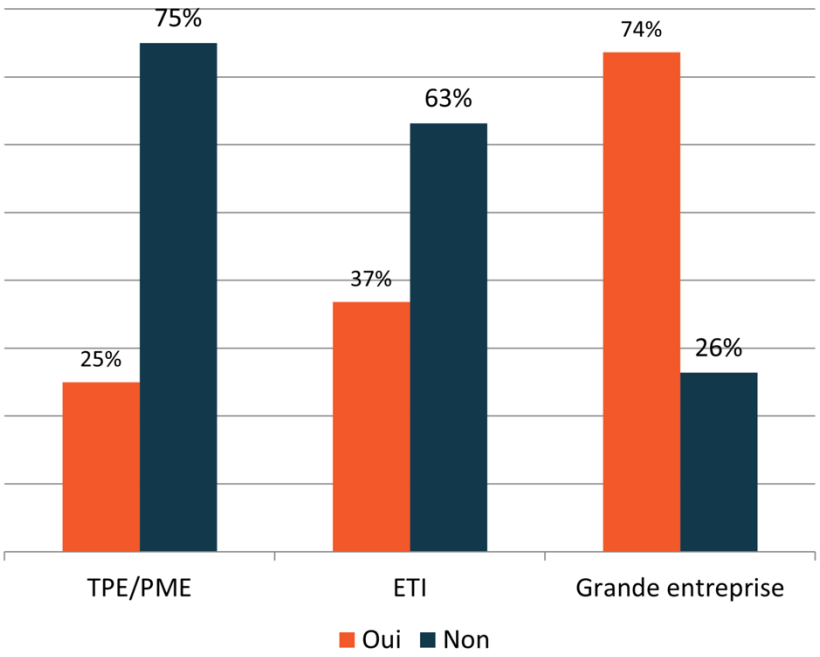
- **74%** ont mis en place des RSSI locaux ;
- **26%** n'ont pas mis en place de RSSI locaux.

Parmi les **ETI :**

- **37%** ont mis en place des RSSI locaux ;
- **63%** n'ont pas mis en place des RSSI locaux.

Parmi les **TPE/PME** :

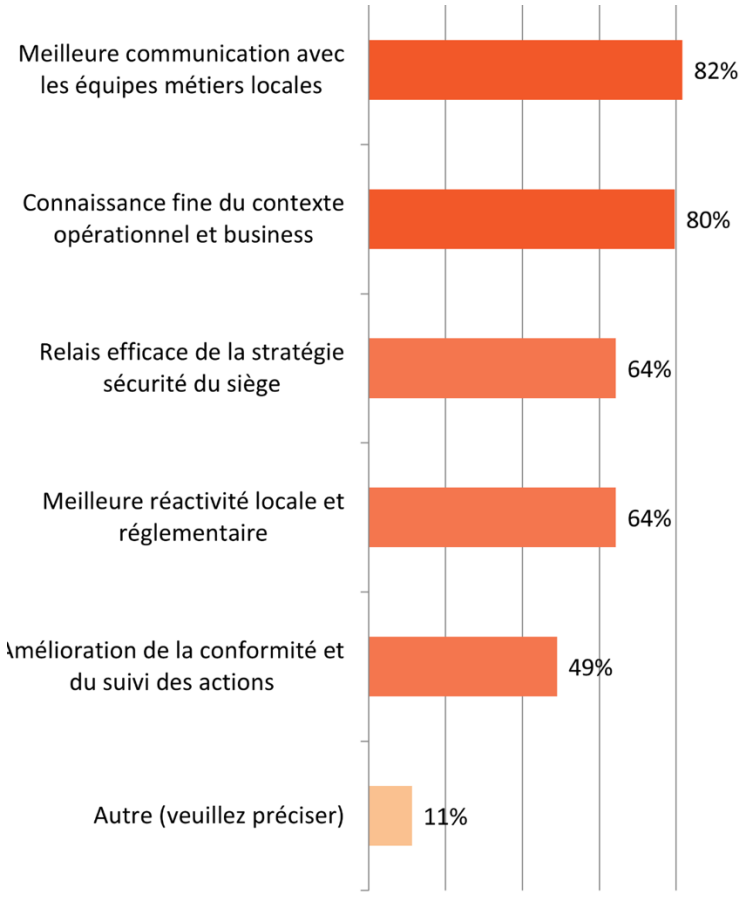
- **25%** ont mis en place des RSSI locaux ;
- **75%** n'ont pas mis en place des RSSI locaux.



Quels sont selon vous les principaux avantages de cette approche ? *(plusieurs réponses possibles)*

Parmi ceux qui ont mis en place des RSSI locaux, les avantages principaux avancés sont :

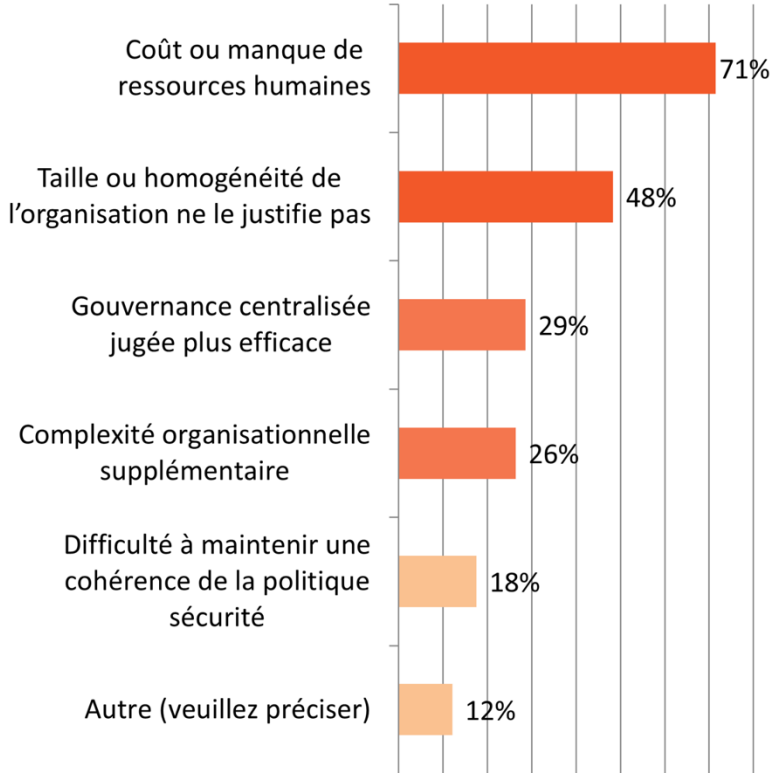
- Pour **82%** une meilleure communication avec les équipes métiers locales ;
- Pour **80%** une connaissance fine du contexte opérationnel et business ;
- Pour **64%** une meilleure réactivité locale et réglementaire ;
- Pour **64%** un relais efficace de la stratégie sécurité du siège ;
- Pour **49%** une amélioration de la conformité et du suivi des actions ;
- Pour **11%** autre chose, notamment car cette approche permet d'assurer une conformité locale adaptée aux exigences de chaque pays, ou d'améliorer la réactivité face aux incidents cyber, le suivi des prestataires ou la gestion des risques spécifiques, ou encore de renforcer la relation avec les clients et leur satisfaction.



Quelles sont les principales raisons de ne pas avoir de RSSI locaux *(plusieurs réponses possibles)*

Parmi ceux qui n'ont pas mis en place des RSSI locaux, les principales raisons sont :

- Pour **71%** à cause du coût ou un manque de ressources humaines ;
- Pour **48%** la taille ou l'homogénéité de l'organisation ne le justifie pas ;
- Pour **29%** la gouvernance centralisée est jugée plus efficace ;
- Pour **26%** cela représente une complexité organisationnelle supplémentaire ;
- Pour **18%** cela représente une difficulté à maintenir une cohérence de la politique sécurité ;
- Pour **12%** pour une autre raison, notamment en raison de :
    - Une gouvernance cyber centralisée, où les équipes locales sont intégrées dans une direction unique, sans autonomie décisionnelle.
    - Un manque de profils qualifiés, compensé par des correspondants sécurité locaux, mais sans expertise ou titre de RSSI.
    - Des expériences négatives, où les RSSI locaux, influencés par leur hiérarchie directe, ont parfois légitimé le non-respect des règles globales.
    - Des contraintes organisationnelles, avec des difficultés à convaincre la direction générale d'augmenter rapidement les effectifs dédiés, faute de soutien hiérarchique.



[Q187] Chantiers prioritaires 2026 : Quels sont vos 3 chantiers prioritaires en 2026 ?

Parmi les **Grandes entreprises**, les chantiers prioritaires sont :

- **46%** Conformité réglementaire et/ou normative ;
- **43%** Usages IA en priorité la sécurité de l'IA dans votre organisation ;
- **43%** Gestion de vos tiers ;
- **40%** Gouvernance de la cybersécurité ;
- **27%** Détection et proactivité ;
- **21%** Réponse et remédiation ;
- **21%** Gestion des assets (tout domaine : applicatif, hardware, etc.) ;
- **19%** Sensibilisation Cloud : transition et/ou sécurité de vos services dans le cloud Protection des données (tout type de données) ;
- **8%** Souveraineté et indépendance numérique de votre organisation ;
- **25%** Autre comme la protection des données (tous types), de la sécurité des systèmes industriels et de leur cyber résilience, du Zéro Trust, de la réduction de l'obsolescence, de la sécurisation des réseaux et des Active Directory, de la détection et sécurisation des assets OT via un EDR, de l'IAM/IAG, du MFA résistant au phishing, de la classification des données et de la prévention des pertes (DLP), de la sécurité du Cloud, de la gestion de la surface exposée, et de l'intégration de la partie OT dans la gouvernance cybersécurité.

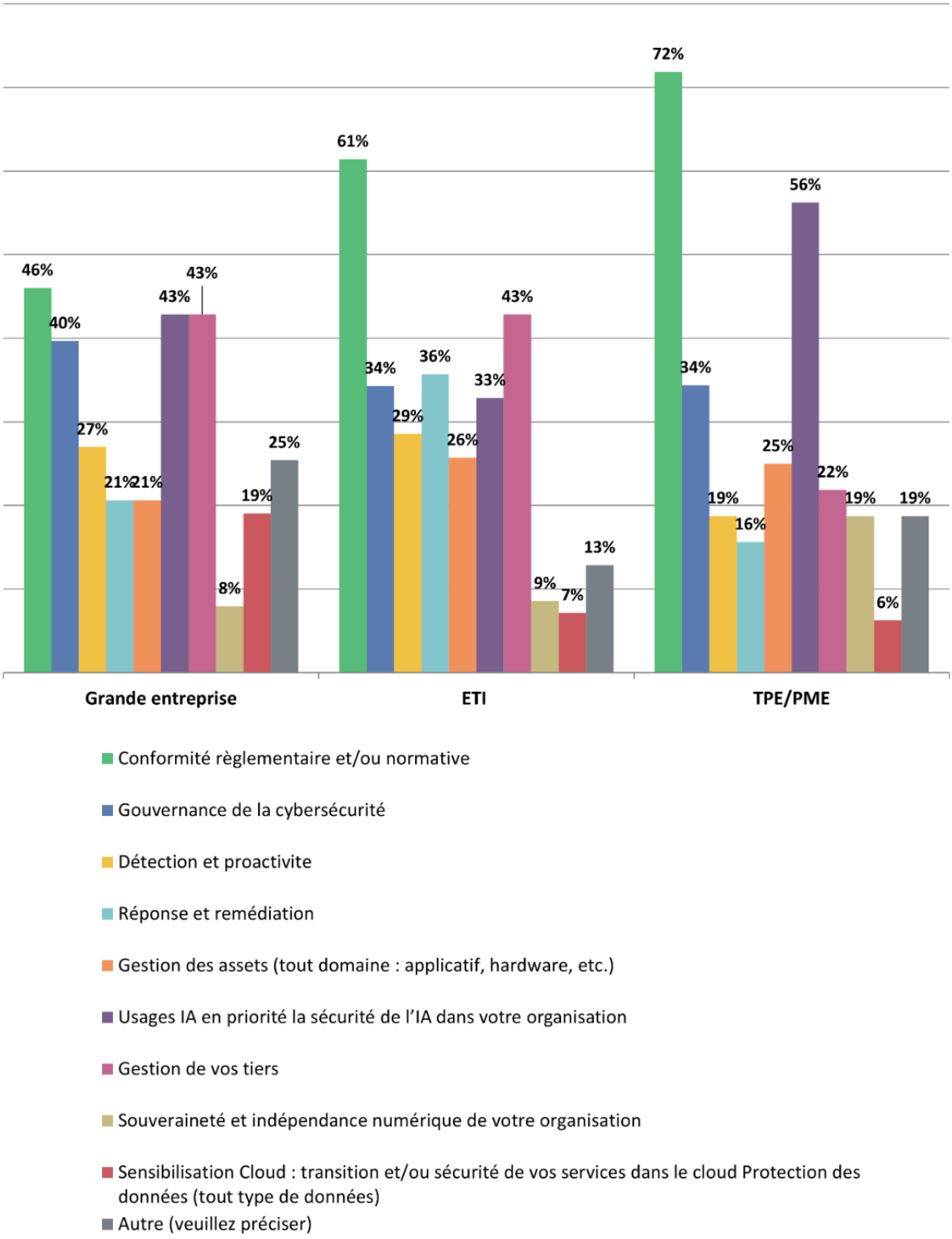
Parmi les **ETI**, les chantiers prioritaires sont :

- **61%** Conformité réglementaire et/ou normative ;
- **43%** Gestion de vos tiers ;
- **36%** Réponse et remédiation ;
- **34%** Gouvernance de la cybersécurité ;
- **33%** Usages IA en priorité la sécurité de l'IA dans votre organisation ;
- **29%** Détection et proactivité ;
- **26%** Gestion des assets (tout domaine : applicatif, hardware, etc.) ;
- **9%** Souveraineté et indépendance numérique de votre organisation ;

- **7%** Sensibilisation Cloud : transition et/ou sécurité de vos services dans le cloud Protection des données (tout type de données) ;
- **13%** Autre comme audit de sécurité, sensibilisation générale, sauvegarde externalisée, cybersécurité industrielle, contrôle d'accès aux données, généralisation des habilitations (comme le MFA sur le SI interne), segmentation des réseaux, rationalisation dans un contexte économique tendu, et intégration de la sécurité dans les projets.

Parmi les **TPE/PME,** les chantiers prioritaires sont :

- **72%** Conformité réglementaire et/ou normative ;
- **56%** Usages IA en priorité la sécurité de l'IA dans votre organisation ;
- **34%** Gouvernance de la cybersécurité ;
- **25%** Gestion des assets (tout domaine : applicatif, hardware, etc.) ;
- **22%** Gestion de vos tiers ;
- **19%** Détection et proactivité ;
- **19%** Souveraineté et indépendance numérique de votre organisation ;
- **16%** Réponse et remédiation ;
- **6%** Sensibilisation Cloud : transition et/ou sécurité de vos services dans le cloud Protection des données (tout type de données) ;
- **19%** Autre comme l'intégration de nouvelles technologies de cybersécurité, la gestion des habilitations, la mise en place d'une protection contre les malwares polymorphes avec l'aide de l'IA et d'experts, le management des données, la création d'un SOC, ainsi que la qualification SecNumCloud.


46%
40%
27%
21%
21%
43%
43%
8%
19%
25%
61%
34%
29%
36%
26%
33%
43%
9%
7%
13%
72%
34%
19%
16%
25%
56%
22%
19%
6%
19%
Grande entreprise
ETI
TPE/PME
Conformité règlementaire et/ou normative
Gouvernance de la cybersécurité
Détection et proactivite
Réponse et remédiation
Gestion des assets (tout domaine : applicatif, hardware, etc.)
Usages IA en priorité la sécurité de l'IA dans votre organisation
Gestion de vos tiers
Souveraineté et indépendance numérique de votre organisation
Sensibilisation Cloud : transition et/ou sécurité de vos services dans le cloud Protection des données (tout type de données)
Autre (veuillez préciser)

[Q188] Budget et ROI : Quelles méthodes utilisez-vous pour justifier votre budget cybersécurité et en mesurer le ROI ? *(Plusieurs réponses possibles)*

Voici les méthodes utilisées par les **Grandes entreprises** :

- **86%** Priorisation des investissements en fonction des risques métiers identifiés (ex : protection des données critiques, conformité réglementaire) ;
- **34%** Indicateurs clés (KPI) : Utilisation de métriques pour démontrer l'efficacité des dépenses (ex : réduction du nombre d'incidents, temps de détection/résolution) ;
- **48%** Benchmark sectoriel : Comparaison des budgets et des coûts avec ceux d'autres organisations du secteur ;
- **11%** Retour sur expérience : Mise en avant des économies réalisées grâce à la prévention (ex : coûts évités liés à des incidents majeurs) ;
- **30%** Retour sur expérience : Mise en avant du chiffrage d'un incident connu (en propre ou d'une autre organisation) ;
- **66%** Collaboration avec la direction : Présentation de scénarios de risque et d'impact financier pour convaincre les décideurs ;
- **13%** Autre notamment par l'utilisation de la quantification des risques cyber (CRQ) et des pertes financières évitées, l'intégration dans des programmes pluriannuels avec un ratio Cyber/IT, ou encore la négociation des primes d'assurance. Certains s'appuient sur des benchmarks sectoriels (budget IT/CA) ou des collaborations avec des cabinets de conseil pour structurer leur démarche.

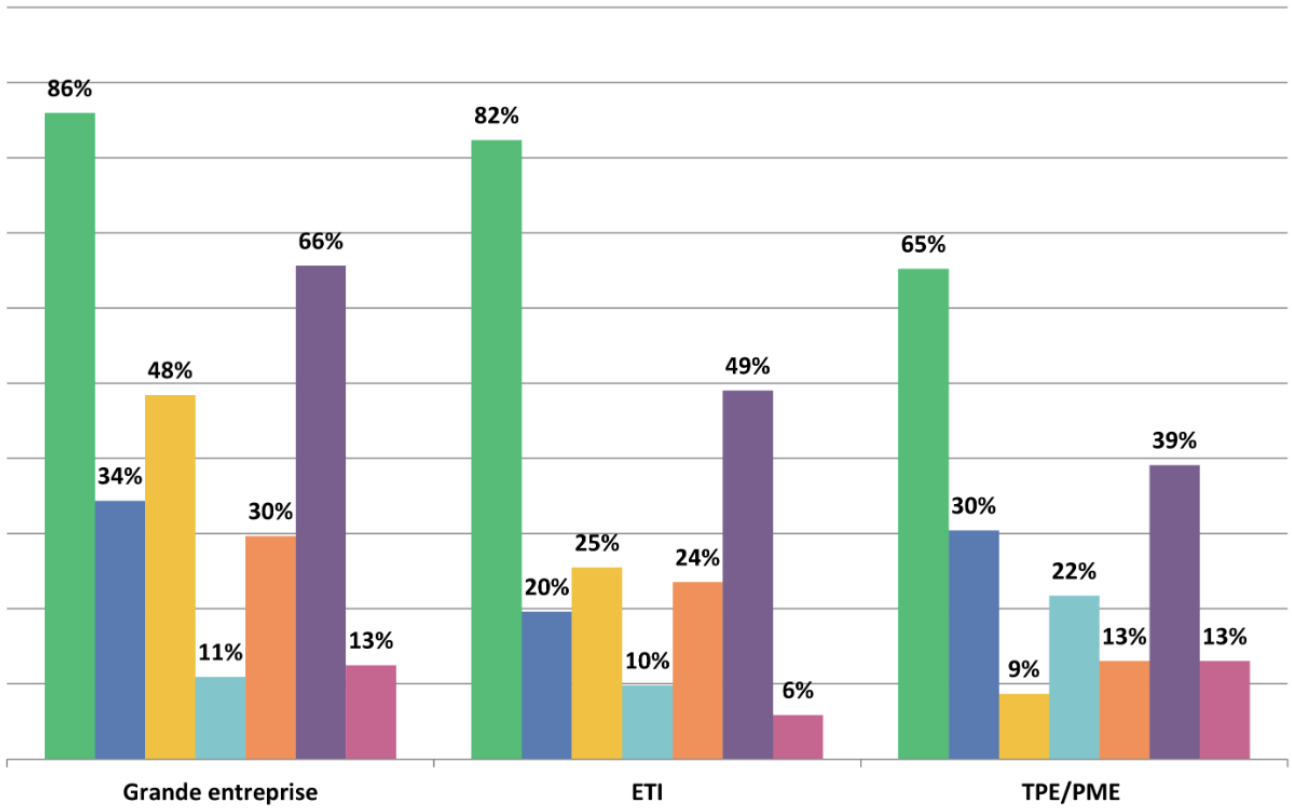
Voici les méthodes utilisées par les **ETI** :

- **82%** Priorisation des investissements en fonction des risques métiers identifiés (ex : protection des données critiques, conformité réglementaire) ;
- **20%** Indicateurs clés (KPI) : Utilisation de métriques pour démontrer l'efficacité des dépenses (ex : réduction du nombre d'incidents, temps de détection/résolution) ;
- **25%** Benchmark sectoriel : Comparaison des budgets et des coûts avec ceux d'autres organisations du secteur ;
- **10%** Retour sur expérience : Mise en avant des économies réalisées grâce à la prévention (ex : coûts évités liés à des incidents majeurs) ;

- **24%** Retour sur expérience : Mise en avant du chiffrage d'un incident connu (en propre ou d'une autre organisation) ;
- **49%** Collaboration avec la direction : Présentation de scénarios de risque et d'impact financier pour convaincre les décideurs ;
- **6%** Autre notamment pour renforcer la différenciation commerciale et marketing, tout en répondant aux exigences croissantes des clients—que ce soit pour décrocher des contrats ou maintenir leur confiance.

Voici les méthodes utilisées par les **TPE/PME** :

- **65%** Priorisation des investissements en fonction des risques métiers identifiés (ex : protection des données critiques, conformité réglementaire) ;
- **30%** Indicateurs clés (KPI) : Utilisation de métriques pour démontrer l'efficacité des dépenses (ex : réduction du nombre d'incidents, temps de détection/résolution) ;
- **9%** Benchmark sectoriel : Comparaison des budgets et des coûts avec ceux d'autres organisations du secteur ;
- **22%** Retour sur expérience : Mise en avant des économies réalisées grâce à la prévention (ex : coûts évités liés à des incidents majeurs) ;
- **13%** Retour sur expérience : Mise en avant du chiffrage d'un incident connu (en propre ou d'une autre organisation) ;
- **39%** Collaboration avec la direction : Présentation de scénarios de risque et d'impact financier pour convaincre les décideurs ;
- **13%** Autre principalement pour répondre aux exigences clients (audits, contrats) ou éviter des pertes commerciales.



- Priorisation des investissements en fonction des risques métiers identifiés (ex : protection des données critiques, conformité réglementaire).
- Indicateurs clés (KPI) : Utilisation de métriques pour démontrer l'efficacité des dépenses (ex : réduction du nombre d'incidents, temps de détection/résolution).
- Benchmark sectoriel : Comparaison des budgets et des coûts avec ceux d'autres organisations du secteur.
- Retour sur expérience : Mise en avant des économies réalisées grâce à la prévention (ex : coûts évités liés à des incidents majeurs).
- Retour sur expérience : Mise en avant du chiffrage d'un incident connu (en propre ou d'une autre organisation).
- Collaboration avec la direction : Présentation de scénarios de risque et d'impact financier pour convaincre les décideurs.
- Autre (veuillez préciser)

[Q189] Honey Pots : des « clochettes » indispensables : Avez-vous déjà mis en place cette stratégie ?

