Panorama ESET 2026 de la Cybersécurité des PME en France

Entre Confiance et Nouvelles Réalités

Cybersecurity
Progress. Protected.

Message du vice-président

Michal Jankech

Vice-président chargé des grandes entreprises, des PME et des MSP

Même si votre entreprise est une PME, les menaces qui la ciblent reflètent une réalité bien plus vaste.

En 2026, relever les défis de la cybersécurité implique de comprendre la corrélation des besoins de votre entreprise, du comportement humain, de la démocratisation de puissantes technologies telles que l'IA, des priorités réglementaires et du paysage plutôt instable des menaces. Par conséquent, pour faire face à tout cela, il n'y a qu'une seule solution : devenir plus résilient, en commençant par évaluer son propre niveau de préparation.

Au nom des milliers de PME prises en charge par ESET, et de leurs homologues, qui représentent 90 % de l'activité économique mondiale, nous avons dressé ce bilan de préparation à la cybersécurité afin de mettre en lumière les progrès accomplis pour relever ces défis persistants, ainsi que les enseignements tirés des nouveaux enjeux. Ces éléments sont répertoriés dans l'index afin de rendre compte des récentes décisions prises par les PME en matière de sécurité, qui s'inscrivent dans une démarche visant à renforcer leur résilience.

Table des matières

Ce rapport s'articule autour de 6 thématiques, qui rassemblent des données comparatives sur les résultats mondiaux et français. Lorsque les résultats français se distinguent, elles ont été incluses afin d'apporter un éclairage supplémentaire sur l'évolution des préoccupations et des choix des PME en matière de sécurité.

1

Chiffres clés

Chiffres FRANCE

73 % **des entreprises craignent d'être victimes d'une cyberattaque au cours de l'année à venir**

Menaces les plus préoccupantes

Malwares s'appuyant sur l'IA (36 %), vol d'identifiants et de données d'authentification (34 %), hameçonnage/hameçonnage ciblé (26 %).

Préoccupations pour l'activité

Perte de données (51 %), conséquences financières (42 %) et perturbations opérationnelles (33 %).

Résilience

78 % ont confiance en leur résilience (28 % beaucoup, 18 % un peu).

Incidents

44 % des entreprises ont subi au moins un incident au cours de l'année écoulée (dont 12 % plusieurs incidents et 32 % un seul). Le niveau de risque augmente avec le nombre d'endpoints déployés

Reporting

34 % signalent les incidents à leurs clients et 33 % à leur assureur cyber. Seules 2 % des entreprises ne procèdent à aucun signalement.

Enquêtes et rétablissement

Les enquêtes consécutives à un incident durent généralement jusqu'à deux semaines (42 %) ou entre deux et six semaines (30 %).

Causes des incidents

Les campagnes de phishing (31 %) constituent la première cause d'incident, devant les vulnérabilités non corrigées (24 %) et une mauvaise gestion des comptes et des accès (20 %).

Assurance

71 % ont souscrit une assurance contre les cyber-risques (dont 37 % assortie d'exigences spécifiques de contrôles de sécurité). Les exigences spécifiques sont les plus strictes pour les entreprises ayant connu plusieurs incidents (55 %).

Chiffres FRANCE

Formation et sensibilisation

- 87 % considèrent que la formation est essentielle ou très importante.
- 45 % ont recours à des programmes de qualité, notamment des simulations d'hameçonnage, et 28 % ont recours à des formations complètes (le recours à ce type de formation augmente avec la taille de l'entreprise).
- 53 % organisent plusieurs sessions de formation par an, tandis que 28 % forment leurs collaborateurs au moins une fois par an. Les formations sont plus fréquentes dans les infrastructures critiques et les organisations ayant déjà subi une cyberattaque.

Investissements et ressources

- 80 % jugent leur budget consacré à la cybersécurité suffisant, voire plus que suffisant. 42 % s'attendent à une augmentation de leur budget l'année prochaine.
- Parmi les principaux investissements prévus figurent la formation et la sensibilisation des collaborateurs (41 %), et la sécurité du cloud (31 %).
- Les principaux obstacles sont les contraintes budgétaires (24 %), la complexité et les difficultés d'intégration (21 %) ainsi que la pénurie de talents et de compétences (20 %).

IA et avenir

- Perception : 78 % estiment que la cyberguerre constitue une menace réelle pour leur entreprise. Seuls 35 % estiment que les autorités et les forces de l'ordre prennent actuellement l'avantage sur les cybercriminels.
- Intégration de l'IA : 66 % intègrent l'IA, bien que 72 % reconnaissent qu'elle engendre de nouveaux risques. 62 % disposent d'une politique en matière d'IA.
- Stratégie : les PME souhaitent utiliser l'IA principalement pour anticiper les menaces et neutraliser plus rapidement les attaques.

2

La résilience dans le contexte actuel des menaces

Amélioration de la résilience

En 2022, l'enquête d'ESET concernant les PME avait été publiée le 11 novembre, soit deux semaines seulement avant l'apparition de ChatGPT et avant que les services de détection et de réponse managées (MDR) ne se généralisent auprès des PME.

Quatre ans plus tard, nous sommes revenus sur la question pour comprendre comment les PME gèrent leurs choix en matière de sécurité.

ESET Releases New SMB Research, Finds Cybersecurity Investments Not Keeping Pace with Threat Landscape

Next story

SMBs in the US are more likely to experience a security breach/incident than those in Canada

ESET, a global leader in cybersecurity, today released its 2022 SMB Digital Security Sentiment Report, which surveyed over 1,200 cybersecurity decision makers from small- to medium-sized businesses in Europe and North America. According to the new data, 74% of SMBs in North America and Europe believe that they are more vulnerable to cyberattacks than enterprises. And while these decision makers are concerned about the possible implications of an attack – most notably loss of data, financial impacts and loss of customer confidence and trust – 70% of businesses surveyed admitted that their investment in cybersecurity has not kept pace with recent changes to their operational models (i.e., hybrid working).

Closer to home, the top three challenges identified by SMBs in North American were:

- An inability to keep up with the latest cybersecurity threats (54%)
- Keeping up with the latest cybersecurity approaches and technologies (50%)
- Budget limitations/lack of investment in cybersecurity (49%)

Given these challenges, it's no surprise that over half (51%) of the respondents in North America describe themselves as being not at all confident/slightly confident in their cybersecurity resilience over the upcoming 12 months. The top factors impacting the risk of a cyberattack in the next 12 months, in their perspective, were a lack of employee cybersecurity awareness, continued hybrid or home working, and migrating services to the cloud.

"Earlier this month, it was reported that financial institutions witnessed over $1 billion in potential ransomware-related payments in 2021 — more than double the amount from 2020 and the most ever reported – and yet our research shows that SMBs are not investing enough in cybersecurity solutions, services or employee awareness," said Ryan Grant, vice president of sales for ESET North America. "Many are not following basic cybersecurity best practices, such as using multifactor authentication, updating software regularly and conducting regular cybersecurity audits. This is why ESET continues to invest in, and make available, foundational cybersecurity awareness resources, the latest threat data and intelligence and a comprehensive suite of security solutions to protect companies."

While SMBs in the United States and Canada face similar concerns and investment challenges, the cybersecurity landscape has its differences. For instance, 74% of U.S. respondents vs. 56% of Canadian respondents say they have experienced or acted on strong indications of a data security incident or breach in the last 12 months. And 43% of U.S. respondents noted they had more than one incident in the same time period vs. 28% of Canadian respondents.

"What the data suggests is that Canadian businesses are experiencing fewer data breaches, which could be due to good privacy legislation that includes the requirement for cybersecurity," said Tony Anscombe, Chief Security Evangelist for ESET. "The data provides a clear indication of a disconnect between the cyber threat faced by SMBs and the investment they are making in cybersecurity. With current efforts by enterprises, critical infrastructure and governments to improve their cybersecurity, cybercriminals are likely to shift their efforts to lower-tier targets in order to monetize their activities - making it essential for SMBs to improve their cybersecurity posture."

Here are some other top highlights from the 2022 SMB Digital Security Sentiment Report:

Other Press Releases

ESET opens Women in Cybersecurity Scholarship 2026 applications on International Women's Day

ESET's Ryan Grant named a 2026 CRN Channel Chief

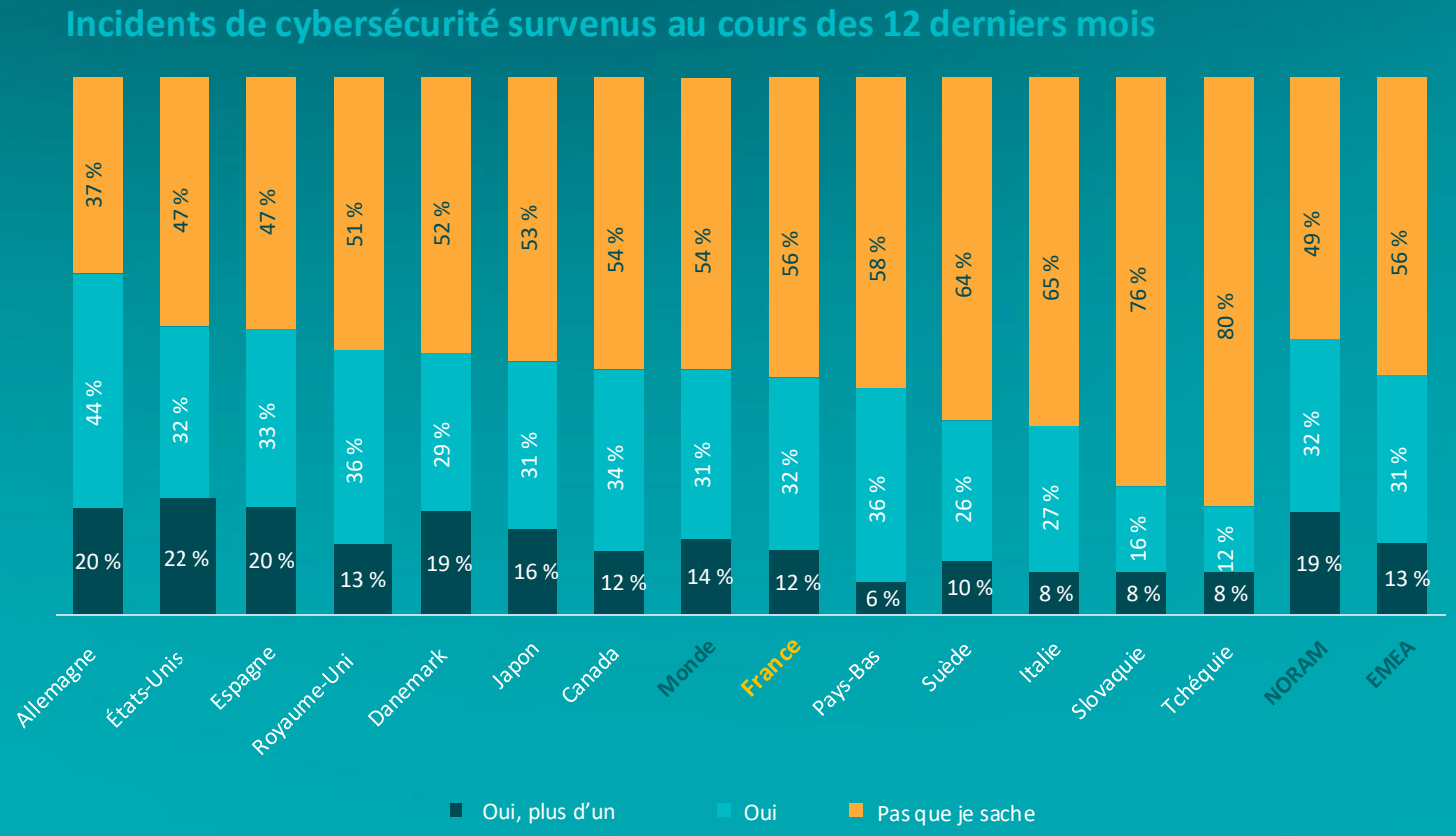
ESET's Chief Security Evangelist Tony Anscombe to Speak at NetDiligence Cyber Risk Summit

ESET Wins Gender Parity Award at CRN's 2025 Women of the Year Awards Gala

- La démocratisation de l'accès à des technologies telles que l'IA, la maturation des plateformes de collaboration et l'évolution du contexte géopolitique ont fait de 2026 une année marquée par un contexte sécuritaire très différent.
- Les PME ont dû revoir leur stratégie de sécurité, ce qui a mis à rude épreuve leurs budgets et leurs choix technologiques pour devenir, et rester, résilientes.
- Dans cette enquête, nous avons cherché à déterminer comment tous ces changements ont influencé les principales préoccupations de sécurité des PME en 2026.

Les anciennes vérités demeurent pertinentes : au niveau mondial, les petites entreprises ne sont pas à l'abri des attaques

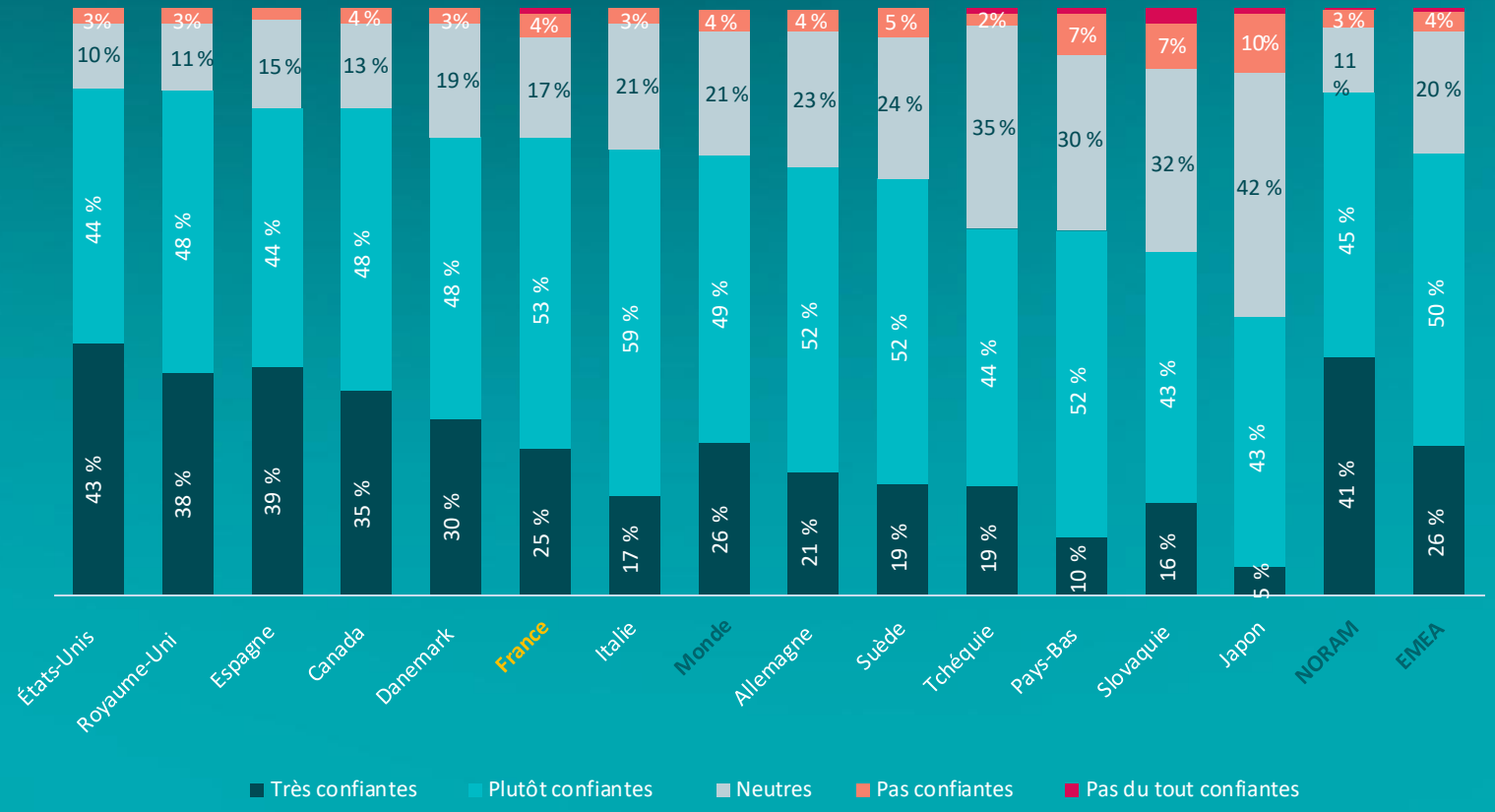
- Près d'une PME sur deux interrogées a déclaré avoir été victime d'un incident au cours des 12 derniers mois.
- L'Allemagne arrive en tête avec le taux le plus élevé d'incidents enregistrés (un ou plusieurs), suivie des États-Unis et de l'Espagne.
- Le Royaume-Uni, le Danemark, le Japon et le Canada suivent, affichant des résultats supérieurs à la moyenne mondiale.
- La **France**, les Pays-Bas, la Suède et l'Italie ont des résultats inférieurs à la moyenne mondiale.



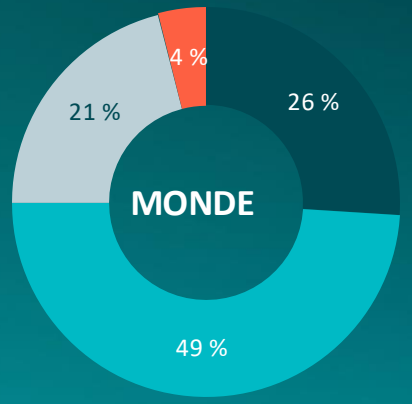
À l’échelle mondiale, la majorité des PME se montrent confiantes quant à leur résilience

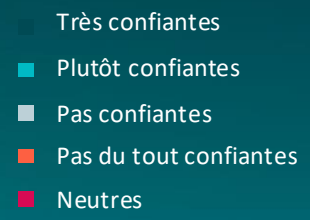
- Les personnes interrogées aux États-Unis et au Royaume-Uni affichent le niveau de confiance le plus élevé.
- Avec en tête l’Espagne, le Danemark, la France et l’Italie, les personnes interrogées en Europe ont également des résultats supérieurs à la moyenne mondiale. L’Allemagne et la Suède ont des résultats juste en dessous.
- Le Japon fait figure d’exception, avec un faible nombre de réponses « Très confiantes » et, à l’inverse, un taux très élevé de réponses « Neutres ».
- Le niveau de confiance global (75 %) a considérablement augmenté par rapport à notre enquête de 2022 (48 %).

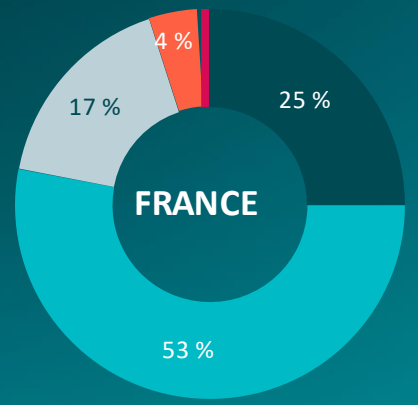
Confiance dans la résilience face aux cyberattaques

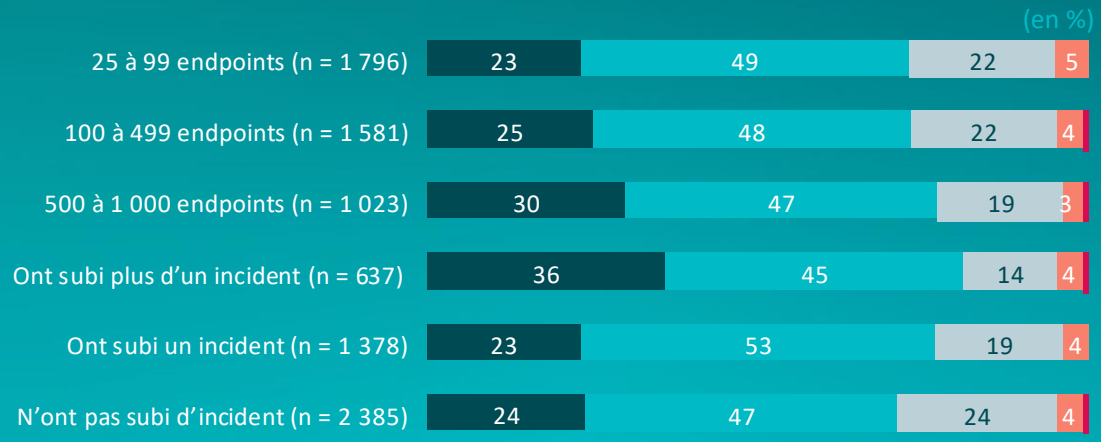


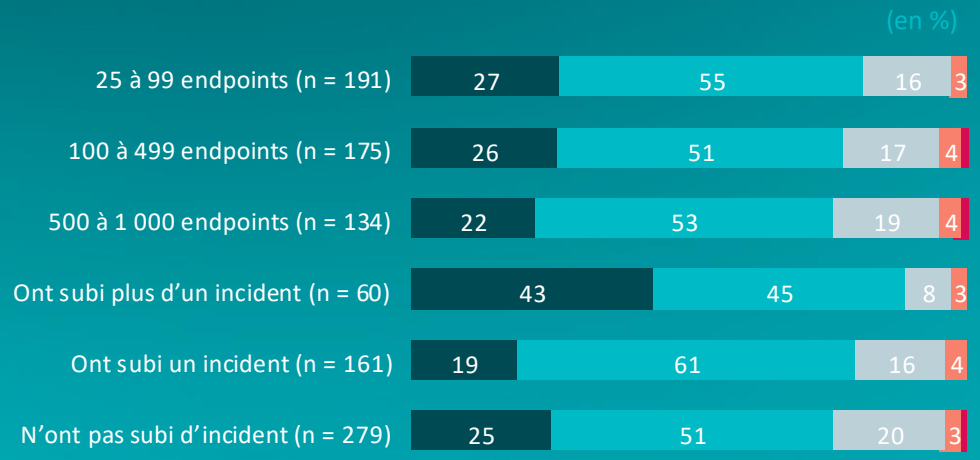
La confiance dans la résilience cyber demeure forte : 75% des organisations, en France comme dans le monde, estiment être en mesure de faire face à une cyberattaque et d'en limiter les impacts











À l’échelle mondiale, les préoccupations concernant les menaces sont globalement similaires

Les 2 principales sources d’inquiétude

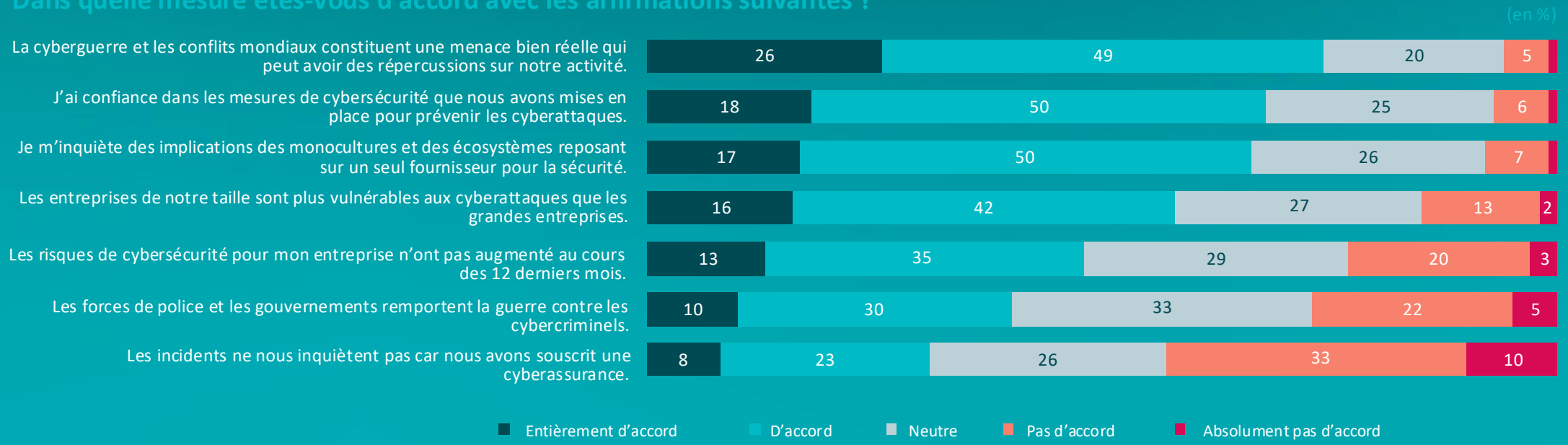
- CYBERGUERRE

Les PME ont peut-être confiance dans leur sécurité, mais 75 % d’entre elles conviennent que les conflits mondiaux et la cyberguerre leur semblent très proches.

