opinionway

POUR CESIN

Baromètre de la cybersécurité des entreprises

Rapport d'étude – Vague 11

Janvier 2026

Contact presse :
Véronique LOQUET – ***AL'X COMMUNICATION***
06 68 42 79 68 - vloquet@alx-communication.com

Crédits : Photo de Josh Sorenson sur Pexels

Crédits : benjamin-davies

opinionway

Les objectifs

Le contexte

Le CESIN a lancé en 2015 avec OpinionWay sa première grande enquête auprès de ses membres.

Le CESIN lance cette année la 11ème vague de son baromètre de la cybersécurité.

Les objectifs

– 1 –

Connaître la perception de la cybersécurité et de ses enjeux auprès des membres du CESIN

– 2 –

Connaître la réalité concrète du risque cyber dans les entreprises

– 3 –

Mesurer les évolutions sur un domaine en perpétuel changement

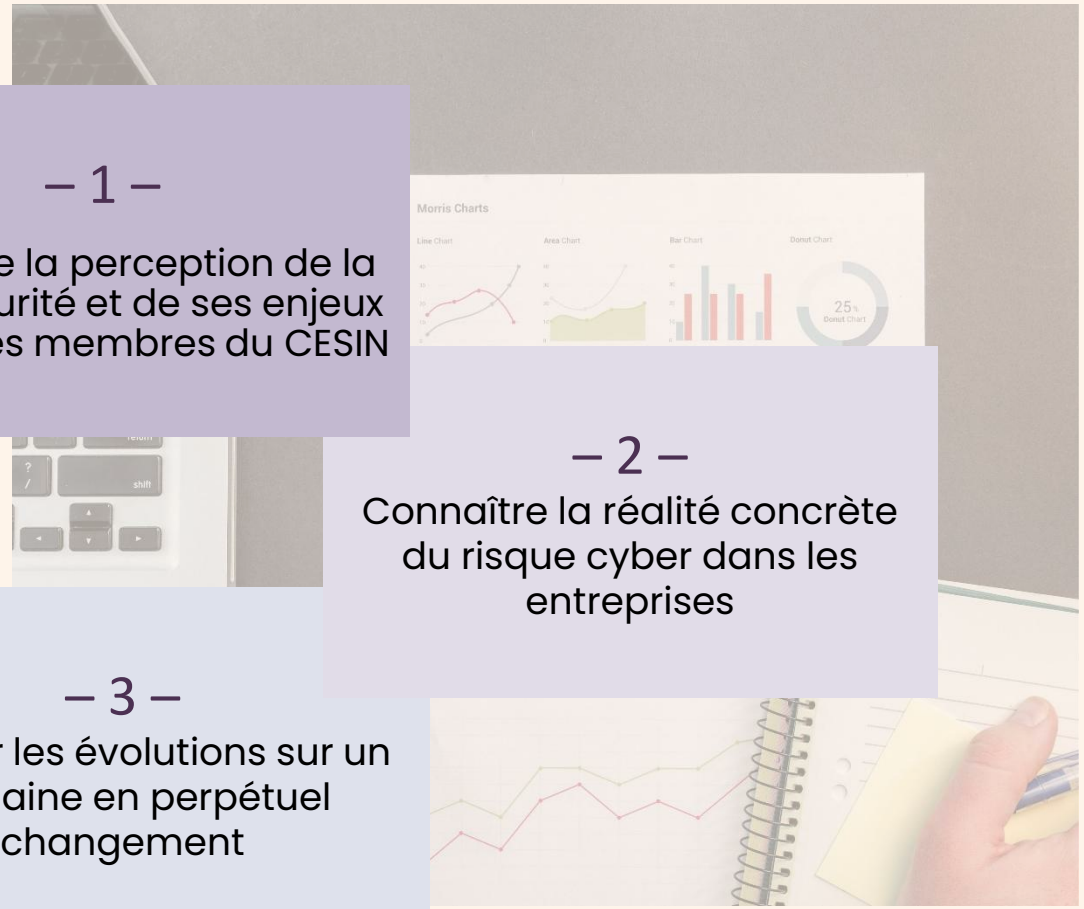


Photo de Lukas: https://www.pexels.com/fr-fr/photo/personne-tenant-un-stylo-a-bille-bleu-sur-un-ordinateur-portable-blanc-669610/