Parmi les **Grandes entreprises** :

- **8%** ont répondu : oui, nous utilisons des Honey Pots et ils nous ont permis de détecter des tentatives d'intrusion non identifiées par nos autres outils (ex. : scans malveillants, attaques ciblées) ;
- **11%** ont répondu : oui, nous les testons en environnement contrôlé avant un déploiement à grande échelle, pour évaluer leur efficacité et leur impact ;
- **23%** ont répondu : oui et nous combinons Honey Pots et autres outils pour une détection multi-couches (ex. : Honey Pots pour les leurres + EDR pour la surveillance des endpoints) ;
- **11%** ont répondu : oui, mais l'intérêt reste à démontrer ;
- **21%** ont répondu : non, nous n'avons pas les ressources internes (expertise, temps, budget) pour les maintenir et les surveiller 24/7 ;
- **8%** ont répondu : non, en raison des risques juridiques/éthiques (conséquences juridiques vis à vis des attaquants, collecte de données sensibles, etc.) ;
- **32%** ont répondu : non, nous privilégions d'autres solutions (SIEM avancé, EDR, analyse comportementale, etc.), jugées plus adaptées à nos besoins ;
- **11%** ont répondu : non, mais c'est à l'étude ;
- **13%** ont répondu : Autres. Les retours révèlent une approche mitigée des Honey Pots, souvent perçus comme trop artisanaux, chronophages ou peu rentables : plusieurs organisations ont testé ou utilisé cette solution de manière limitée, mais l'ont abandonnée faute de retour sur investissement, de temps pour l'exploitation, ou en raison de la gestion des faux positifs. Certains soulignent aussi un manque de maturité du marché et une préférence pour des alternatives plus intégrées (comme les SIEM ou l'EDR), tandis que d'autres expriment un scepticisme quant à leur efficacité réelle ou n'y ont tout simplement pas réfléchi.

Parmi les **ETI** :

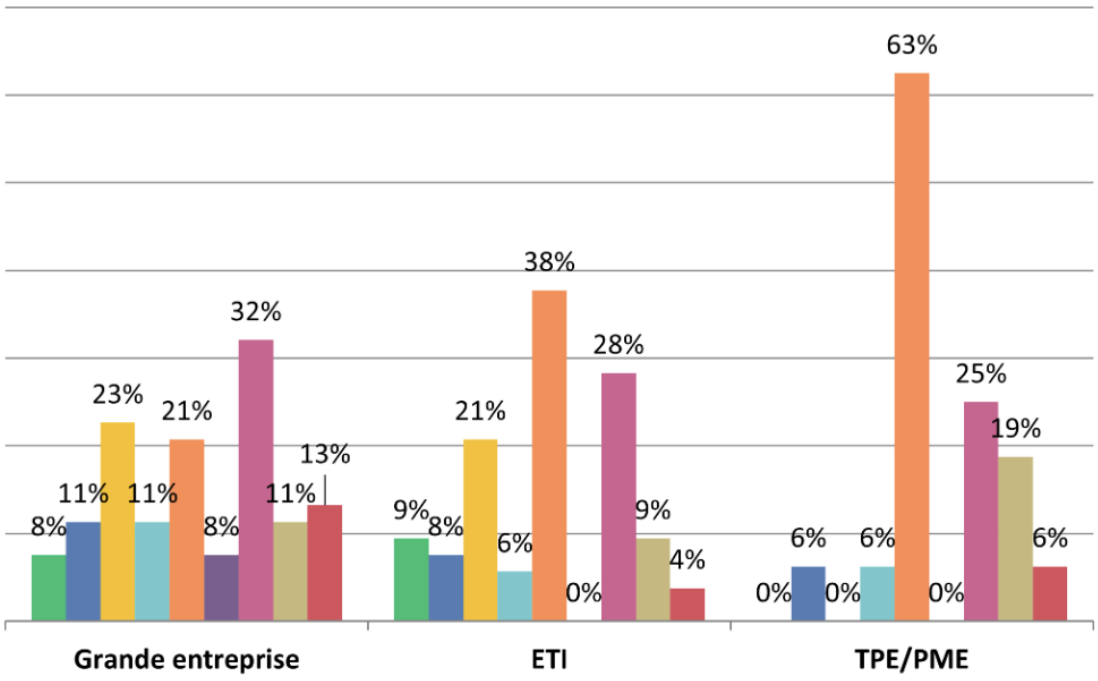
- **9%** ont répondu : oui, nous utilisons des Honey Pots et ils nous ont permis de détecter des tentatives d'intrusion non identifiées par nos autres outils (ex. : scans malveillants, attaques ciblées) ;

- **8%** ont répondu : oui, nous les testons en environnement contrôlé avant un déploiement à grande échelle, pour évaluer leur efficacité et leur impact ;
- **21%** ont répondu : oui et nous combinons Honey Pots et autres outils pour une détection multi-couches (ex. : Honey Pots pour les leurres + EDR pour la surveillance des endpoints) ;
- **6%** ont répondu : oui, mais l'intérêt reste à démontrer ;
- **38%** ont répondu : non, nous n'avons pas les ressources internes (expertise, temps, budget) pour les maintenir et les surveiller 24/7 ;
- **0%** ont répondu : non, en raison des risques juridiques/éthiques (conséquences juridiques vis à vis des attaquants, collecte de données sensibles, etc.) ;
- **28%** ont répondu : non, nous privilégions d'autres solutions (SIEM avancé, EDR, analyse comportementale, etc.), jugées plus adaptées à nos besoins ;
- **9%** ont répondu : non, mais c'est à l'étude ;
- **4%** ont répondu : Autres. Les retours révèlent une approche mitigée des Honey Pots, souvent perçus comme trop artisanaux, chronophages ou peu rentables : plusieurs organisations ont testé ou utilisé cette solution de manière limitée, mais l'ont abandonnée faute de retour sur investissement, de temps pour l'exploitation, ou en raison de la gestion des faux positifs. Certains soulignent aussi un manque de maturité du marché et une préférence pour des alternatives plus intégrées (comme les SIEM ou l'EDR), tandis que d'autres expriment un scepticisme quant à leur efficacité réelle ou n'y ont tout simplement pas réfléchi.

Parmi les **TPE/PME** :

- **0%** ont répondu : oui, nous utilisons des Honey Pots et ils nous ont permis de détecter des tentatives d'intrusion non identifiées par nos autres outils (ex. : scans malveillants, attaques ciblées) ;
- **6%** ont répondu : oui, nous les testons en environnement contrôlé avant un déploiement à grande échelle, pour évaluer leur efficacité et leur impact ;
- **0%** ont répondu : oui et nous combinons Honey Pots et autres outils pour une détection multi-couches (ex. : Honey Pots pour les leurres + EDR pour la surveillance des endpoints) ;
- **6%** ont répondu : oui, mais l'intérêt reste à démontrer ;
- **63%** ont répondu : non, nous n'avons pas les ressources internes (expertise, temps, budget) pour les maintenir et les surveiller 24/7 ;

- **0%** ont répondu : non, en raison des risques juridiques/éthiques (conséquences juridiques vis à vis des attaquants, collecte de données sensibles, etc.) ;
- **25%** ont répondu : non, nous privilégions d'autres solutions (SIEM avancé, EDR, analyse comportementale, etc.), jugées plus adaptées à nos besoins ;
- **19%** ont répondu : non, mais c'est à l'étude ;
- **6%** ont répondu : Autres. Les retours révèlent une approche mitigée des Honey Pots, souvent perçus comme trop artisanaux, chronophages ou peu rentables : plusieurs organisations ont testé ou utilisé cette solution de manière limitée, mais l'ont abandonnée faute de retour sur investissement, de temps pour l'exploitation, ou en raison de la gestion des faux positifs. Certains soulignent aussi un manque de maturité du marché et une préférence pour des alternatives plus intégrées (comme les SIEM ou l'EDR), tandis que d'autres expriment un scepticisme quant à leur efficacité réelle ou n'y ont tout simplement pas réfléchi.

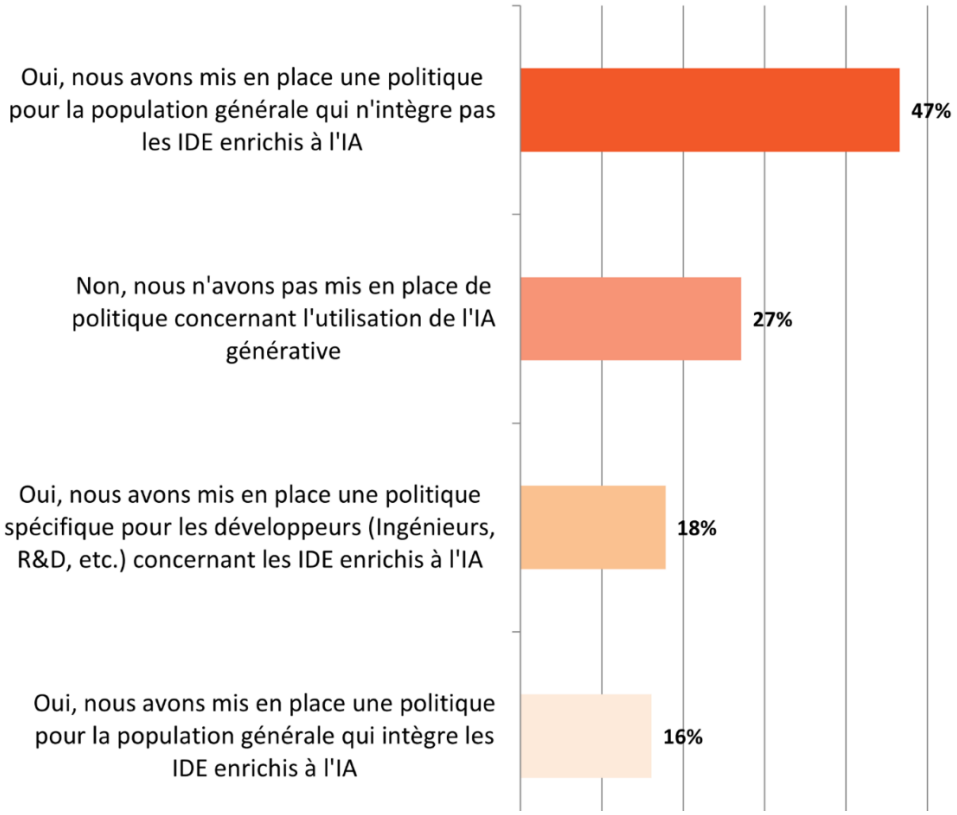


- Oui, nous utilisons des Honey Pots et ils nous ont permis de détecter des tentatives d'intrusion non identifiées par nos autres outils (ex. : scans malveillants, attaques ciblées).
- Oui, nous les testons en environnement contrôlé avant un déploiement à grande échelle, pour évaluer leur efficacité et leur impact.
- Oui, et nous combinons Honey Pots et autres outils pour une détection multi-couches (ex. : Honey Pots pour les leurres + EDR pour la surveillance des endpoints).
- Oui, mais l'intérêt reste à démontrer.
- Non, nous n'avons pas les ressources internes (expertise, temps, budget) pour les maintenir et les surveiller 24/7.
- Non, en raison des risques juridiques/éthiques (conséquences juridiques vis à vis des attaquants, collecte de données sensibles, etc.).
- Non, nous privilégions d'autres solutions (SIEM avancé, EDR, analyse comportementale, etc.), jugées plus adaptées à nos besoins.
- Non, mais c'est à l'étude.
- Autre (veuillez préciser)

[Q190] Politique IA générative et IDE enrichis à l'IA : Avez-vous défini et appliqué une politique concernant l'utilisation de l'IA générative et notamment de l'installation des environnements de développement intégrés (IDE) enrichis à l'IA ? (Plusieurs réponses possibles)

Globalement :

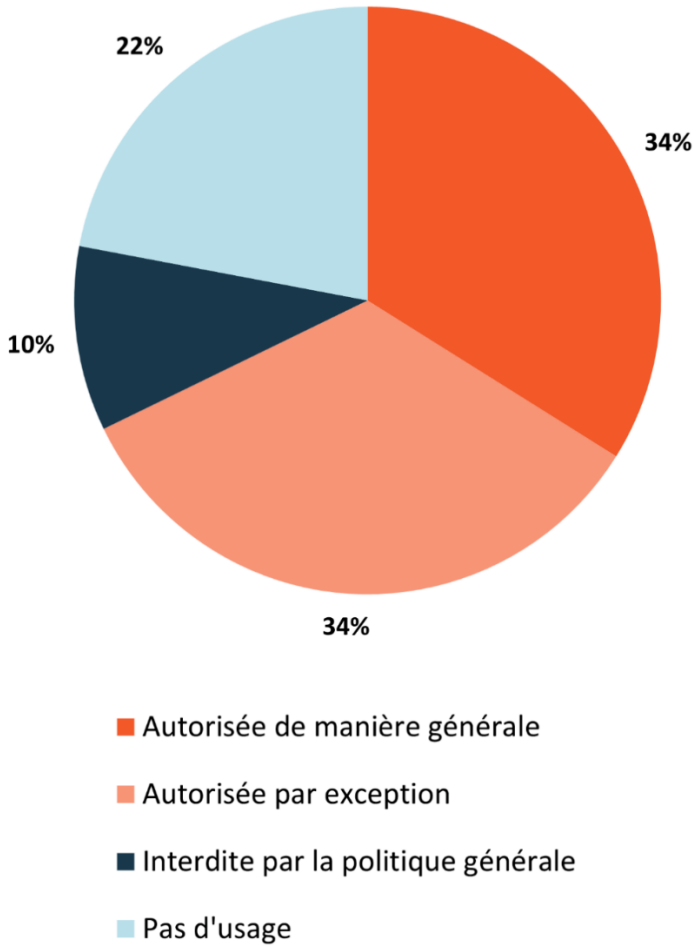
- **47%** ont mis en place une politique pour la population générale qui n'intègre pas les IDE enrichis à l'IA ;
- **27%** n'ont pas mis en place de politique concernant l'utilisation de l'IA générative ;
- **18%** ont mis en place une politique spécifique pour les développeurs (Ingénieurs, R&D, etc.) concernant les IDE enrichis à l'IA ;
- **16%** ont mis en place une politique pour la population générale qui intègre les IDE enrichis à l'IA.



Dans le cadre de l'utilisation des IDE enrichis à l'IA, l'installation de ces IDE

Globalement :

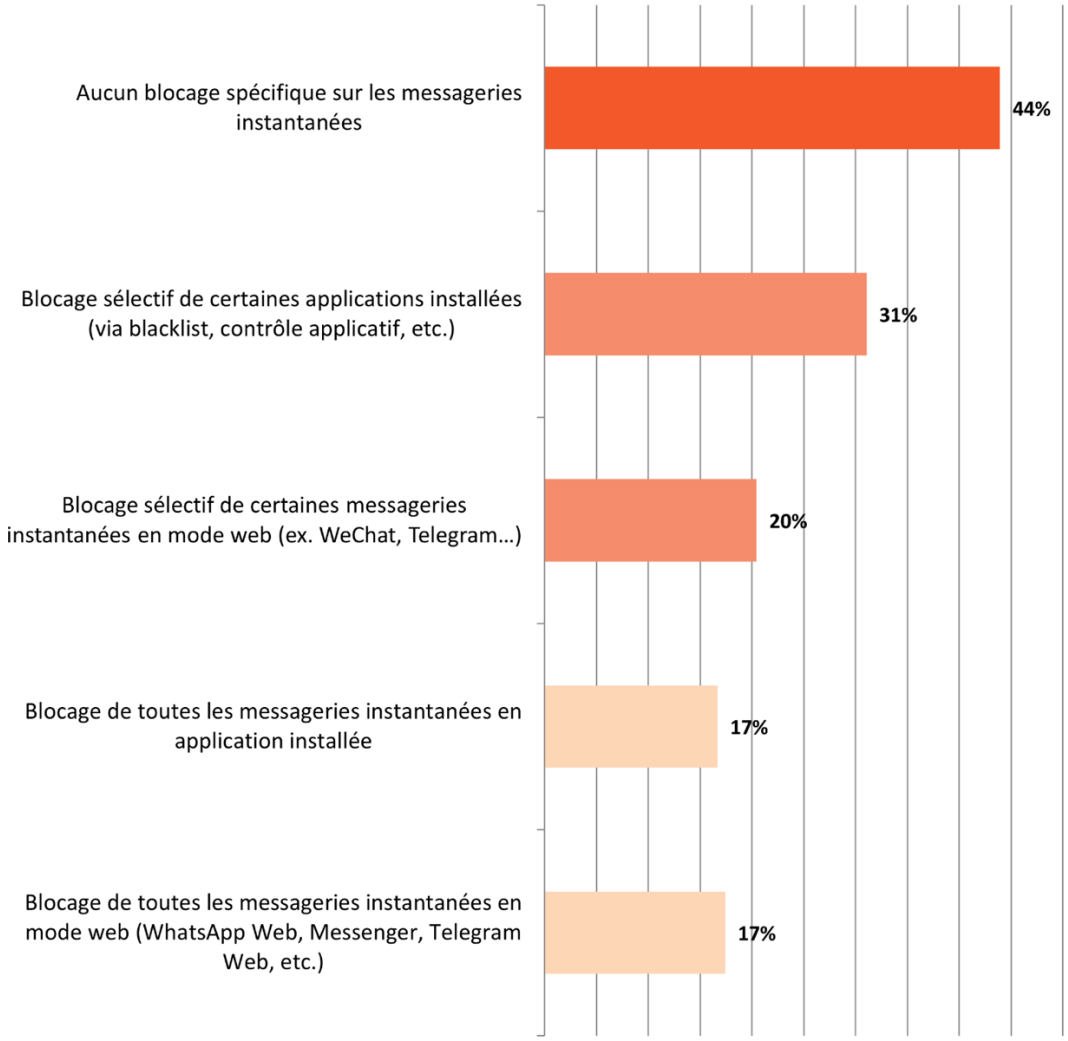
- **34%** l'autorisent de manière générale ;
- **34%** l'autorisent par exception ;
- **10%** l'interdisent par la politique générale ;
- **22%** n'ont pas d'usage.



[Q191] Usage d'applications de messagerie sur les postes de travail de l'organisation : Votre organisation bloque-t-elle l'usage de services de messagerie, d'e-mail ou de stockage en ligne lorsqu'ils ne sont pas gérés ou approuvés par l'entreprise ?

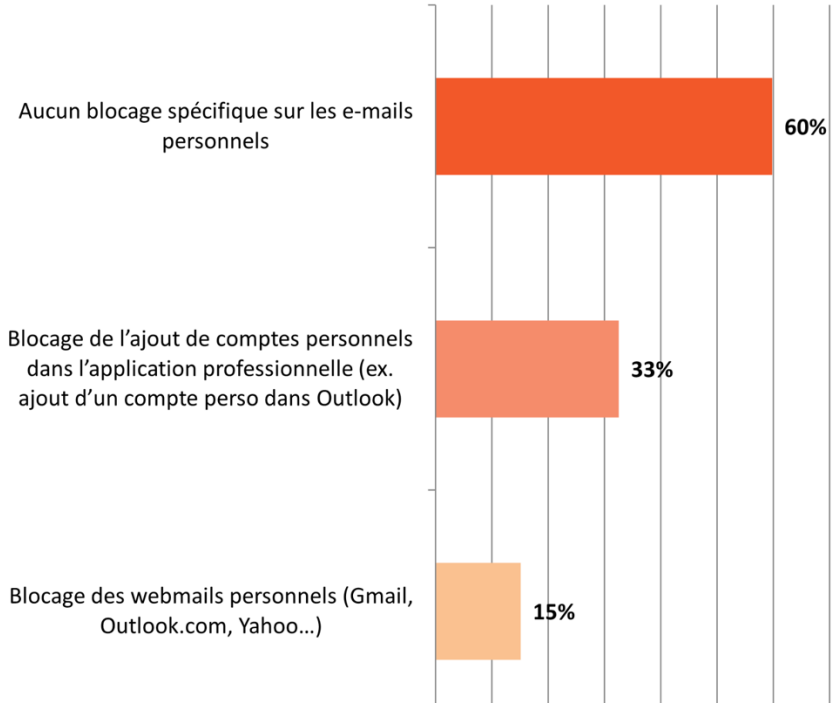
Messagerie instantanée : Globalement :

- **44%** n'ont mis en place aucun blocage spécifique sur les messageries instantanées ;
- **31%** ont mis en place un blocage sélectif de certaines applications installées (via blacklist, contrôle applicatif, etc.) ;
- **20%** ont mis en place un blocage sélectif de certaines messageries instantanées en mode web (ex. WeChat, Telegram…) ;
- **17%** ont mis en place un blocage de toutes les messageries instantanées en application installée ;
- **17%** ont mis en place un blocage de toutes les messageries instantanées en mode web (WhatsApp Web, Messenger, Telegram Web, etc.).



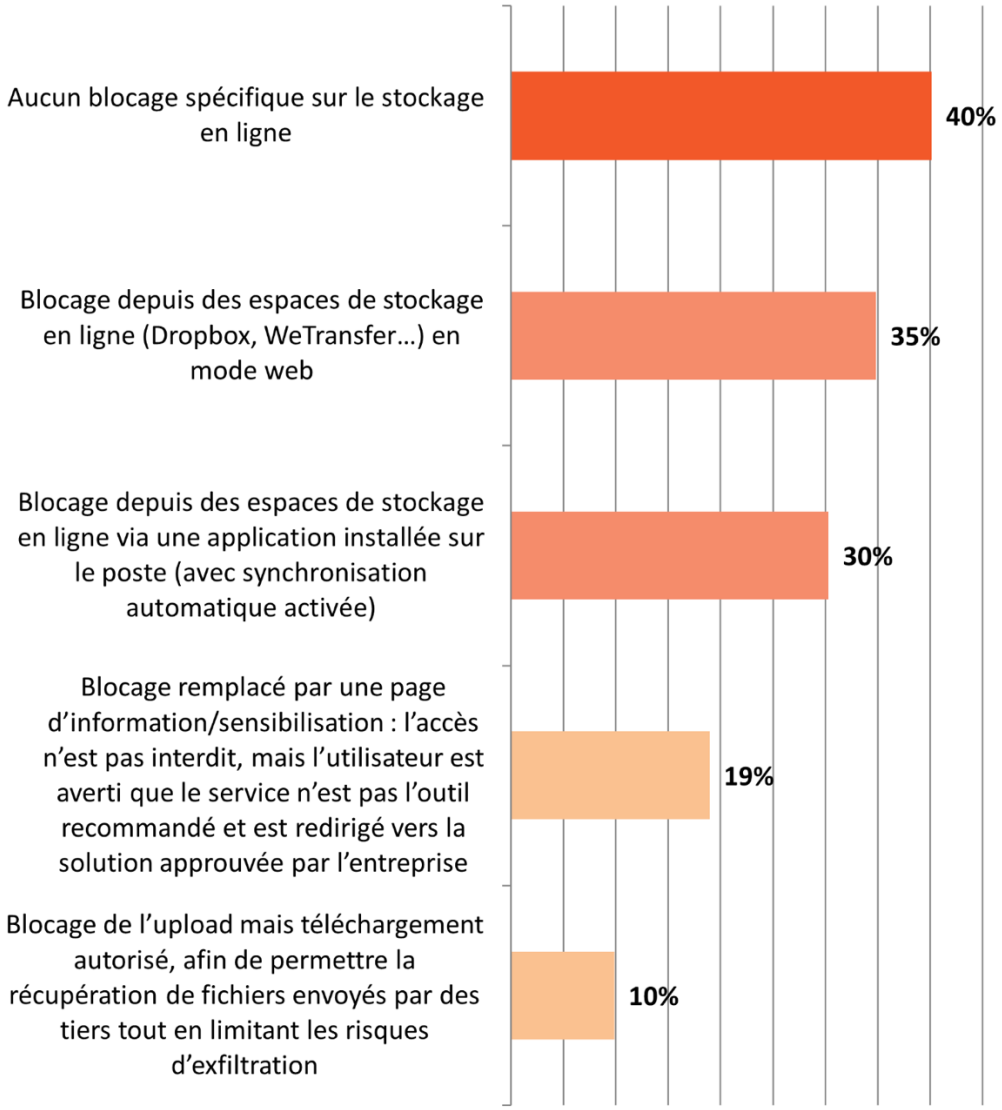
Emails : Globalement :

- **60%** n'ont mis en place aucun blocage spécifique sur les e-mails personnels ;
- **33%** ont mis en place un blocage de l'ajout de comptes personnels dans l'application professionnelle (ex. ajout d'un compte perso dans Outlook) ;
- **15%** ont mis en place un blocage des webmails personnels (Gmail, Outlook.com, Yahoo...).



Stockage en ligne : Globalement :

- **40%** n'ont mis en place aucun blocage spécifique sur le stockage en ligne ;
- **35%** ont mis en place un blocage depuis des espaces de stockage en ligne (Dropbox, WeTransfer…) en mode web ;
- **30%** ont mis en place un blocage depuis des espaces de stockage en ligne via une application installée sur le poste (avec synchronisation automatique activée) ;
- **19%** ont mis en place un blocage remplacé par une page d'information/sensibilisation : l'accès n'est pas interdit, mais l'utilisateur est averti que le service n'est pas l'outil recommandé et est redirigé vers la solution approuvée par l'entreprise ;
- **10%** ont mis en place un blocage de l'upload mais téléchargement autorisé, afin de permettre la récupération de fichiers envoyés par des tiers tout en limitant les risques d'exfiltration.