- CONSOLIDATION DES FOURNISSEURS

67 % des PME s’inquiètent des monocultures et des écosystèmes reposant sur un seul fournisseur.

Dans quelle mesure êtes-vous d’accord avec les affirmations suivantes ?

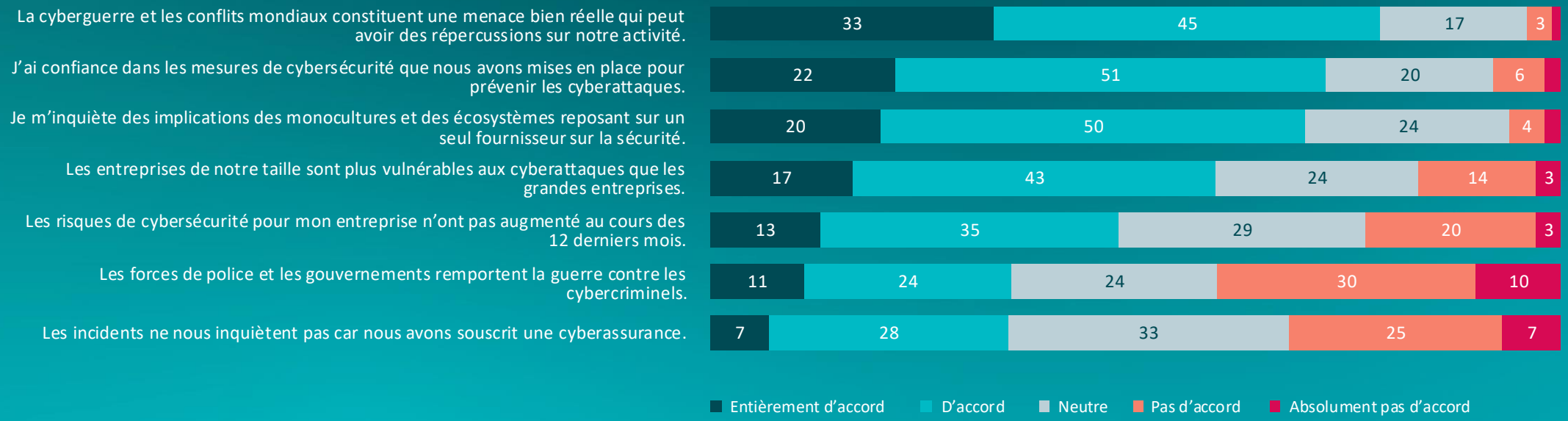


Entre vigilance et incertitude : le regard des entreprises sur l’évolution de la menace cyber

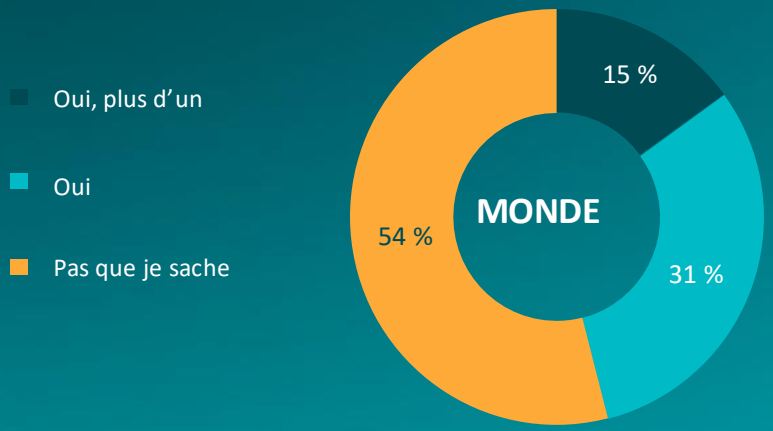
Les organisations françaises reconnaissent largement la réalité et l'intensification des cybermenaces, tout en affichant une confiance limitée dans la capacité des acteurs publics à inverser durablement la tendance.

Dans quelle mesure êtes-vous d’accord avec les affirmations suivantes ?

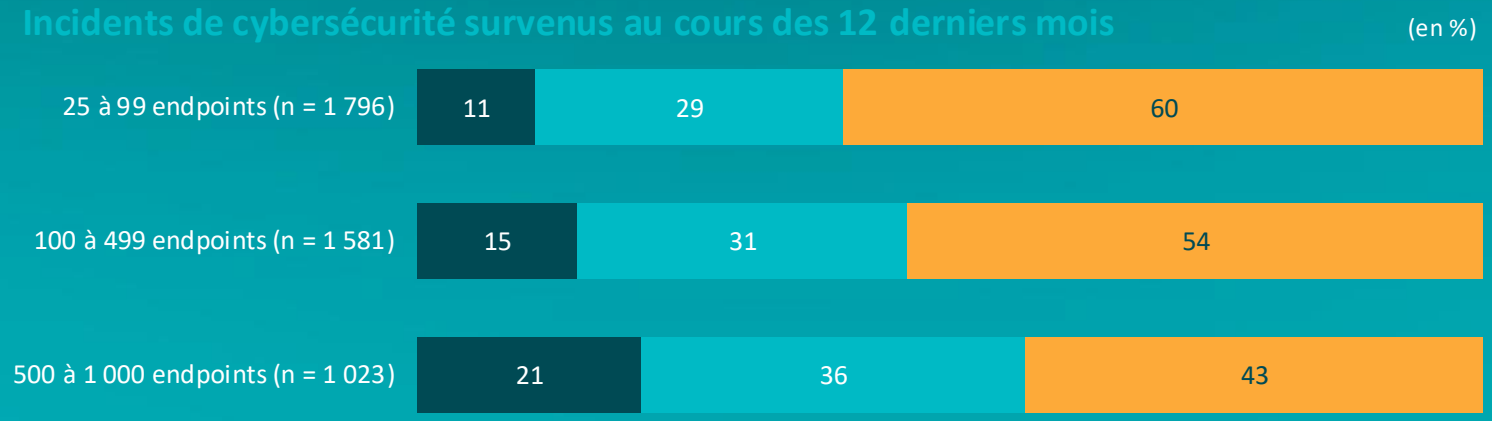
(en %)



Près de la moitié des PME à travers le monde ont été victimes d'au moins un incident au cours de l'année écoulée



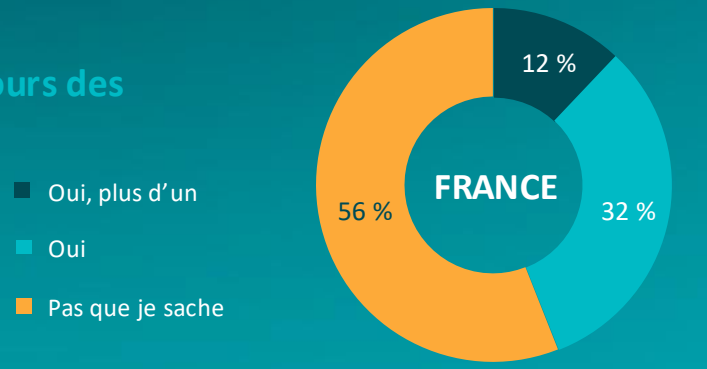
- À l'échelle mondiale, la majorité des PME comptant plus de 500 endpoints ont été confrontées à un ou plusieurs incidents.
- Les plus petites PME interrogées, celles comptant entre 25 et 99 endpoints, ont indiqué avoir connu 30 % d'incidents en moins que celles comptant entre 500 et 1 000 endpoints.



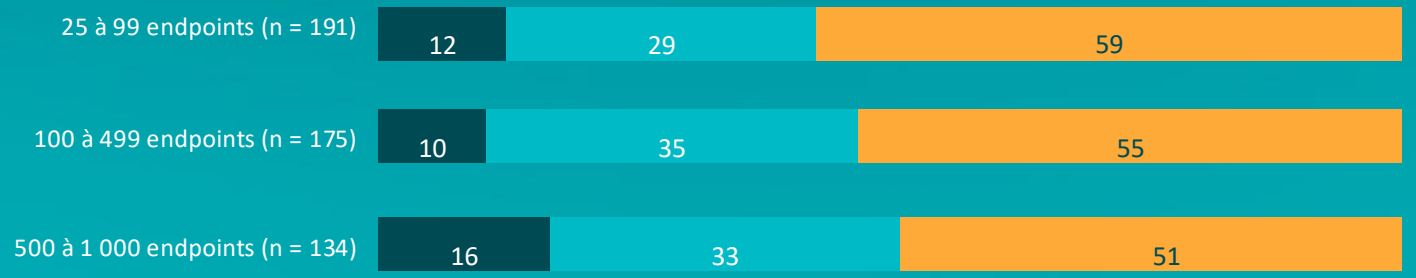
En France, l'exposition aux incidents cyber demeure élevée, en particulier dans les environnements les plus étendus.

- Les incidents de cybersécurité restent une réalité pour de nombreuses **organisations françaises : 44 % déclarent en avoir subi au moins un au cours des 12 derniers mois.**
- Cette proportion atteint près d'une organisation sur deux parmi celles comptant 500 à 1 000 endpoints, soulignant **l'augmentation de la surface d'attaque et de la complexité de sécurisation des infrastructures à mesure que celles-ci grandissent.**

Incidents de cybersécurité survenus au cours des 12 derniers mois



(en %)

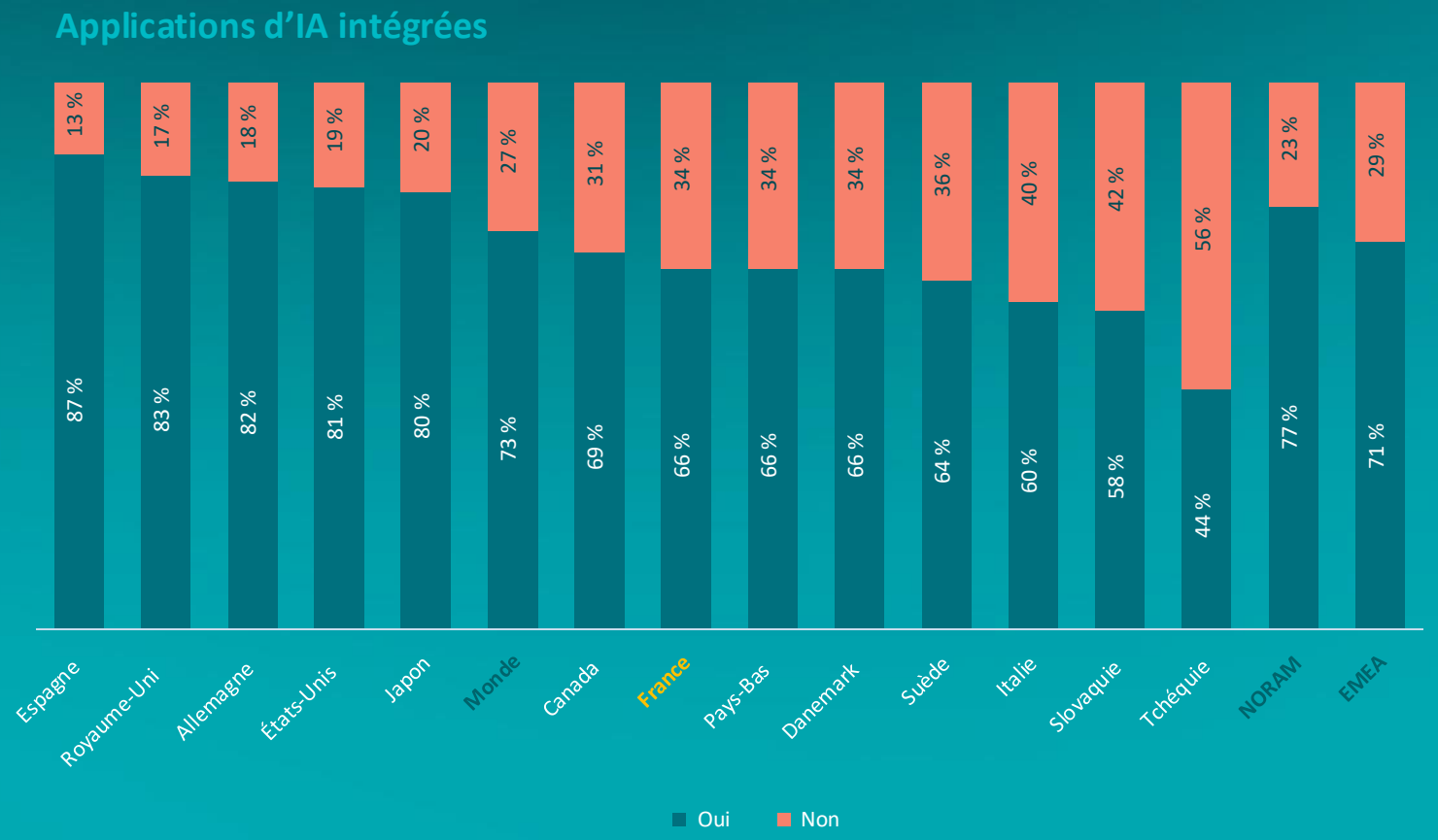


3

L’IA doit-elle contribuer à la résilience ?

L’intérêt mondial pour l’intégration de l’IA varie

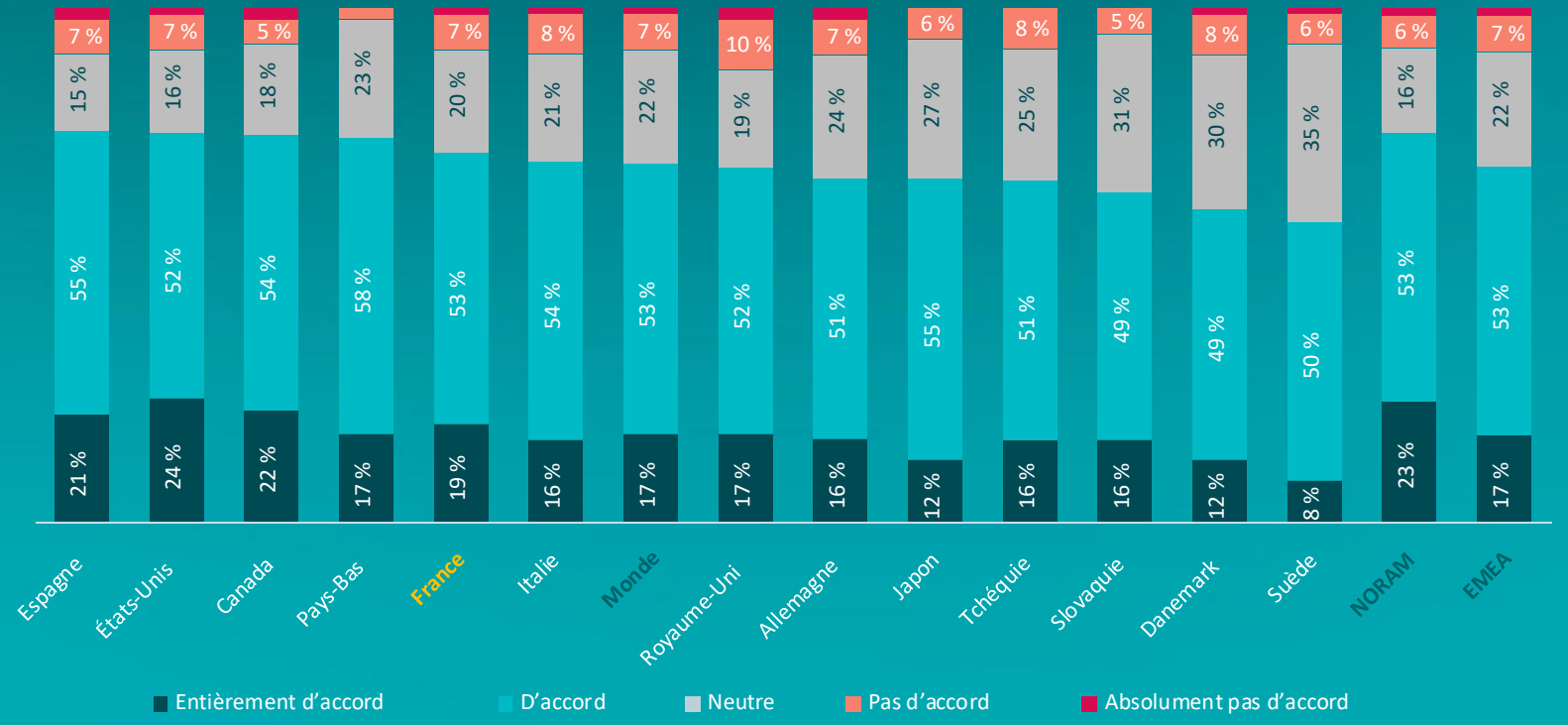
- Le taux d’intégration d’IA en Europe atteint 71 %, mais l’intérêt au niveau national varie d’un pays à l’autre.
- La **France** affiche un **taux d’intégration de l’IA de 66 %**, légèrement inférieur à la moyenne mondiale (73 %) et européenne (71 %). Si elle reste en retrait par rapport aux pays les plus avancés comme l’Espagne ou le Royaume-Uni, l’IA est désormais utilisée par près de deux entreprises sur trois, qui témoigne d’une adoption déjà significative et d’un potentiel de développement encore important.



L'adoption de l'IA progresse indépendamment des préoccupations de sécurité

Malgré des niveaux de préoccupation variables selon les pays, aucune corrélation nette n'apparaît entre la perception des risques de sécurité liés à l'IA et son niveau d'adoption. Les PME les plus engagées dans l'utilisation de l'IA ne sont pas nécessairement les plus inquiètes, suggérant que les bénéfices perçus l'emportent souvent sur les préoccupations de sécurité.

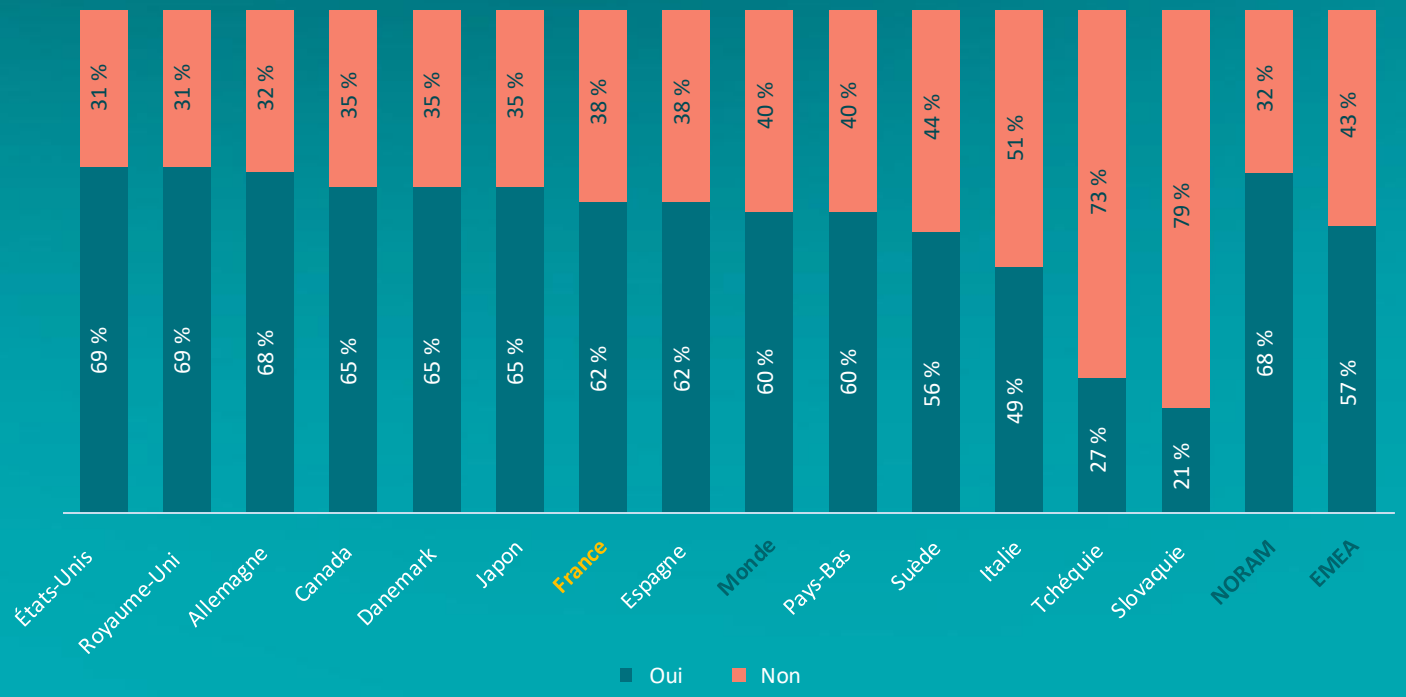
L'utilisation d'applications d'IA entraîne des risques supplémentaires de sécurité



Les pays les plus avancés dans l'adoption de l'IA encadrent davantage son utilisation

- De manière générale, les pays où les taux d'intégration et d'utilisation de l'IA sont plus élevés mettent également mieux en œuvre les politiques d'IA.
- **La France** se distingue par une approche relativement proactive de la gouvernance de l'IA : 62 % des entreprises déclarent avoir mis en place des politiques visant à restreindre l'utilisation d'applications d'IA non approuvées, un niveau supérieur à la moyenne mondiale (60 %). Ce résultat traduit une prise de conscience des enjeux de sécurité et de conformité liés à l'IA, même si une part importante des organisations (38 %) n'a pas encore formalisé de telles mesures.

Politique d'IA visant à restreindre l'utilisation d'applications d'IA en dehors des plateformes ou des processus approuvés



Perception vs réalité : les PME s’inquiètent-elles des bonnes menaces ?

01

Les PME affirment que les malwares s’appuyant sur l’IA constituent leur principale préoccupation pour l’année à venir, ce qui témoigne de la place prépondérante qu’occupe désormais l’IA dans l’actualité et les discussions au sein des conseils d’administration.

02

Cependant, les causes réelles des incidents brossent un tableau très différent : elles mettent en évidence l’hameçonnage, l’absence de surveillance de la sécurité, les failles de sécurité non corrigées et la faiblesse des mots de passe comme facteurs à l’origine de ces incidents.

03

Pourtant, l’un des risques les plus graves, à savoir la compromission de la chaîne d’approvisionnement, ne figure pratiquement pas parmi les principales préoccupations des PME, malgré le risque d’un impact en cascade à grande échelle.

Au niveau mondial, les inquiétudes concernant les malwares basés sur l'IA sont vives… mais injustifiées

0

L'ensemble de données de MDR d'ESET ne recense aucun incident dans lequel l'IA générative aurait joué un rôle significatif. Si de nombreuses menaces s'appuient sur l'IA, l'utilisation opérationnelle de l'IA, mobilisée en temps réel pour des tâches automatisées, reste toutefois peu courante.

Les actualités concernant les malwares s'appuyant sur l'IA ne manquent pas. Il n'est donc pas étonnant que de nombreuses entreprises s'en inquiètent.

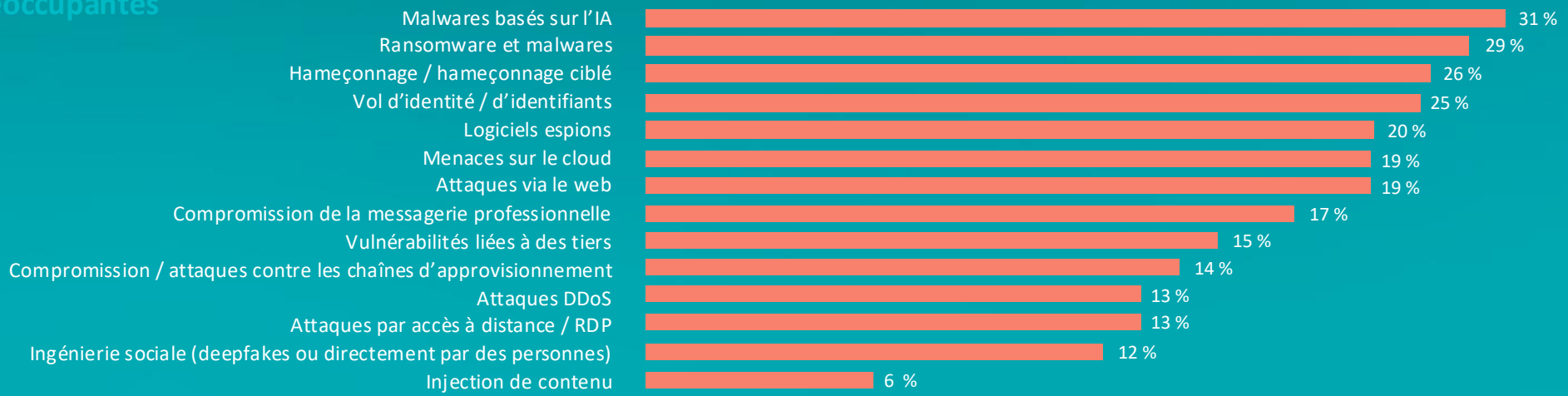
Les malwares basés sur l'IA sont rares. Il s'agit de malwares qui utilisent l'IA de manière automatisée et en temps réel.