La méthodologie

La méthodologie

Toute publication totale ou partielle doit impérativement utiliser la mention complète suivante :

« Sondage OpinionWay pour CESIN »

et aucune reprise de l'enquête ne pourra être dissociée de cet intitulé

Echantillon de **397 membres du CESIN**, à partir du fichier des membres du CESIN.

L'échantillon a été interrogé par **questionnaire auto-administré en ligne sur système CAWI** (Computer Assisted Web Interview).

Questionnaire CESIN 2025

Les interviews ont été réalisées **du 17 novembre au 12 décembre 2025.**

OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la **norme ISO 20252**

Les résultats de ce sondage doivent être lus en tenant compte **des marges d'incertitude** : 4,9 points au plus pour un échantillon de 400 répondants.*

** Compte tenu de la taille de l'échantillon, les résultats pourraient varier d'environ plus ou moins 4,9 points autour de la valeur mesurée, ce qui représente l'incertitude statistique.*

Le profil de l’échantillon

Le profil de l'échantillon

Vous répondez en tant que :	
Groupe	46%
Entreprise indépendante / administration	35%
Entité (direction ou entité) d'un groupe	19%

Nombre de salariés de l'entreprise	
Grandes entreprises	**40%**
50 000 salariés ou plus	12%
Entre 10 000 et 49 999 salariés	16%
Entre 5 000 et 9 999 salariés	12%
ETI	**43%**
Entre 1 000 et 4 999 salariés	26%
Entre 250 et 999 salariés	17%
TPE / PME (moins de 250 salariés)	**17%**

Dans quel pays est implanté le siège de votre entreprise ?	
France	93%
Allemagne	<1%
Royaume-Uni	<1%
Etats-Unis	<1%
Suède	<1%
Pays-Bas	<1%
Canada	<1%
Italie	<1%
Autres pays	3%

Sur quel périmètre intervenez-vous ?	
Uniquement dans mon pays	41%
Européen	17%
International	42%

Crédits : Icone de Storyset.com

Le profil de l'échantillon

Secteur d'activité de l'entreprise	
Services	**40%**
Information et communication	20%
Activités financières et d'assurance	16%
Activités spécialisées, scientifiques et techniques	2%
Arts, spectacles et activités récréatives	1%
Activités immobilières	1%
Industrie / BTP	**26%**
Industrie manufacturière	13%
Construction	5%
Production et distribution d'électricité, gaz, vapeur, air conditionné	4%
Agriculture, sylviculture et pêche	2%
Production et distribution d'eau, assainissement, gestion des déchets et dépollution	2%
Industries extractives	<1%
Services publics	**17%**
Administration publique et défense, collectivité	9%
Santé humaine et action sociale	7%
Enseignement	1%
Commerce	**13%**
Commerce	6%
Transports et entreposage	5%
Hébergement et restauration	2%
Autres secteurs	**4%**

Secteur Commerce	
Activités BtoB	16%
Activités BtoC	20%
Activités BtoB et BtoC	64%

Crédits : Icone de Storyset.com

Les résultats

opinionway

01

Un volume de cyberattaques significatives en baisse, mais des conséquences plus importantes pour les entreprises