Aucun blocage spécifique sur le stockage en ligne
40%
Blocage depuis des espaces de stockage en ligne (Dropbox, WeTransfer…) en mode web
35%
Blocage depuis des espaces de stockage en ligne via une application installée sur le poste (avec synchronisation automatique activée)
30%
Blocage remplacé par une page d'information/sensibilisation : l'accès n'est pas interdit, mais l'utilisateur est averti que le service n'est pas l'outil recommandé et est redirigé vers la solution approuvée par l'entreprise
19%
Blocage de l'upload mais téléchargement autorisé, afin de permettre la récupération de fichiers envoyés par des tiers tout en limitant les risques d'exfiltration
10%

[Q192] Préparation au Cyber Resilience Act : Êtes-vous directement impactés par le CRA et devez-vous mettre en place les mesures prévues par ce règlement ?

Parmi les **Grandes entreprises** :

- **35%** sont directement impactés par le CRA et ont pris connaissance du règlement. Les projets de mise en conformité sont en cours afin d'être prêts à la date du 11 septembre 2026 ;
- **12%** sont directement impactés par le CRA et ont pris connaissance du règlement. Les projets de mise en conformité sont en cours mais ils ne seront pas prêts pour le 11 septembre 2026 ;
- **15%** sont directement impactés par le CRA mais les travaux de mise en conformité n'ont pas démarré ;
- **38% ne sont pas directement impactés** par le CRA mais sont clients de fournisseurs impactés par le CRA.

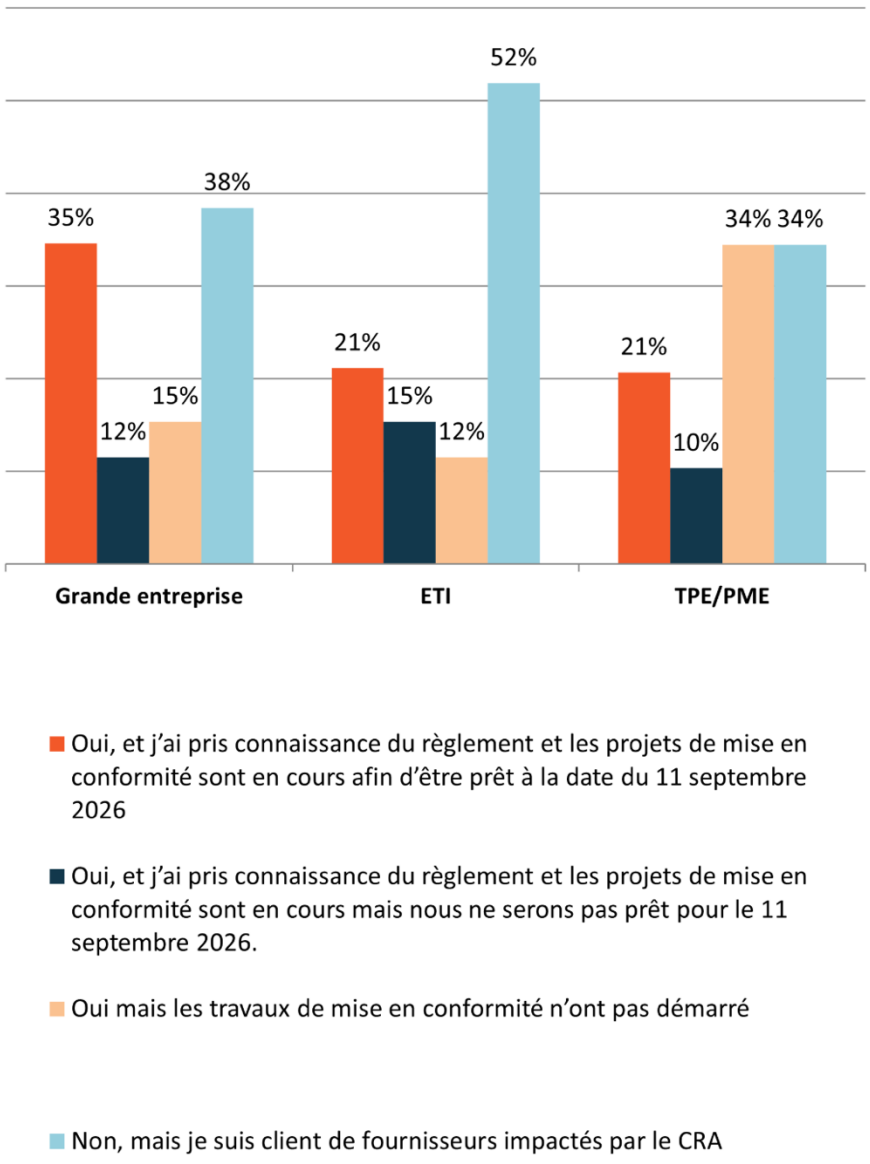
Parmi les **ETI** :

- **21%** sont directement impactés par le CRA et ont pris connaissance du règlement. Les projets de mise en conformité sont en cours afin d'être prêts à la date du 11 septembre 2026.
- **15%** sont directement impactés par le CRA et ont pris connaissance du règlement. Les projets de mise en conformité sont en cours mais ils ne seront pas prêts pour le 11 septembre 2026 ;
- **12%** sont directement impactés par le CRA mais les travaux de mise en conformité n'ont pas démarré ;
- **52%** ne sont pas directement impactés par le CRA mais sont clients de fournisseurs impactés par le CRA.

Parmi les **TPE/PME** :

- **21%** sont directement impactés par le CRA et ont pris connaissance du règlement. Les projets de mise en conformité sont en cours afin d'être prêts à la date du 11 septembre 2026 ;
- **10%** sont directement impactés par le CRA et ont pris connaissance du règlement. Les projets de mise en conformité sont en cours mais ils ne seront pas prêts pour le 11 septembre 2026 ;
- **34%** sont directement impactés par le CRA mais les travaux de mise en conformité n'ont pas démarré ;

- **34%** ne sont pas directement impactés par le CRA mais sont clients de fournisseurs impactés par le CRA.

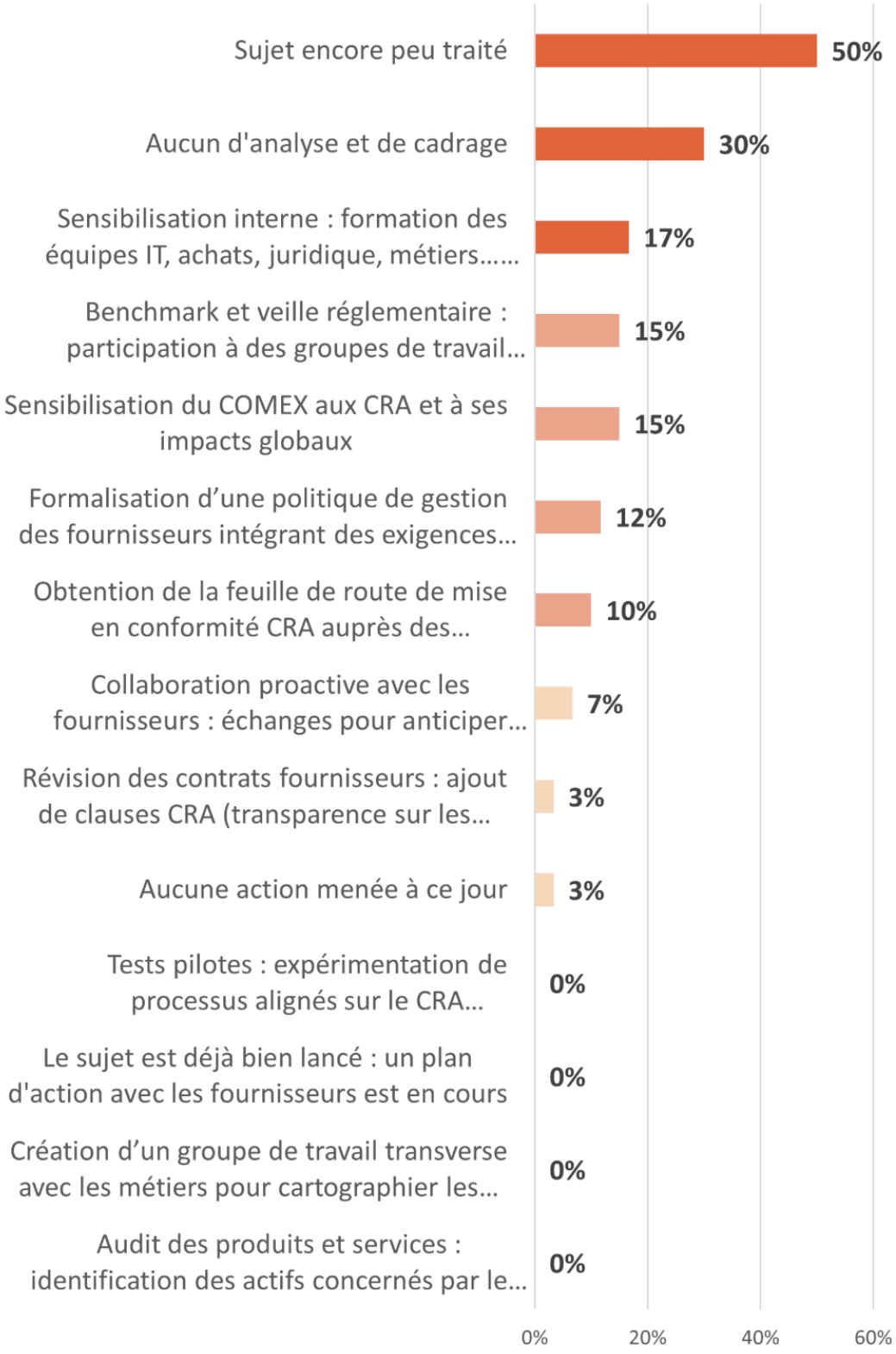


Si non, quelles actions concrètes avez-vous déjà entreprises pour préparer votre organisation au Cyber Resilience Act (CRA) ? *(Plusieurs réponses possibles)*

Globalement, les actions mises en place sont pour :

- **50%** un sujet encore peu traité ;
- **30%** Aucune action d'analyse et de cadrage ;

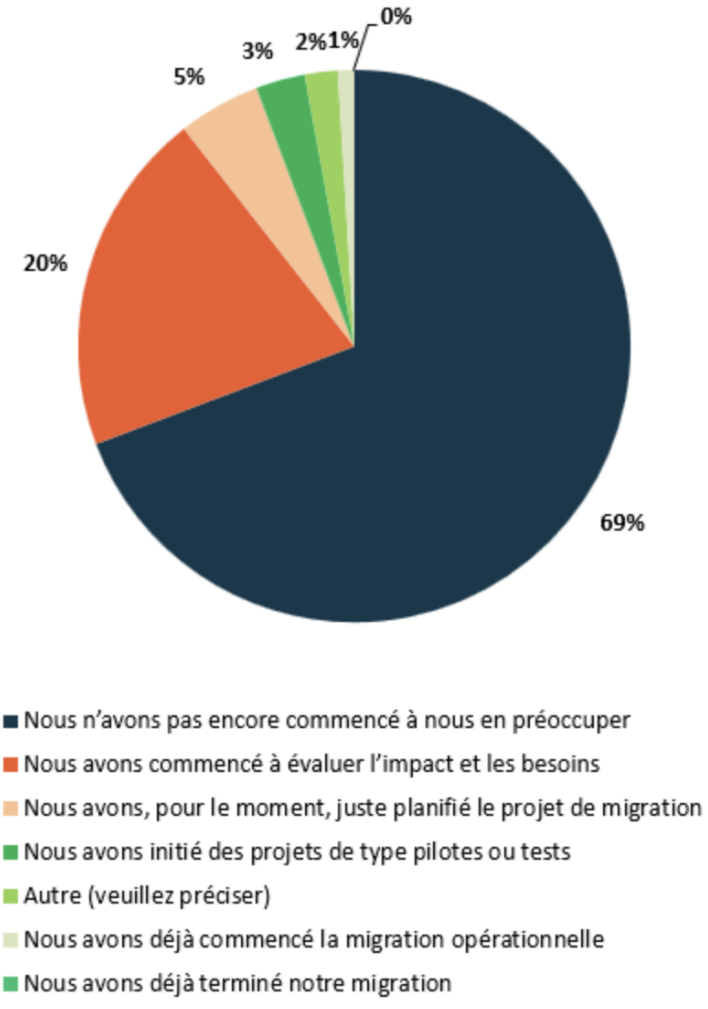
- **17%** Une sensibilisation interne : formation des équipes IT, achats, juridique, métiers… sur la réglementation et leurs implications opérationnelles vis à vis des fournisseurs (futurs et en cours) ;
- **15%** Une sensibilisation du COMEX aux CRA et à ses impacts globaux ;
- **15%** un benchmark et veille réglementaire : participation à des groupes de travail (CESIN, ANSSI…), utilisation de ressources (ENISA, Commission européenne…), suivi des évolutions du texte ;
- **12%** une formalisation d'une politique de gestion des fournisseurs intégrant des exigences spécifiques liées au CRA (clauses, obligations, responsabilités) ;
- **10%** une obtention de la feuille de route de mise en conformité CRA auprès des fournisseurs critiques ;
- **7%** une collaboration proactive avec les fournisseurs : échanges pour anticiper leurs plans de conformité et leurs capacités à répondre aux exigences du CRA ;
- **3%** aucune action menée à ce jour ;
- **3%** une révision des contrats fournisseurs : ajout de clauses CRA (transparence sur les vulnérabilités, engagements de mise à jour, obligations de notification…) ;
- **0%** un audit des produits et services : identification des actifs concernés par le CRA (logiciels embarqués, équipements industriels, IoT, services cloud…) et recensement des éditeurs qui sont donc concernés par le CRA ;
- **0%** une création d'un groupe de travail transverse avec les métiers pour cartographier les produits concernés ;
- **0%** un sujet déjà bien lancé : un plan d'action avec les fournisseurs est en cours ;
- **0%** des tests pilotes : expérimentation de processus alignés sur le CRA (documentation des correctifs, industrialisation du MCS, tests de résilience, gestion des vulnérabilités…).


Sujet encore peu traité
50%
Aucun d'analyse et de cadrage
30%
Sensibilisation interne : formation des équipes IT, achats, juridique, métiers……
17%
Benchmark et veille réglementaire : participation à des groupes de travail…
15%
Sensibilisation du COMEX aux CRA et à ses impacts globaux
15%
Formalisation d'une politique de gestion des fournisseurs intégrant des exigences…
12%
Obtention de la feuille de route de mise en conformité CRA auprès des…
10%
Collaboration proactive avec les fournisseurs : échanges pour anticiper…
7%
Révision des contrats fournisseurs : ajout de clauses CRA (transparence sur les…
3%
Aucune action menée à ce jour
3%
Tests pilotes : expérimentation de processus alignés sur le CRA…
0%
Le sujet est déjà bien lancé : un plan d'action avec les fournisseurs est en cours
0%
Création d'un groupe de travail transverse avec les métiers pour cartographier les…
0%
Audit des produits et services : identification des actifs concernés par le…
0%
0%
20%
40%
60%

[Q193] Migration vers la PQC : Avez-vous lancé le projet de migration PQC ?

Globalement :

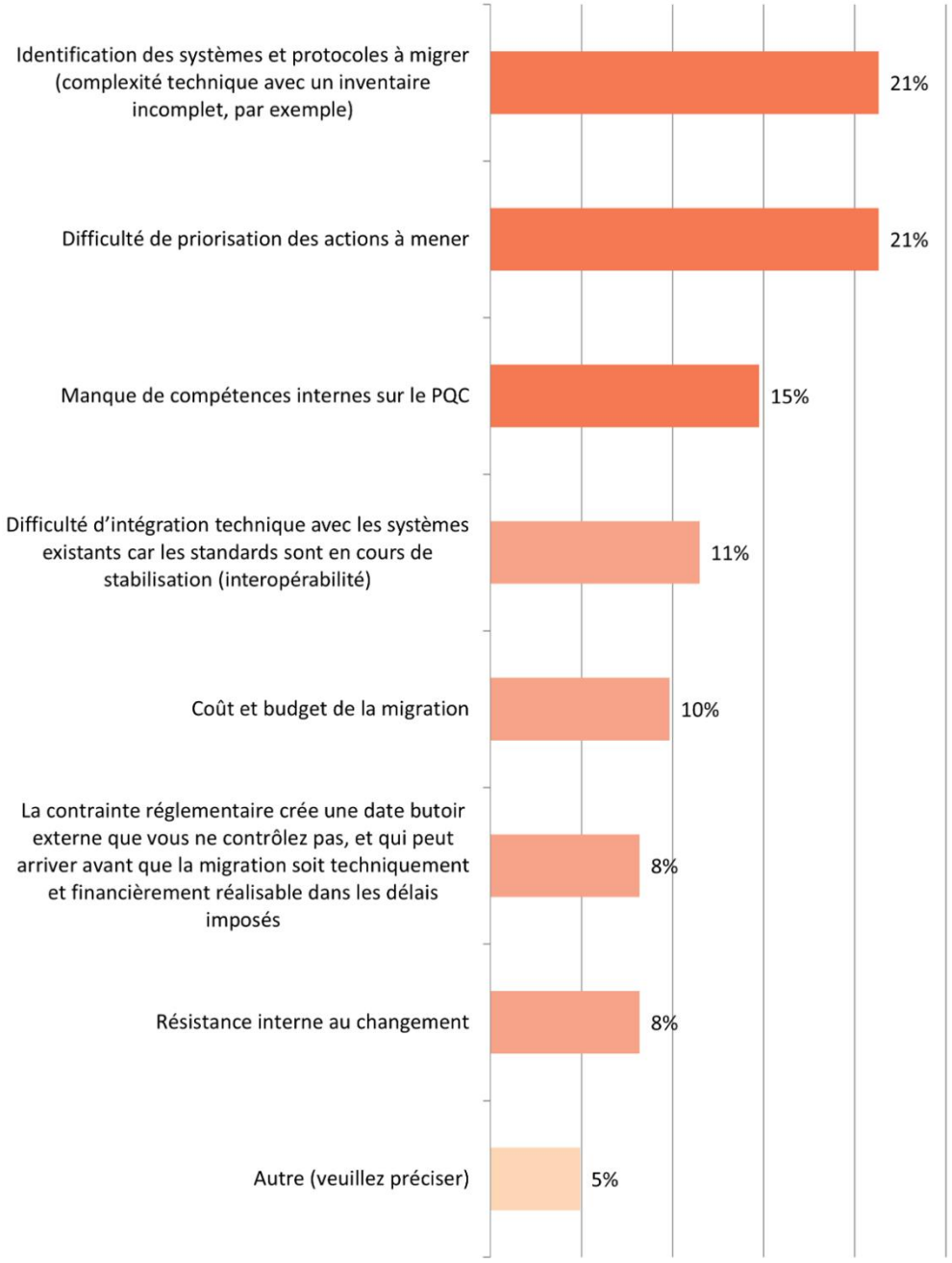
- 69% n'ont pas encore commencé à s'en préoccuper ;
- 20% ont commencé à évaluer l'impact et les besoins ;
- 5% ont, pour le moment, juste planifié le projet de migration ;
- 3% ont initié des projets de type pilotes ou tests ;
- 2% ont répondu « Autre » notamment car ils ont ajouté une clause contractuelle demandant aux fournisseurs la livraison d'une version post quantique dès disponibilité de cette dernière ou encore parce qu'ils ont documenté les changements opérationnels mais pas encore imposé le changement ;
- 1% ont déjà commencé la migration opérationnelle ;
- 0% ont déjà terminé leur migration.



Si vous avez commencé la migration ou effectué des tests PQC, quelles sont les principales difficultés rencontrées ? (Plusieurs réponses possibles)

Globalement, les principales difficultés rencontrées sont :

- **21%** Identification des systèmes et protocoles à migrer (complexité technique avec un inventaire incomplet, par exemple) ;
- **21%** Difficulté de priorisation des actions à mener ;
- **15%** Manque de compétences internes sur le PQC ;
- **11%** Difficulté d'intégration technique avec les systèmes existants car les standards sont en cours de stabilisation (interopérabilité) ;
- **10%** Coût et budget de la migration ;
- **8%** La contrainte réglementaire crée une date butoir externe que vous ne contrôlez pas, et qui peut arriver avant que la migration soit techniquement et financièrement réalisable dans les délais imposés ;
- **8%** Résistance interne au changement ;
- **5%** Autre soit car la transition vers le post-quantique est freinée par un manque de solutions disponibles chez les éditeurs, des contraintes de ressources humaines et financières, ou encore une difficulté à prioriser un sujet perçu comme encore lointain. La surcharge globale des équipes, rendant la mobilisation et l'adaptation des pratiques (comme la mise à jour des algorithmes et cyphers) plus complexes, est aussi mise en avant.


Identification des systèmes et protocoles à migrer (complexité technique avec un inventaire incomplet, par exemple)
21%
Difficulté de priorisation des actions à mener
21%
Manque de compétences internes sur le PQC
15%
Difficulté d'intégration technique avec les systèmes existants car les standards sont en cours de stabilisation (interopérabilité)
11%
Coût et budget de la migration
10%
La contrainte réglementaire crée une date butoir externe que vous ne contrôlez pas, et qui peut arriver avant que la migration soit techniquement et financièrement réalisable dans les délais imposés
8%
Résistance interne au changement
8%
Autre (veuillez préciser)
5%

[Q194] Patching applicatif : réactivité vs. risque : Comment arbitrez-vous entre la nécessité de patcher rapidement vos librairies applicatives et le risque d'introduire un nouveau risque ? (Plusieurs choix possibles)

Parmi les **Grandes entreprises** :

- **81%** ont priorisé selon la criticité (CVSS, exposition, exploit disponible) et appliquent des SLA différenciés : fast-track sous 72h pour les vulnérabilités critiques, cycles mensuels pour le reste ;
- **35%** documentent chaque arbitrage : si on ne patche pas immédiatement, on acte la décision d'accepter le risque. On pose des mesures compensatoires (WAF, segmentation) et on fixe une échéance (liée à l'acceptation de risque) ;
- **29%** combinent plusieurs de ces approches ci-dessus ;
- **23%** appliquent exclusivement les patchs critiques dès leur publication, en acceptant de nouveaux risques ;
- **16%** demandent l'avis du réseau (communauté CESIN, etc.) ;
- **13%** réduisent d'abord leur surface de dépendances. Pour le reste, la maturité de leurs tests automatisés leur permettent de pousser un patch en production rapidement avec un niveau de confiance suffisant ;
- **10%** valident chaque mise à jour avant déploiement via un registre proxy interne : épinglage des versions, vérification des signatures, audit des packages. On ne patche que ce qu'on a vérifié ;
- **6%** automatisent le pipeline de patch pour patcher rapidement sans sacrifier la qualité. Le cycle sécurité est découplé du cycle de release fonctionnel ;
- **3%** ont répondu « Autre » notamment car les pratiques sont hétérogènes selon les organisations : certaines privilégient un patch rapide, d'autres un déploiement progressif avec tests, ou encore s'appuient sur des outils, des partenaires ou des mesures compensatoires lorsque le patch n'est pas possible. L'arbitrage dépend donc de la maturité, des responsabilités et du niveau de criticité ;
- **0%** retardent les mises à jour jusqu'à avoir mené des audits internes, externes ou via des outils automatisés (SBOM, analyse de code, etc.) sur les nouvelles versions des bibliothèques.