À l'heure actuelle, ces malwares sont un sujet brûlant pour les chercheurs en cybersécurité, mais pas pour les équipes informatiques des PME.

Les découvertes d'ESET :

- PromptLock : 1er ransomware basé sur l'IA, en phase expérimentale
- PromptSpy : 1er malware Android utilisant l'IA pour assurer sa persistance

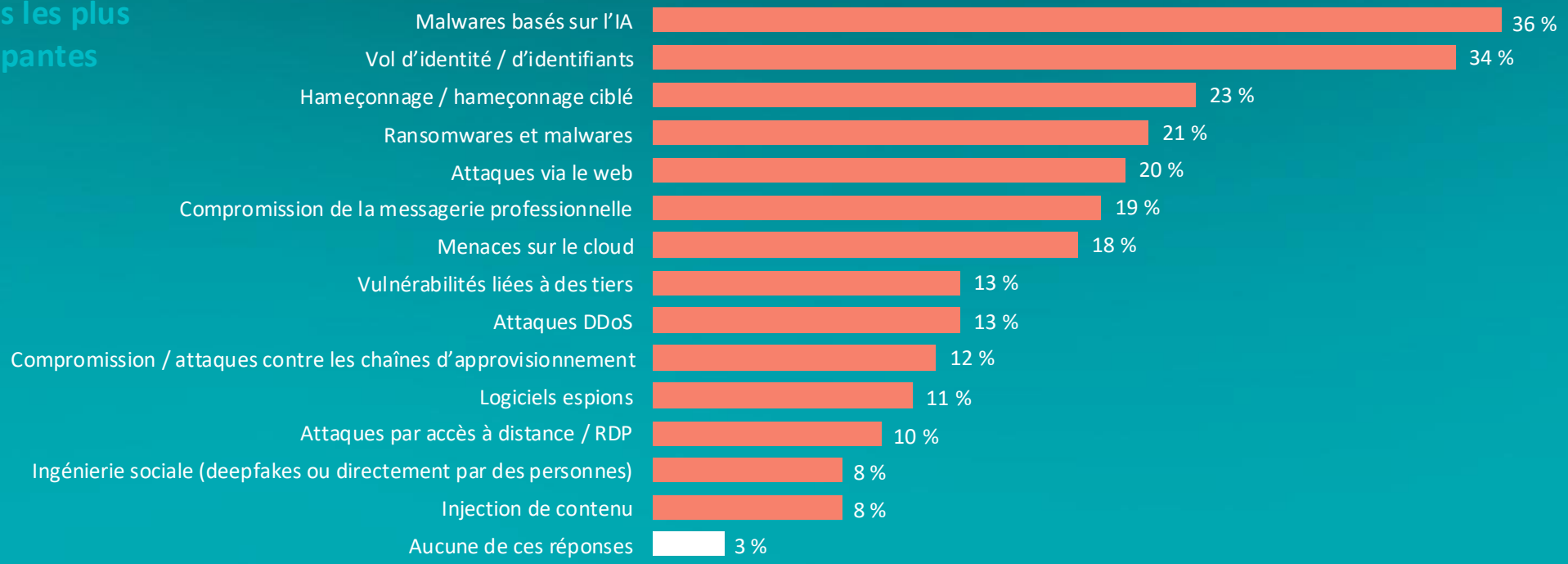
Menaces les plus préoccupantes



Les menaces liées à l'IA arrivent également en tête des préoccupations cyber des entreprises françaises.

L'IA cristallise les inquiétudes des entreprises françaises, qui la perçoivent comme un accélérateur potentiel des cybermenaces, devant des risques pourtant plus fréquemment observés tels que les ransomwares ou l'hameçonnage.

Menaces les plus préoccupantes



Menaces par l’IA

- La principale menace actuelle liée à l’IA réside dans le fait que les attaquants s’en servent pour automatiser certaines phases d’attaques existantes, tout comme les collaborateurs l’utilisent pour automatiser des tâches fastidieuses, simples ou répétitives.
- Pour les attaquants, l’IA est actuellement un outil qui leur permet de créer et de mener des campagnes malveillantes plus facilement et plus rapidement.
- Quelles en sont les conséquences concrètes ? Une augmentation du nombre de messages d’hameçonnage de plus en plus convaincants et une multiplication rapide des nouvelles variantes de malwares en circulation.

Nous constatons que toute utilisation directe de l’IA pour créer des malwares et des scripts reste limitée et ponctuelle. En réalité, l’évolution du paysage des menaces s’articule autour de l’ingénierie sociale et de l’accélération générale des attaques, y compris celles visant la chaîne d’approvisionnement. Cependant, à mesure que la qualité des outils de programmation s’améliore, nous prévoyons une augmentation similaire dans le développement de malwares.

Il est évident que le principal défi reste la multiplication constante des messages qui incluent des vecteurs d’attaque générés par l’IA. Toutes ces améliorations permettent même à des attaquants peu expérimentés d’orchestrer des escroqueries sophistiquées à grande échelle et à moindre coût, car ils disposent désormais de moyens qui n’étaient auparavant accessibles qu’aux APT.

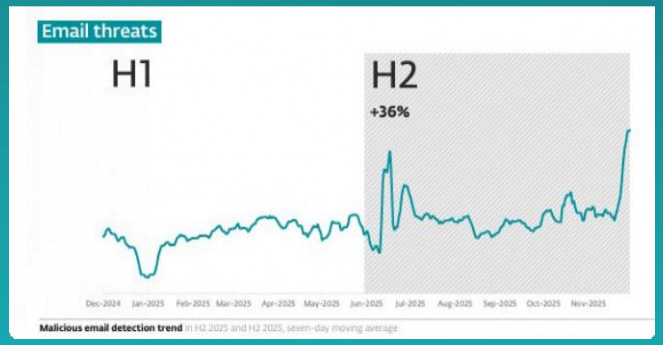
Les attaquants s’appuient de plus en plus sur l’automatisation et sur la création d’une apparence de fiabilité plutôt que sur la mise en place de véritables fonctionnalités d’IA, en utilisant l’IA pour imiter des présentations et des interactions de qualité professionnelle, qui font de l’ingénierie sociale l’un des principaux champs de bataille des cyberdéfenses.

Juraj Jánošík

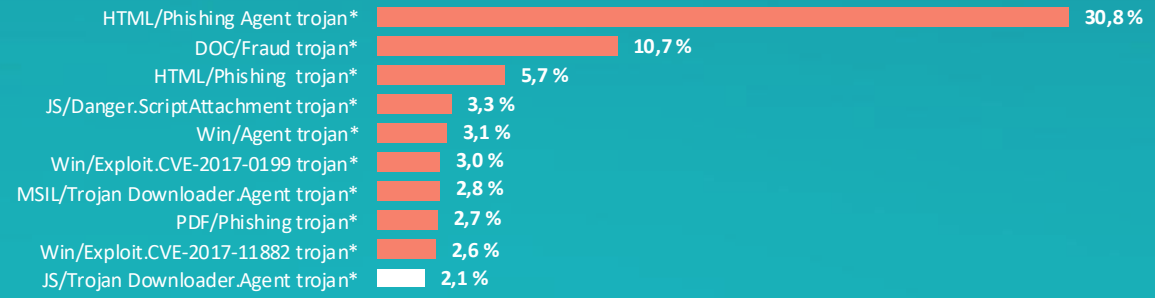
Vice-président chargé de l’IA chez ESET

À l’échelle mondiale, l’hameçonnage reste la principale menace

L’hameçonnage dans la télémétrie d’ESET



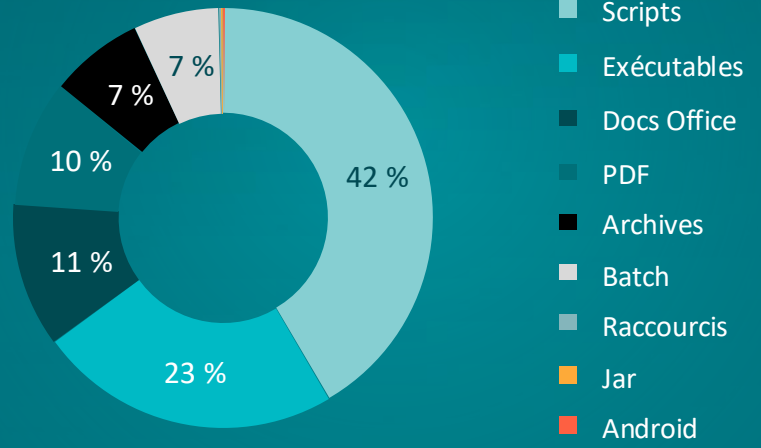
Les données de télémétrie d’ESET montrent que l’hameçonnage est la principale menace détectée et que le nombre de détections est en hausse, selon le Rapport général sur les menaces du S2 2025.



* Cheval de Troie

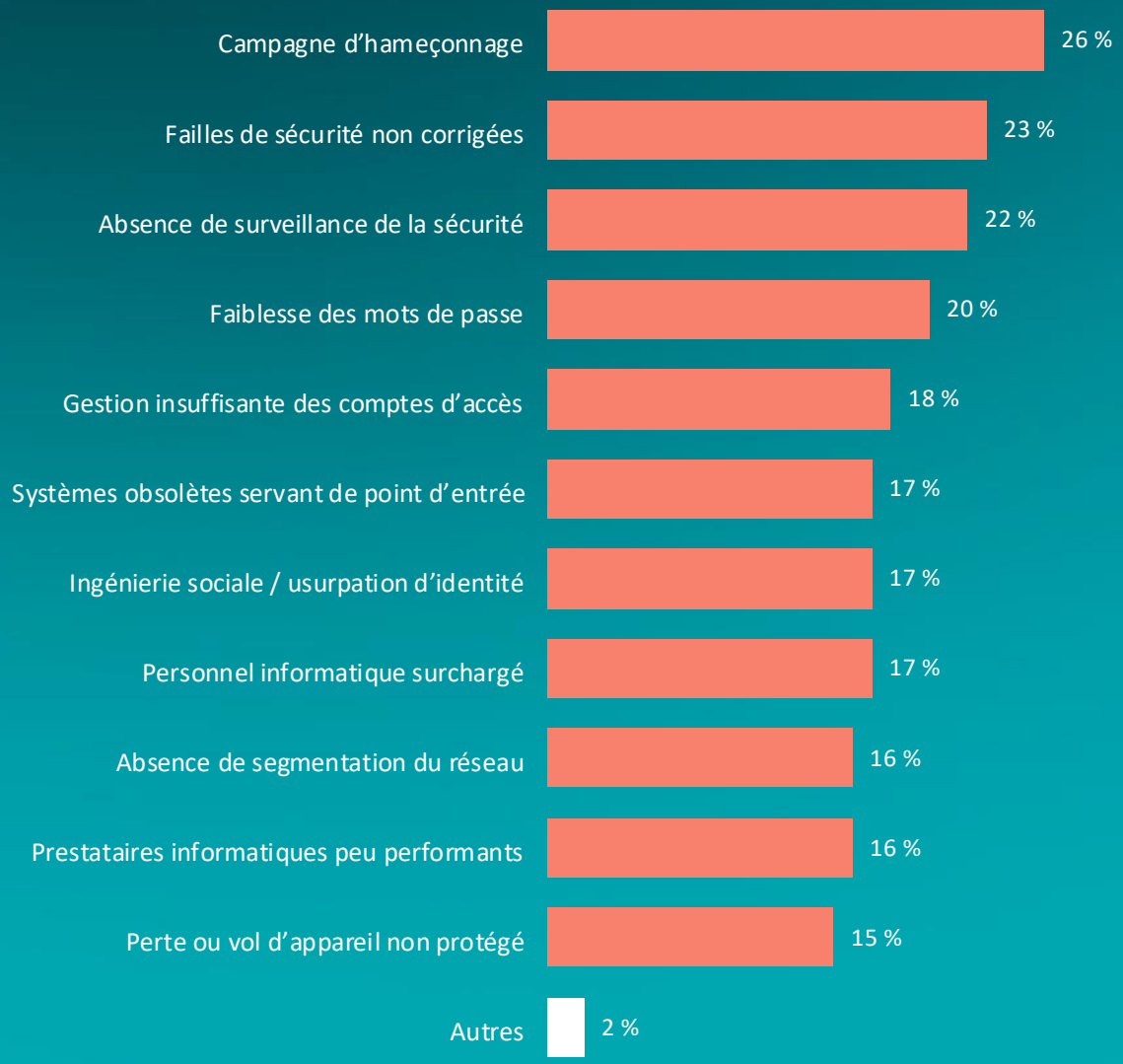
Top 10 des menaces détectées dans les emails au H2 2025

Bien entendu, l’hameçonnage se reflète également dans le nombre de menaces par e-mail.



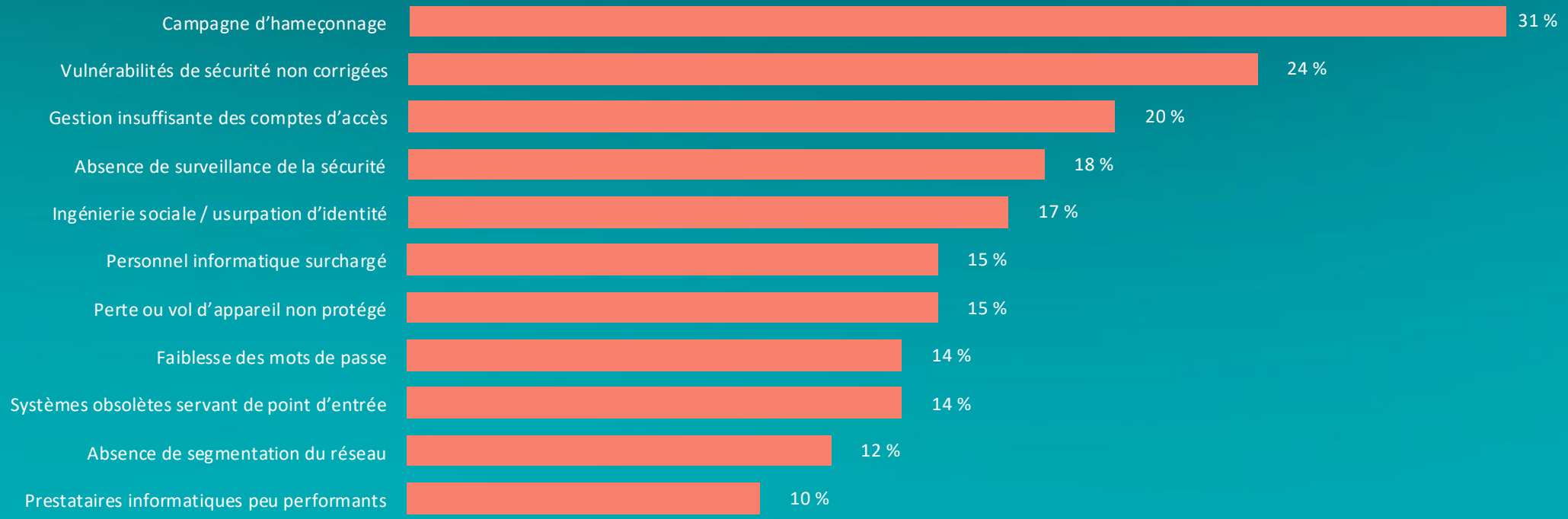
Ce n’est pas de l’IA mais d’anciennes cybermenaces automatisées

- Les personnes interrogées s’inquiètent des malwares basés sur l’IA.
- Au contraire, elles doivent se préparer à faire face à une recrudescence des mêmes menaces que d’habitude, désormais automatisées et accélérées par des outils d’IA.



Les entreprises françaises identifient avant tout des faiblesses opérationnelles et humaines comme principales portes d'entrée des cyberattaques.

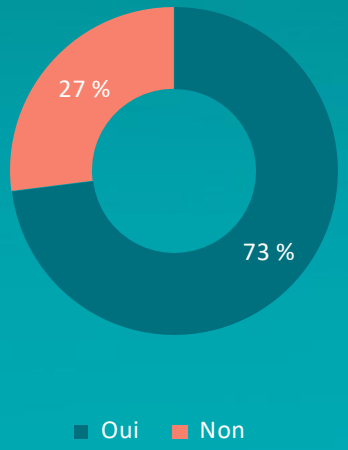
Si l'IA concentre de nombreuses inquiétudes, les entreprises françaises estiment que les cybercriminels continueront principalement à tirer parti de vecteurs éprouvés : phishing, manque de supervision, vulnérabilités non corrigées et faiblesses organisationnelles. Cette perception rappelle que les fondamentaux de la cybersécurité restent la première ligne de défense face aux menaces actuelles.

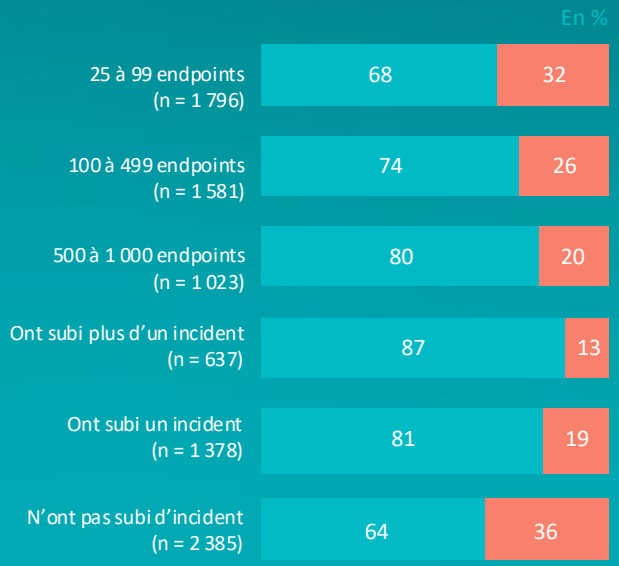


L’IA interne est une menace, que cela vous plaise ou non

- En seulement trois ans, l’IA a révolutionné la manière dont les collaborateurs accomplissent leurs tâches quotidiennes. De nombreuses entreprises ont intégré des outils d’IA pour gagner en efficacité.
- Mais comme toute nouvelle technologie, les outils d’IA attirent les cybercriminels. Les PME interrogées semblent conscientes des risques liés à l’intégration de l’IA.
- Les entreprises qui ont subi davantage d’incidents ont davantage recours à l’IA et sont plus conscientes des risques associés.

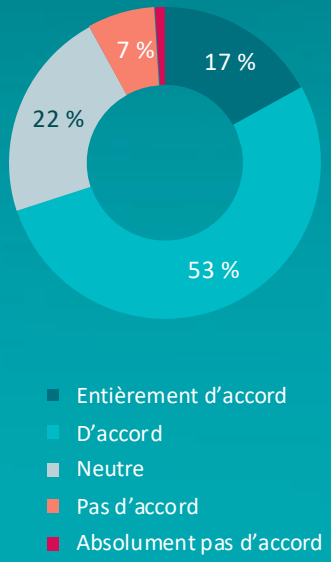
Applications d’IA intégrées

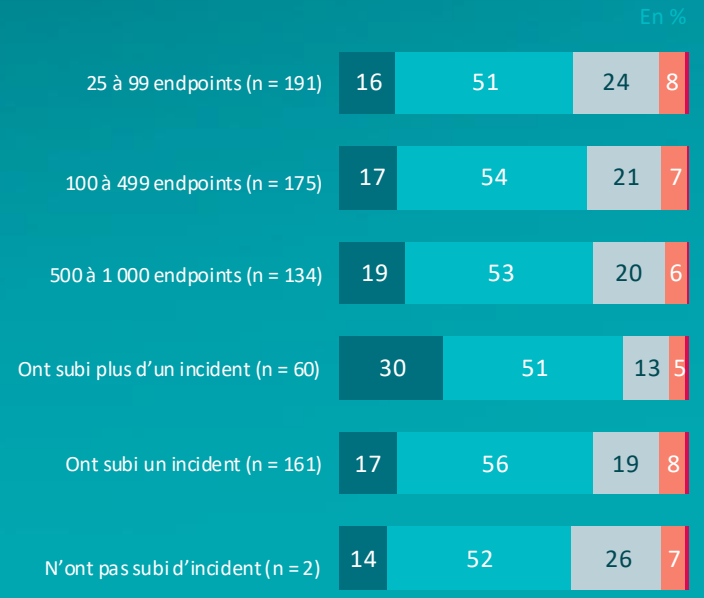




Je suis d’accord avec cette affirmation :

« L’utilisation d’applications d’IA entraîne des risques de sécurité supplémentaires »





Outils et agents d’IA émergents

- Les outils et les agents d’IA peuvent être des « collègues » efficaces, mais les attaquants peuvent les tromper et détourner leurs privilèges.
- Par exemple, ESET a recensé des attaques par l’IA qui exploitent des compétences agentiques* accessibles au public, transformant ainsi les agents d’IA en menaces internes au sein d’un système compromis.
- Pour en savoir plus : article d’ESET : La crise de sécurité qui se profile sur les plateformes d’agents d’IA

** Une compétence d’IA est un ensemble d’instructions, de scripts et de documents de référence pouvant remplacer des séries complexes de commandes, ce qui simplifie considérablement le travail avec les agents d’IA.*

Des milliers de compétences de ce type sont ajoutées chaque jour.

1.

Une analyse de 60 000 compétences accessibles au public a révélé que des milliers d’entre elles sont pour le moins suspectes et que des centaines sont véritablement malveillantes.

2.

Les catégories de malwares les plus fréquemment détectées étaient les chevaux de Troie, les téléchargeurs, les portes dérobées, les logiciels espions, les enregistreurs de frappe et les extracteurs de cryptomonnaie.

3.

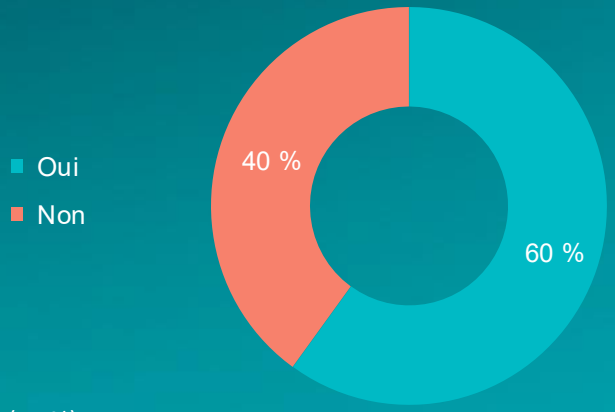
Des dizaines de compétences comprenaient des techniques d’ingénierie sociale et d’hameçonnage, tant au sein même de la compétence qu’au sein de l’écosystème qui l’entoure.

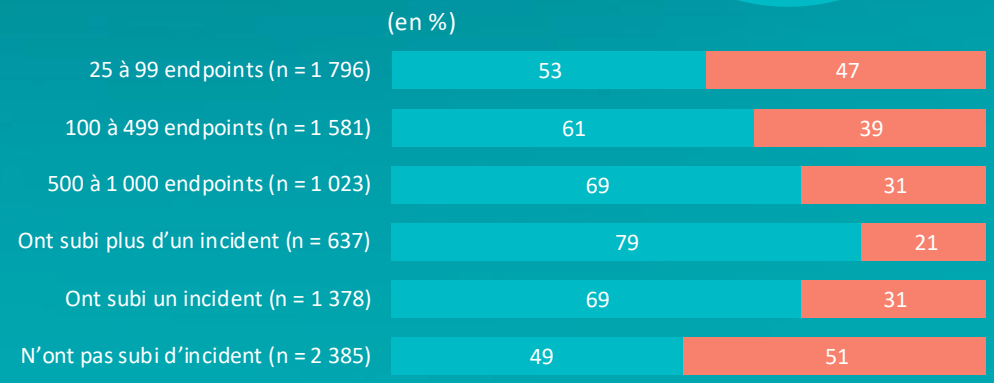
Certaines PME ignorent l'IA à leurs risques et périls

Au niveau mondial, 73 % des entreprises qui n'intègrent pas d'outils d'IA ne disposent pas non plus de politiques d'IA

- Bien que les cybercriminels recourent massivement aux outils d'IA, de nombreuses entreprises ne prennent toujours pas les mesures adéquates pour faire face à ces menaces : (40 %) des entreprises ne disposent pas d'une politique d'IA adéquate.
- Les données ont également révélé que la plupart des entreprises qui n'intègrent pas d'outils d'IA ont également tendance à négliger l'importance des politiques d'IA. Les collaborateurs continuent cependant d'utiliser des outils librement accessibles pour améliorer leurs performances à l'insu de la direction.