Définition d’une cyberattaque

« Une cyberattaque significative, telle que nous l’entendons dans cette enquête, est le fait que l’organisation soit victime directement ou indirectement à travers ses tiers d’un acte malveillant envers tout ou partie du Système d’Information, impactant des processus métiers en portant atteinte de manière significative à la confidentialité et/ou à l’intégrité de l'information de l’entreprise ou encore à la disponibilité du système d’information. Cette cyberattaque peut avoir notamment entraîné des pertes financières significatives, une atteinte à l’image de l’entreprise, une sanction règlementaire, des impacts sanitaires ou environnementaux, et/ou avoir nécessité des efforts significatifs de défense pour contenir et traiter l’attaque. Nous ne comptons pas là ***les tentatives*** *d’attaques qui ont été arrêtées, ou atténuées par les systèmes de prévention, protection et de réponse aux incidents. »*

4 entreprises sur 10 ont subi au moins une cyberattaque significative en 2025, un constat en baisse depuis l'an passé et qui décroit d'année en année. Les grandes entreprises sont toujours les plus attaquées.

Q4. Au total, combien de **cyberattaques significatives ont été subies par votre entreprise** au cours des 12 derniers mois ?

Base : ensemble (397)

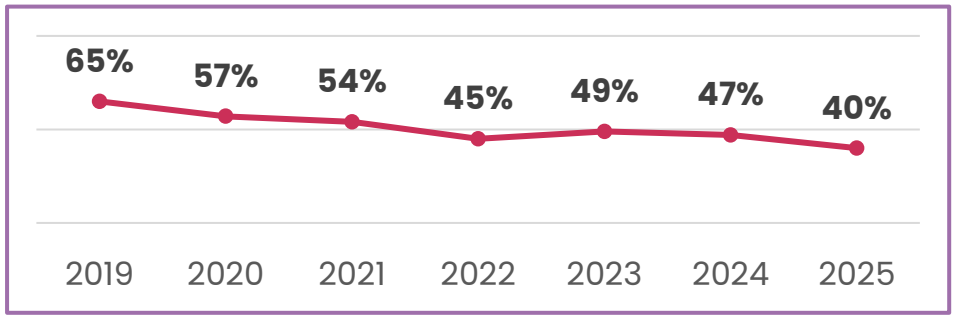
40% ☒ *(47%)*

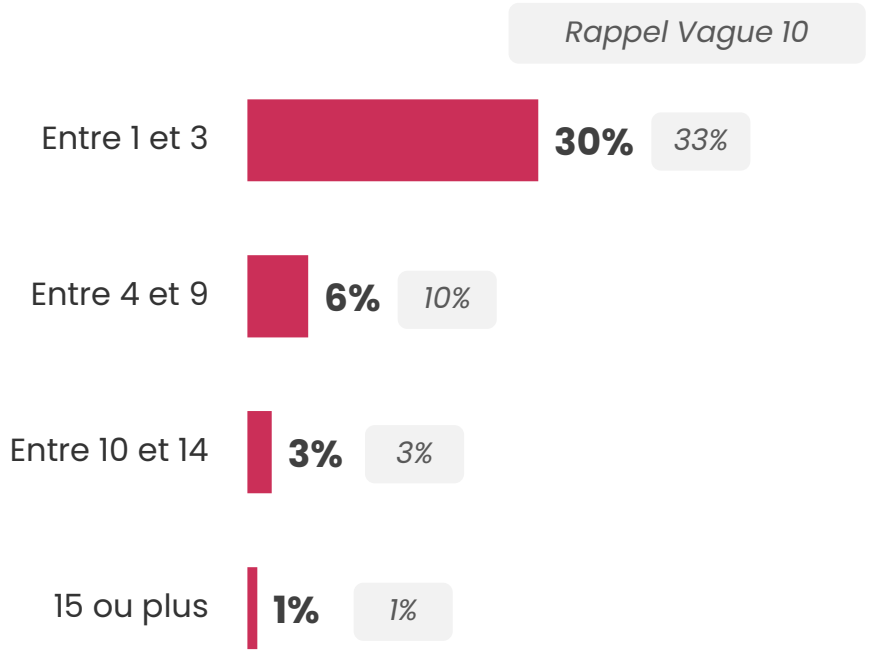
des entreprises ont constaté au moins une cyberattaque significative