Parmi les **ETI** :

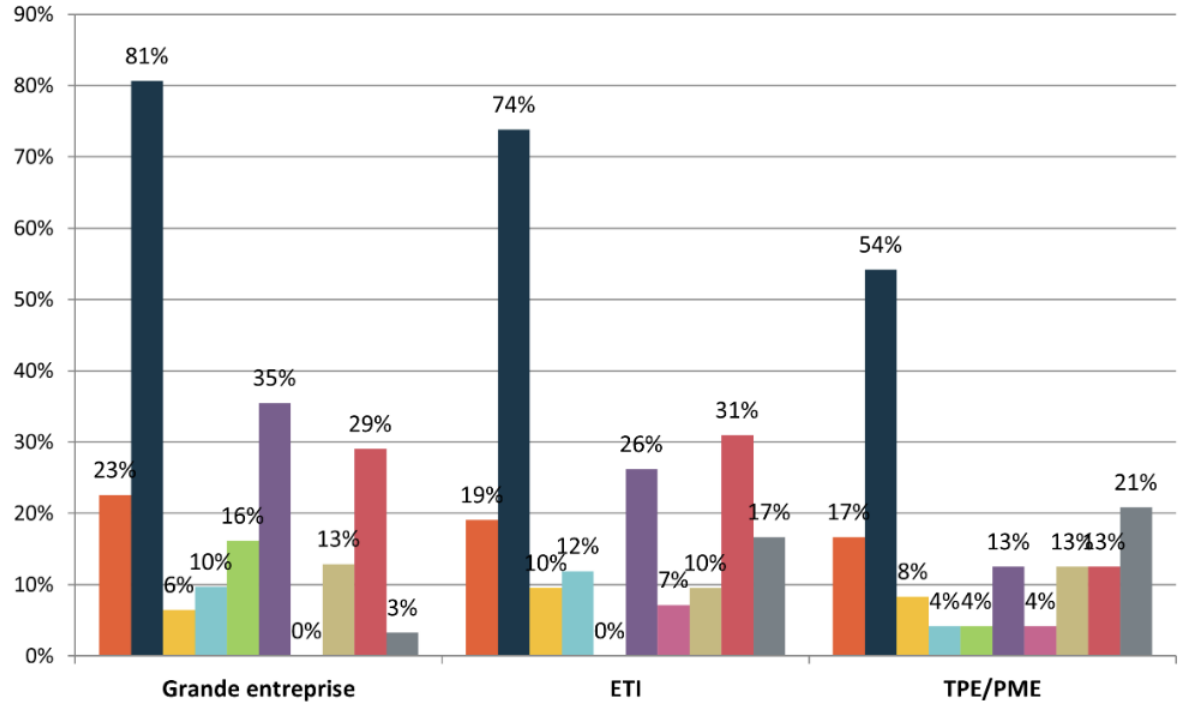
- **74%** priorisent selon la criticité (CVSS, exposition, exploit disponible) et appliquent des SLA différenciés : fast-track sous 72h pour les vulnérabilités critiques, cycles mensuels pour le reste ;
- **31%** combinent plusieurs de ces approches ci-dessus ;
- **26%** documentent chaque arbitrage : si on ne patche pas immédiatement, on acte la décision d'accepter le risque. On pose des mesures compensatoires (WAF, segmentation) et on fixe une échéance (liée à l'acceptation de risque) ;
- **19%** appliquent exclusivement les patchs critiques dès leur publication, en acceptant de nouveaux risques ;
- **17%** ont répondu « Autre » notamment car les pratiques sont hétérogènes selon les organisations : certaines privilégient un patch rapide, d'autres un déploiement progressif avec tests, ou encore s'appuient sur des outils, des partenaires ou des mesures compensatoires lorsque le patch n'est pas possible. L'arbitrage dépend donc de la maturité, des responsabilités et du niveau de criticité ;
- **12%** valident chaque mise à jour avant déploiement via un registre proxy interne : épinglage des versions, vérification des signatures, audit des packages. On ne patche que ce qu'on a vérifié ;
- **10%** automatisent le pipeline de patch pour patcher rapidement sans sacrifier la qualité. Le cycle sécurité est découplé du cycle de release fonctionnel ;
- **10%** réduisent d'abord leur surface de dépendances. Pour le reste, la maturité de leurs tests automatisés leur permettent de pousser un patch en production rapidement avec un niveau de confiance suffisant ;
- **7%** retardent les mises à jour jusqu'à avoir mené des audits internes, externes ou via des outils automatisés (SBOM, analyse de code, etc.) sur les nouvelles versions des bibliothèques ;
- **0%** demandent l'avis du réseau (communauté CESIN, etc.).

Parmi les **TPE/PME** :

- **54%** priorisent selon la criticité (CVSS, exposition, exploit disponible) et appliquent des SLA différenciés : fast-track sous 72h pour les vulnérabilités critiques, cycles mensuels pour le reste ;
- **21%** ont répondu « Autre » notamment car les pratiques sont hétérogènes selon les organisations : certaines privilégient un patch rapide, d'autres un déploiement progressif avec

tests, ou encore s'appuient sur des outils, des partenaires ou des mesures compensatoires lorsque le patch n'est pas possible. L'arbitrage dépend donc de la maturité, des responsabilités et du niveau de criticité ;

- **17%** appliquent exclusivement les patchs critiques dès leur publication, en acceptant de nouveaux risques ;
- **13%** documentent chaque arbitrage : si on ne patche pas immédiatement, on acte la décision d'accepter le risque. On pose des mesures compensatoires (WAF, segmentation) et on fixe une échéance (liée à l'acceptation de risque) ;
- **13%** réduisent d'abord leur surface de dépendances. Pour le reste, la maturité de leurs tests automatisés leur permettent de pousser un patch en production rapidement avec un niveau de confiance suffisant ;
- **13%** combinent plusieurs de ces approches ci-dessus ;
- **4%** retardent les mises à jour jusqu'à avoir mené des audits internes, externes ou via des outils automatisés (SBOM, analyse de code, etc.) sur les nouvelles versions des bibliothèques ;
- **8%** automatisent le pipeline de patch pour patcher rapidement sans sacrifier la qualité. Le cycle sécurité est découplé du cycle de release fonctionnel ;
- **4%** valident chaque mise à jour avant déploiement via un registre proxy interne : épinglage des versions, vérification des signatures, audit des packages. On ne patche que ce qu'on a vérifié ;
- **4%** demandent l'avis du réseau (communauté CESIN, etc.).



Nous appliquons exclusivement les patchs critiques dès leur publication, en acceptant de nouveaux risques.

Nous priorisons selon la criticité (CVSS, exposition, exploit disponible) et appliquons des SLA différenciés : fast-track sous 72h pour les vulnérabilités critiques, cycles mensuels pour le reste.

Nous avons automatisé le pipeline de patch pour patcher rapidement sans sacrifier la qualité. Le cycle sécurité est découplé du cycle de release fonctionnel.

Nous validons chaque mise à jour avant déploiement via un registre proxy interne : épinglage des versions, vérification des signatures, audit des packages. On ne patche que ce qu'on a vérifié.

Nous demandons l'avis à notre réseau (communauté CESIN, etc.)

Nous documentons chaque arbitrage : si on ne patche pas immédiatement, on acte la décision d'accepter le risque. Sur pose des mesures compensatoires (WAF, segmentation) et sur fixe une échéance (liée à l'acceptation de risque).

Nous retardons les mises à jour jusqu'à avoir mené des audits internes, externes ou via des outils automatisés (SBOM, analyse de code, etc.) sur les nouvelles versions des bibliothèques.

Nous réduisons d'abord notre surface de dépendances. Pour le reste, la maturité de nos tests automatisés nous permet de pousser un patch en production rapidement avec un niveau de confiance suffisant.

Nous combinons plusieurs de ces approches ci-dessus (merci de cocher les méthodes combinées)

Autre (veuillez préciser)

[Q195] Indice de Résilience Numérique (IRN) : Avez-vous adopté l'IRN ?

Parmi les **Grandes entreprises** :

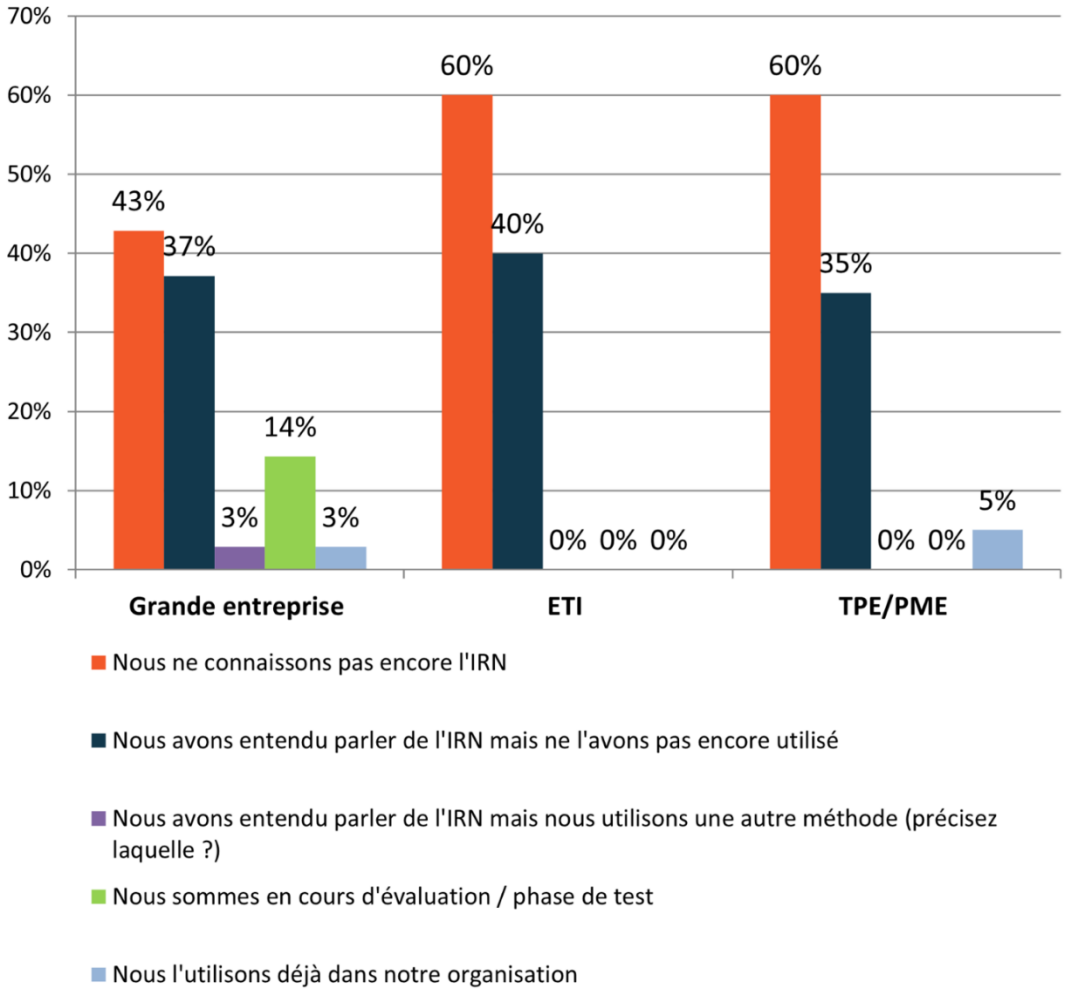
- **43%** ne connaissent pas encore l'IRN ;
- **37%** ont entendu parler de l'IRN mais ne l'utilisent pas encore ;
- **3%** ont entendu parler de l'IRN mais utilisent une autre méthode ;
- **14%** sont en cours d'évaluation / phase de test ;
- **3%** l'ont déjà utilisé dans leur organisation.

Parmi les **ETI** :

- **60%** ne connaissent pas encore l'IRN ;
- **40%** ont entendu parler de l'IRN mais ne l'utilisent pas encore ;
- **0%** ont entendu parler de l'IRN mais utilisent une autre méthode ;
- **0%** sont en cours d'évaluation / phase de test ;
- **0%** l'ont déjà utilisé dans leur organisation.

Parmi les **TPE/PME** :

- **60%** ne connaissent pas encore l'IRN ;
- **35%** ont entendu parler de l'IRN mais ne l'utilisent pas encore ;
- **0%** ont entendu parler de l'IRN mais utilisent une autre méthode ;
- **0%** sont en cours d'évaluation / phase de test ;
- **5%** l'ont déjà utilisé dans leur organisation.

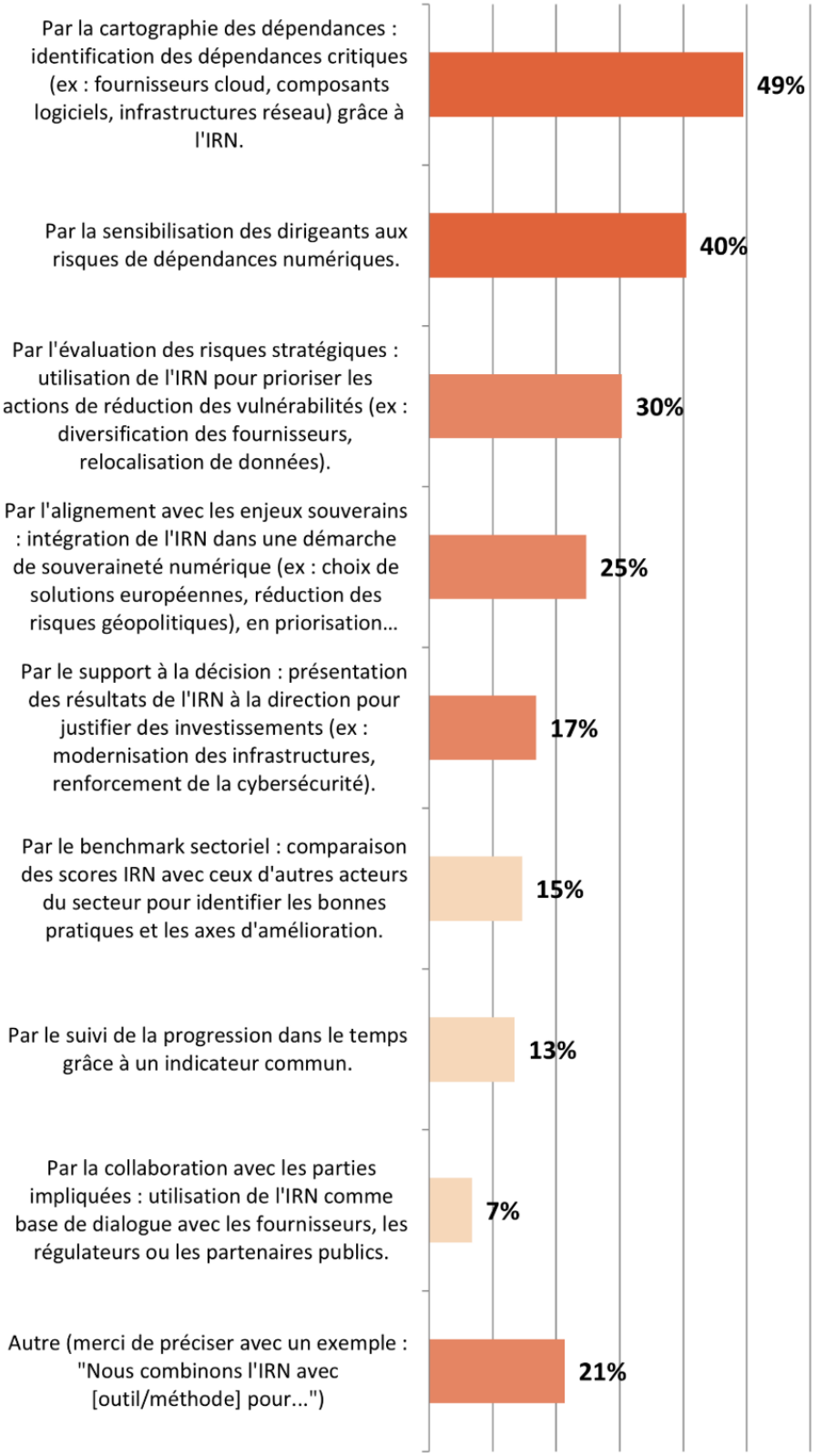


De quelle manière envisagez-vous d'utiliser l'IRN ou de quelle manière l'utilisez-vous déjà ? ***(Plusieurs réponses possibles)***

Globalement, vous envisagez ou utilisez déjà l'IRN de la manière suivante :

- **49%** Par la cartographie des dépendances : identification des dépendances critiques (ex : fournisseurs cloud, composants logiciels, infrastructures réseau) grâce à l'IRN ;
- **40%** Par la sensibilisation des dirigeants aux risques de dépendances numériques ;
- **30%** Par l'évaluation des risques stratégiques : utilisation de l'IRN pour prioriser les actions de réduction des vulnérabilités (ex : diversification des fournisseurs, relocalisation de données) ;
- **25%** Par l'alignement avec les enjeux souverains : intégration de l'IRN dans une démarche de souveraineté numérique (ex : choix de solutions européennes, réduction des risques géopolitiques), en priorisation notamment les investissements en cybersécurité et souveraineté ;

- **17%** Par le support à la décision : présentation des résultats de l'IRN à la direction pour justifier des investissements (ex : modernisation des infrastructures, renforcement de la cybersécurité) ;
- **15%** Par le benchmark sectoriel : comparaison des scores IRN avec ceux d'autres acteurs du secteur pour identifier les bonnes pratiques et les axes d'amélioration ;
- **13%** Par le suivi de la progression dans le temps grâce à un indicateur commun ;
- **7%** Par la collaboration avec les parties impliquées : utilisation de l'IRN comme base de dialogue avec les fournisseurs, les régulateurs ou les partenaires publics ;
- **21%** Autre notamment car les répondants ne connaissent pas l'IRN, n'ont pas encore étudié le sujet ou n'ont pas d'avis à ce stade, avec un besoin exprimé de clarification sur sa méthodologie et son utilité. Certains questionnent sa pertinence ou son intérêt concret, voire le perçoivent comme un indicateur supplémentaire peu utile ou sans perspective d'usage.


Par la cartographie des dépendances : identification des dépendances critiques (ex : fournisseurs cloud, composants logiciels, infrastructures réseau) grâce à l'IRN.
49%
Par la sensibilisation des dirigeants aux risques de dépendances numériques.
40%
Par l'évaluation des risques stratégiques : utilisation de l'IRN pour prioriser les actions de réduction des vulnérabilités (ex : diversification des fournisseurs, relocalisation de données).
30%
Par l'alignement avec les enjeux souverains : intégration de l'IRN dans une démarche de souveraineté numérique (ex : choix de solutions européennes, réduction des risques géopolitiques), en priorisation...
25%
Par le support à la décision : présentation des résultats de l'IRN à la direction pour justifier des investissements (ex : modernisation des infrastructures, renforcement de la cybersécurité).
17%
Par le benchmark sectoriel : comparaison des scores IRN avec ceux d'autres acteurs du secteur pour identifier les bonnes pratiques et les axes d'amélioration.
15%
Par le suivi de la progression dans le temps grâce à un indicateur commun.
13%
Par la collaboration avec les parties impliquées : utilisation de l'IRN comme base de dialogue avec les fournisseurs, les régulateurs ou les partenaires publics.
7%
Autre (merci de préciser avec un exemple : "Nous combinons l'IRN avec [outil/méthode] pour...")
21%

[Q196] Rachat important dans la cyber : Quels sont les impacts ? *(Plusieurs réponses possibles)*

Parmi les **Grandes entreprises** on constate les impacts suivants :

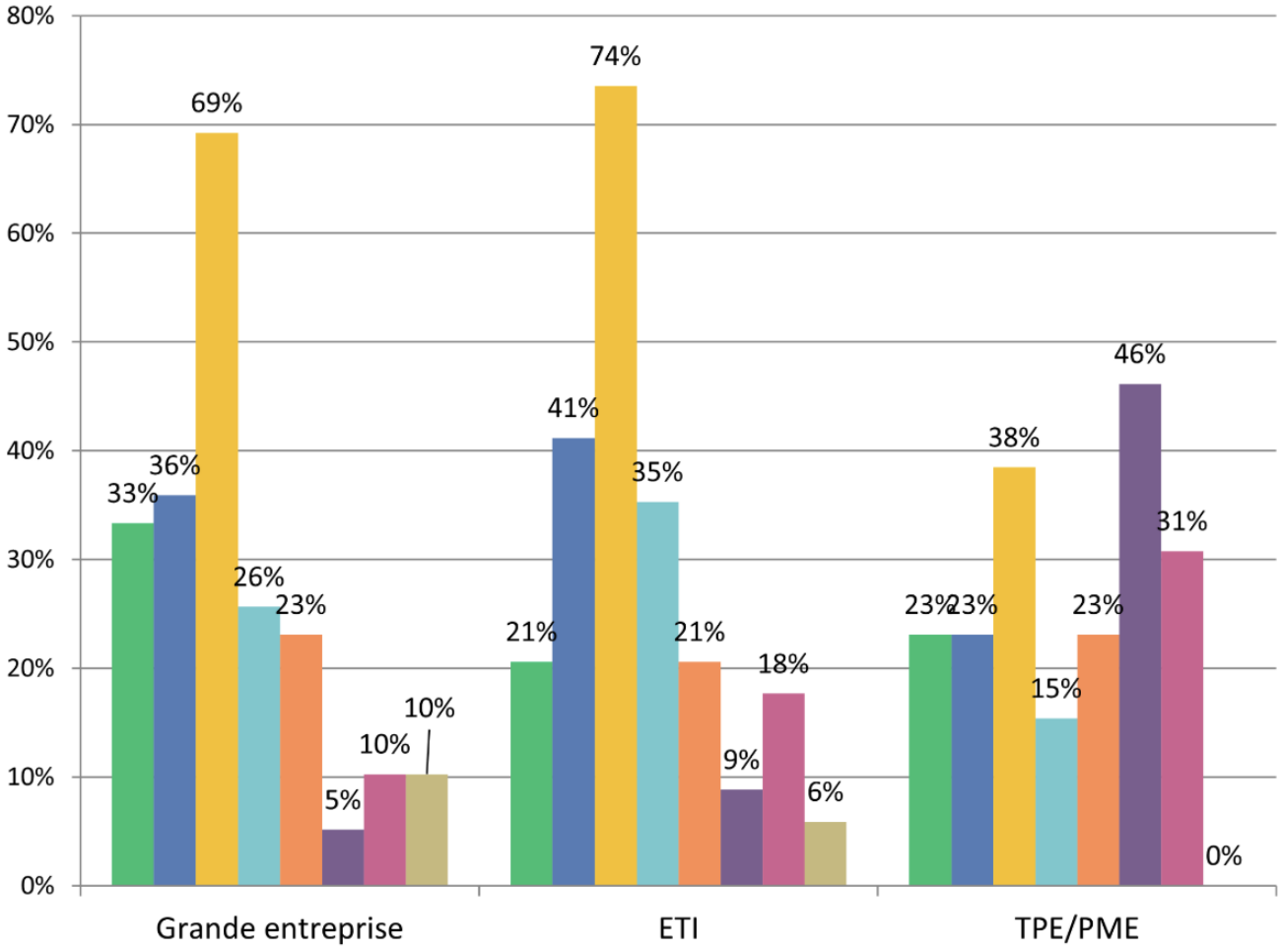
- **69%** Explosion des coûts : « Les tarifs ont augmenté après le rachat, poussant à renégocier ou à chercher des alternatives (ex : open source, acteurs européens). » ;
- **36%** Enfermement technologique : « ils ont été contraints de migrer vers une suite unique, rendant les changements futurs plus complexes et coûteux. » ;
- **33%** Offre plus complète : « Les rachats ont permis d'accéder à des solutions intégrées (ex : XDR, SOC unifié), simplifiant la gestion et réduisant les silos. » ;
- **26%** Dilution de l'innovation : « La solution rachetée a perdu en agilité, incitant à compléter avec des outils spécialisés (ex : startups, éditeurs niche). » ;
- **23%** Stratégie de diversification : « ils ont diversifié leurs fournisseurs pour éviter les dépendances et garder une flexibilité (ex : multi-cloud, solutions best-of-breed). » ;
- **10%** Aucun ;
- **10%** Autre ;
- **5%** Non concerné.

Parmi les **ETI** on constate les impacts suivants :

- **74%** Explosion des coûts : « Les tarifs ont augmenté après le rachat, poussant à renégocier ou à chercher des alternatives (ex : open source, acteurs européens). » ;
- **41%** Enfermement technologique : « ils ont été contraints de migrer vers une suite unique, rendant les changements futurs plus complexes et coûteux. » ;
- **35%** Dilution de l'innovation : « La solution rachetée a perdu en agilité, incitant à compléter avec des outils spécialisés (ex : startups, éditeurs niche). » ;
- **21%** Offre plus complète : « Les rachats ont permis d'accéder à des solutions intégrées (ex : XDR, SOC unifié), simplifiant la gestion et réduisant les silos. » ;
- **21%** Stratégie de diversification : « ils ont diversifié leurs fournisseurs pour éviter les dépendances et garder une flexibilité (ex : multi-cloud, solutions best-of-breed). » ;
- **18%** Aucun ;
- **9%** Non concerné ;
- **6%** Autre.