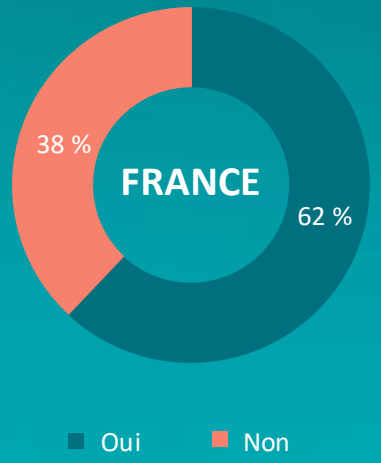
Politique d'IA visant à restreindre l'utilisation d'applications d'IA en dehors des plateformes ou des processus approuvés

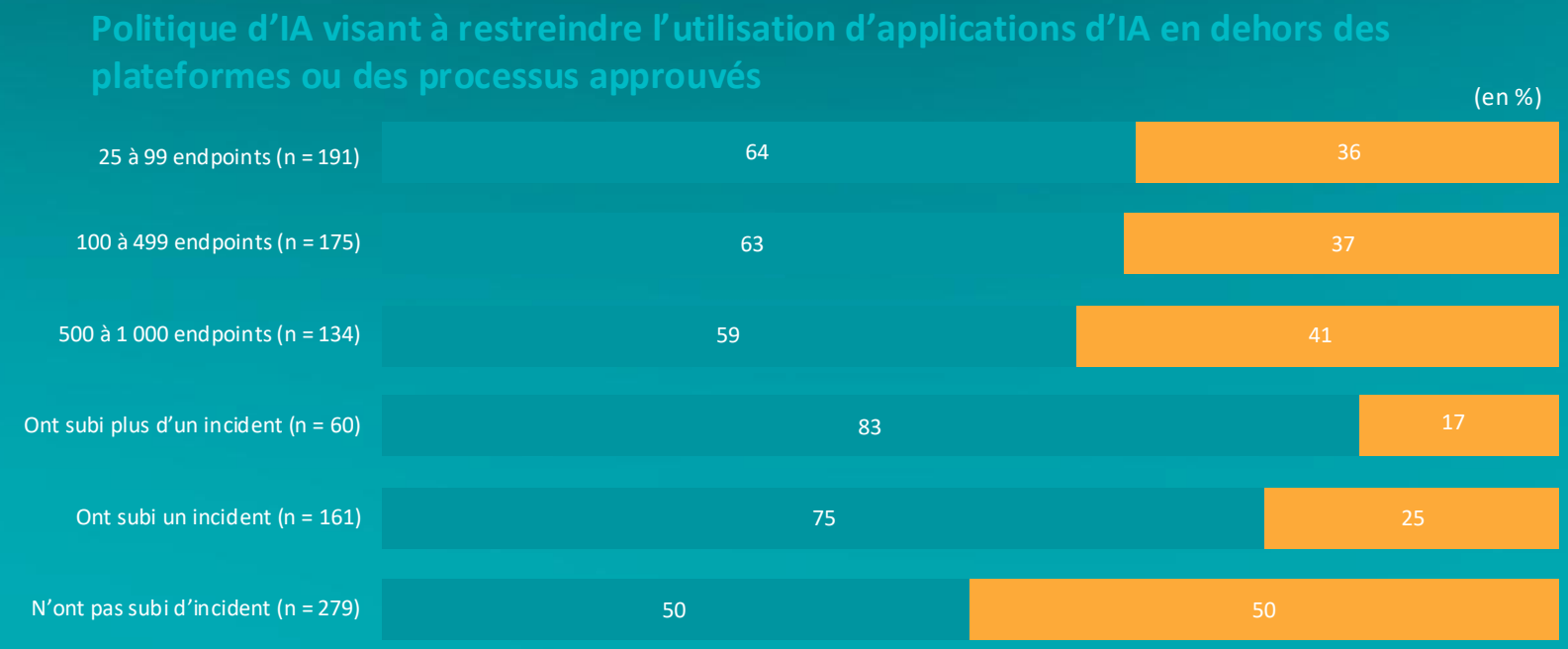




En France, les entreprises confrontées aux cyberincidents renforcent davantage leur gouvernance de l'IA

Si près de deux tiers des entreprises françaises ont instauré des règles encadrant l'usage de l'IA, cette proportion atteint plus de 80 % parmi les organisations ayant subi plusieurs incidents de cybersécurité. À l'inverse, une entreprise sur deux n'ayant jamais connu d'incident ne dispose toujours pas de politique dédiée, illustrant un décalage entre l'adoption de l'IA et sa gouvernance.

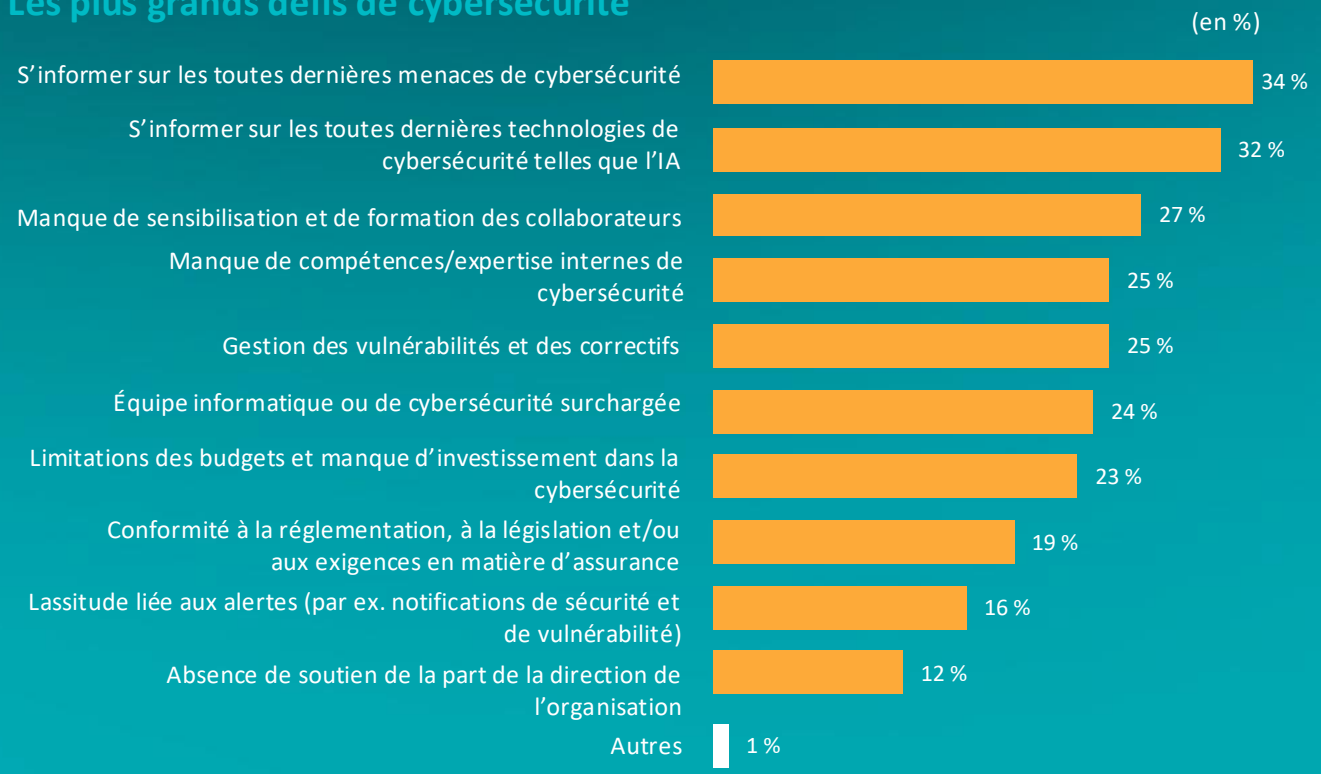




Les PME souhaitent mieux comprendre et anticiper les attaques. L'IA peut aider.

- Quel est le plus grand défi de cybersécurité pour les PME ? S'informer sur les toutes dernières menaces de cybersécurité.
- Le second ? Maîtriser les technologies d'IA pour les aider à y parvenir.
- Les PME reconnaissent clairement l'utilité de l'IA pour la cyberdéfense, mais soit les outils ne sont pas encore au point, soit ils ne sont pas disponibles.
- Par rapport à 2022 (43 %), les PME sont désormais beaucoup moins préoccupées par le manque d'accès à une formation de qualité en matière de sensibilisation à la cybersécurité pour leurs collaborateurs (27 %).

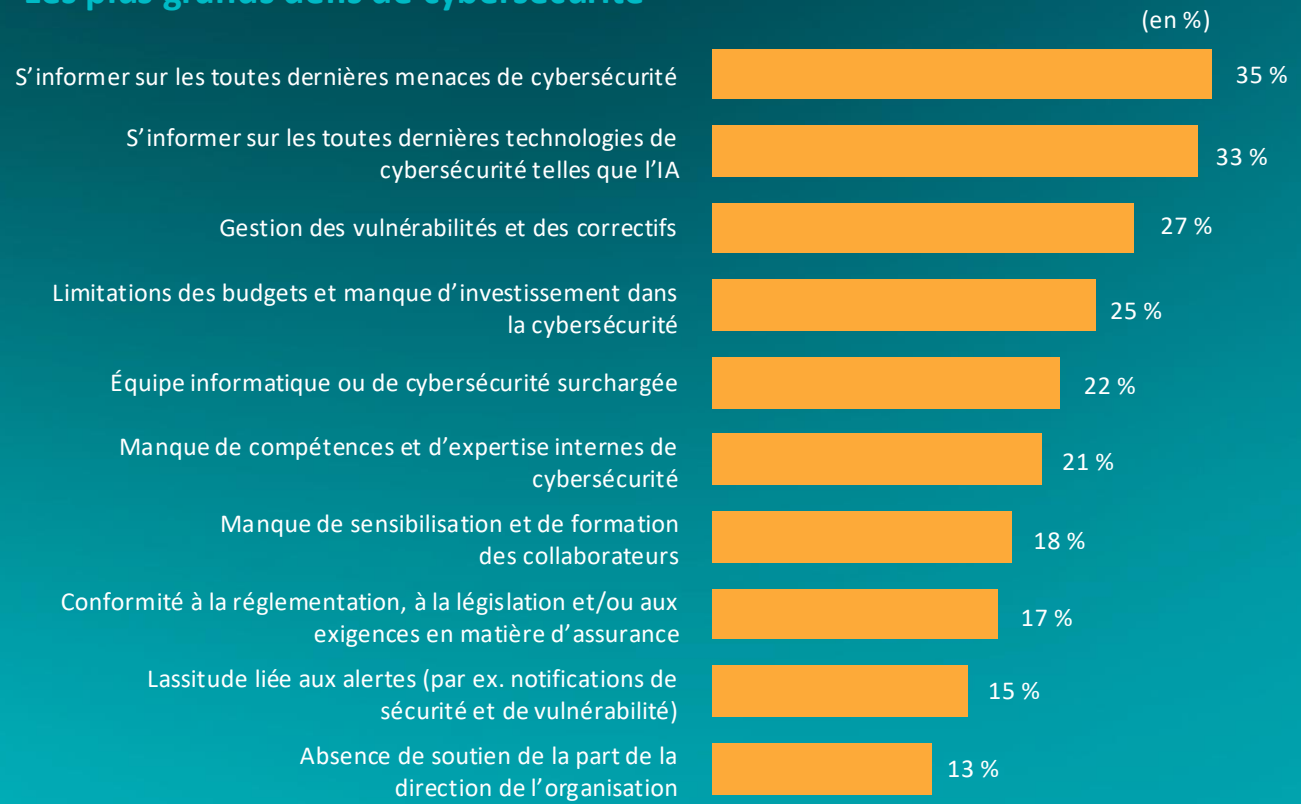
Les plus grands défis de cybersécurité



En France, le défi n'est plus seulement de se protéger, mais de suivre le rythme de l'évolution des menaces et des technologies

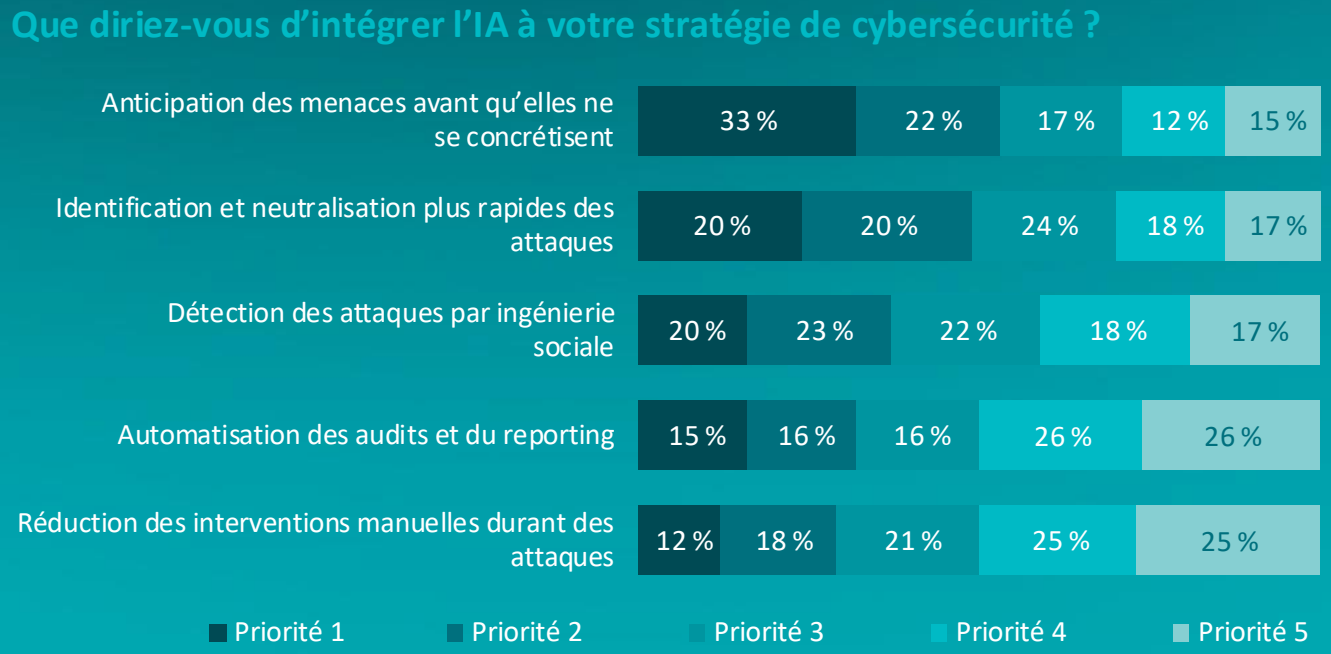
Les entreprises françaises placent l'accès à l'information et à l'expertise au cœur de leurs préoccupations cyber. Les deux premiers défis concernent la compréhension des nouvelles menaces et des technologies émergentes, devant les enjeux de ressources ou de gouvernance. Cette tendance illustre la difficulté croissante à maintenir un niveau de connaissance adapté dans un paysage cyber en mutation rapide.

Les plus grands défis de cybersécurité



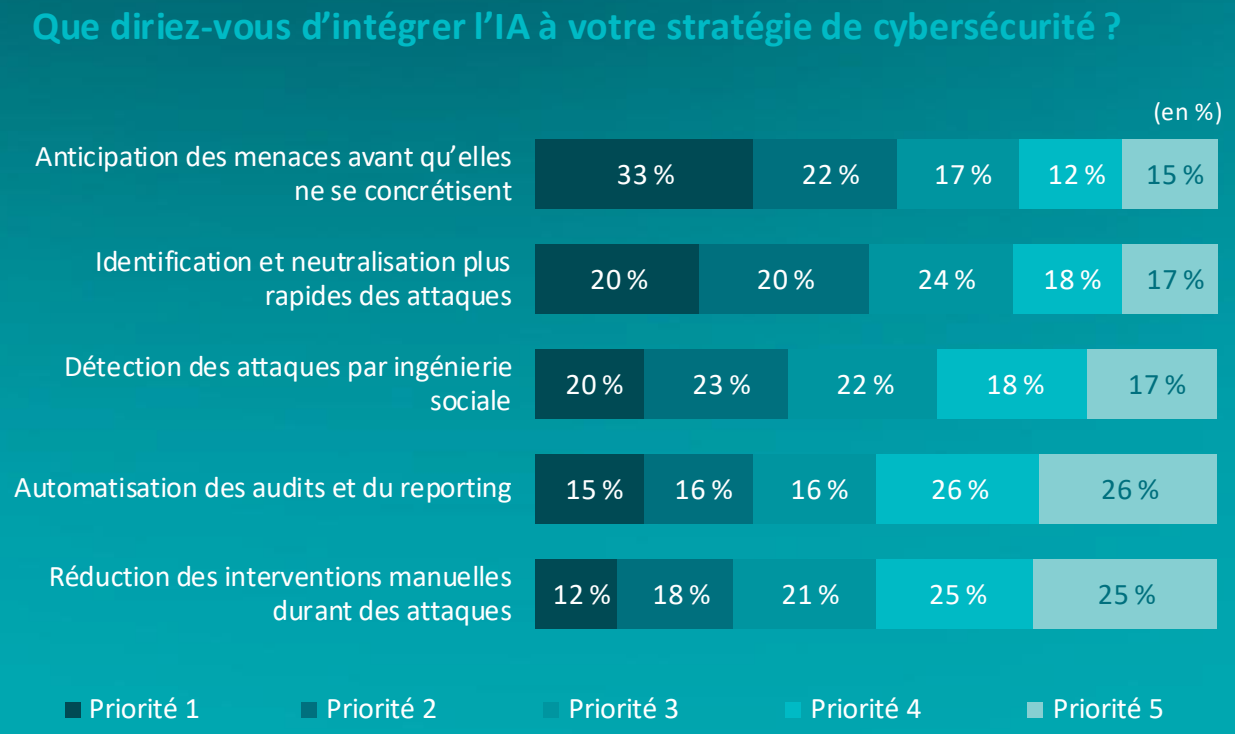
Les menaces liées à l'IA préoccupent les PME, sans occulter ses bénéfices

- Les PME s'inquiètent excessivement des menaces liées à l'IA, mais souhaitent également exploiter cette technologie pour aller plus loin, notamment améliorer la cybersécurité, en particulier les moyens de prévention et d'atténuation.
- Elles reconnaissent l'intérêt réel de toutes les options, mais les audits et les rapports automatisés, ainsi que l'idée que l'IA puisse remplacer l'intervention humaine manuelle dans la réponse à une attaque active, semblent être les éléments jugés les moins utiles.



Les PME françaises voient dans l'IA un levier de cybersécurité avant tout orienté vers l'anticipation et la détection des menaces

- Les entreprises françaises perçoivent principalement l'IA comme un outil permettant d'anticiper les menaces avant qu'elles ne se concrétisent : 55 % des répondants classent cet usage parmi leurs deux principales attentes (33 % en première position).
- Les bénéfices les plus attendus concernent également l'identification et la neutralisation plus rapides des attaques ainsi que la détection des attaques par ingénierie sociale, deux cas d'usage jugés prioritaires par près de 40 % des répondants.
- À l'inverse, les usages liés à l'automatisation des audits et du reporting ou à la réduction des interventions manuelles lors des attaques suscitent moins d'adhésion, illustrant une préférence pour une IA qui assiste les équipes de sécurité plutôt qu'elle ne remplace l'expertise humaine.



4

Budgétisation de la cybersécurité

Les PME soucieuses de leur budget dépensent intelligemment

Ressources

Les PME sont confrontées à des attaques de plus en plus sophistiquées, tout en devant souvent composer avec des budgets qui ne leur permettent pas de réaliser des investissements importants ni d'engager des dépenses opérationnelles substantielles.

Elles ne disposent tout simplement pas des mêmes ressources que les grandes entreprises pour faire face aux défis de la cybersécurité, et doivent donc s'appuyer sur une gestion budgétaire rigoureuse et l'externalisation via des services managés.

MDR

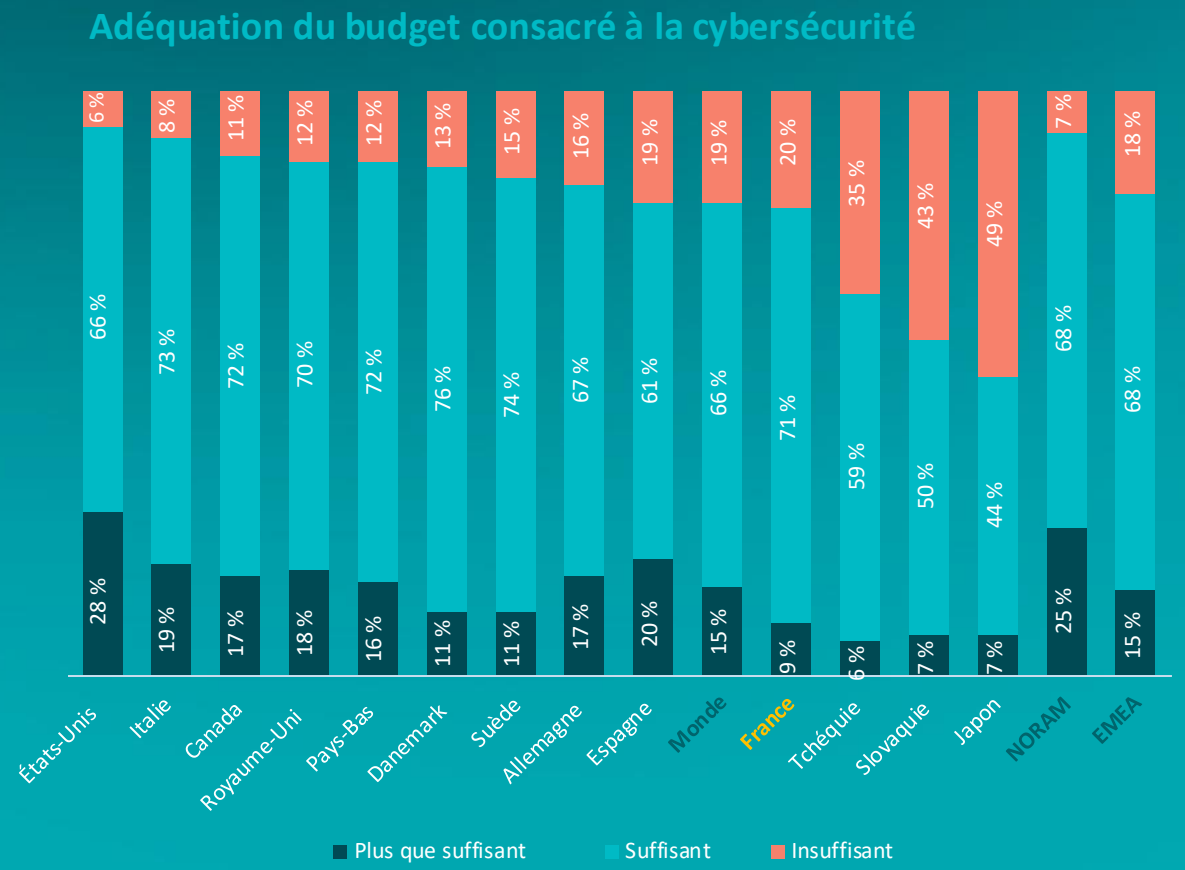
Les solutions de sécurité les plus sophistiquées et/ou les plus performantes, dotées de l'IA, sont peut-être hors de portée, mais un service de détection et de réponse managées (MDR) offre une défense approfondie ainsi que des renseignements détaillés sur les menaces.

Optimisation budgétaire

Malgré des ressources limitées, les PME cherchent à maximiser l'efficacité de leurs investissements en cybersécurité. La rationalisation des outils et le recours à des services managés permettent de mieux exploiter les budgets existants tout en renforçant le niveau de protection.