Grandes entreprises : **50%**

ETI : **34%**

Rappel vagues précédentes





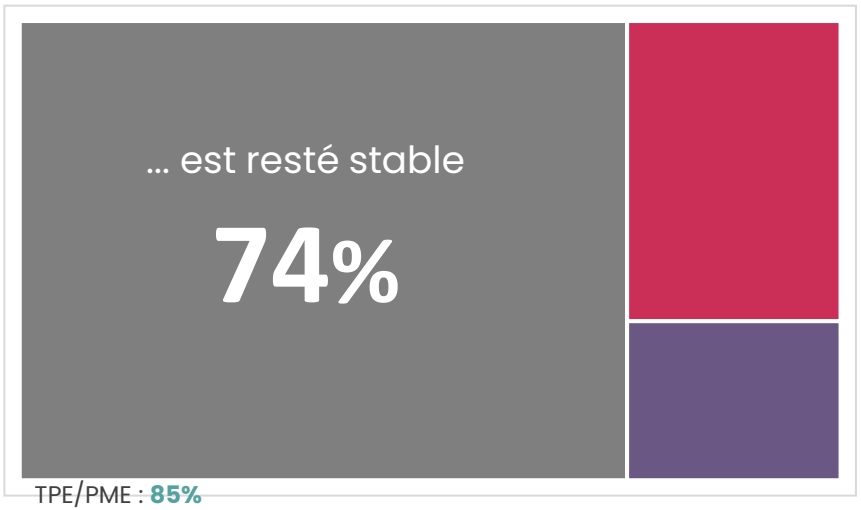
Comme lors de la vague précédente, le nombre d'attaques subies est resté stable pour la majorité des entreprises.

Q4bis. Et par rapport à l'année dernière, **ce nombre d'attaques constatées dans votre entreprise**… ?

Base : ensemble (397)