Parmi les **TPE/PME** on constate les impacts suivants :

- **46%** Non concerné ;
- **38%** Explosion des coûts : « Les tarifs ont augmenté après le rachat, poussant à renégocier ou à chercher des alternatives (ex : open source, acteurs européens). » ;
- **31%** Aucun ;
- **23%** Stratégie de diversification : « ils ont diversifié leurs fournisseurs pour éviter les dépendances et garder une flexibilité (ex : multi-cloud, solutions best-of-breed). » ;
- **23%** Offre plus complète : « Les rachats ont permis d'accéder à des solutions intégrées (ex : XDR, SOC unifié), simplifiant la gestion et réduisant les silos. » ;
- **23%** Enfermement technologique : « ils ont été contraints de migrer vers une suite unique, rendant les changements futurs plus complexes et coûteux. » ;
- **15%** Dilution de l'innovation : « La solution rachetée a perdu en agilité, incitant à compléter avec des outils spécialisés (ex : startups, éditeurs niche). » ;
- **0%** Autre.


80%
70%
60%
50%
40%
30%
20%
10%
0%
33%
36%
69%
26%
23%
5%
10%
10%
21%
41%
74%
35%
21%
9%
18%
6%
23%
23%
38%
15%
23%
46%
31%
0%
Grande entreprise
ETI
TPE/PME
Offre plus complète : "Les rachats ont permis d'accéder à des solutions intégrées (ex : XDR, SOC unifié), simplifiant la gestion et réduisant les silos."
Enfermement technologique : "Nous avons été contraints de migrer vers une suite unique, rendant les changements futurs plus complexes et coûteux."
Explosion des coûts : "Les tarifs ont augmenté après le rachat, nous poussant à renégocier ou à chercher des alternatives (ex : open source, acteurs européens)."
Dilution de l'innovation : "La solution rachetée a perdu en agilité, nous incitant à compléter avec des outils spécialisés (ex : startups, éditeurs niche)."
Stratégie de diversification : "Nous avons diversifié nos fournisseurs pour éviter les dépendances et garder une flexibilité (ex : multi-cloud, solutions best-of-breed)."
Nous ne sommes pas concernés.
Nous n'avons pas eu d'impacts.
Autre (merci de préciser : "Nous avons [action] car [impact observé]..."

Quelles actions avez-vous mis en œuvre en conséquence ? *(Plusieurs réponses possibles)*

Parmi les **Grandes entreprises** :

- **44%** ont engagé une revue de leurs contrats et ouvert des appels d'offres pour identifier des alternatives en vue de changer de solution ;
- **33%** ont renforcé leurs clauses contractuelles (réversibilité, portabilité des données, SLA) pour limiter leur exposition en cas de changement de stratégie d'un éditeur post-acquisition ;
- **26%** ont identifié le fait que ces rachats les ont conduits à rationaliser leur portefeuille : moins de fournisseurs, mais mieux intégrés. Ils privilégient désormais les éditeurs proposant des plateformes consolidées plutôt que des solutions ponctuelles ;
- **26%** ont fait le choix inverse : diversifier davantage leurs fournisseurs pour éviter tout enfermement. Quitte à assumer une complexité opérationnelle plus élevée ;
- **21%** n'ont pas encore observé d'impact direct, mais ils suivent ces évolutions de marché de près dans leur veille stratégique ;
- **13%** se rendent compte que ces mouvements ont accéléré leur réflexion sur le build vs buy. Pour certaines briques critiques, ils ont choisi de développer ou d'internaliser plutôt que de dépendre d'acteurs en cours de consolidation.

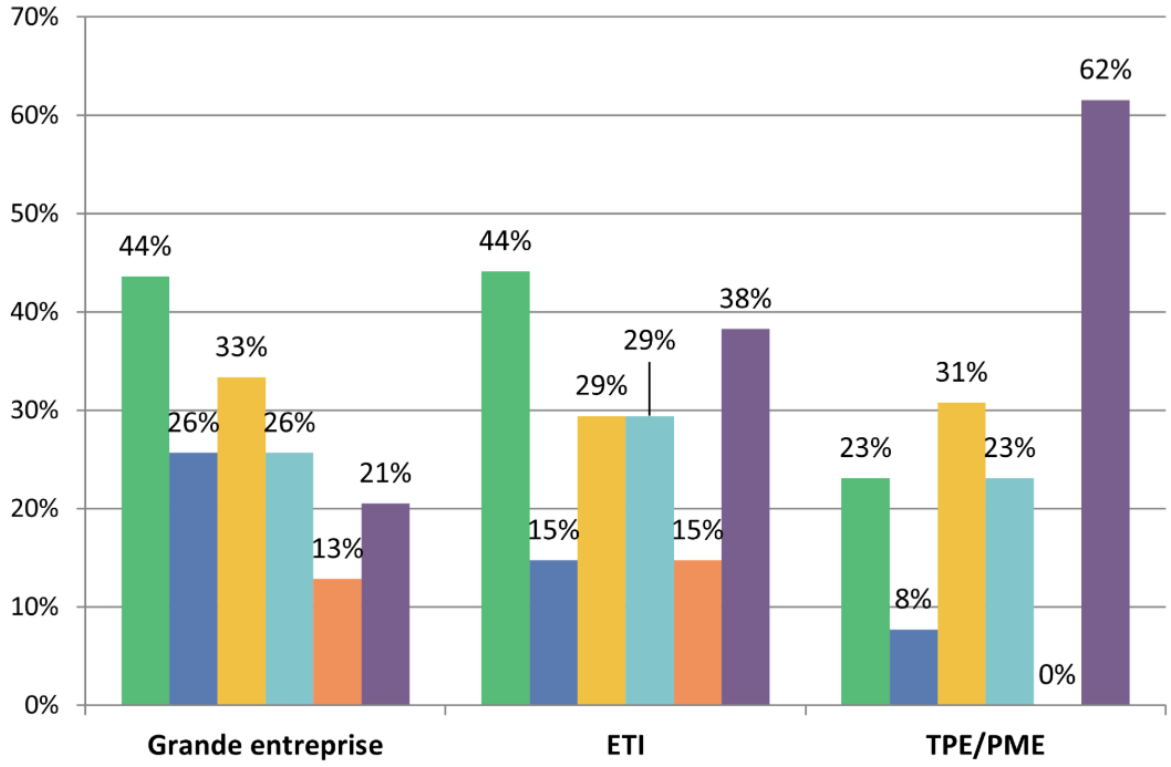
Parmi les **ETI** :

- **44%** ont engagé une revue de leurs contrats et ouvert des appels d'offres pour identifier des alternatives en vue de changer de solution ;
- **38%** n'ont pas encore observé d'impact direct, mais ils suivent ces évolutions de marché de près dans leur veille stratégique ;
- **29%** ont renforcé leurs clauses contractuelles (réversibilité, portabilité des données, SLA) pour limiter leur exposition en cas de changement de stratégie d'un éditeur post-acquisition ;
- **29%** ont fait le choix inverse : diversifier davantage leurs fournisseurs pour éviter tout enfermement. Quitte à assumer une complexité opérationnelle plus élevée ;
- **15%** ont identifié le fait que ces rachats les ont conduits à rationaliser leur portefeuille : moins de fournisseurs, mais mieux intégrés. Ils privilégient désormais les éditeurs proposant des plateformes consolidées plutôt que des solutions ponctuelles ;

- **15%** se rendent compte que ces mouvements ont accéléré leur réflexion sur le build vs buy. Pour certaines briques critiques, ils ont choisi de développer ou d'internaliser plutôt que de dépendre d'acteurs en cours de consolidation.

Parmi les TPE/PME :

- **62%** n'ont pas encore observé d'impact direct, mais ils suivent ces évolutions de marché de près dans leur veille stratégique ;
- **31%** ont renforcé leurs clauses contractuelles (réversibilité, portabilité des données, SLA) pour limiter leur exposition en cas de changement de stratégie d'un éditeur post-acquisition ;
- **23%** ont engagé une revue de leurs contrats et ouvert des appels d'offres pour identifier des alternatives en vue de changer de solution ;
- **23%** ont fait le choix inverse : diversifier davantage leurs fournisseurs pour éviter tout enfermement. Quitte à assumer une complexité opérationnelle plus élevée ;
- **8%** ont identifié le fait que ces rachats les ont conduits à rationaliser leur portefeuille : moins de fournisseurs, mais mieux intégrés. Ils privilégient désormais les éditeurs proposant des plateformes consolidées plutôt que des solutions ponctuelles ;
- **0%** se rendent compte que ces mouvements ont accéléré leur réflexion sur le build vs buy. Pour certaines briques critiques, ils ont choisi de développer ou d'internaliser plutôt que de dépendre d'acteurs en cours de consolidation.

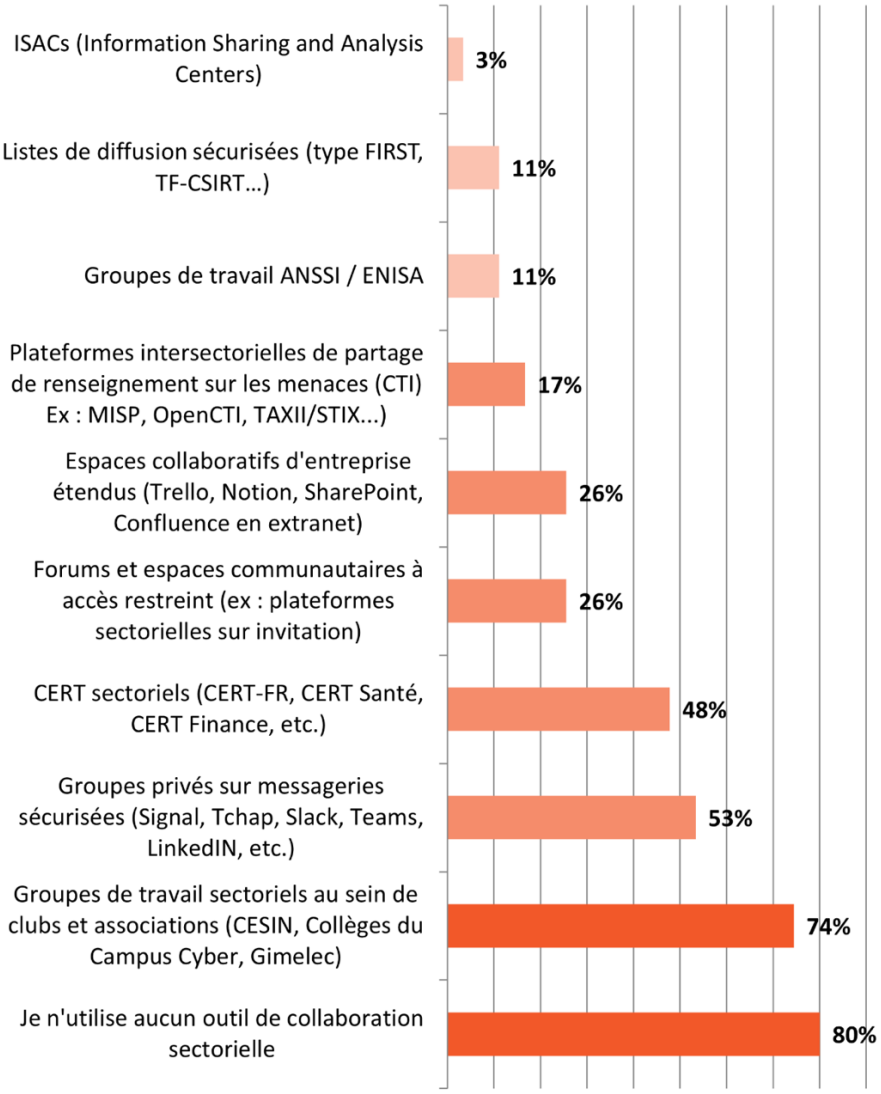


- Nous avons engagé une revue de nos contrats et ouvert des appels d'offres pour identifier des alternatives en vue de changer de solution.
- Ces rachats nous ont conduits à rationaliser notre portefeuille : moins de fournisseurs, mais mieux intégrés. Nous privilégions désormais les éditeurs proposant des plateformes consolidées plutôt que des solutions ponctuelles.
- Nous avons renforcé nos clauses contractuelles (réversibilité, portabilité des données, SLA) pour limiter notre exposition en cas de changement de stratégie d'un éditeur post-acquisition.
- Nous avons fait le choix inverse : diversifier davantage nos fournisseurs pour éviter tout enfermement. Quitte à assumer une complexité opérationnelle plus élevée.
- Ces mouvements ont accéléré notre réflexion sur le build vs buy. Pour certaines briques critiques, nous avons choisi de développer ou d'internaliser plutôt que de dépendre d'acteurs en cours de consolidation.
- Nous n'avons pas encore observé d'impact direct, mais nous suivons ces évolutions de marché de près dans notre veille stratégique.

[Q197] Outils de collaboration sectorielle : Quels moyens utilisez-vous pour faciliter la collaboration sectorielle ? *(Plusieurs réponses possibles)*

Globalement :

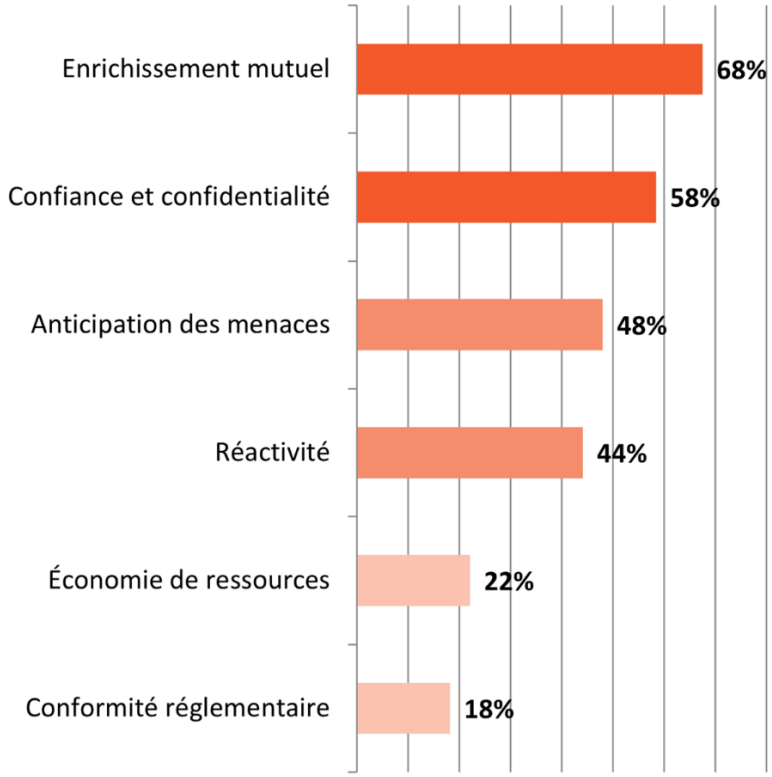
- **80%** n'utilisent aucun outil de collaboration sectorielle ;
- **74%** utilisent des groupes de travail sectoriels au sein de clubs et association (CESIN, Collèges du Campus Cyber, Gimelec) ;
- **53%** utilisent des groupes privés sur messageries sécurisées (Signal, Tchap, Slack, Teams, LinkedIn, etc.) ;
- **48%** utilisent des CERT sectoriels (CERT-FR, CERT Santé, CERT Finance, etc.) ;
- **26%** utilisent des forums et espaces communautaires à accès restreint (ex : plateformes sectorielles sur invitation) ;
- **17%** utilisent des plateformes intersectorielles de partage de renseignement sur les menaces (CTI) Ex : MISP, OpenCTI, TAXII/STIC...) ;
- **11%** utilisent des groupes de travail ANSSI / ENISA ;
- **11%** utilisent des listes de diffusion sécurisées (type FIRST, TF-CSIRT...) ;
- **3%** utilisent des ISACs (Information Sharing and Analysis Centers).



Globalement, pourquoi utilisez-vous ces outils ou plateformes ? *(Plusieurs réponses possibles)*

Globalement, les raisons sont :

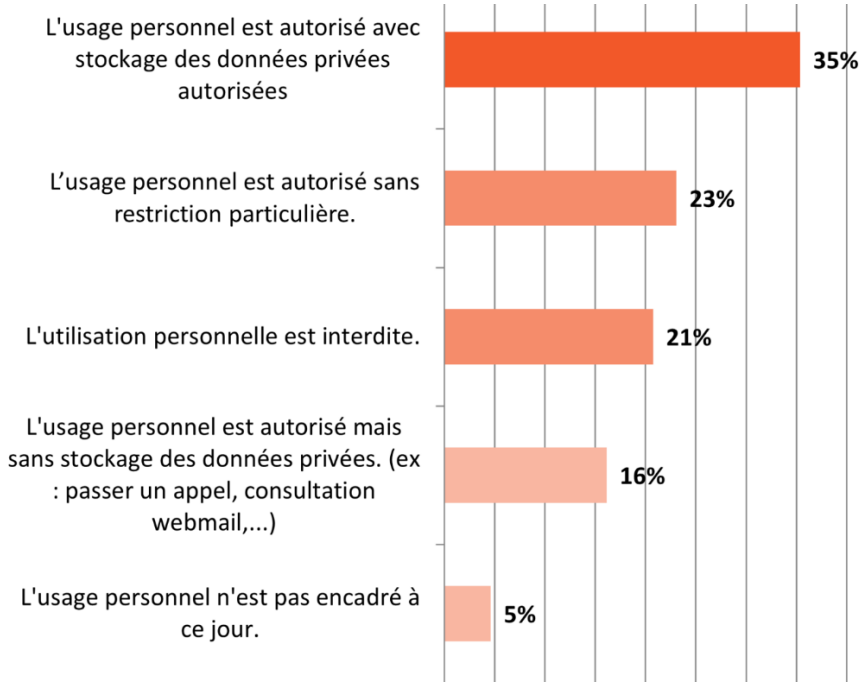
- 68% enrichissement mutuel ;
- 58% confiance et confidentialité ;
- 48% anticipation des menaces ;
- 44% réactivité ;
- 22% économie de ressources ;
- 18% conformité réglementaire.



[Q198] Responsabilité de l'organisation concernant les données privées sur équipements professionnels : Au sein de votre organisation, l'utilisation des équipements professionnels (ordinateur, téléphone, tablette, etc.) pour un usage personnel est-il encadré ?

Globalement, pour :

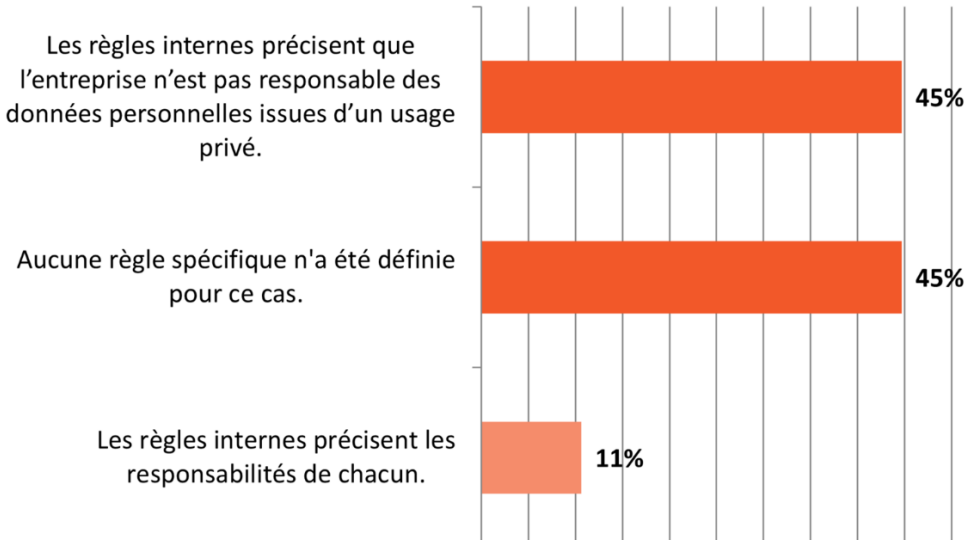
- **35%** L'usage personnel est autorisé avec stockage des données privées autorisées ;
- **23%** L'usage personnel est autorisé sans restriction particulière ;
- **21%** L'utilisation personnelle est interdite ;
- **16%** L'usage personnel est autorisé mais sans stockage des données privées. (ex : passer un appel, consultation webmail,...) ;
- **5%** L'usage personnel n'est pas encadré à ce jour.



Dans le cas d'une autorisation, si un appareil professionnel contenant des données privées est perdu, volé ou victime d'une cyberattaque, quelle est la politique de votre organisation ?

Globalement, la politique de leur organisation est la suivante :

- **45%** les règles internes précisent que l'entreprise n'est pas responsable des données personnelles issues d'un usage privé ;
- **45%** aucune règle spécifique n'a été définie pour ce cas ;
- **11%** les règles internes précisent les responsabilités de chacun.



[Q199] Cybersécurité écoresponsable : Dans votre organisation, quels leviers avez-vous déjà concrètement intégrés pour concilier sécurité et sobriété numérique ? (*Plusieurs réponses possibles)*

Parmi les **Grandes entreprises,** les leviers mis en place sont :

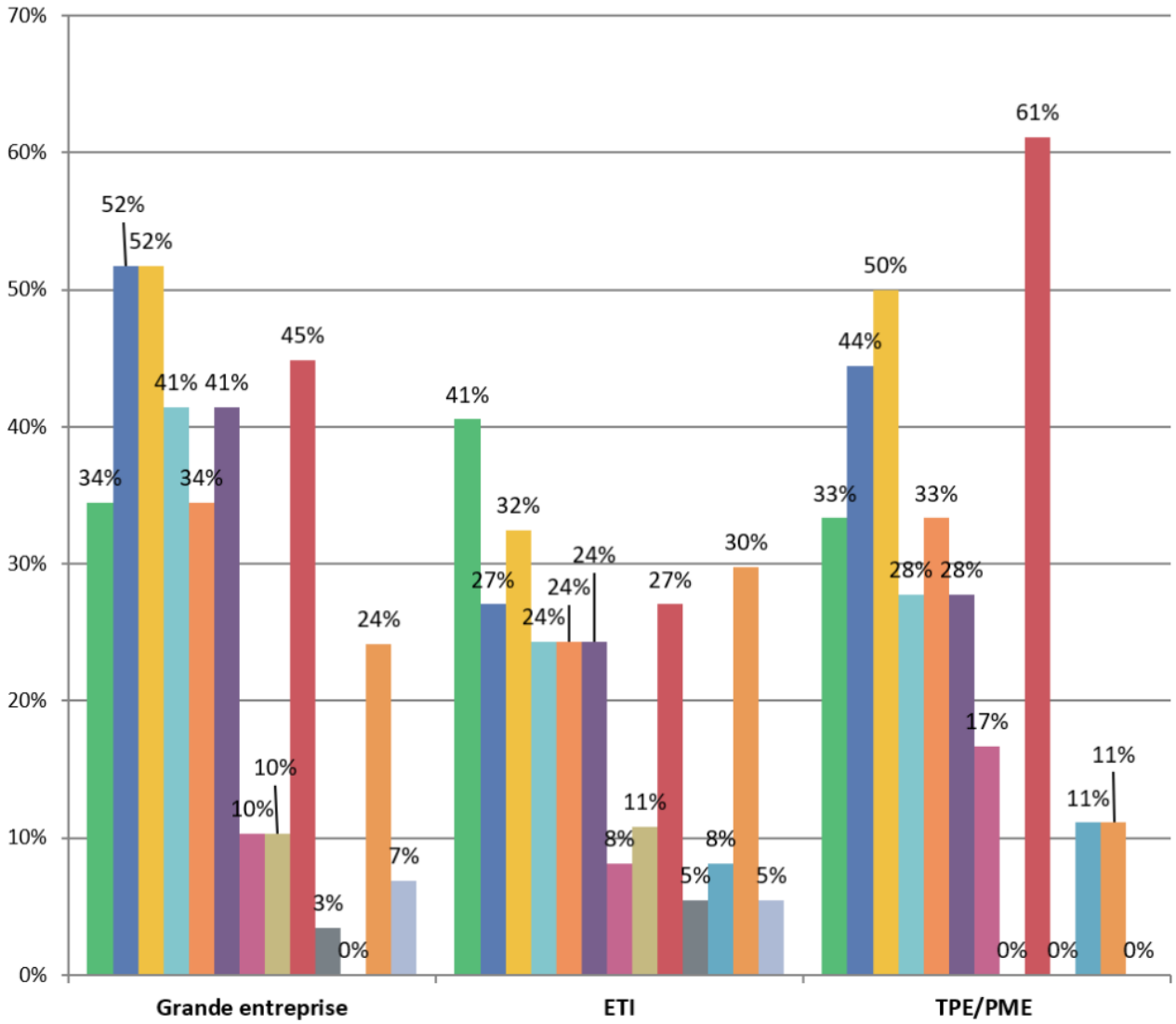
- **52%** Sécurité intégrée dès la conception (secure & sustainable by design) ;
- **52%** Réduction de la surface d'attaque et des ressources inutiles ;
- **45%** Sensibilisation des utilisateurs et priorité à l'humain ;
- **41%** Optimisation de la collecte et de la rétention des logs ;
- **41%** Rationalisation et mutualisation des outils de sécurité ;
- **34%** Sécurisation proportionnée au risque réel ;
- **34%** Dimensionnement des outils (SOC, SIEM, XDR) à l'usage réel ;
- **10%** Prolongation du cycle de vie des actifs de sécurité ;
- **10%** Automatisation ciblée pour limiter le bruit et les traitements inutiles ;
- **3%** Mesure et pilotage de l'empreinte environnementale de la fonction cyber ;
- **7%** Autre ;
- Enfin, **24%** n'ont mis en place aucun de ces leviers et ce n'est pas à l'ordre du jour.