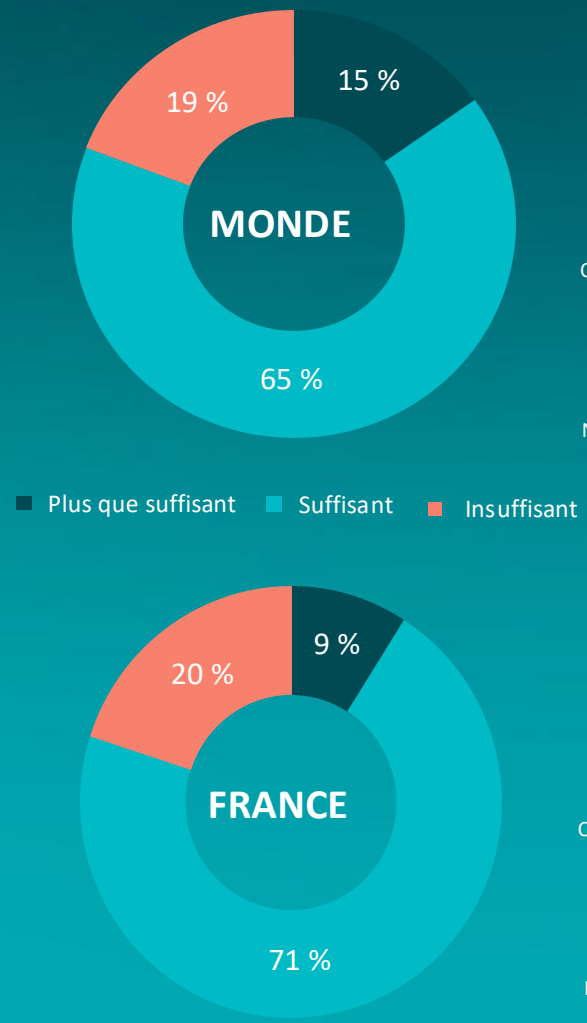
Les responsables de la sécurité des PME sont généralement satisfaits de leurs budgets consacrés à la cybersécurité, ce qui peut paraître surprenant

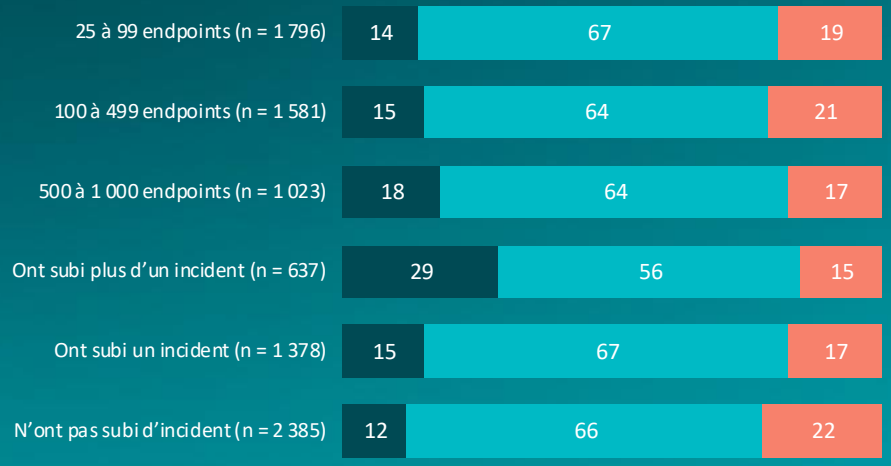
- Les responsables de la cybersécurité des PME aux États-Unis, en Italie, au Canada et au Royaume-Uni semblent plutôt satisfaits de leurs budgets.
- La majorité des personnes interrogées jugent leur budget « Suffisant » ou « Plus que suffisant ». Seules 6 % à 12 % des personnes interrogées dans ces pays déclarent que leur budget est « Insuffisant ».
- Les États-Unis sont également en tête pour la réponse « Plus que suffisant », le budget étant perçu ainsi dans 28 % des cas. L'Espagne occupe la seconde place en termes de réponses « Plus que suffisant », même si elle ne figure pas parmi les premières places au classement général.
- Le Japon constitue un cas particulier intéressant, car s'il se classe parmi les premiers pays en termes de données sur les incidents, il affiche en même temps un faible niveau de confiance et des budgets insuffisants.



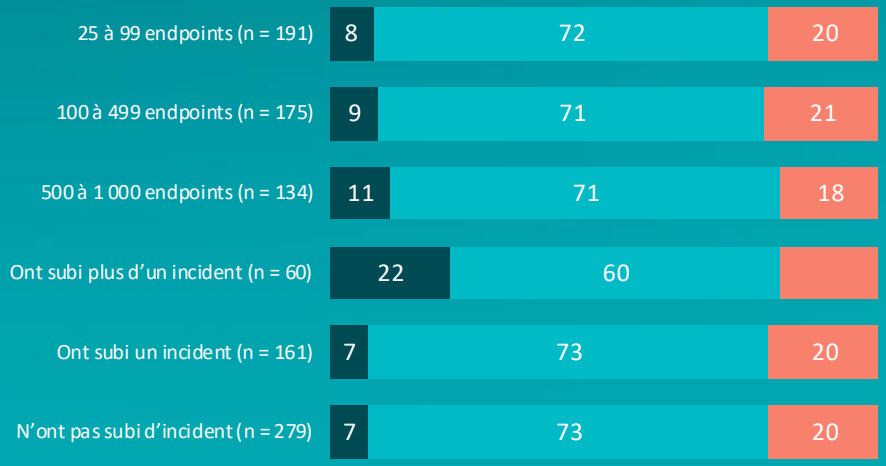
Les entreprises françaises globalement plus satisfaites de leurs budgets cybersécurité que la moyenne mondiale

- Alors que les entreprises françaises citent régulièrement le manque d'investissement, les compétences limitées ou la surcharge des équipes parmi leurs principaux défis, seules 20 % estiment que leur budget cybersécurité est insuffisant.
- Cette apparente contradiction suggère que les enjeux perçus relèvent davantage de l'allocation des ressources, de l'expertise disponible ou de la complexité croissante des menaces que du niveau de budget lui-même.





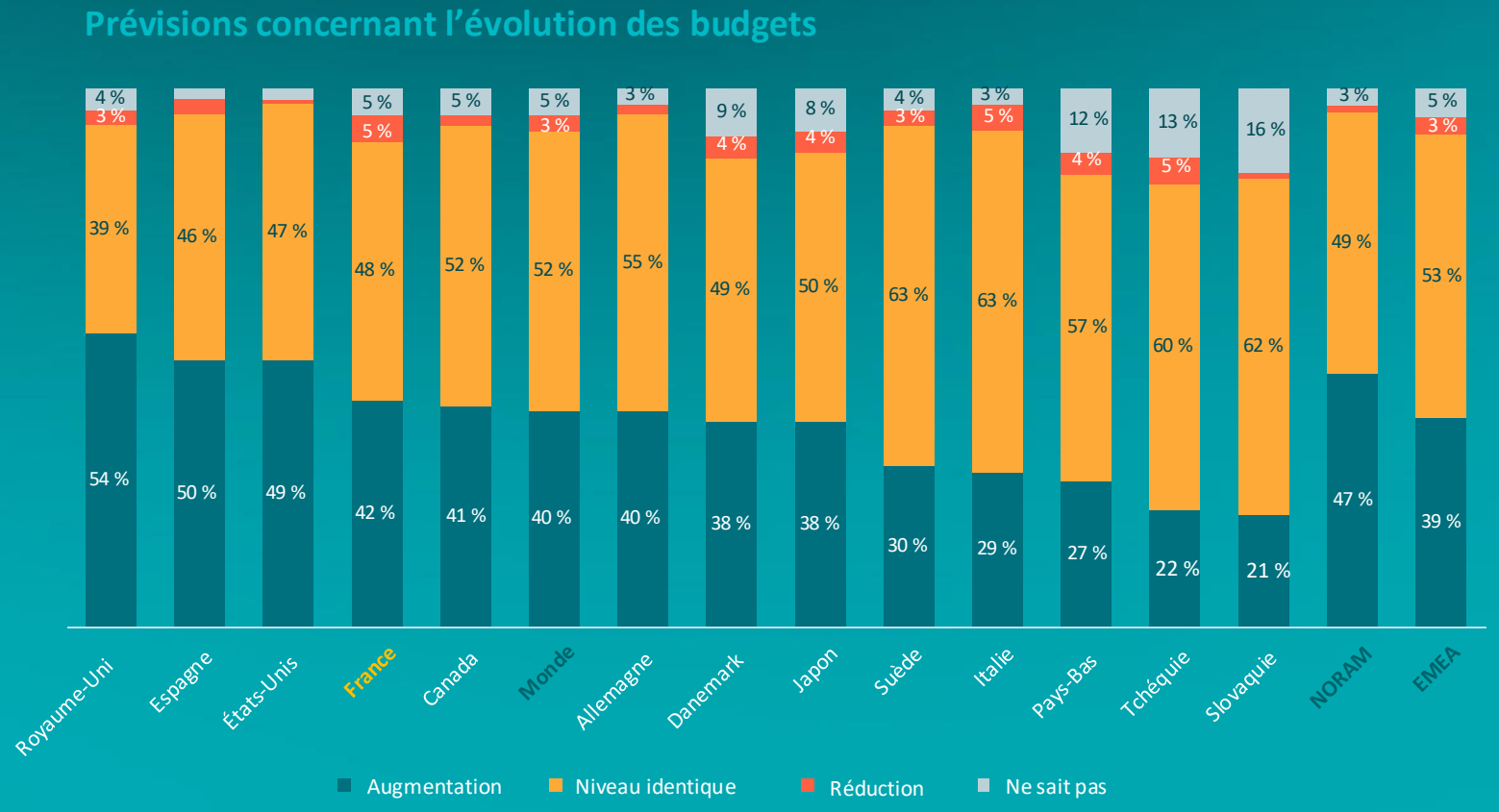
(en %)



Face aux cybermenaces, nombreuses sont les PME qui prévoient d'augmenter leur budget cyber

- En France, 42 % des PME prévoient une augmentation de leurs budgets cybersécurité, soit un niveau supérieur à la moyenne mondiale (40 %). Seules 5 % envisagent une réduction, tandis que 48 % s'attendent à un budget stable. Ces résultats traduisent une volonté de poursuivre les investissements, tout en privilégiant une approche mesurée et orientée vers l'optimisation des dépenses existantes.

- Cette dynamique reflète une prise de conscience croissante des risques cyber et de la nécessité de financer durablement les initiatives de protection, de détection et de réponse aux menaces, sans pour autant s'engager dans une inflation incontrôlée des budgets.

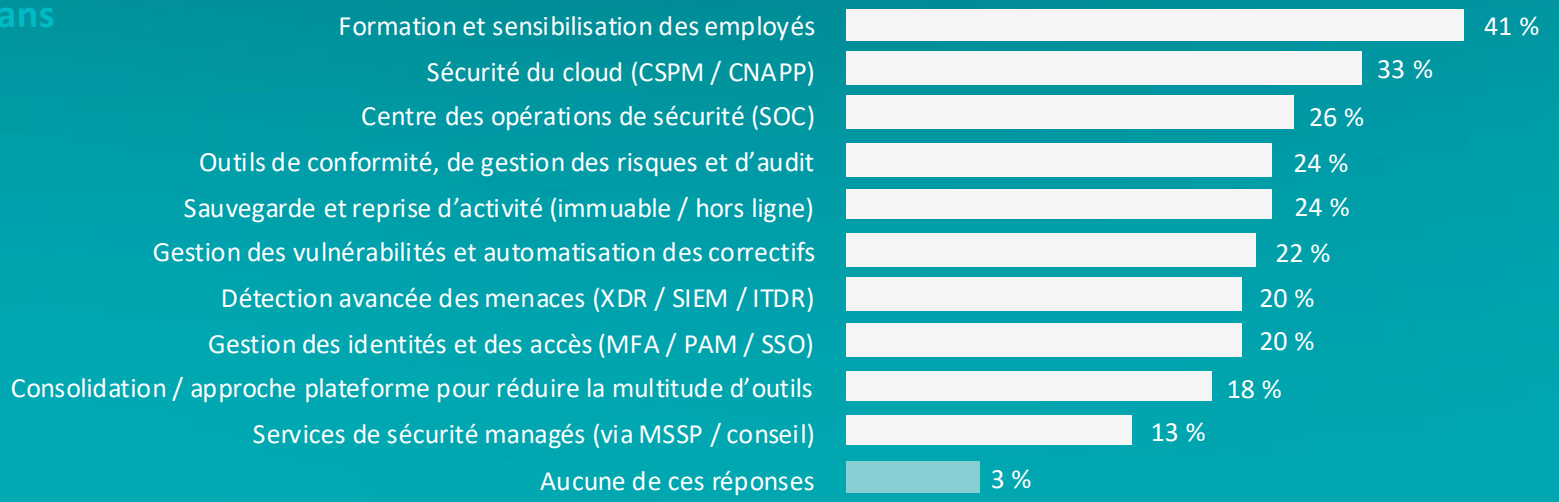


Établissement d’un budget pour la cyber-résilience à l’ère de l’IA

À l’heure où des emails d’hameçonnage crédibles peuvent être générés en quelques secondes et où les deepfakes sont presque impossibles à distinguer de la réalité, la sensibilisation à la cybersécurité revêt plus d’importance que jamais.

À mesure que les cyberattaques gagnent en sophistication, les PME ont elles aussi besoin de solutions de cybersécurité avancées, telles que l’XDR, la sécurité du cloud ou des outils de détection des menaces, pour faire face aux dernières tactiques et aux malwares.

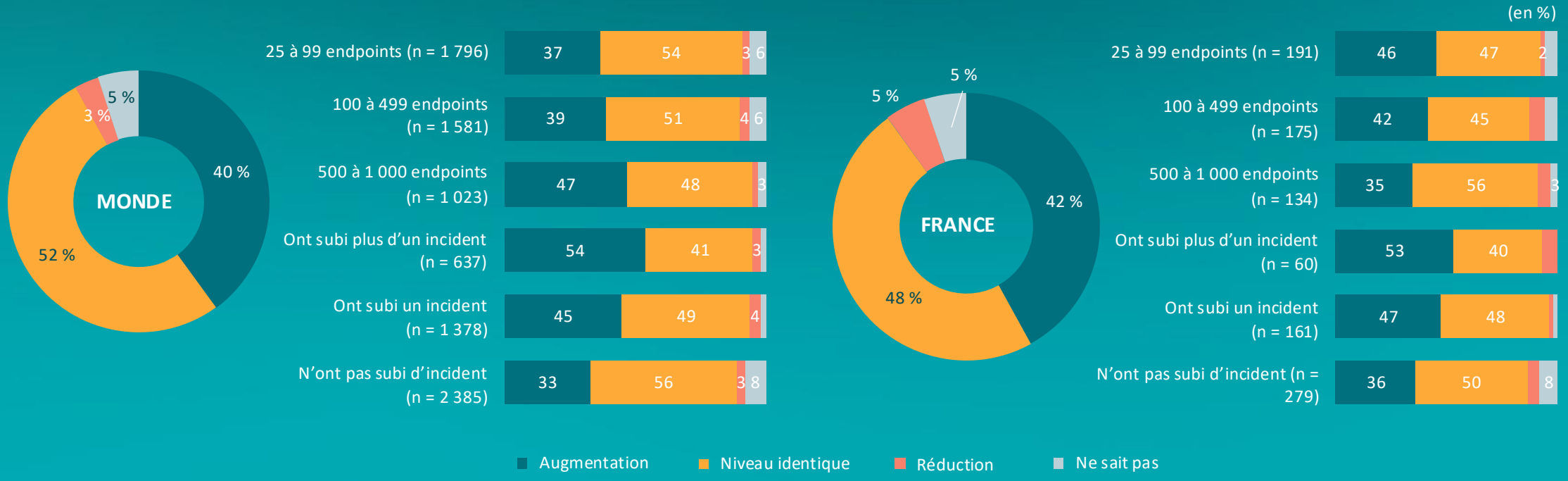
Investissements prévus dans les 12 prochains mois



Les entreprises françaises affichent un optimisme budgétaire croissant malgré un contexte mondial plus prudent

42 % des entreprises françaises prévoient d'augmenter leurs budgets de cybersécurité, un niveau supérieur à la moyenne mondiale. À l'échelle internationale, les intentions d'investissement restent majoritairement stables, avec une légère baisse des perspectives de hausse.

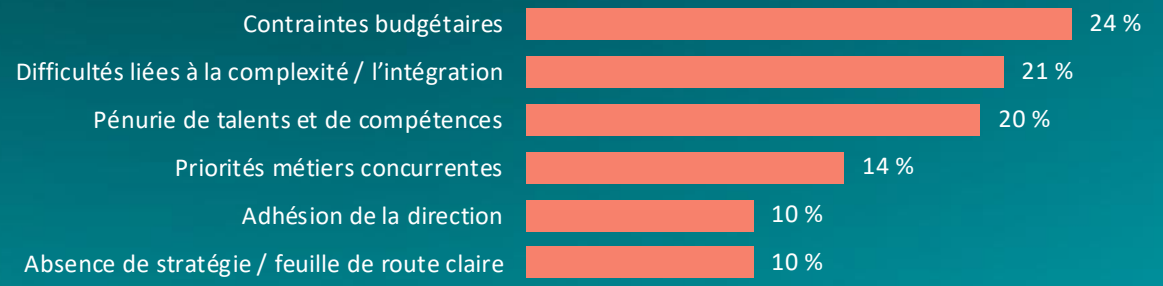
Prévisions concernant l'évolution des budgets



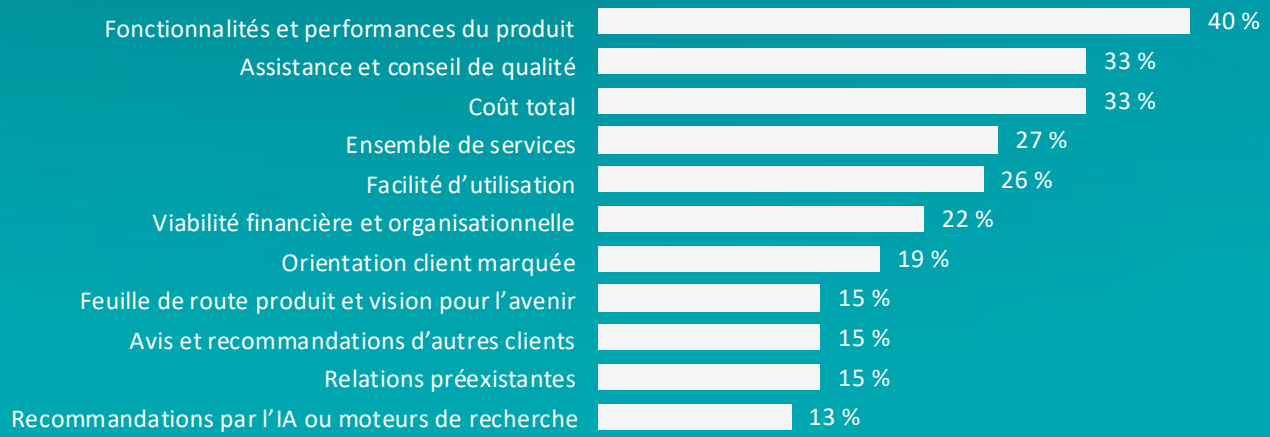
Le budget reste le principal obstacle, puis la complexité et la rapidité

- Près d'une PME sur quatre estime qu'une augmentation de son budget lui permettrait d'améliorer plus rapidement sa cybersécurité.
- La complexité et l'intégration font également partie des principaux défis. Elles sont un problème courant pour les entreprises qui tentent de gérer elles-mêmes leur cybersécurité.
- Cela correspond aux préférences des personnes interrogées en matière de cybersécurité : les PME recherchent des services et des solutions fiables et riches en fonctionnalités, ainsi qu'une protection facile à utiliser.

Obstacles actuels à l'amélioration de la cybersécurité dans l'entreprise



Les facteurs les plus importants pour le choix de solutions de cybersécurité



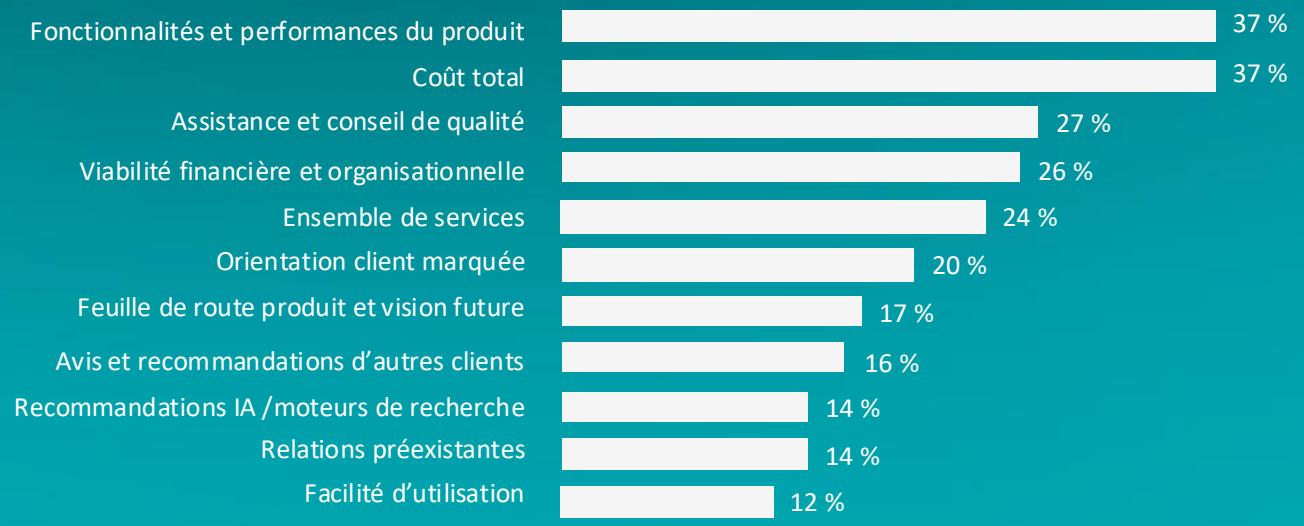
Pour les entreprises françaises, la performance des produits et leur coût sont des facteurs clés

- Les critères de choix des entreprises françaises révèlent une approche particulièrement rationnelle des investissements en cybersécurité. La performance des solutions (37 %) et leur coût total (37 %) arrivent largement en tête, montrant que les PME arbitrent leurs décisions en fonction de la valeur concrète apportée au regard des ressources engagées.

- Les facteurs liés à l'accompagnement (27 %) et aux retours d'expérience d'autres clients (26 %) occupent également une place importante, traduisant un besoin de réduire les risques associés aux décisions d'achat et de s'appuyer sur des solutions éprouvées.

- À l'inverse, les considérations liées à la marque, aux relations historiques ou aux recommandations automatisées pèsent moins dans les choix. Les PME françaises privilégient ainsi une logique de retour sur investissement, d'efficacité opérationnelle et de résultats mesurables plutôt qu'une approche fondée sur la notoriété des fournisseurs.

Les facteurs les plus importants pour le choix de solutions de cybersécurité



5

Les PME investissent dans la sécurité

Les PME investissent dans la sécurité

La bonne nouvelle

Les petites et moyennes entreprises investissent avant qu'une attaque ne se produise. Elles se tournent vers la cyberassurance car les conséquences des incidents deviennent à la fois réelles et inévitables.

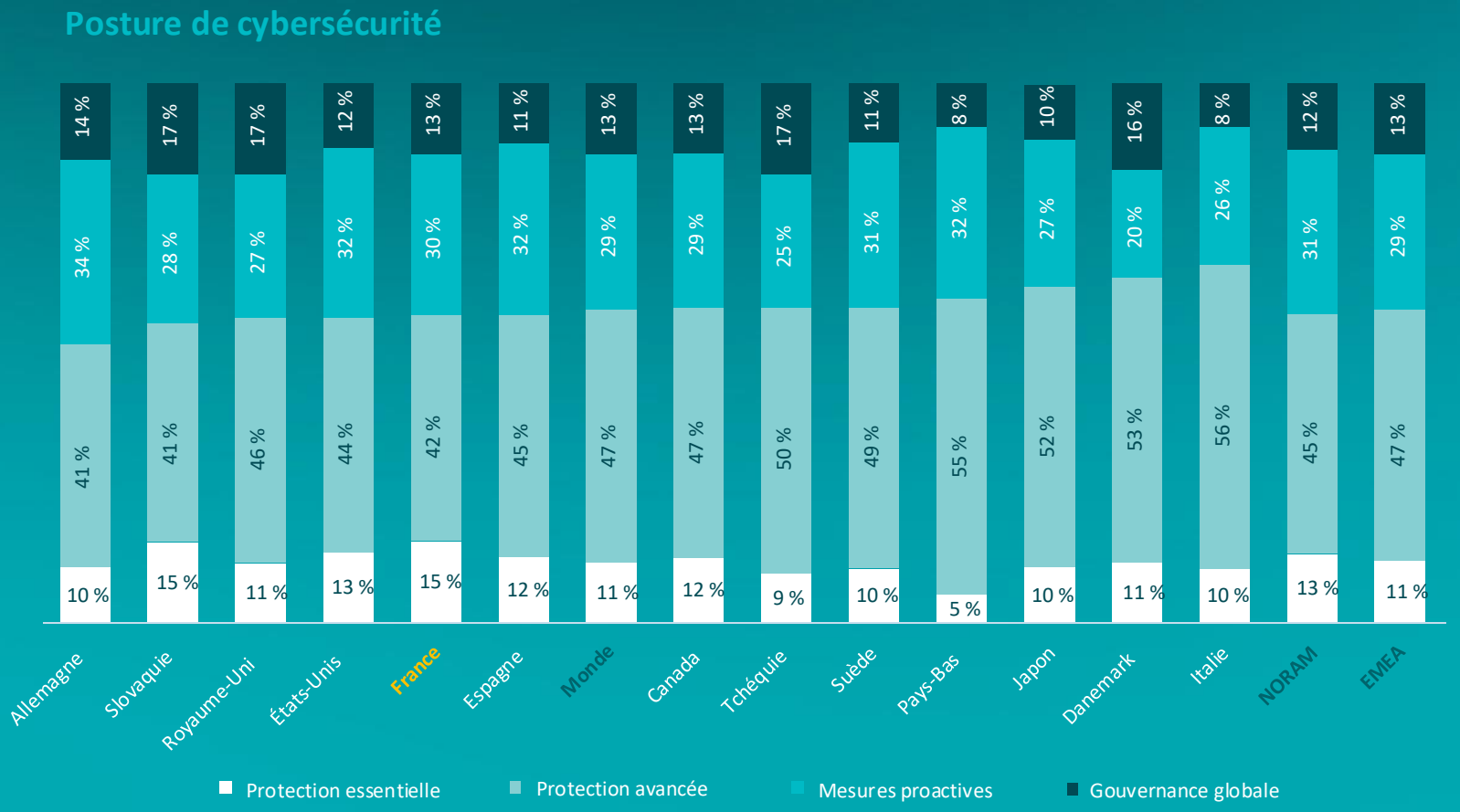
Elles investissent également dans la formation. Ensemble, ces facteurs font que la cyber-résilience des PME montre des signes réels de progression.