Parmi toutes les entreprises

En un an, le nombre d'attaques…



… a augmenté
17% *19%*

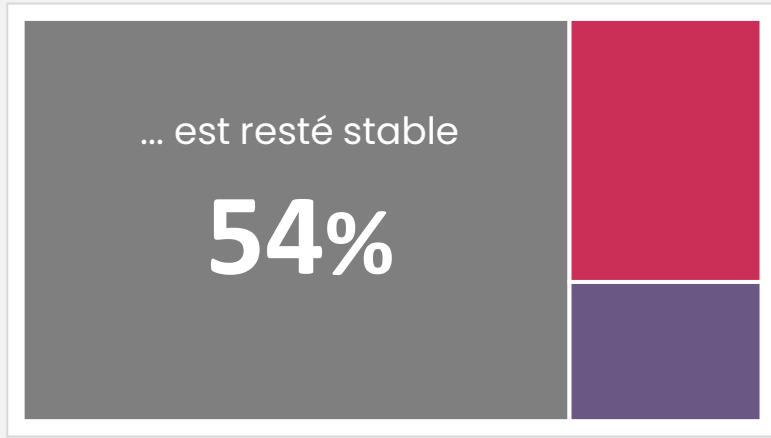
… a diminué
9% *11%*

TPE/PME : **85%**

Rappel Vague 10 *69%*

Parmi les entreprises ayant subi au moins une attaque significative

En un an, le nombre d'attaques…



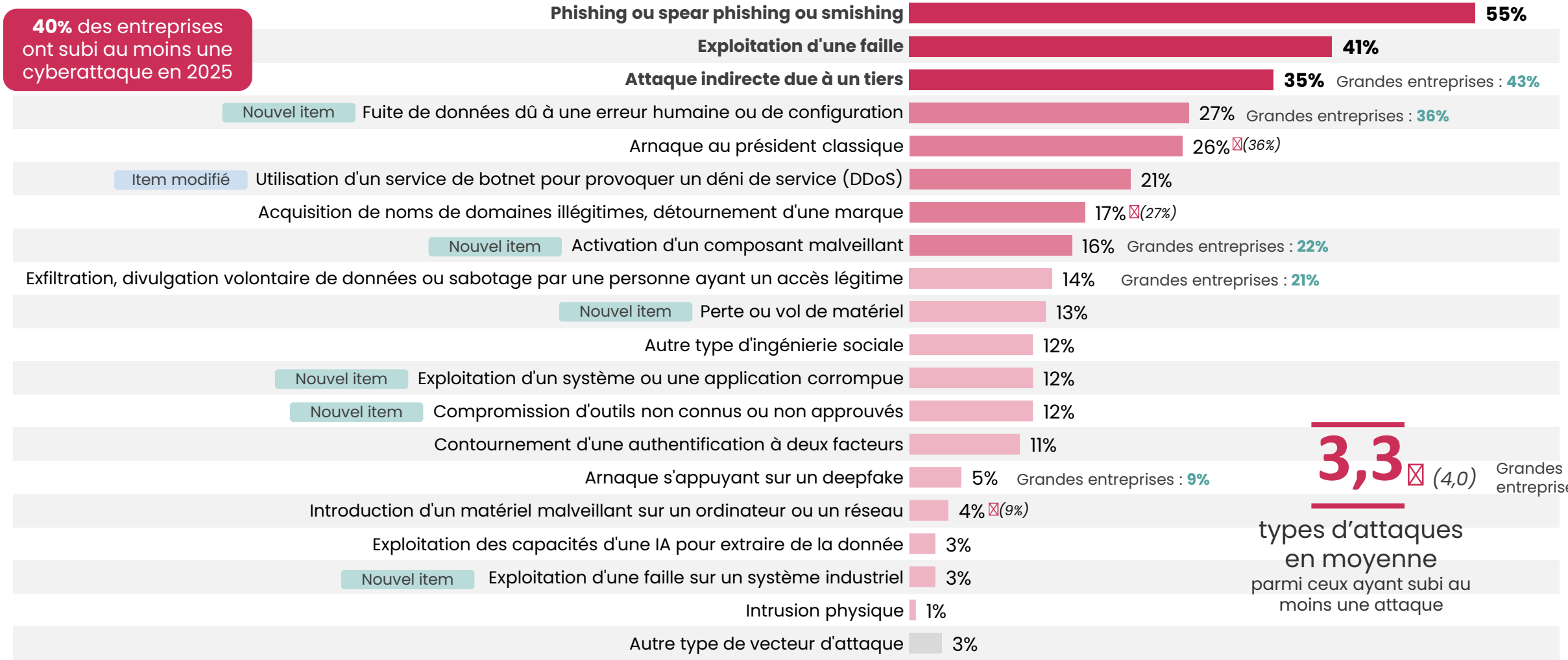
… a augmenté
42%

… a diminué
4%

Malgré la baisse de la diversité des vecteurs d'attaque, le phishing, le spear phishing et le smishing restent les plus courants, suivis de l'exploitation d'une faille. L'attaque indirecte due à un tiers reste un vecteur prioritaire, surtout pour les grandes entreprises, alors que les arnaques au président et l'acquisition des noms de domaines reculent.