Parmi les **ETI,** les leviers mis en place sont :

- **41%** Sécurisation proportionnée au risque réel ;
- **32%** Réduction de la surface d'attaque et des ressources inutiles ;
- **27%** Sécurité intégrée dès la conception (secure & sustainable by design) ;
- **27%** Sensibilisation des utilisateurs et priorité à l'humain ;
- **24%** Dimensionnement des outils (SOC, SIEM, XDR) à l'usage réel ;
- **24%** Optimisation de la collecte et de la rétention des logs ;
- **24%** Rationalisation et mutualisation des outils de sécurité ;
- **8%** Prolongation du cycle de vie des actifs de sécurité ;
- **11%** Automatisation ciblée pour limiter le bruit et les traitements inutiles ;
- **5%** Mesure et pilotage de l'empreinte environnementale de la fonction cyber ;
- **5%** Autre ;
- Enfin, **38%** n'ont mis en place aucun de ces leviers et ce n'est pas à l'ordre du jour pour 8% mais pour 30% c'est à l'étude.

Parmi les **TPE/PME**, les leviers mis en place sont :

- **33%** Sécurisation proportionnée au risque réel ;
- **61%** Sensibilisation des utilisateurs et priorité à l'humain ;
- **44%** Sécurité intégrée dès la conception (secure & sustainable by design) ;
- **50%** Réduction de la surface d'attaque et des ressources inutiles ;
- **33%** Optimisation de la collecte et de la rétention des logs ;
- **28%** Rationalisation et mutualisation des outils de sécurité ;
- **33%** Dimensionnement des outils (SOC, SIEM, XDR) à l'usage réel ;
- **17%** Prolongation du cycle de vie des actifs de sécurité ;
- **0%** Automatisation ciblée pour limiter le bruit et les traitements inutiles ;
- **0%** Mesure et pilotage de l'empreinte environnementale de la fonction cyber ;
- **0%** Autre ;
- Enfin, 22% n'ont mis en place aucun de ces leviers et ce n'est pas à l'ordre du jour pour 11% mais pour 11% c'est à l'étude.



- Sécurisation proportionnée au risque réel
- Sécurité intégrée dès la conception (secure & sustainable by design)
- Réduction de la surface d'attaque et des ressources inutiles
- Optimisation de la collecte et de la rétention des logs
- Dimensionnement des outils (SOC, SIEM, XDR) à l'usage réel
- Rationalisation et mutualisation des outils de sécurité
- Prolongation du cycle de vie des actifs de sécurité
- Automatisation ciblée pour limiter le bruit et les traitements inutiles
- Sensibilisation des utilisateurs et priorité à l'humain
- Mesure et pilotage de l'empreinte environnementale de la fonction cyber
- Aucun de ces leviers mais c'est à l'étude
- Aucun de ces leviers et ce n'est pas à l'ordre du jour
- Autre (veuillez préciser)

[Q200] Claude Mythos & Project Glasswing : quel impact pour les équipes sécurité ? Avez-vous connaissance de Claude Mythos et du Project Glasswing ?

Parmi les **Grandes entreprises** :

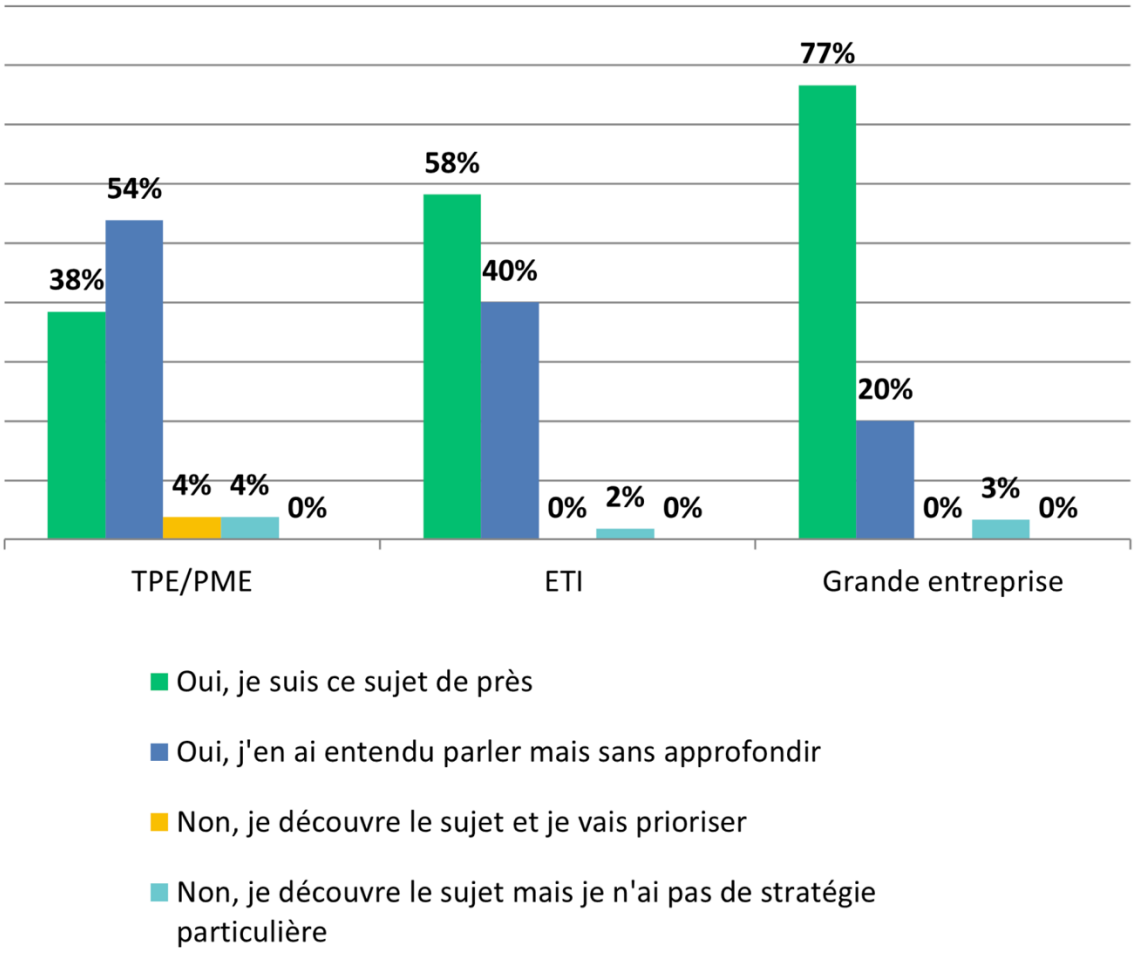
- **54%** ont entendu parler mais sans approfondir ;
- **38%** suivent ce sujet de près ;
- **4%** découvrent le sujet et vont prioriser ;
- **4%** découvrent le sujet mais n'ont pas de stratégie particulière ;
- **0%** estiment le sujet non prioritaire pour le moment.

Parmi les **ETI** :

- **58%** suivent ce sujet de près ;
- **40%** ont entendu parler mais sans approfondir ;
- **0%** découvrent le sujet et vont prioriser ;
- **2%** découvrent le sujet mais n'ont pas de stratégie particulière ;
- **0%** estiment le sujet non prioritaire pour le moment.

Parmi les **TPE/PME** :

- **77%** suivent ce sujet de près ;
- **20%** ont entendu parler mais sans approfondir ;
- **3% découvrent le sujet mais n'ont pas de stratégie particulière** ;
- **0% découvrent le sujet et vont prioriser** ;
- **0%** estiment le sujet non prioritaire pour le moment.

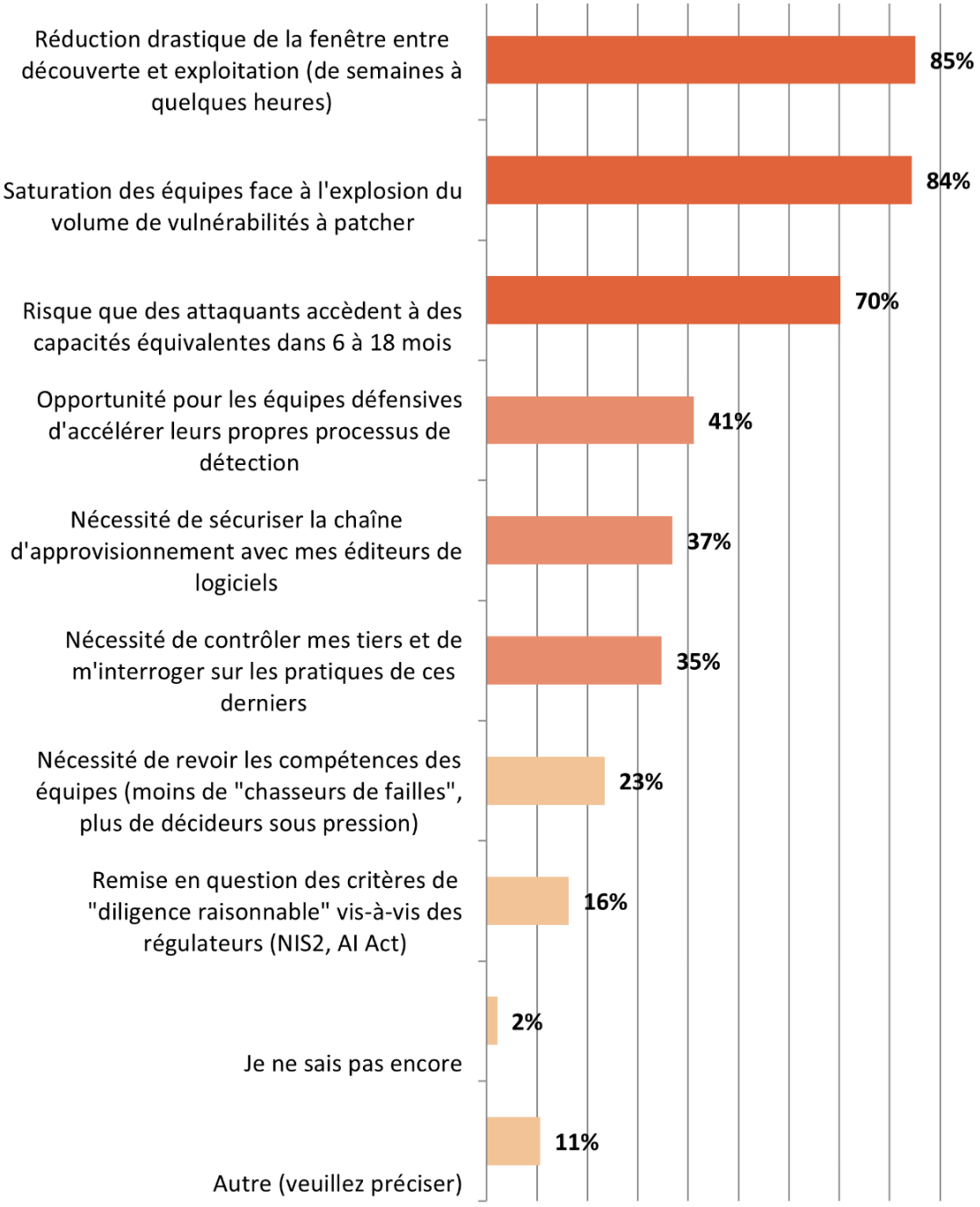


Selon vous, quels sont les principaux impacts de l'émergence de modèles IA de type Mythos pour les équipes sécurité ? (*Plusieurs réponses possibles)*

Globalement, les principaux impacts sont :

- **85%** Réduction drastique de la fenêtre entre découverte et exploitation (de semaines à quelques heures) ;
- **84%** Saturation des équipes face à l'explosion du volume de vulnérabilités à patcher ;
- **70%** Risque que des attaquants accèdent à des capacités équivalentes dans 6 à 18 mois ;
- **41%** Opportunité pour les équipes défensives d'accélérer leurs propres processus de détection ;
- **37%** Nécessité de sécuriser la chaîne d'approvisionnement avec leurs éditeurs de logiciels ;
- **35%** Nécessité de contrôler leurs tiers et de s'interroger sur les pratiques de ces derniers ;

- **23%** Nécessité de revoir les compétences des équipes (moins de « chasseurs de failles », plus de décideurs sous pression) ;
- **16% Remise en question des critères de « diligence raisonnable » vis-à-vis des régulateurs (NIS2, AI Act)** ;
- **2%** Je ne sais pas encore ;
- **11%** Autre car les priorités identifiées portent sur l'automatisation de la détection, du patching et de la remédiation, ainsi que sur l'adoption rapide de solutions d'IA défensives capables de s'auto-tester et de réagir en continu. Les répondants évoquent également la nécessité de mieux maîtriser leur exposition (shadow IT, OSINT, segmentation, réduction de surface d'attaque) et de revoir les modèles opérationnels des équipes infra, dev et sécurité. Enfin, plusieurs soulignent un risque d'écart croissant entre les organisations capables d'investir et de s'adapter rapidement — notamment les grands éditeurs — et les acteurs plus petits ou reposant sur des environnements legacy et open source moins maintenus.


Réduction drastique de la fenêtre entre découverte et exploitation (de semaines à quelques heures)
85%
Saturation des équipes face à l'explosion du volume de vulnérabilités à patcher
84%
Risque que des attaquants accèdent à des capacités équivalentes dans 6 à 18 mois
70%
Opportunité pour les équipes défensives d'accélérer leurs propres processus de détection
41%
Nécessité de sécuriser la chaîne d'approvisionnement avec mes éditeurs de logiciels
37%
Nécessité de contrôler mes tiers et de m'interroger sur les pratiques de ces derniers
35%
Nécessité de revoir les compétences des équipes (moins de "chasseurs de failles", plus de décideurs sous pression)
23%
Remise en question des critères de "diligence raisonnable" vis-à-vis des régulateurs (NIS2, AI Act)
16%
Je ne sais pas encore
2%
Autre (veuillez préciser)
11%

[Q201] Gestion du risque Deep fake (Mise à jour 2026) : Votre organisation a-t-elle déjà été victime de ce type d'attaques ?

Parmi les **Grandes entreprises :**

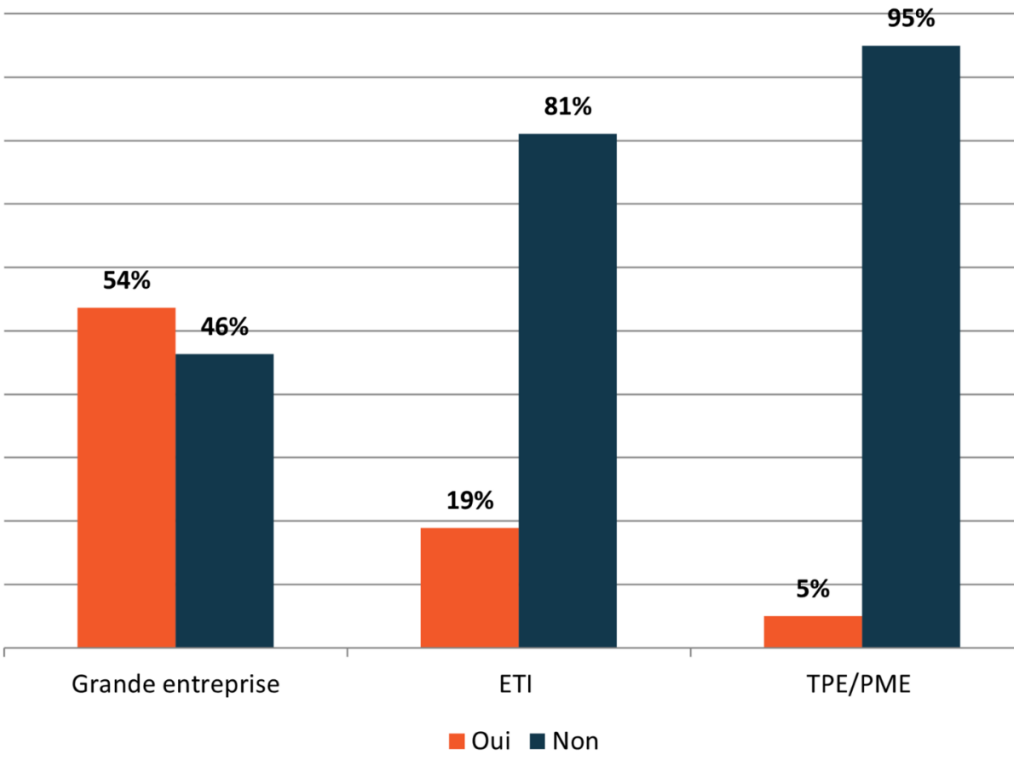
- **54%** ont déjà été victime de ce type d'attaques ;
- **46%** n'ont jamais été victime de ce type d'attaques.

Parmi les **ETI** :

- **19%** ont déjà été victime de ce type d'attaques ;
- **81%** n'ont jamais été victime de ce type d'attaques.

Parmi les **TPE/PME** :

- **5%** ont déjà été victime de ce type d'attaques ;
- **95%** n'ont jamais été victime de ce type d'attaques.



Quelles solutions organisationnelles et/ou technologiques avez-vous mis en œuvre ou envisagez-vous pour mieux prévenir, détecter et répondre à ce type de menaces ? *(Plusieurs réponses possibles)*

Parmi les **Grandes entreprises** :

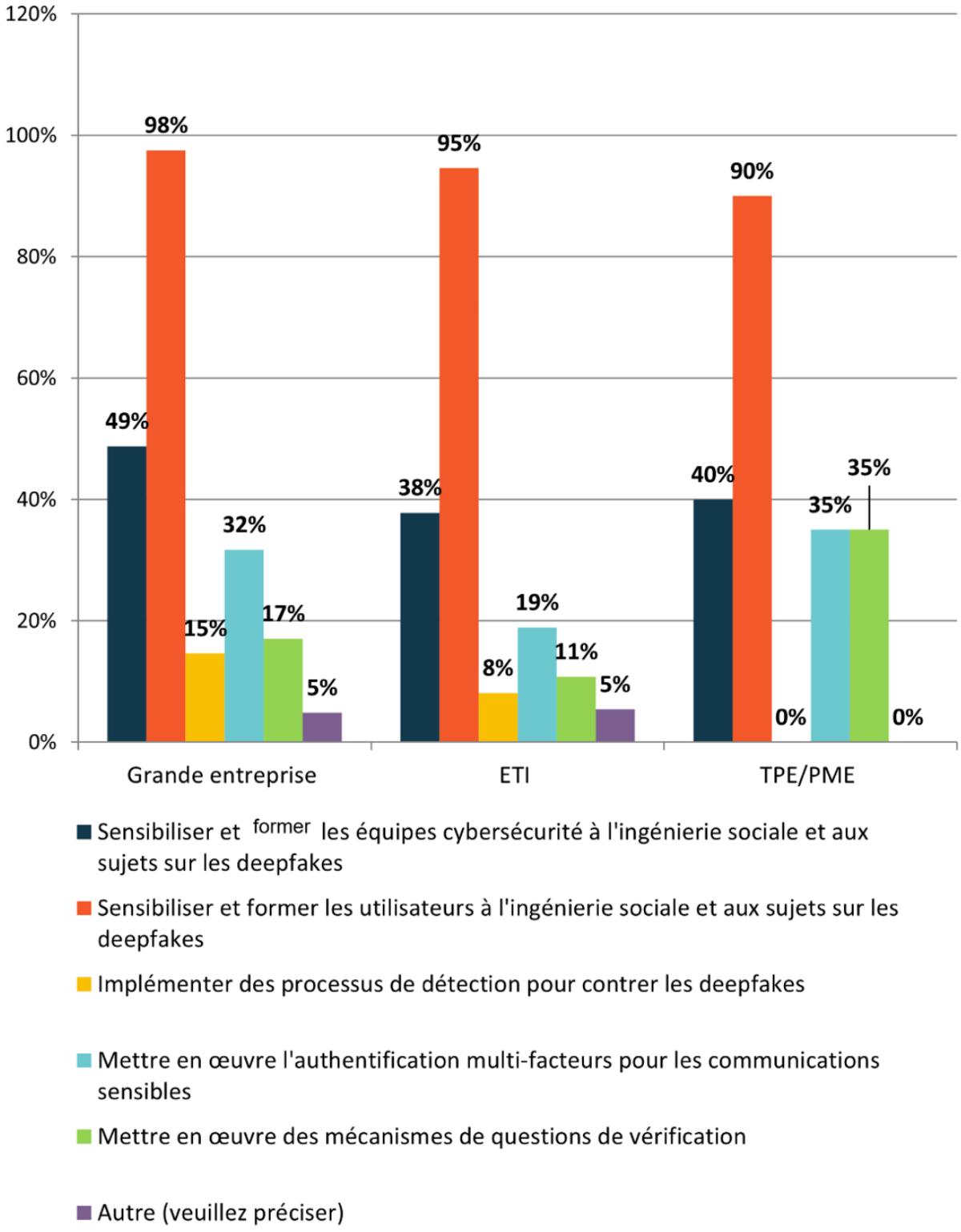
- **49%** sensibilisent et forment les équipes cybersécurité à l'ingénierie sociale et aux sujets sur les deepfakes ;
- **98%** sensibilisent et forment les utilisateurs à l'ingénierie sociale et aux sujets sur les deepfakes ;
- **15%** implémentent des processus de détection pour contrer les deepfakes ;
- **32%** mettent en œuvre l'authentification multifacteurs pour les communications sensibles ;
- **17%** mettent en œuvre des mécanismes de questions de vérification ;
- **5%** ont répondu « Autre ».

Parmi les **ETI** :

- **38%** sensibilisent et forment les équipes cybersécurité à l'ingénierie sociale et aux sujets sur les deepfakes ;
- **95%** sensibilisent et forment les utilisateurs à l'ingénierie sociale et aux sujets sur les deepfakes ;
- **8%** implémentent des processus de détection pour contrer les deepfakes ;
- **19%** mettent en œuvre l'authentification multifacteurs pour les communications sensibles ;
- **11%** mettent en œuvre des mécanismes de questions de vérification ;
- **5%** ont répondu « Autre ».

Parmi les **TPE/PME** :

- **40%** sensibilisent et forment les équipes cybersécurité à l'ingénierie sociale et aux sujets sur les deepfakes ;
- **90%** sensibilisent et forment les utilisateurs à l'ingénierie sociale et aux sujets sur les deepfakes ;
- **0%** implémentent des processus de détection pour contrer les deepfakes ;
- **35%** mettent en œuvre l'authentification multifacteurs pour les communications sensibles ;
- **35%** mettent en œuvre des mécanismes de questions de vérification ;
- **0%** ont répondu « Autre ».


120%
100%
80%
60%
40%
20%
0%
98%
95%
90%
49%
38%
40%
32%
35%
35%
19%
17%
15%
11%
8%
5%
5%
0%
0%
Grande entreprise
ETI
TPE/PME
Sensibiliser et former les équipes cybersécurité à l'ingénierie sociale et aux sujets sur les deepfakes
Sensibiliser et former les utilisateurs à l'ingénierie sociale et aux sujets sur les deepfakes
Implémenter des processus de détection pour contrer les deepfakes
Mettre en œuvre l'authentification multi-facteurs pour les communications sensibles
Mettre en œuvre des mécanismes de questions de vérification
Autre (veuillez préciser)

[Q202] Préparation à la communication de crise cyber : Quel est le niveau de préparation de votre organisation en matière de communication de crise en cas d'incident cyber ?