Modèles d'externalisation diversifiés

Pour les organisations qui ont recours à l'externalisation, les services de sécurité managés revêtent une importance cruciale et peuvent être obtenus de différentes manières. Cela peut être motivé par le recours à des assureurs et, dans certains cas, par de précédents incidents de sécurité.

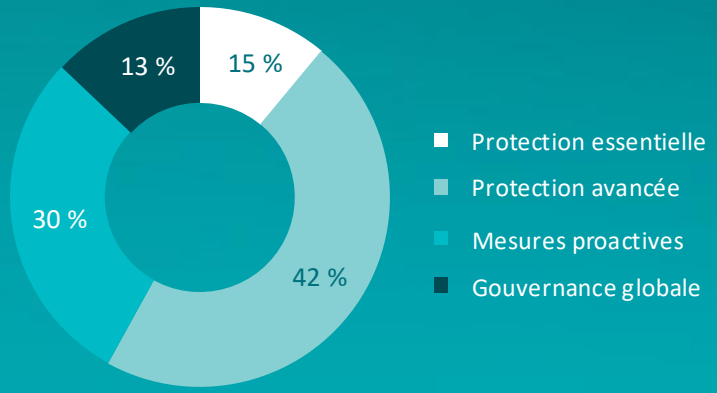
Les petites et moyennes entreprises prennent leur sécurité très au sérieux

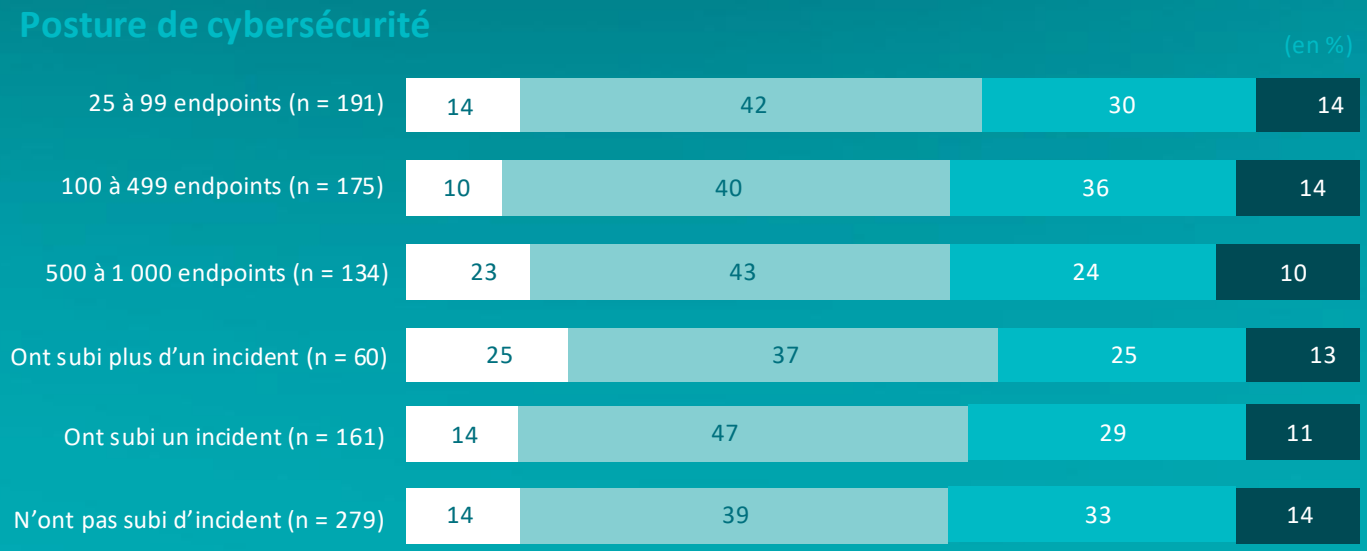
- La posture de cybersécurité varie considérablement d'un pays à l'autre, même si, naturellement, ce sont les niveaux intermédiaires qui sont les plus prisés.
- C'est en Allemagne que l'on recherche le plus souvent les niveaux les plus élevés de cybersécurité, puis la Slovaquie, le Royaume-Uni et les États-Unis. En parallèle, les États-Unis, ainsi que la France, la Slovaquie et l'Espagne, privilégient les niveaux essentiels de cybersécurité.



La maturité cyber des PME françaises est élevée, mais reste inégale face aux risques

- En France, la maturité cyber des PME est globalement élevée : 42 % disposent d'une protection avancée et 43 % ont mis en place des mesures proactives ou une gouvernance globale.
- Les entreprises ayant subi plusieurs incidents présentent toutefois un profil plus contrasté, avec une proportion plus importante au niveau de protection essentielle (25 %).
- Ces résultats montrent que si la majorité des PME ont renforcé leur posture de sécurité, des écarts de maturité subsistent selon leur niveau d'exposition aux risques.

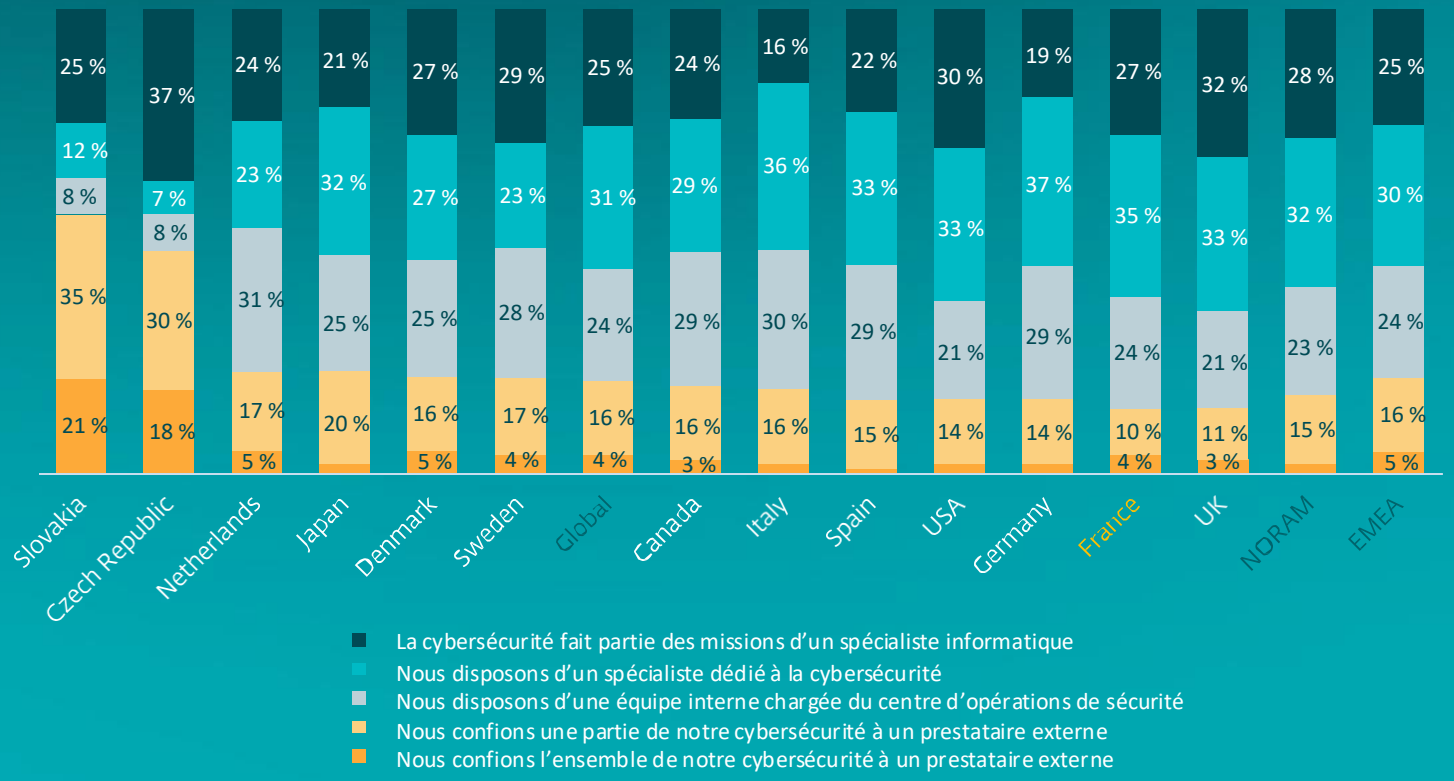




Externalisation ou gestion interne : Les PME gardent majoritairement la main sur leur cybersécurité - à deux exceptions près

- À l'échelle mondiale, les PME privilégient majoritairement une gestion interne de leur cybersécurité, l'externalisation complète restant minoritaire.
- En France, cette tendance est encore plus marquée : 62 % des entreprises s'appuient sur des ressources internes dédiées à la cybersécurité, qu'il s'agisse d'un spécialiste, d'une équipe interne ou d'un SOC. Les organisations françaises figurent ainsi parmi celles qui investissent le plus dans le développement de compétences internes.
- L'externalisation reste néanmoins présente, avec 14 % des PME qui confient une partie de leur cybersécurité à un prestataire et 4 % qui la délèguent entièrement. Les entreprises françaises privilégient donc une approche où les partenaires externes viennent compléter, plutôt que remplacer, les capacités internes.

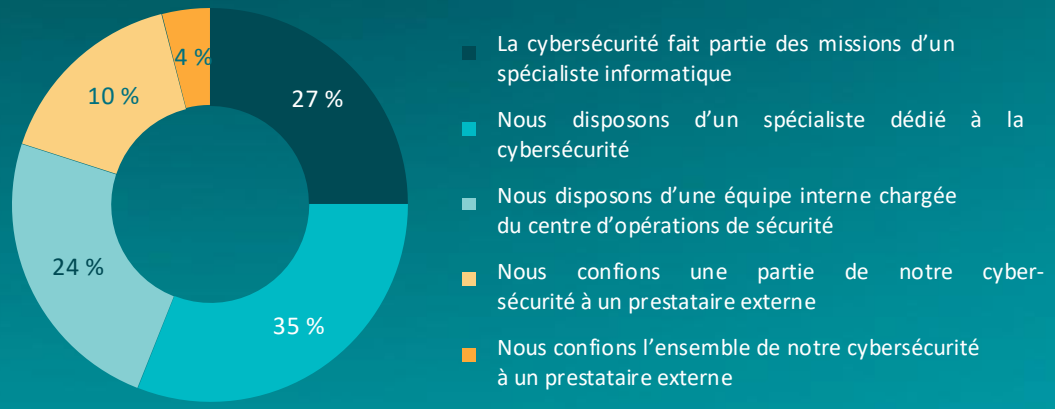
Gestion de la cybersécurité dans l'entreprise



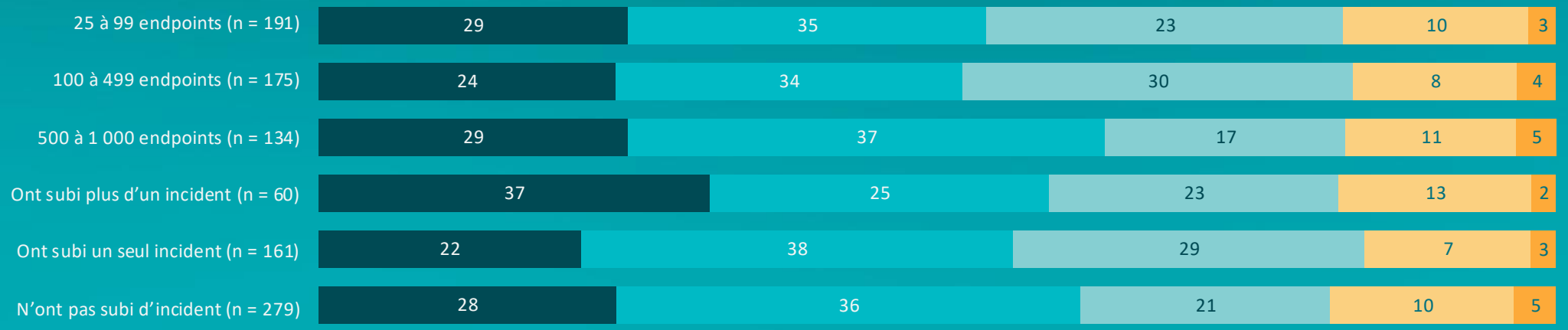
Les entreprises privilégient une expertise interne pour gérer leur cybersécurité

La gestion de la cybersécurité repose avant tout sur des ressources internes. 35 % des entreprises disposent d'un spécialiste cybersécurité dédié, tandis que 27 % confient cette mission à un spécialiste informatique et 24 % s'appuient sur une équipe SOC interne. À l'inverse, seules 14 % externalisent tout ou partie de cette fonction, confirmant que les organisations privilégient une gouvernance assurée en interne de la cybersécurité.

Gestion de la cybersécurité dans l'entreprise



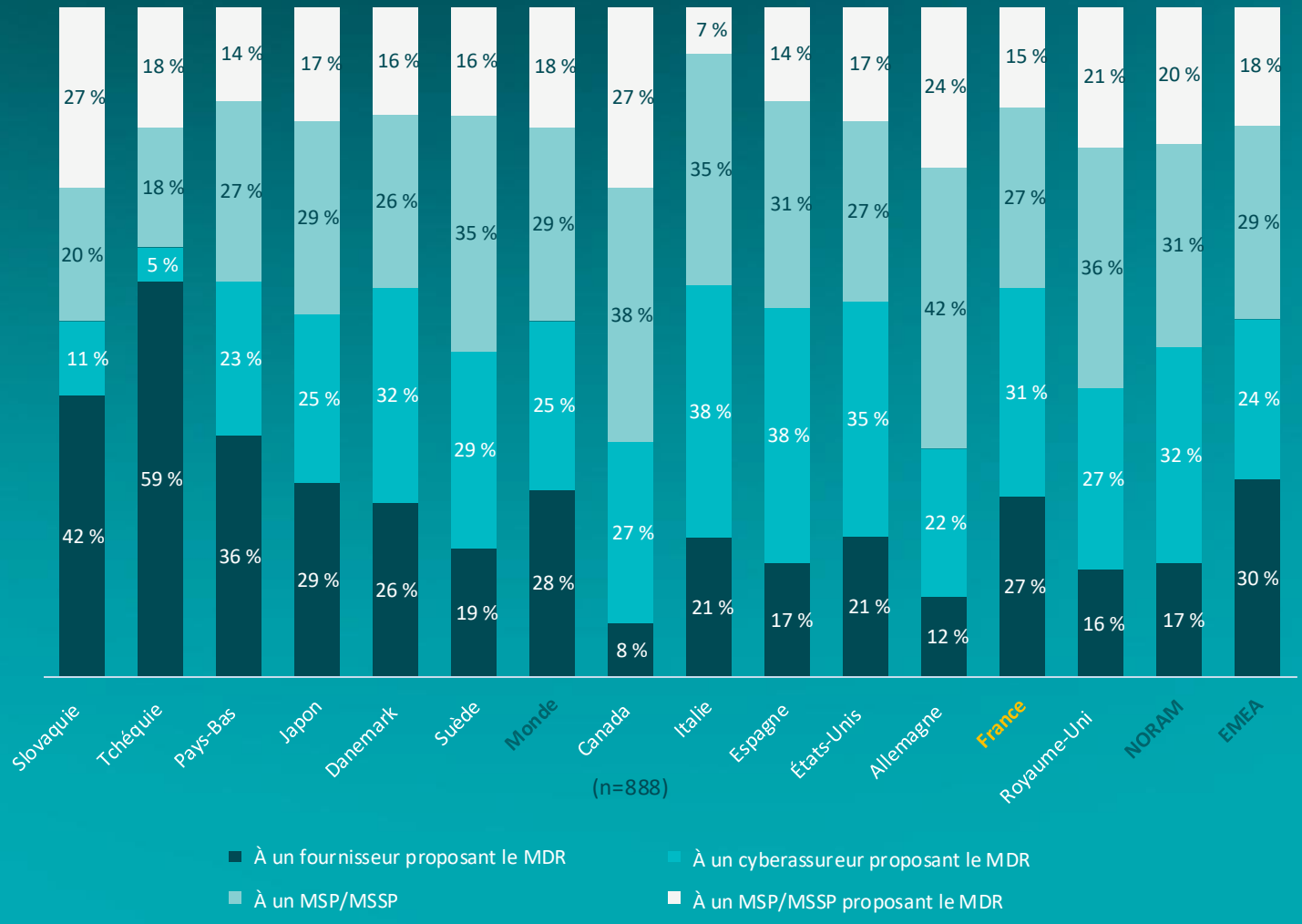
(en %)



Le MDR se popularise

- À l'échelle mondiale, les entreprises externalisent leur cybersécurité via différents modèles, avec une adoption croissante des services MDR.
- En France, le MDR occupe une place centrale : 58 % des entreprises ayant recours à l'externalisation choisissent un fournisseur proposant des capacités MDR, directement ou via un MSP/MSSP.
- Cette tendance reflète la volonté des PME d'accéder à des capacités avancées de détection et de réponse aux menaces sans renforcer significativement leurs équipes internes.

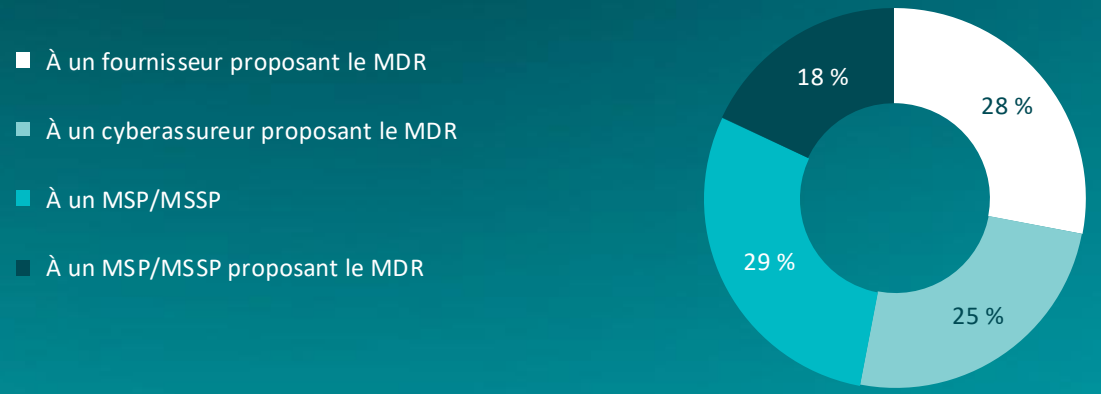
Externalisation des services de cybersécurité

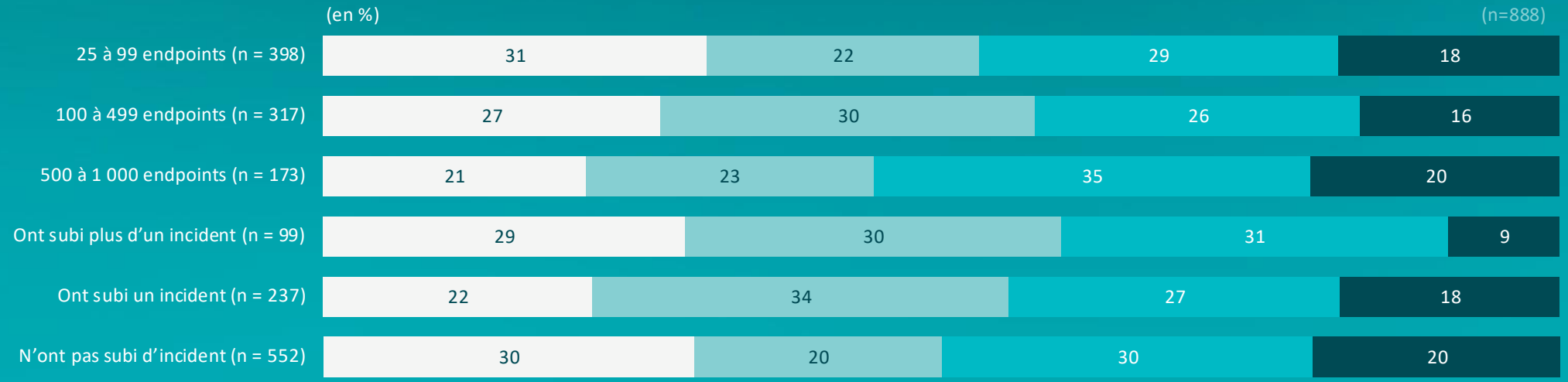


- À l'échelle mondiale, les PME qui choisissent d'externaliser leur cybersécurité se tournent dans des proportions équivalentes vers des fournisseurs proposant du MDR, des assureurs cyber incluant du MDR et des MSP/MSSP sans MDR. Les MSP/MSSP proposant du MDR constituent l'option la moins privilégiée.

- Les MSP/MSSP (qu'ils proposent ou non du MDR) sont davantage plébiscités par les entreprises de plus grande taille ainsi que par celles n'ayant pas subi d'incident de cybersécurité.

Externalisation des services de cybersécurité

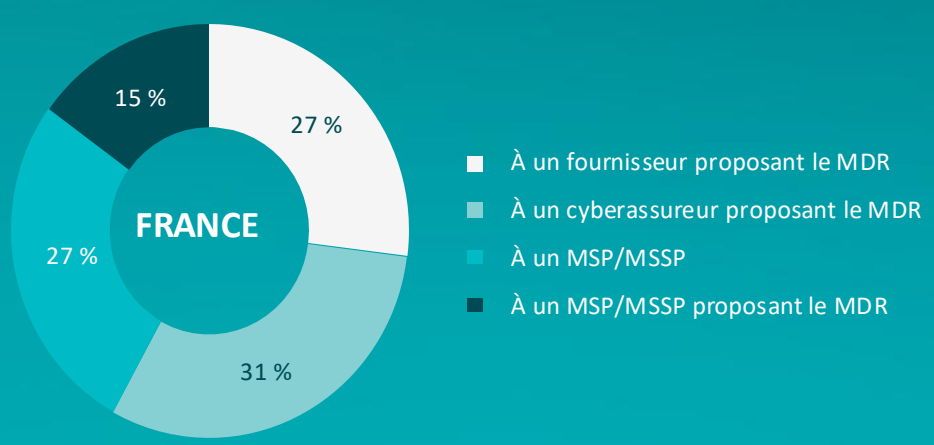


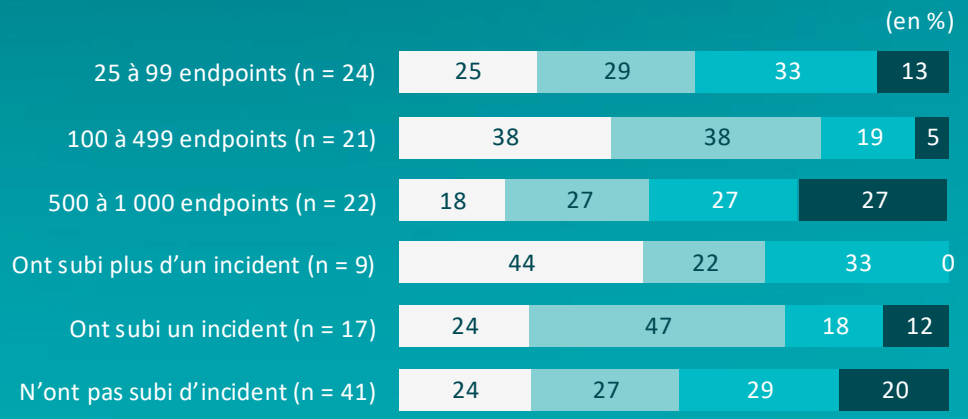


Les entreprises françaises ayant externalisé leur MDR se tournent davantage vers les cyberassureurs

Parmi les entreprises françaises ayant choisi d'externaliser leurs capacités de détection et de réponse managées (MDR), les cyberassureurs proposant ces services sont plus fréquemment cités que dans la moyenne mondiale (31 % contre 25 %). Bien que cette observation repose sur un sous-échantillon limité, elle suggère un intérêt particulier pour les acteurs combinant gestion du risque cyber et accompagnement opérationnel en matière de détection et de réponse aux incidents.

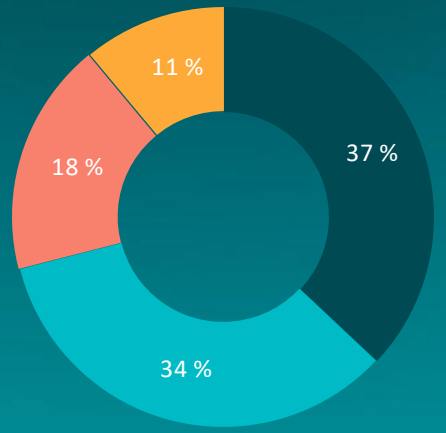
Externalisation des services de cybersécurité





Les cyberassureurs entrent en jeu

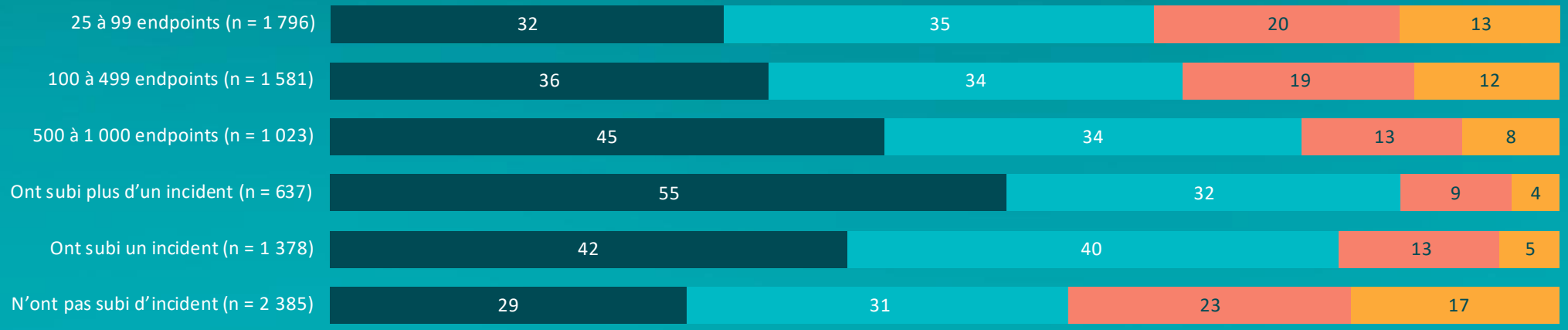
- Les PME aux moyens limités se tournent vers l'assurance pour se prémunir des risques. 84 % des PME nord-américaines ont souscrit à une cyberassurance, dont 51 % comportent des exigences spécifiques de contrôles de sécurité.
- Dans le reste du monde, une plus grande partie des entreprises ont souscrit à une cyberassurance avec peu ou pas d'exigences spécifiques, voire n'ont pas de cyberassurance du tout.



Votre entreprise a-t-elle souscrit à une cyberassurance ?

- Oui, avec des exigences spécifiques de contrôles de sécurité
- Oui, sans exigences particulières
- Non
- Ne sait pas

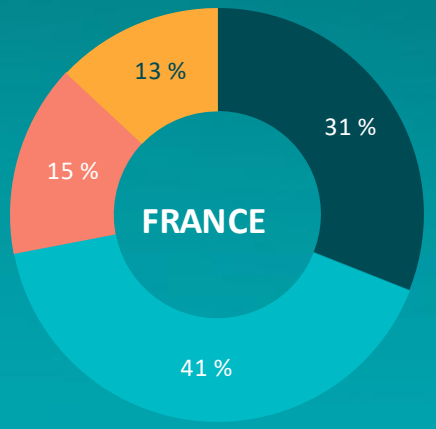
(en %)



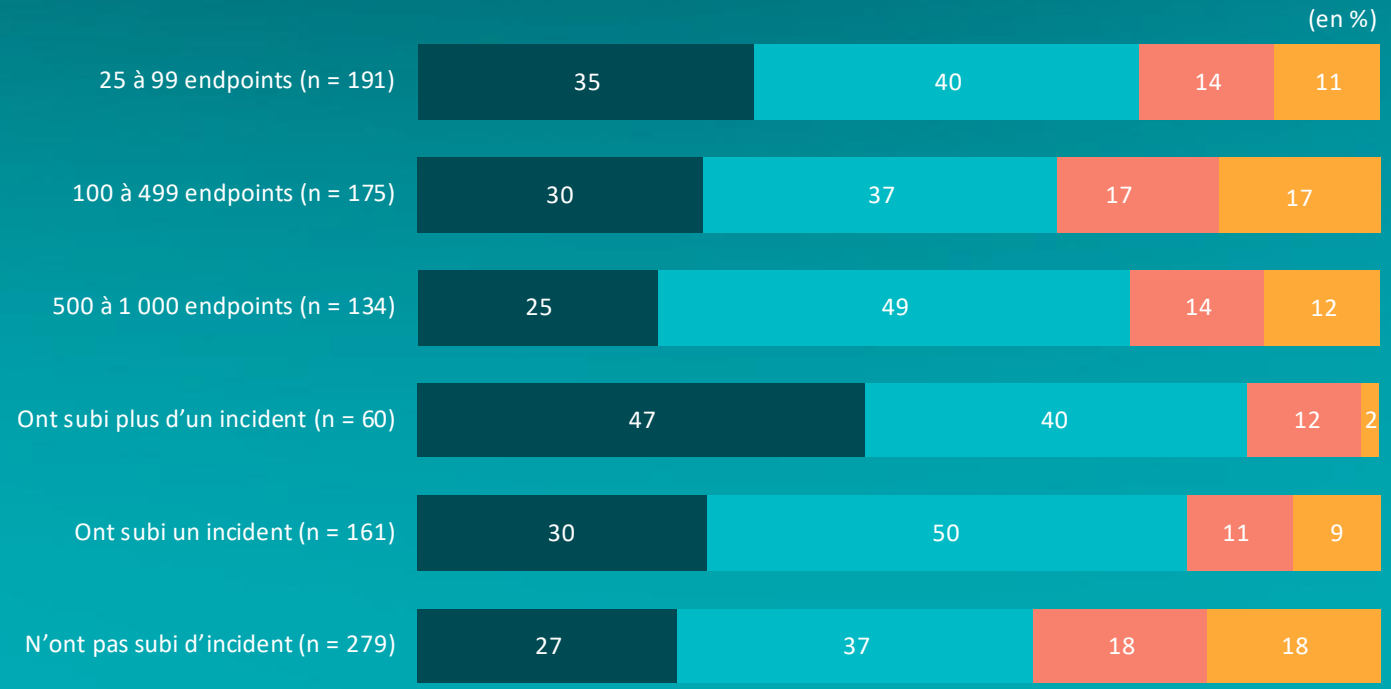
La cyberassurance est largement adoptée, mais reste peu utilisée comme levier d'amélioration de la sécurité

Comparée au niveau mondial, la France affiche une proportion plus élevée d'entreprises assurées sans exigences particulières de sécurité (41 % contre 34 %), tandis que les contrats assortis de contrôles obligatoires sont moins fréquents (31 % contre 37 %). Cette situation laisse entrevoir un potentiel de renforcement du rôle de la cyberassurance comme moteur d'amélioration des pratiques de cybersécurité.

Votre entreprise a-t-elle souscrit une cyberassurance ?



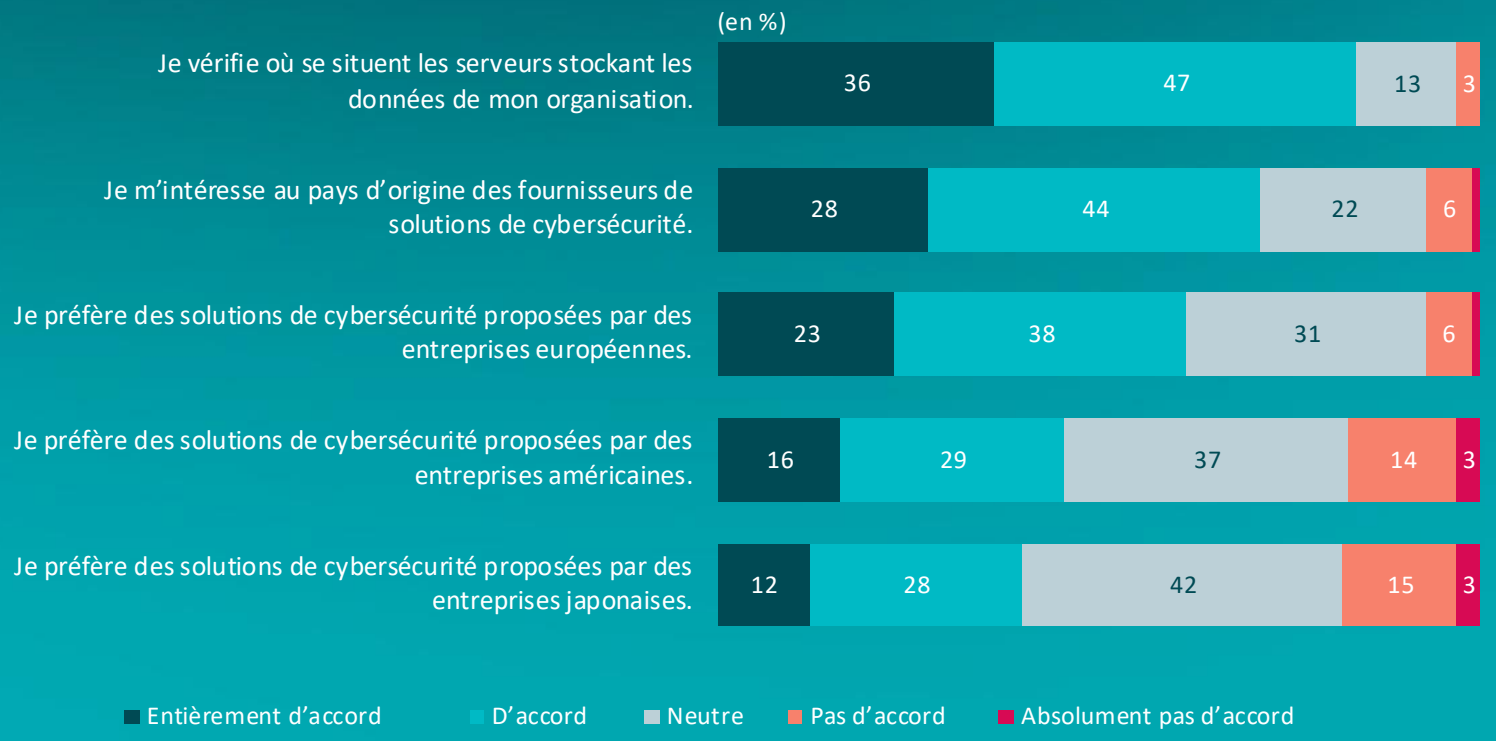
- Oui, avec des exigences spécifiques de contrôles de sécurité
- Oui, sans exigences particulières
- Non
- Je ne sais pas



Le pays d’origine du fournisseur est un critère important pour les PME

- Partout dans le monde, les PME considèrent le pays d’origine de leur fournisseur de services de sécurité et l’emplacement de ses serveurs comme des facteurs importants lors du choix de solutions de cybersécurité.
- Dans l’ensemble, l’Europe apparaît comme la région la plus prisée dans ce rapport, ce qui s’explique sans doute par la composition de l’échantillon, puisque 700 des entreprises interrogées étaient situées dans la région NORAM tandis que 3 200 PME provenaient de la région EMEA.

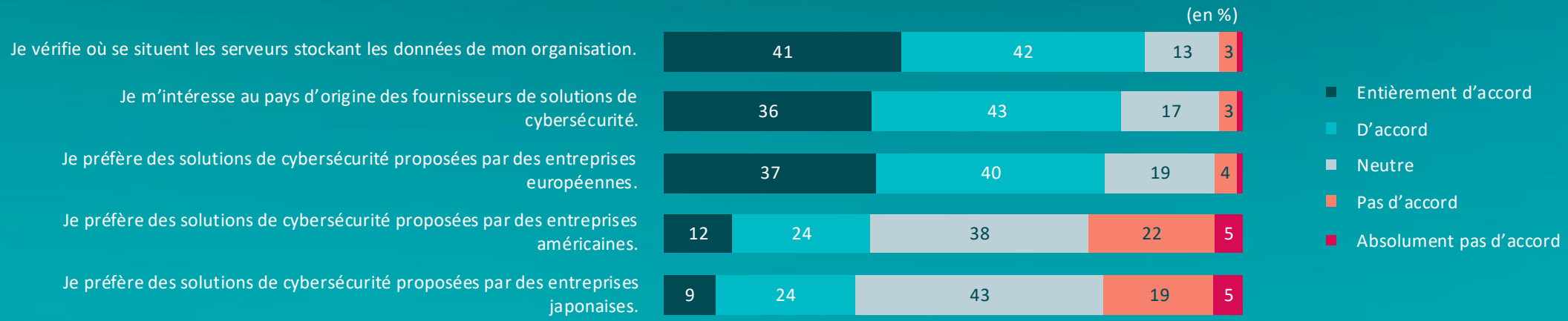
Dans quelle mesure êtes-vous d’accord avec les affirmations suivantes ?



Les entreprises françaises se montrent plus sensibles aux enjeux de souveraineté que la moyenne mondiale.

Si la localisation des données est un critère important à l'échelle mondiale, cette préoccupation est encore plus marquée en France. Les entreprises françaises accordent davantage d'importance à l'origine de leurs fournisseurs et affichent une préférence plus nette pour les solutions européennes, reflétant un attachement fort aux enjeux de souveraineté, de conformité réglementaire et de maîtrise des données stratégiques.

Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes ?



6

La sensibilisation à la cybersécurité s'impose comme une priorité

Les entreprises investissent dans des formations de sensibilisation à la cybersécurité

Confiance

Le niveau élevé de confiance des entreprises interrogées quant à leur capacité à faire face à l'hameçonnage et l'ingénierie sociale s'explique sans doute par leurs investissements dans des programmes de sensibilisation à la cybersécurité.

Sensibilisation

Si de nombreuses entreprises considèrent les tentatives d'hameçonnage comme des incidents, celles-ci ne débouchent souvent pas sur des atteintes à la sécurité ni ne causent de préjudice concret, en partie grâce à la formation dispensée au personnel.

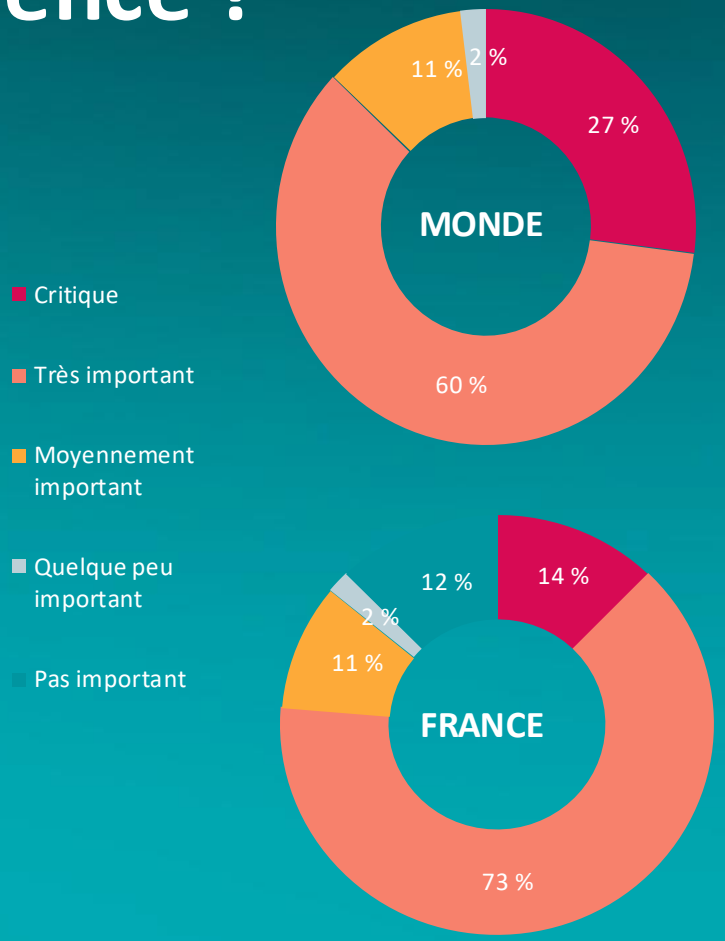
Formation

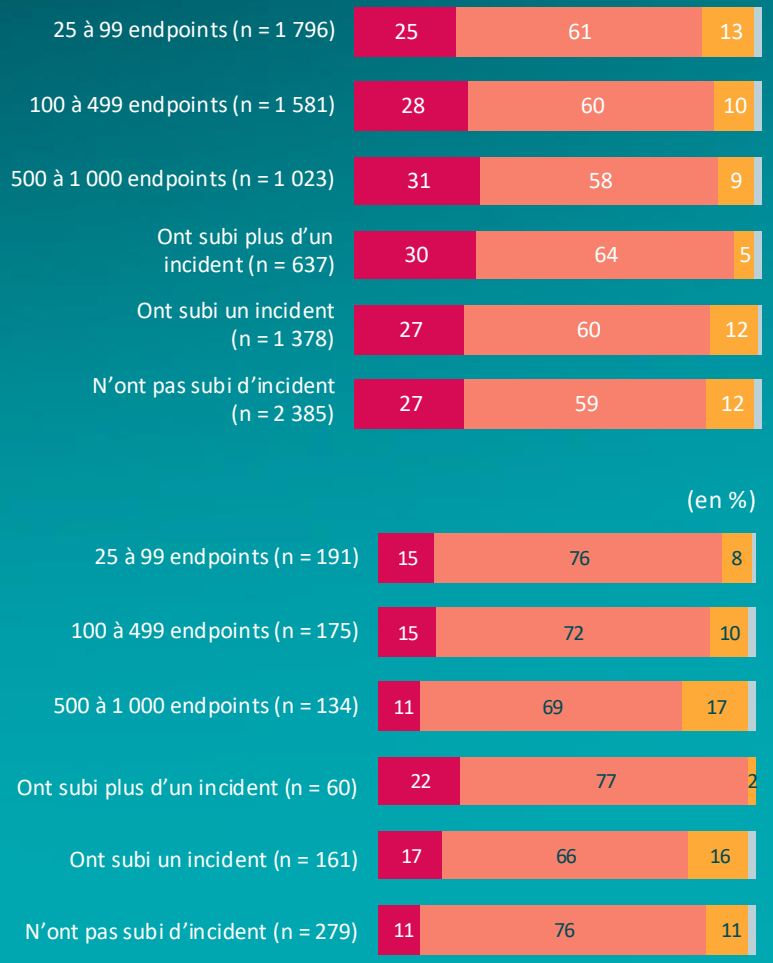
Bien que l'acquisition (ou la location) de solutions technologiques permette de résoudre une partie des problèmes de cybersécurité, elle ne sert à rien sans des collaborateurs formés et capables de repérer les dangers. C'est souvent la première, et la meilleure, ligne de défense.

Faut-il un incident pour renforcer la résilience ?

Les entreprises qui ont connu plus d'un incident prennent les formations de cybersécurité plus au sérieux que les autres, ce qui confirme que le facteur humain est souvent en cause dans les incidents et les atteintes à la sécurité.

L'importance de la formation et de la sensibilisation à la cybersécurité dans la prévention des attaques

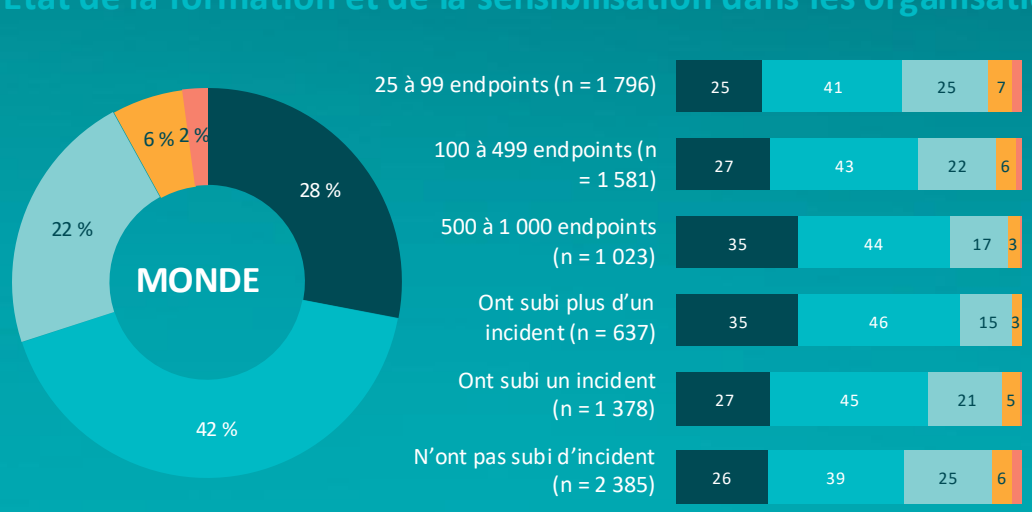


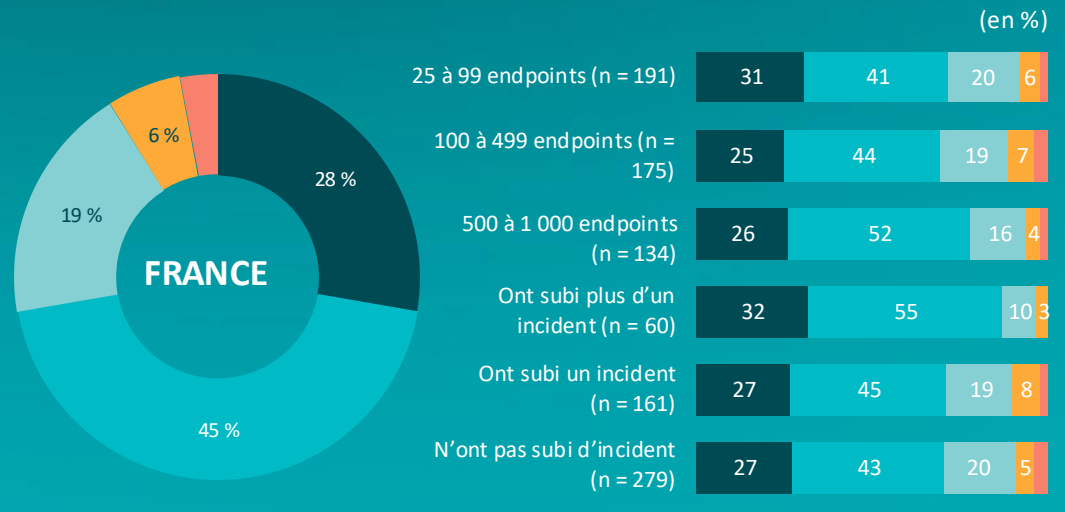


La cybersécurité est désormais perçue autant comme un enjeu humain que technologique.

- En France, 87 % des répondants considèrent la formation et la sensibilisation à la cybersécurité comme critiques dans la prévention des attaques, un niveau supérieur à la moyenne mondiale (87 % contre 86 %, avec davantage de réponses « très importantes »).
- Cette conviction se traduit dans les pratiques : près des ¾ des organisations ont mis en place des programmes structurés de formation, tandis que les entreprises ayant déjà subi plusieurs incidents sont les plus avancées en matière de sensibilisation et de simulations, illustrant le lien entre expérience des incidents et maturité cyber.