Parmi les **Grandes entreprises** le niveau est pour :

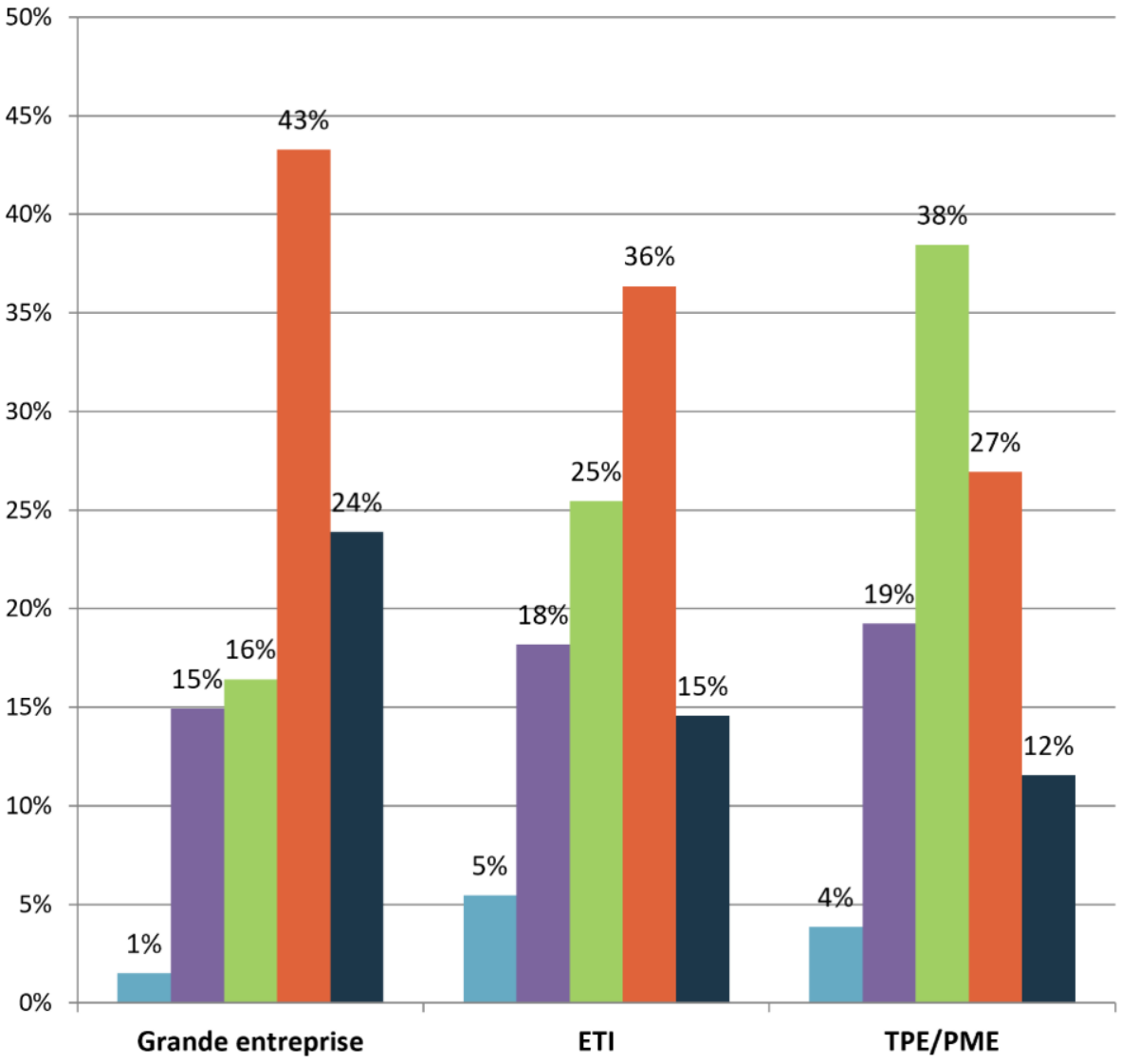
- **1%** Niveau 1 : Aucune préparation spécifique ;
- **15%** Niveau 2 : Réflexion en cours, mais pas de dispositif formalisé ;
- **16%** Niveau 3 : Dispositif partiellement défini (messages clés ou procédures existants, mais non testés) ;
- **43%** Niveau 4 : Dispositif structuré (templates, scénarios, canaux identifiés, parties prenantes définies) mais peu ou pas testé ;
- **24%** Niveau 5 : Dispositif complet et opérationnel (prestataires internes/externes identifiés).

Parmi les **ETI** le niveau est pour :

- **5%** Niveau 1 : Aucune préparation spécifique ;
- **18%** Niveau 2 : Réflexion en cours, mais pas de dispositif formalisé ;
- **25%** Niveau 3 : Dispositif partiellement défini (messages clés ou procédures existants, mais non testés) ;
- **36%** Niveau 4 : Dispositif structuré (templates, scénarios, canaux identifiés, parties prenantes définies) mais peu ou pas testé ;
- **15%** Niveau 5 : Dispositif complet et opérationnel (prestataires internes/externes identifiés).

Parmi les **TPE/PME** le niveau est pour :

- **4%** Niveau 1 : Aucune préparation spécifique ;
- **19%** Niveau 2 : Réflexion en cours, mais pas de dispositif formalisé ;
- **38%** Niveau 3 : Dispositif partiellement défini (messages clés ou procédures existants, mais non testés) ;
- **27%** Niveau 4 : Dispositif structuré (templates, scénarios, canaux identifiés, parties prenantes définies) mais peu ou pas testé ;
- **12%** Niveau 5 : Dispositif complet et opérationnel (prestataires internes/externes identifiés).



- Niveau 1 : Aucune préparation spécifique
- Niveau 2 : Réflexion en cours, mais de dispositif formalisé
- Niveau 3 : Dispositif partiellement défini (messages clés ou procédures existants, mais non testés)
- Niveau 4 : Dispositif structuré (templates, scénarios, canaux identifiés, parties prenants définies) mais peu ou pas testé
- Niveau 5 : Dispositif complet et opérationnel (prestataires internes/externes identifiés, supports prêts, scénarios formalisés, exercices déjà réalisés)

[Q203] Lunettes connectées : nouvelle technologie, nouveau risque ? Avez-vous adressé ce nouveau risque dans votre organisation ?

Globalement :

- **17%** ont adressé ce nouveau risque ;
- **83%** n'ont pas adressé ce nouveau risque.

Parmi les **Grandes entreprises** :

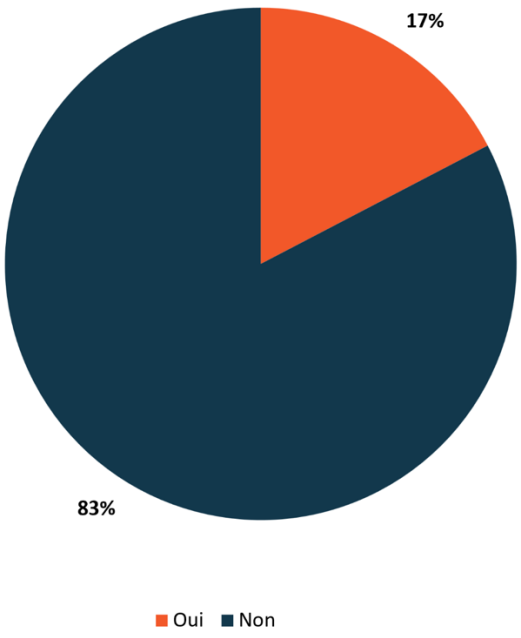
- **24%** ont adressé ce nouveau risque ;
- **76%** n'ont pas adressé ce nouveau risque.

Parmi les **ETI :**

- **9%** ont adressé ce nouveau risque ;
- **91%** n'ont pas adressé ce nouveau risque.

Parmi les **TPE/PME :**

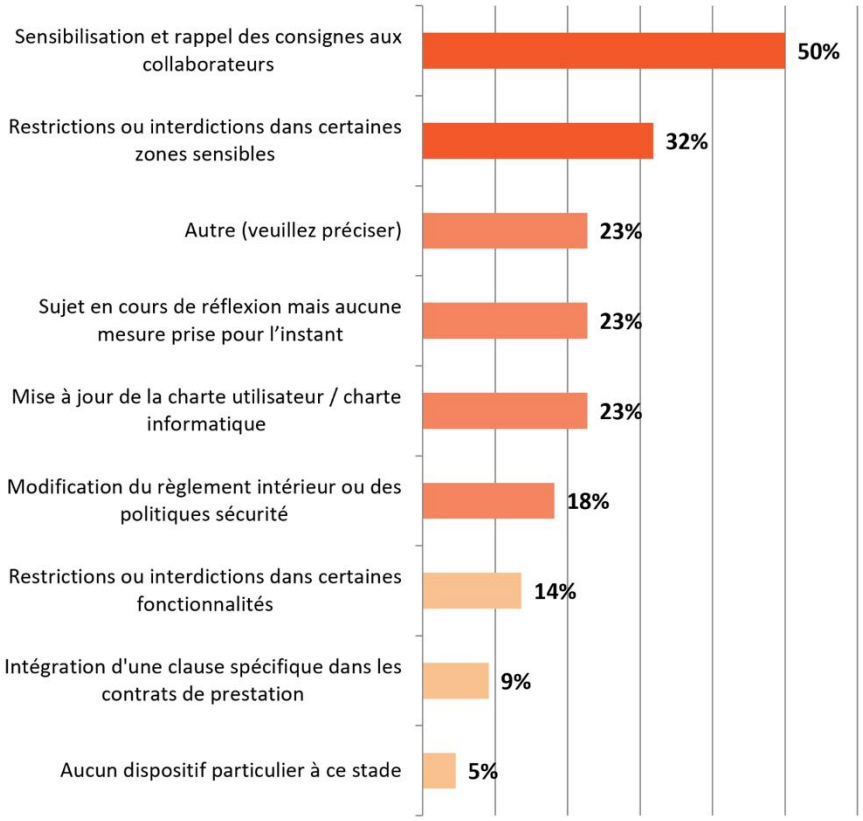
- **15%** ont adressé ce nouveau risque ;
- **85%** n'ont pas adressé ce nouveau risque.



Si oui, de quelle manière ? *(Plusieurs réponses possibles)*

Globalement, la manière de l'adresser est la suivante :

- **50%** par la sensibilisation et rappel des consignes aux collaborateurs ;
- **32%** par les restrictions ou interdictions dans certaines zones sensibles ;
- **23%** par la réflexion sur le sujet mais aucune mesure prise pour l'instant ;
- **23%** par la mise à jour de la charte utilisateur/charte informatique ;
- **18%** par la modification du règlement intérieur ou des politiques sécurité ;
- **14%** par les restrictions ou interdictions dans certaines fonctionnalités ;
- **9%** par l'intégration d'une clause spécifique dans les contrats de prestation ;
- **5%** n'ont aucun dispositif particulier à ce stade ;
- **23%** ont répondu « Autre » notamment car les lunettes connectées sont considérées comme un smartphone ou par la mise en place d'une restriction des droits d'accès aux données internes par les lunettes ou encore une interdiction totale.



[Q204] Réunions : transcriptions et synthèses IA ? Comment gérez-vous l'utilisation des enregistrements, transcriptions et synthèses IA des réunions dans votre organisation ? *(Plusieurs réponses possibles)*

Parmi les **Grandes entreprises** :

- **63%** ont mis en place une autorisation conditionnelle sous validation préalable ou accord explicite des participants ;
- **47%** ont mis en place une utilisation restreinte aux outils validés et approuvés par la DSI / la sécurité / l'organisation ;
- **29%** ont mis en place une sensibilisation des collaborateurs mais pas de contrôle technique spécifique ;
- **16%** ont mis en place un encadrement des conditions de journalisation des sessions enregistrées ;
- **8%** ont mis en place une classification des réunions avec règles associées selon le niveau de sensibilité ;
- **4%** ont mis en place une interdiction explicite des transcriptions / enregistrements IA des réunions ;
- **6%** ont répondu « Autre » ;
- Enfin, pour **8%** ce sujet est en cours de définition / gouvernance et pour **12%** aucun encadrement particulier n'a été mis en place à ce stade.

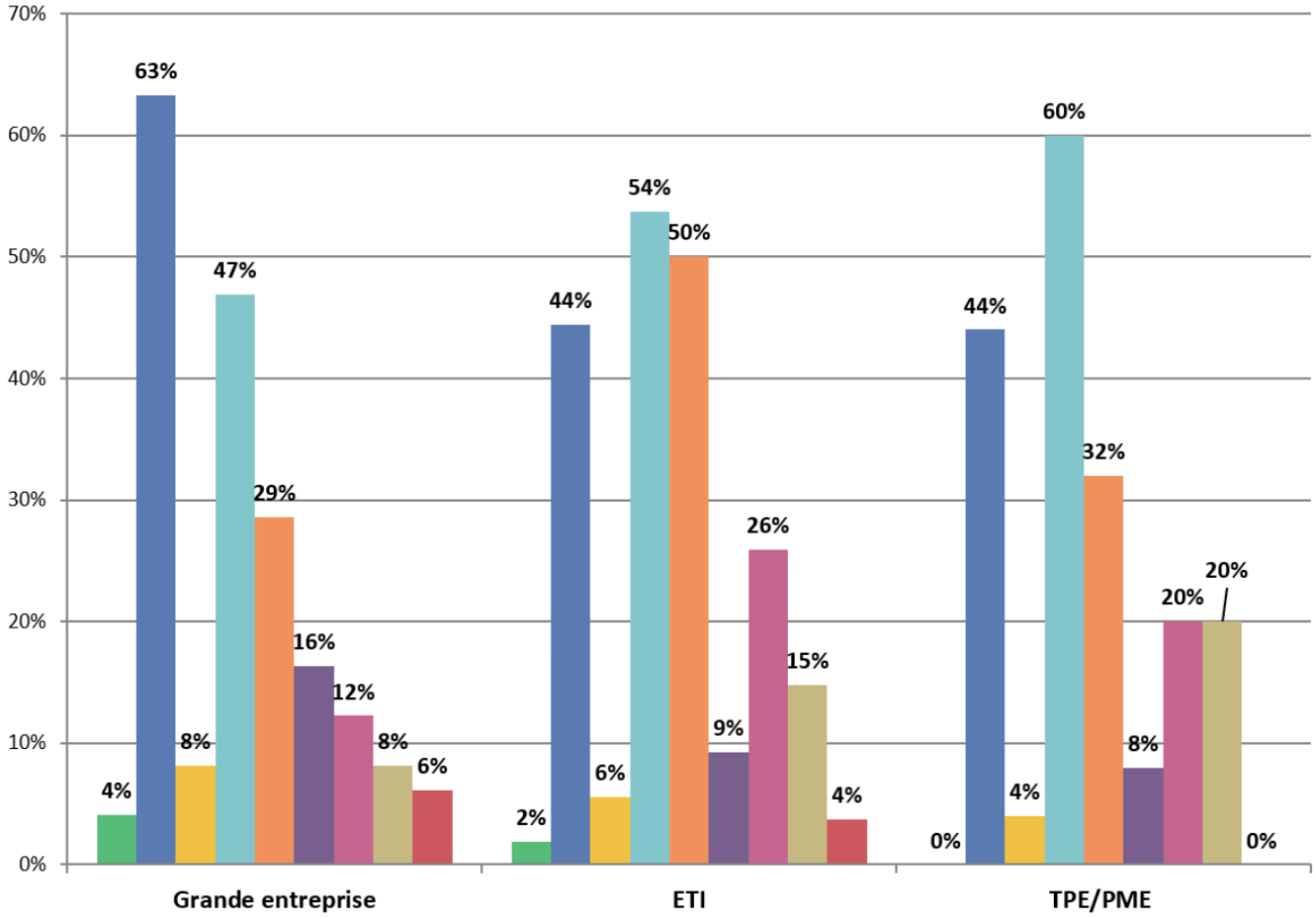
Parmi les **ETI** :

- **54%** ont mis en place une utilisation restreinte aux outils validés et approuvés par la DSI / la sécurité / l'organisation ;
- **50%** ont mis en place une sensibilisation des collaborateurs mais pas de contrôle technique spécifique ;
- **44%** ont mis en place une autorisation conditionnelle sous validation préalable ou accord explicite des participants ;
- **9%** ont mis en place un encadrement des conditions de journalisation des sessions enregistrées ;
- **6%** ont mis en place une classification des réunions avec règles associées selon le niveau de sensibilité ;

- **2%** ont mis en place une interdiction explicite des transcriptions / enregistrements IA des réunions ;
- **4%** ont répondu « Autre » ;
- Enfin, pour **15%** ce sujet est en cours de définition / gouvernance et pour **26%** aucun encadrement particulier n'a été mis en place à ce stade.

Parmi les **TPE/PME** :

- **60%** ont mis en place une utilisation restreinte aux outils validés et approuvés par la DSI / la sécurité / l'organisation ;
- **44%** ont mis en place une autorisation conditionnelle sous validation préalable ou accord explicite des participants ;
- **32%** ont mis en place une sensibilisation des collaborateurs mais pas de contrôle technique spécifique ;
- **8%** ont mis en place un encadrement des conditions de journalisation des sessions enregistrées ;
- **4%** ont mis en place une classification des réunions avec règles associées selon le niveau de sensibilité ;
- **0%** ont mis en place une interdiction explicite des transcriptions / enregistrements IA des réunions ;
- **0%** ont répondu « Autre » ;
- Enfin, pour **20%** ce sujet est en cours de définition / gouvernance et pour **20%** aucun encadrement particulier n'a été mis en place à ce stade.



- Interdiction explicite des transcriptions/enregistrements IA des réunions
- Autorisation conditionnelle sous validation préalable ou accord explicite des participants
- Classification des réunions avec règles associées selon le niveau de sensibilité
- Utilisation restreinte aux outils validés et approuvés par la DSI / la sécurité / l'organisation
- Sensibilisation des collaborateurs mais pas de contrôle technique spécifique
- Encadrement des conditions de journalisation des sessions enregistrées
- Aucun encadrement particulier à ce stade
- Sujet en cours de définition / gouvernance
- Autre (veuillez préciser)

[Q205] Migration vers le post-quantique : qui impliquer dans mon organisation ? Combien de personnes constituent(ront) cette équipe projet ?

Parmi **les Grandes entreprises**, l'équipe projet est (ou sera) constituée pour :

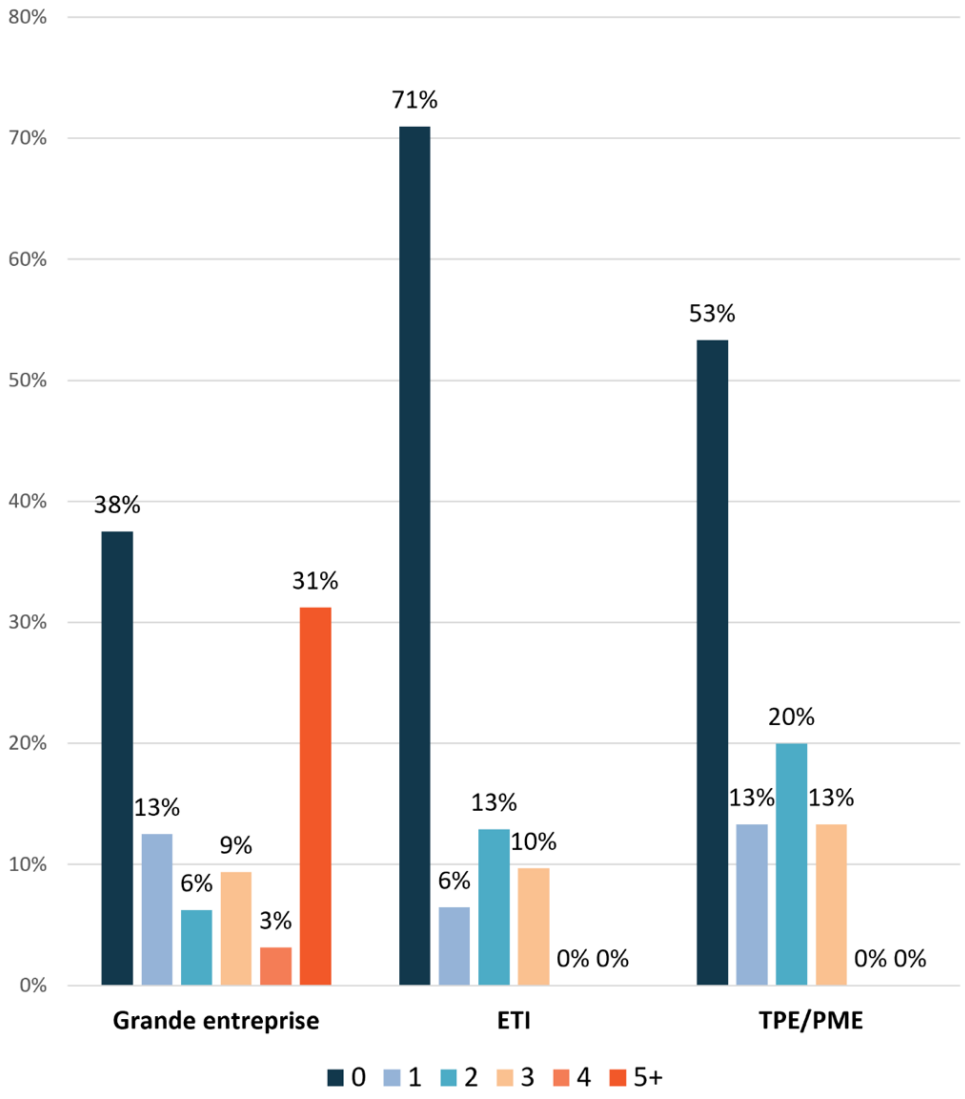
- **31%** : 4 personnes ;
- **13%** : 1 personne ;
- **9%** : 5 + personnes ;
- **6%** : 2 personnes ;
- **3%** : 3 personnes ;
- Et pour **38%** il n'y a pas ou il n'est pas prévu une équipe projet dédiée.

Parmi les **ETI**, l'équipe projet est (ou sera) constituée pour :

- **13%** : 2 personnes ;
- **10%** : 5 + personnes ;
- **6%** : 1 personne ;
- **0%** : 3 personnes ;
- **0%** : 4 personnes ;
- Et pour **71%** il n'y a pas ou il n'est pas prévu une équipe projet dédiée.

Parmi les **TPE/PME**, l'équipe projet est (ou sera) constituée pour :

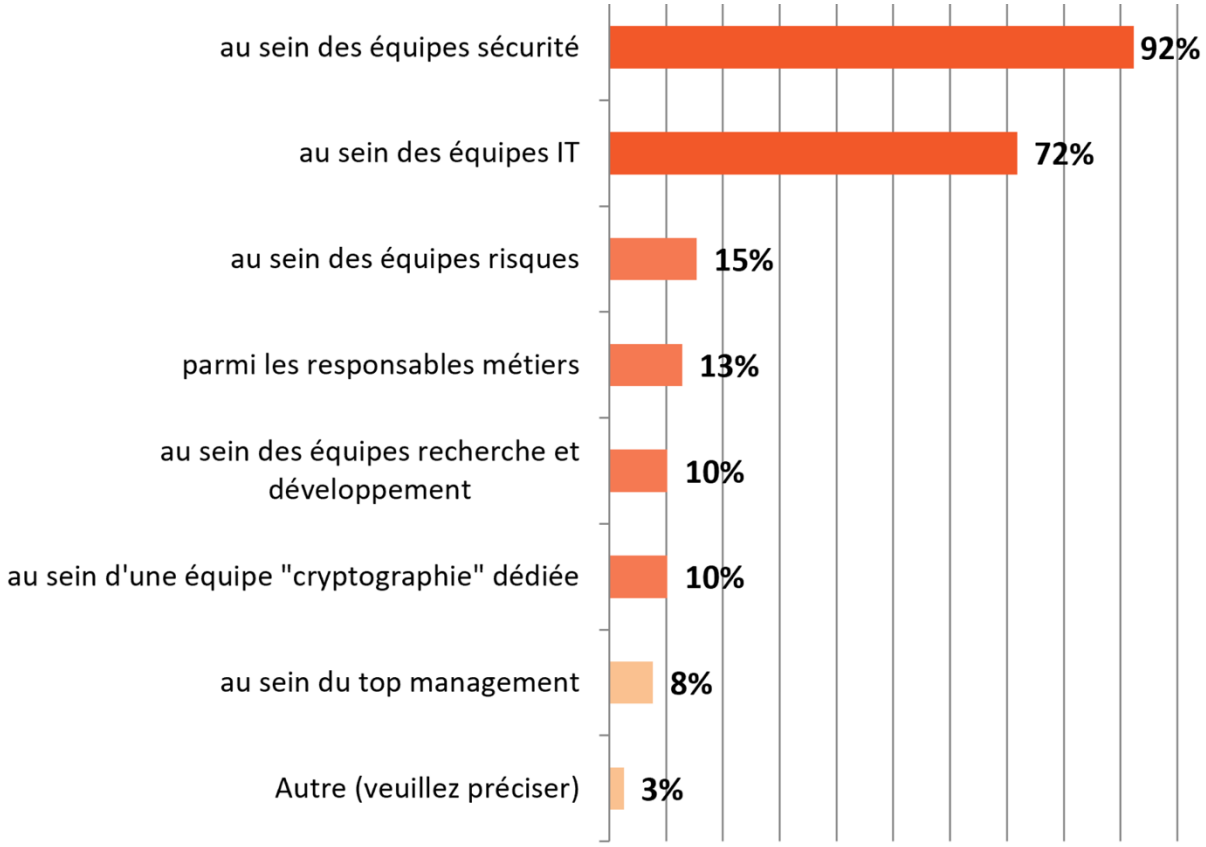
- **20%** : 2 personnes ;
- **13%** : 5 + personnes ;
- **13%** : 1 personne ;
- **0%** : 3 personnes ;
- **0%** : 4 personnes ;
- Et pour **53%** il n'y a pas ou il n'est pas prévu une équipe projet dédiée.