État de la formation et de la sensibilisation dans les organisations





Une formation complète et des simulations sont indispensables pour réduire les risques

Nous investissons dans des programmes de qualité avec simulations d'hameçonnage

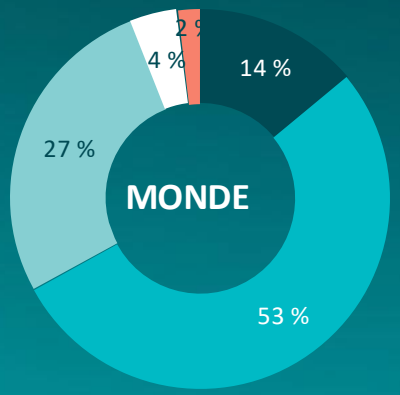
Nous proposons des formations de sensibilisation de base

Une formation minimale axée sur la conformité

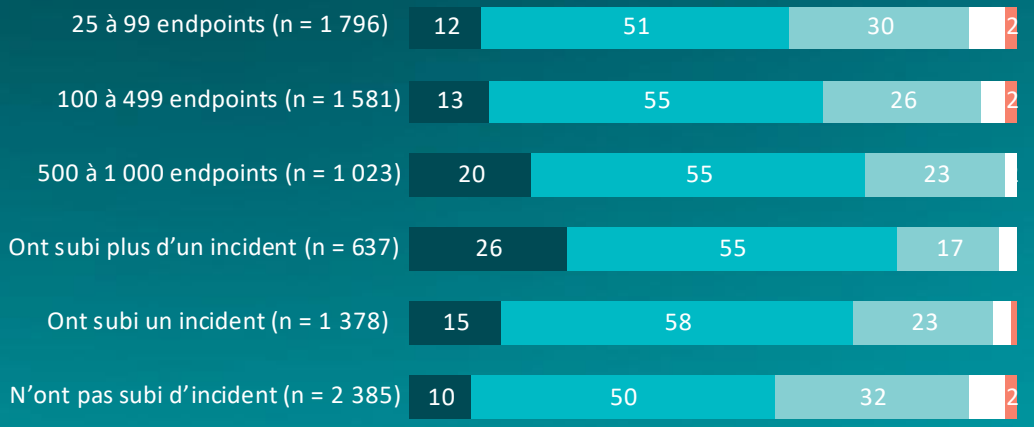
Nous misons plus sur la technologie que sur la formation

C’est en pratiquant que l’on maîtrise… ou du moins que l’on améliore sa sécurité

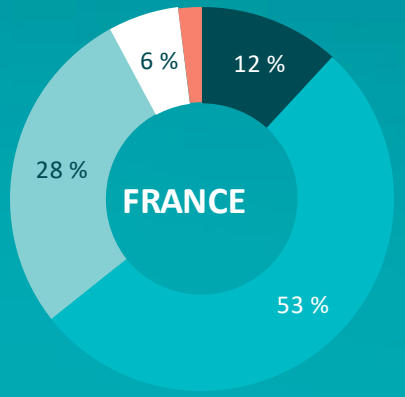
Fréquence des formations de cybersécurité dans les entreprises



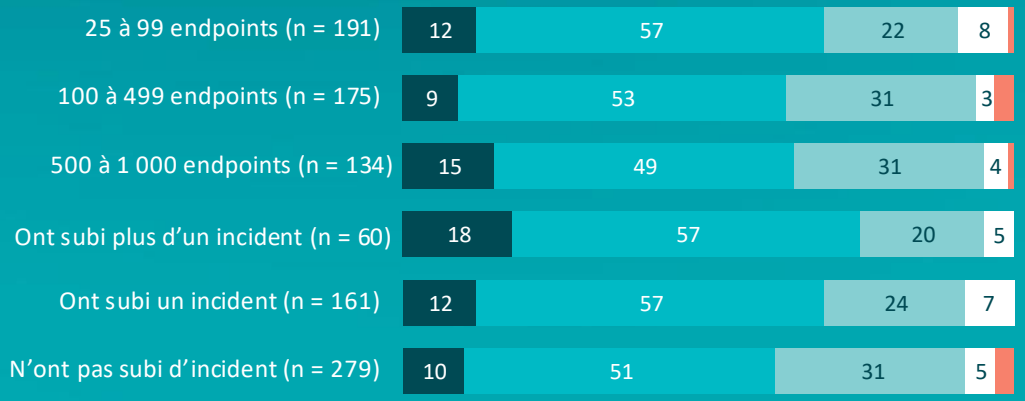
(en %)



Au moins une fois par mois
Au moins une fois par an
Jamais
Plusieurs fois par an
Une fois toutes les quelques années



(en %)



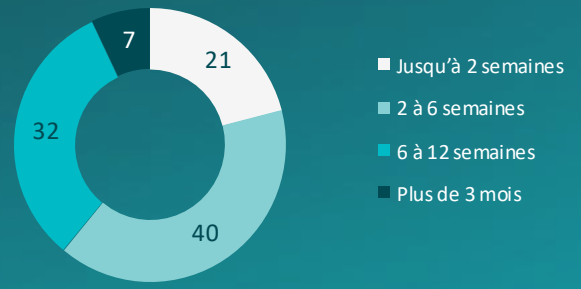
7

La réponse aux incidents s’est améliorée

La durée des enquêtes a diminué au cours des 4 dernières années

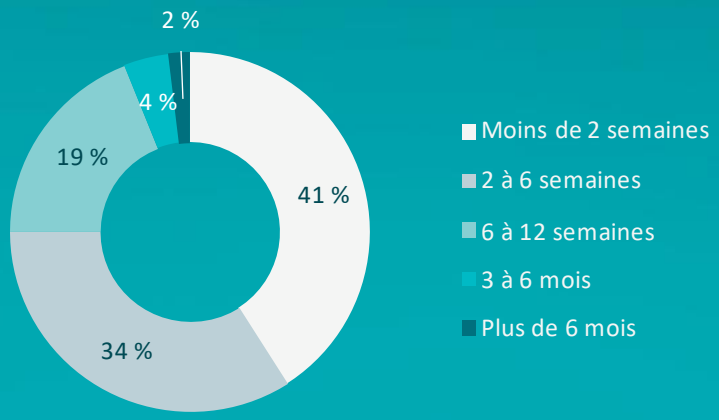
En 2022, la plupart des PME interrogées ont mis plusieurs mois à enquêter sur un incident. Quatre ans plus tard, les chiffres se sont considérablement améliorés, ce qui pourrait expliquer en partie la grande confiance dont font preuve les PME à l'échelle mondiale quant à leur cyber-résilience.

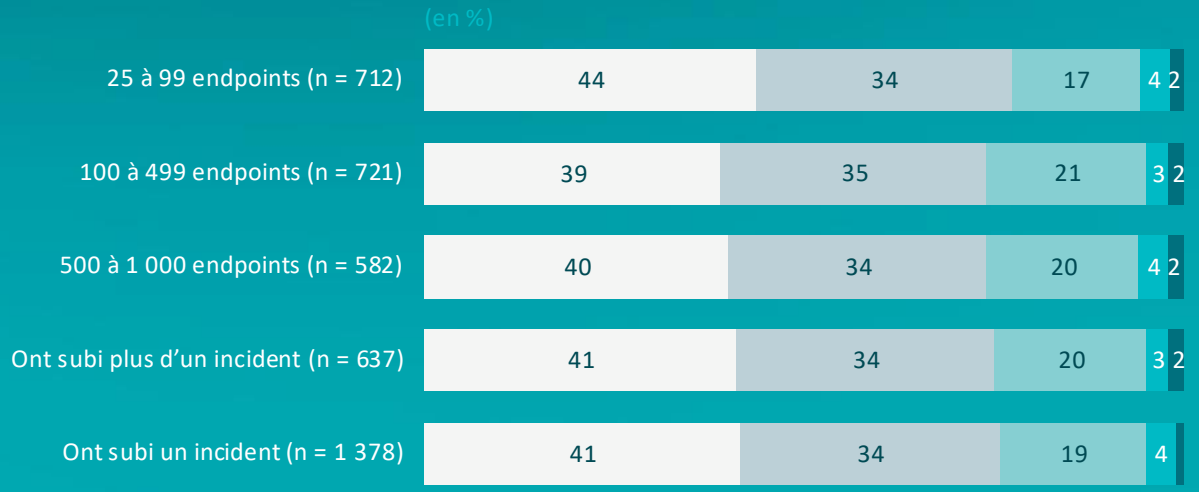
Durée moyenne des enquêtes sur les incidents à l'échelle mondiale en 2022



*Remarque : l'enquête de 2022 n'incluait pas le Japon (la Pologne y figurait à sa place).
Par ailleurs, l'échantillon comptait 838 entreprises en 2022, contre 2 015 en 2026 pour cette même question.

Durée moyenne d'une enquête sur une cyberattaque

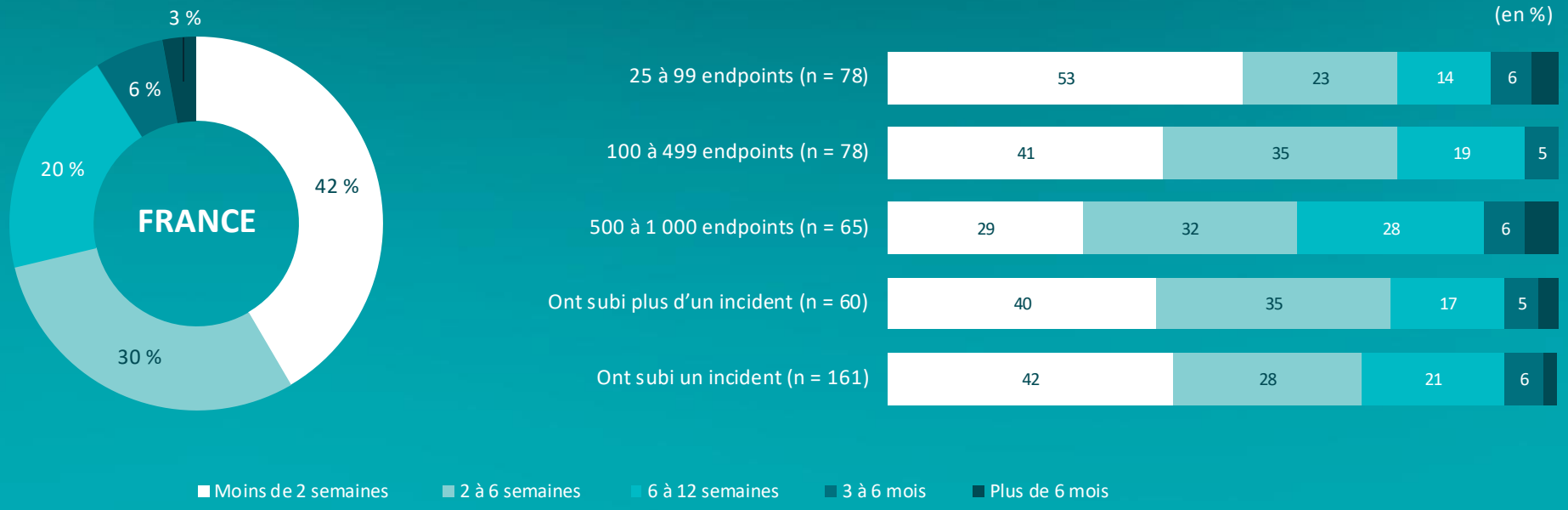




Les entreprises françaises gagnent en réactivité face aux cyberattaques, avec des enquêtes généralement conclues en moins de 6 semaines.

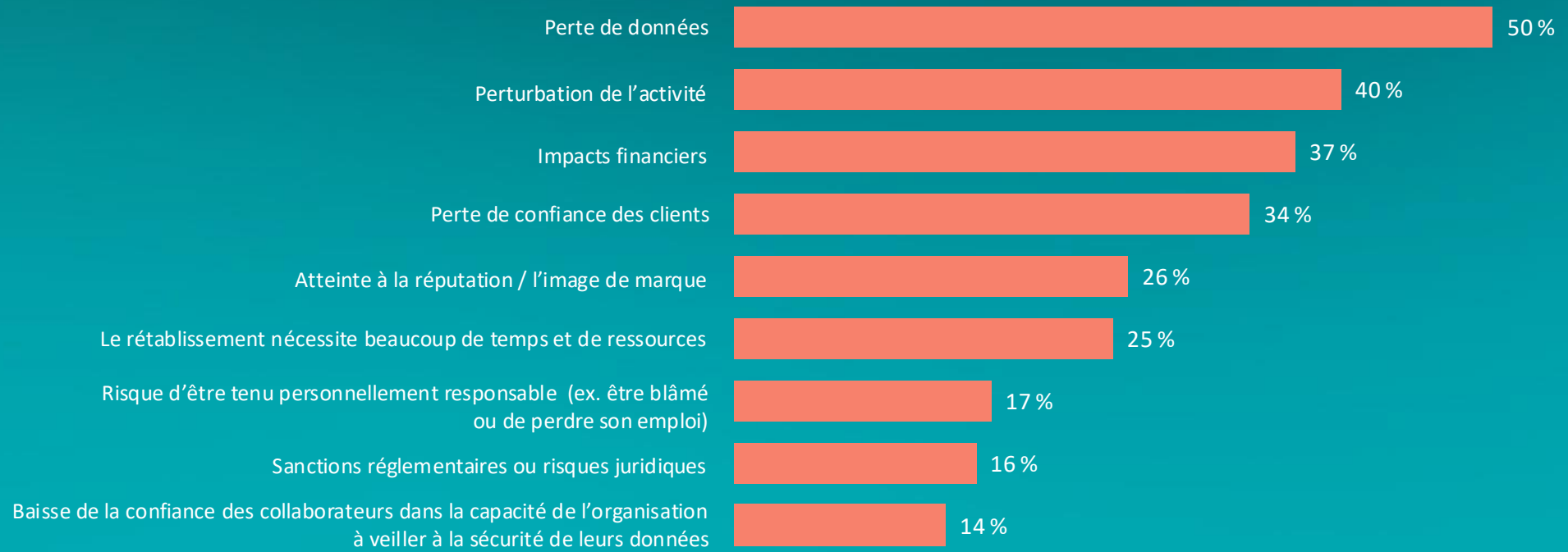
Les délais d'enquête observés en France sont globalement alignés avec ceux constatés à l'échelle mondiale, avec une majorité d'investigations menées à bien en moins de six semaines. Cette convergence suggère une montée en maturité des capacités de réponse aux incidents, même si les environnements les plus complexes continuent de nécessiter des délais d'analyse plus importants.

Durée moyenne d'une enquête sur une cyberattaque



Accélérer l’investigation des incidents permet de limiter les conséquences les plus redoutées des cyberattaques

Principales préoccupations concernant les répercussions des cyberattaques



8

Conclusion

Vers une meilleure résilience cyber

Michal Jankech

ESET, vice-président chargé des grandes entreprises, des PME et des MSP

Même si j'aimerais pouvoir affirmer que l'époque où l'on disait « nous sommes trop petits pour être attaqués » est révolue, il est clair que les PME prennent désormais la cybersécurité plus au sérieux.

L'indice montre un rapprochement croissant entre les PME et les fournisseurs de solutions de sécurité, avec une offre de plus en plus adaptée en termes de solutions et de services sur mesure. Ce regain d'optimisme et de confiance permet de mieux faire face aux incidents de sécurité et y survivre. Le recours accru à des produits de sécurité plus performants, les investissements dans des services tels que la détection et la réponse managées (MDR) ou les mesures de continuité des activités, comme la cyberassurance, constituent autant de signes encourageants.

Cependant, des incertitudes subsistent. Bien que 78 % des PME reconnaissent l'importance stratégique de la cybersécurité, une compréhension inégale des principales menaces, des technologies et de la terminologie, notamment en matière de MDR et de posture de sécurité, confirme qu'il reste encore des progrès à faire. Toute amélioration devra commencer par un rappel à la réalité. Nous avons constaté que les préoccupations des PME sont souvent influencées par les actualités sur les menaces émergentes, telles que les attaques par l'IA, tandis que les risques plus courants, tels que l'hameçonnage, les vulnérabilités non corrigées et le manque de surveillance, sont sous-estimés. Cela laisse entendre que de nombreuses personnes interrogées ont une perception erronée de leur niveau de sécurité et de leur résilience.

Néanmoins, la confiance croissante qui ressort de l'enquête est un indicateur positif des intentions. Mais cela nous rappelle également pourquoi une bonne relation entre les prestataires et les utilisateurs est si importante.

En l'absence d'une protection automatique miracle contre toutes les menaces existantes, pour améliorer véritablement leur degré de préparation et de cyber-résilience, les PME doivent évaluer avec précision leur niveau de sécurité, solliciter l'avis d'experts et garantir une protection continue contre les menaces susceptibles de perturber leurs activités.

9

À propos de l’étude

À propos de l’étude

Sujet
La cybersécurité dans les entreprises de 13 pays.

Groupe cible
Entreprises comptant entre 25 et 1 000 endpoints. La personne interrogée est chargée des décisions en matière de cybersécurité ou exerce une influence sur les décisions prises dans ce domaine.

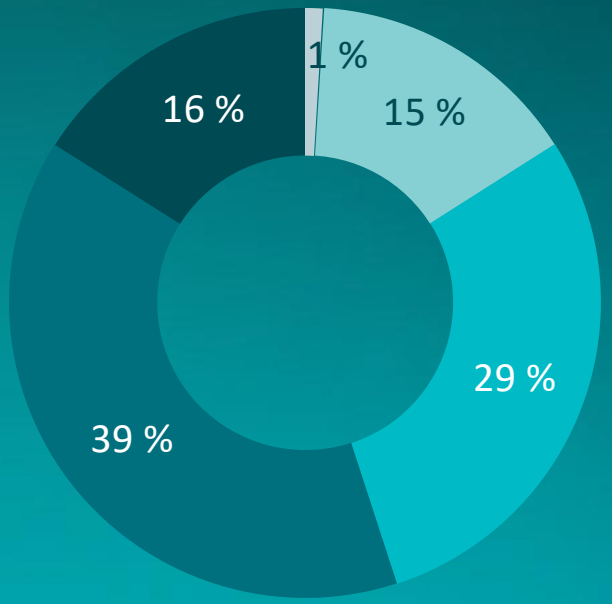
Taille totale de l’échantillon
N = 4 400

Agence de sondages
Go4insight, membre de l’ESOMAR (Société européenne pour les études d’opinion et de marché).

Les rédacteurs de l’Indice de préparation des PME à la cybersécurité en 2026 ont choisi d’arrondir les chiffres à l’entier
le plus proche dans l’ensemble du rapport, ce qui entraîne une marge d’erreur de 1 %.

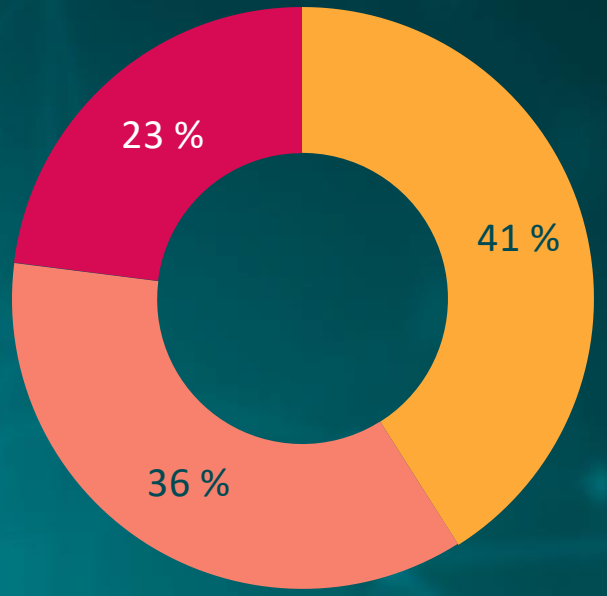
Pays	Nombre de personnes interrogées
Canada	200
Tchéquie	200
Danemark	150
France	500
Allemagne	500
Italie	500
Japon	500
Pays-Bas	100
Slovaquie	200
Espagne	400
Suède	150
Royaume-Uni	500
États-Unis	500
Total	**4 400**

Structure de l'échantillon



Nombre de collaborateurs

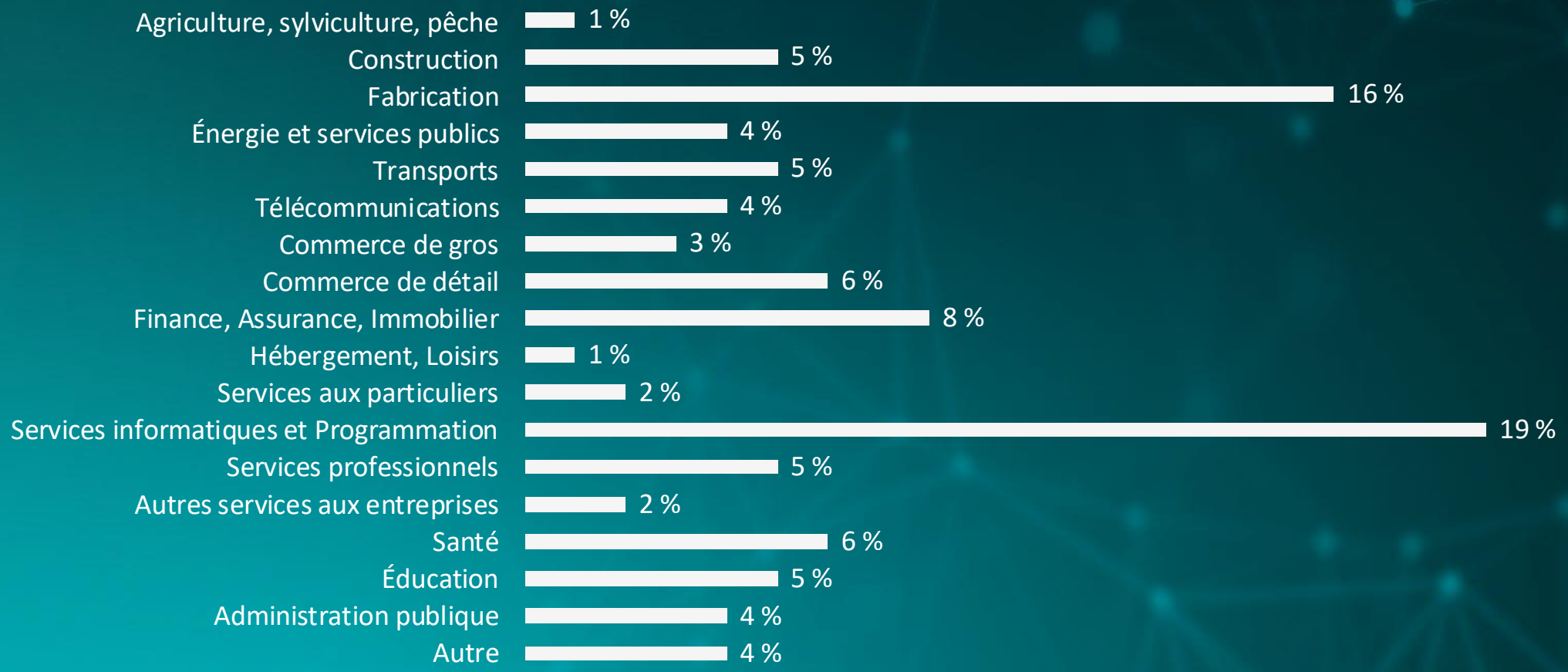
- Moins de 25 collaborateurs
- 25 à 99 collaborateurs
- 100 à 499 collaborateurs
- 500 à 1 000 collaborateurs
- Plus de 1 000 collaborateurs



Nombre d'endpoints

- 25 à 99 endpoints
- 100 à 499 endpoints
- 500 à 1 000 endpoints

Secteur d’activité



10

Annexe

Ce document est à jour au 15 mai 2026 et peut être modifié à tout moment par ESET.
L'utilisation des données, statistiques, chiffres et autres informations contenues dans le rapport est autorisée à condition d'en citer correctement la source : Veuillez citer la source sous l'intitulé « Panorama ESET 2026 de la Cybersécurité des PME en France : entre Confiance et Nouvelles Réalités » et inclure un lien vers le rapport. Les citations doivent être reproduites dans leur intégralité et sans modification. Toute autre utilisation, y compris à des fins commerciales, est soumise à l'accord écrit préalable d'ESET.

Pour plus d'informations, veuillez contacter le service des relations publiques d'ESET à l'adresse presse@eset-nod32.fr.

L’IA au cœur de la prévention des cybermenaces

Portée par plus de 30 années d’expertise humaine,
11 centres de recherche et de développement répartis dans le monde entier ainsi qu’un accompagnement client local.

www.eset.com/fr

ESET Cybersecurity
Progress. Protected.