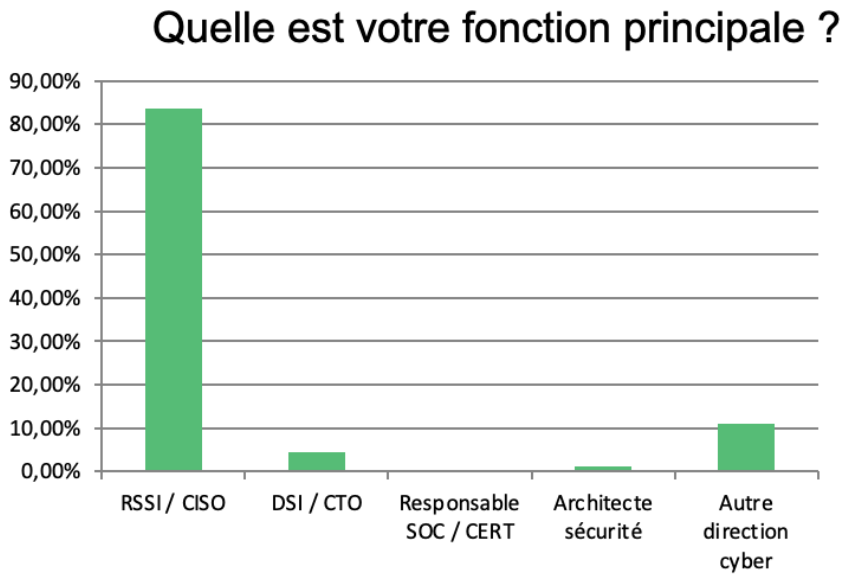
Où seront-elles localisées ? *(Plusieurs réponses possibles)*

Globalement, elles seront localisées :

- **92%** : au sein des équipes sécurité ;
- **72%** : au sein des équipes IT ;
- **15%** : au sein des équipes risques ;
- **13%** : parmi les responsables métiers ;
- **10%** : au sein des équipes recherche et développement ;
- **10%** : au sein d'une équipe « cryptographie » dédiée ;
- **8%** : au sein du top management ;
- **3%** : « Autre » : au sein des équipes développement.



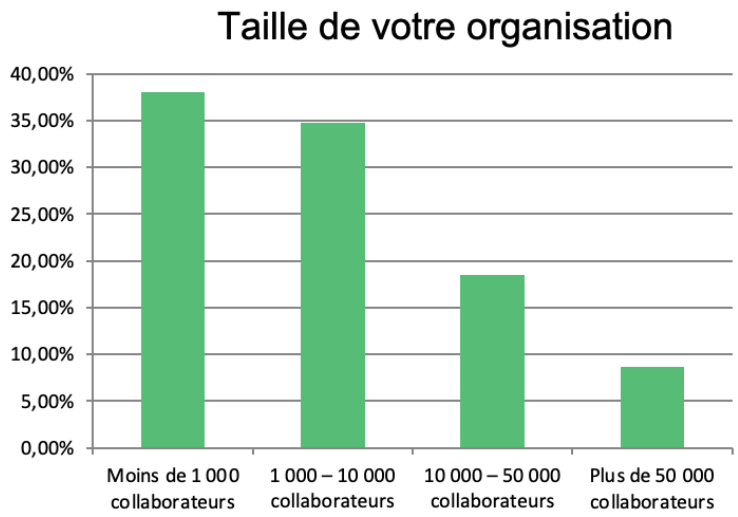
[Q206] IA générative en cyberdéfense : Quelle est votre fonction principale ?



Quelle est la taille de votre organisation ?

Globalement, la taille des organisations répondantes est :

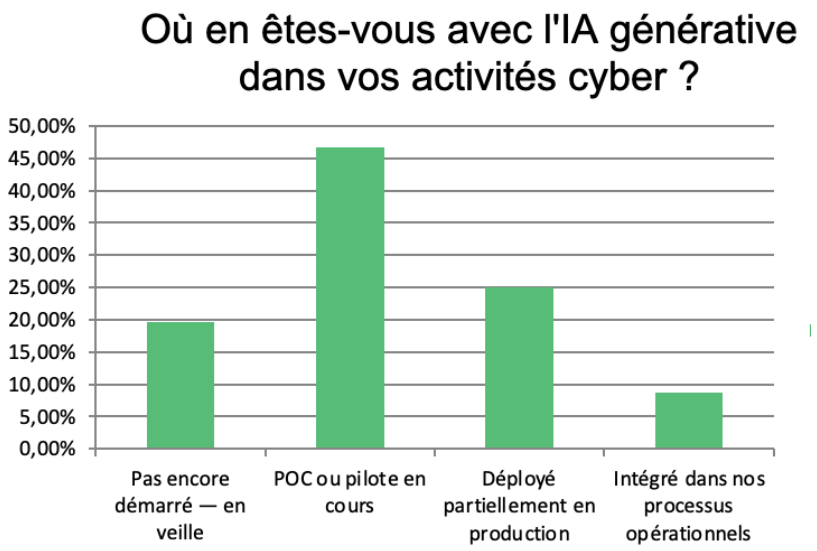
- **38%** : moins de 1 000 collaborateurs ;
- **35%** : 1 000 à 10 000 collaborateurs ;
- **18%** : 10 000 à 50 000 collaborateurs ;
- **9%** : plus de 50 000 collaborateurs.



Où en êtes-vous avec l'IA générative dans vos activités cyber ?

Globalement :

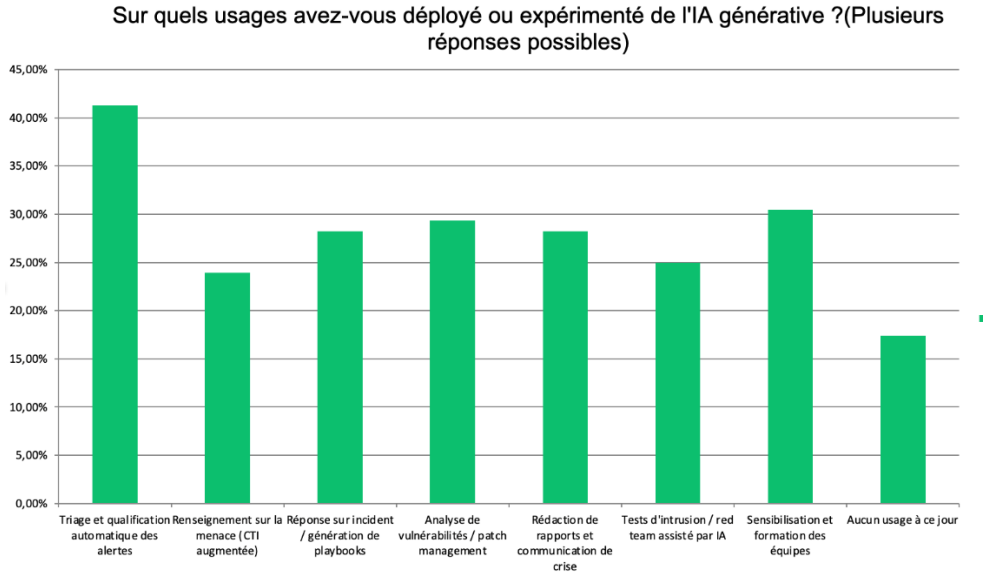
- **47%** : POC ou pilote en cours ;
- **25%** : déployé partiellement en production ;
- **20%** : pas encore démarré, en veille ;
- **9%** : intégré dans nos processus opérationnels.



Sur quels usages avez-vous déployé ou expérimenté de l'IA générative ? (*Plusieurs réponses possibles*)

Globalement :

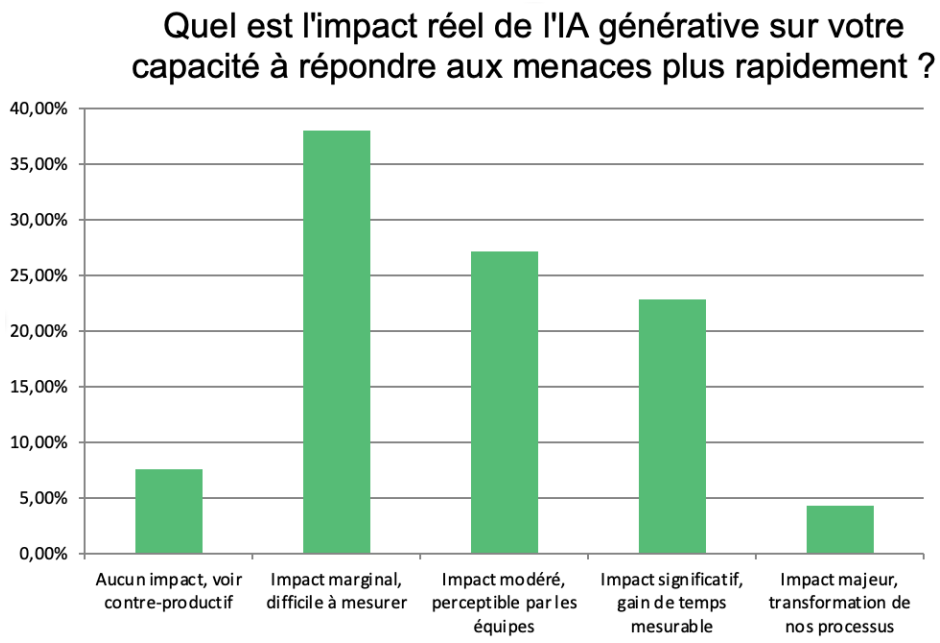
- **41%** : triage et qualification automatique des alertes ;
- **30%** : sensibilisation et formation des équipes ;
- **29%** : analyse de vulnérabilités / patch management ;
- **28%** : réponse sur incident / génération de playbooks ;
- **28%** : rédaction de rapports et communication de crise ;
- **25%** : tests d'intrusion / red team assisté par IA ;
- **24%** : renseignement sur la menace (CTI augmentée).



Quel est l'impact réel de l'IA générative sur votre capacité à répondre aux menaces plus rapidement ?

Globalement :

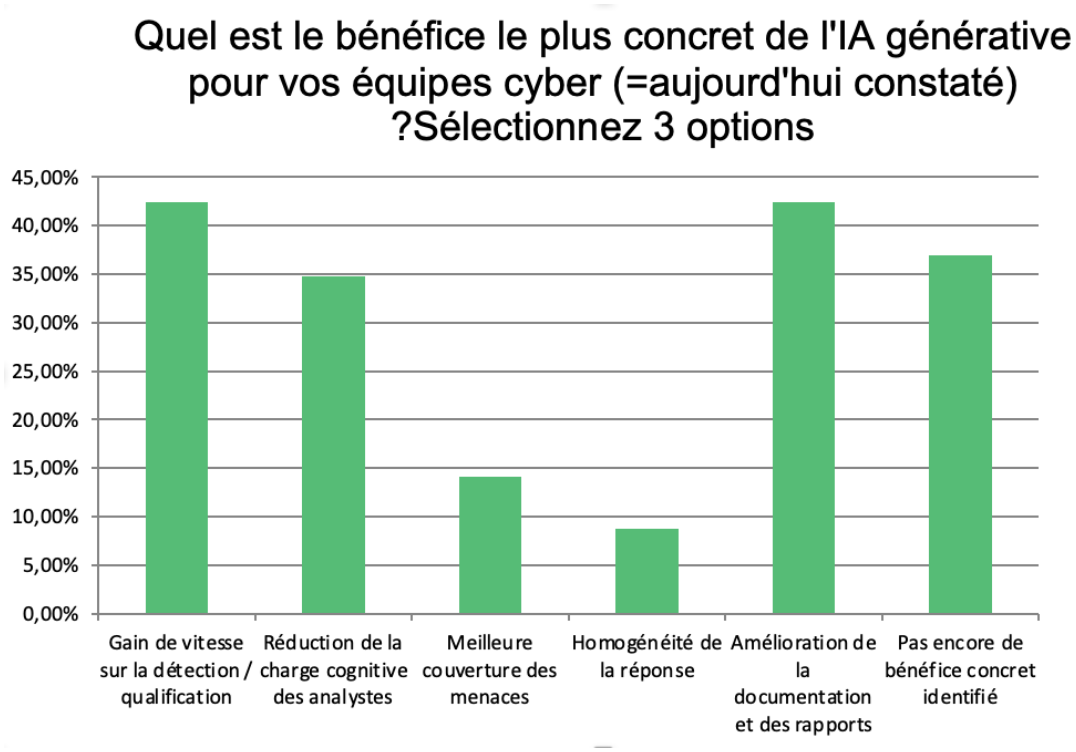
- **38%** : impact marginal, difficile à mesurer ;
- **27%** : impact modéré, perceptible par les équipes ;
- **23%** : impact significatif, gain de temps mesurable ;
- **8%** : aucun impact, voire contre-productif ;
- **4%** : impact majeur, transformation de nos processus.



Quel est le bénéfice le plus concret de l'IA générative pour vos équipes cyber (aujourd'hui constaté) ? (Sélectionnez 3 options)

Globalement :

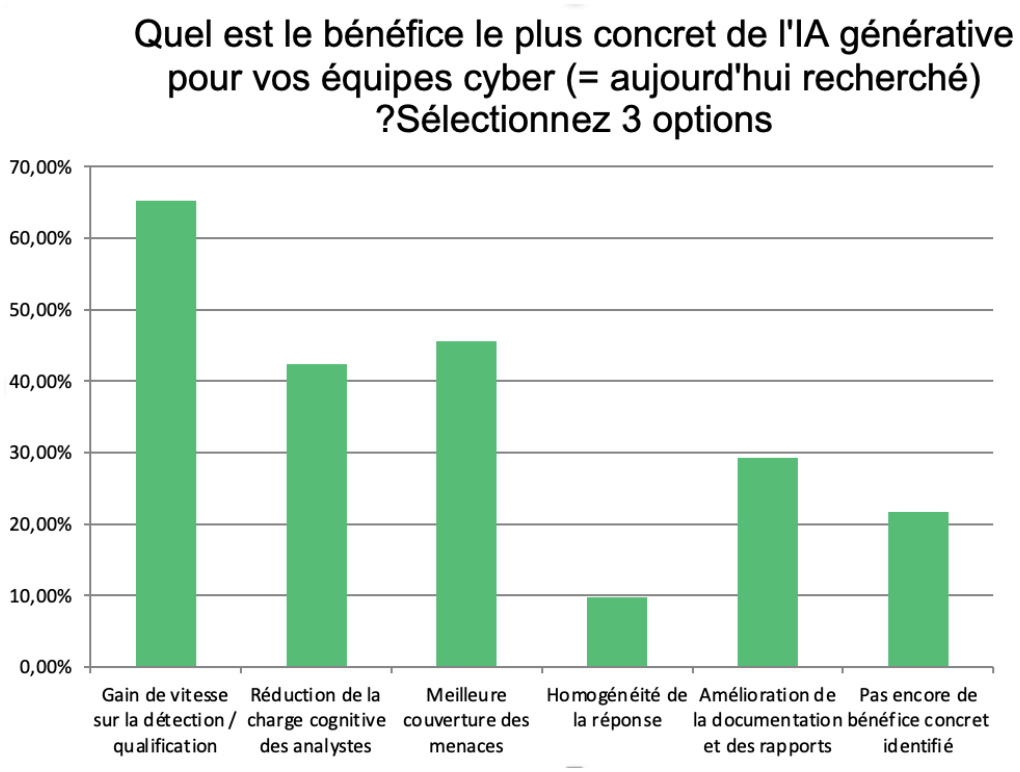
- **42%** : gain de vitesse sur la détection / qualification ;
- **42%** : amélioration de la documentation et des rapports ;
- **37%** : pas encore de bénéfice concret identifié ;
- **35%** : réduction de la charge cognitive des analystes ;
- **14%** : meilleure couverture des menaces ;
- **9%** : homogénéité de la réponse.



Quel est le bénéfice le plus concret de l'IA générative pour vos équipes cyber (aujourd'hui recherché) ? (Sélectionnez 3 options)

Globalement :

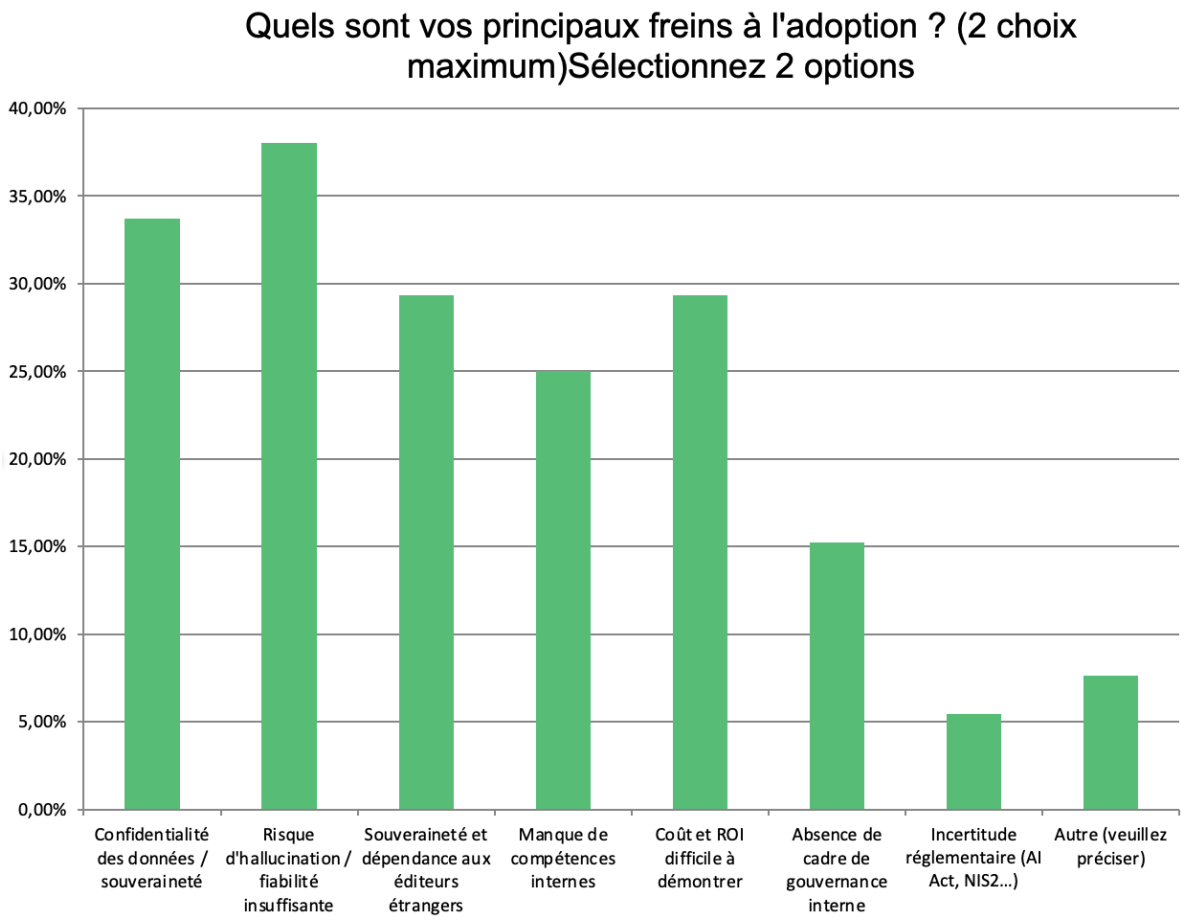
- **65%** : gain de vitesse sur la détection / qualification ;
- **46%** : meilleure couverture des menaces ;
- **42%** : réduction de la charge cognitive des analystes ;
- **29%** : amélioration de la documentation et des rapports ;
- **22%** : pas encore de bénéfice concret identifié ;
- **10%** : homogénéité de la réponse.



Quels sont vos principaux freins à l'adoption ? (2 choix maximum)

Globalement :

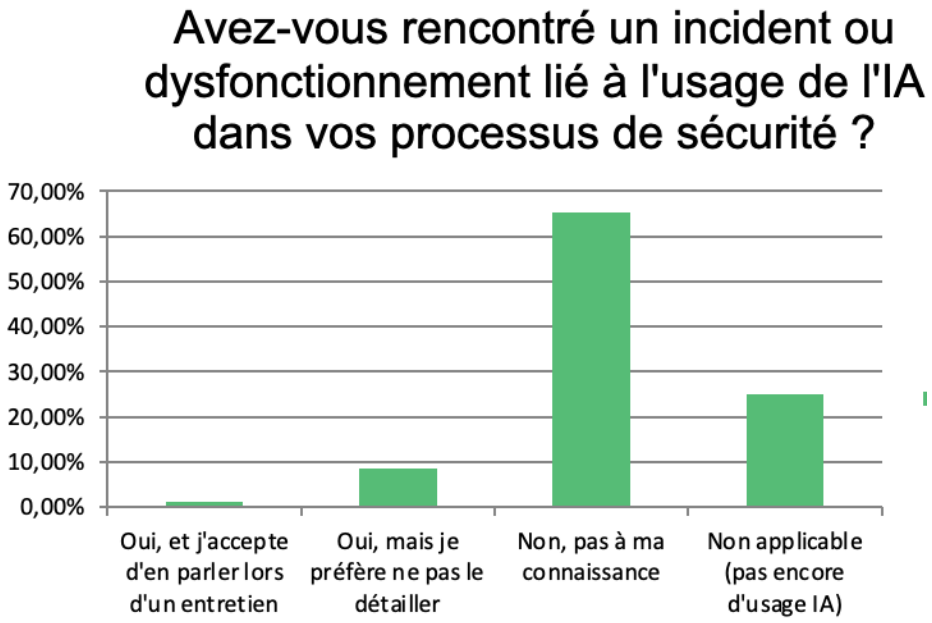
- **38%** : risque d'hallucination / fiabilité insuffisante ;
- **34%** : confidentialité des données / souveraineté ;
- **29%** : souveraineté et dépendance aux éditeurs étrangers ;
- **29%** : coût et ROI difficile à démontrer ;
- **25%** : manque de compétences internes ;
- **15%** : absence de cadre de gouvernance interne ;
- **8%** : « Autre » ;
- **5%** : incertitude réglementaire (AI Act, NIS2...).



Avez-vous rencontré un incident ou dysfonctionnement lié à l'usage de l'IA dans vos processus de sécurité ?

Globalement :

- **65%** : non, pas à leur connaissance ;
- **25%** : non applicable, pas encore d'usage IA ;
- **9%** : oui, mais préfèrent ne pas le détailler ;
- **1%** : oui, et acceptent d'en parler lors d'un entretien.


Avez-vous rencontré un incident ou dysfonctionnement lié à l'usage de l'IA dans vos processus de sécurité ?
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
Oui, et j'accepte d'en parler lors d'un entretien
Oui, mais je préfère ne pas le détailler
Non, pas à ma connaissance
Non applicable (pas encore d'usage IA)