Q5A. Sur l'ensemble des cyberattaques significatives que vous avez subies au cours des 12 derniers mois, indiquez **les vecteurs qui ont permis à ces cyberattaques de démarrer ou de se déployer** ? *Base : ont constaté une attaque (159) - plusieurs réponses possibles*

40% des entreprises ont subi au moins une cyberattaque en 2025



3,3 ⊠ *(4,0)* Grandes entreprises : **3,9**

types d'attaques en moyenne

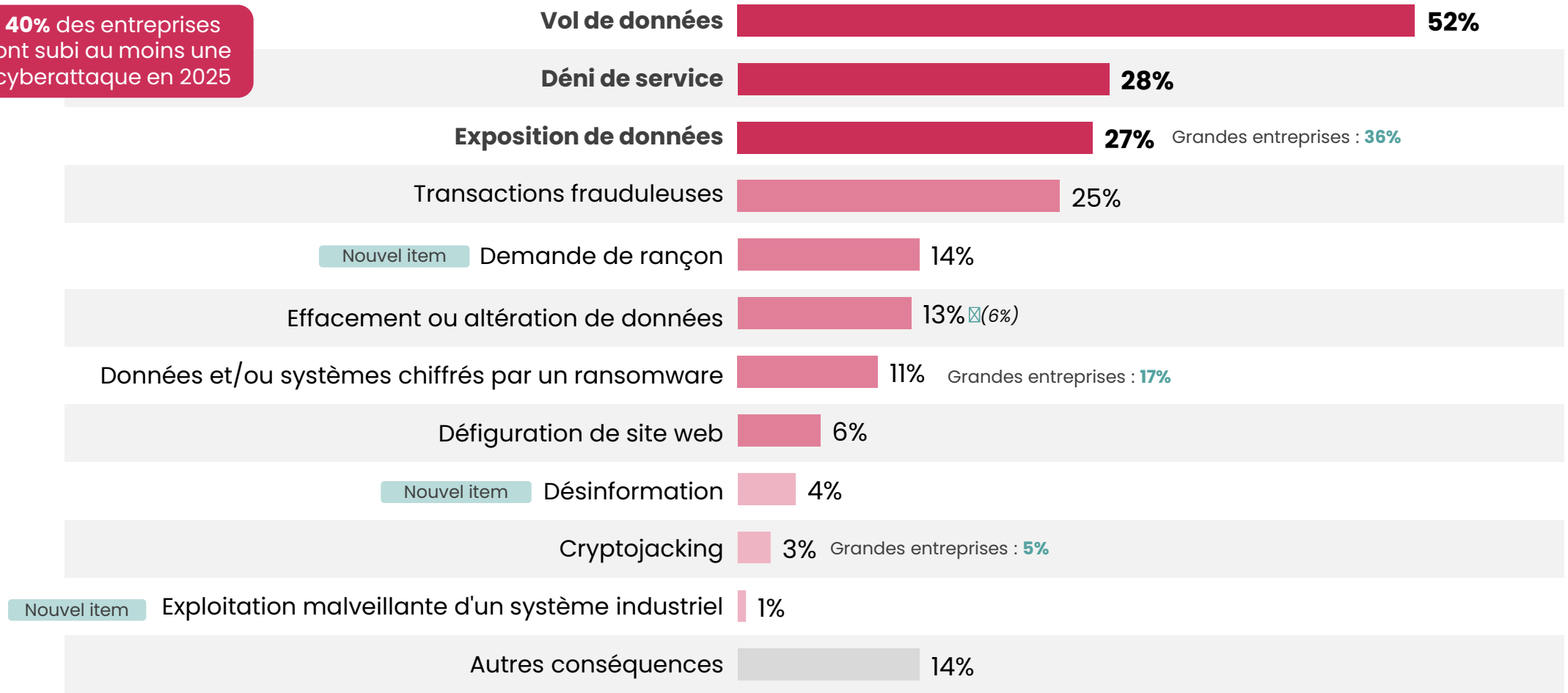
parmi ceux ayant subi au moins une attaque

Le vol de données est très largement la première conséquence de ces cyberattaques. À noter aussi que l'effacement ou l'altération de données est une conséquence deux fois plus constatée que l'année précédente.

Q5B : Et quelles ont été **les conséquences techniques** de cette/ces cyberattaque(s) ?

Base : ont constaté une attaque (159) - plusieurs réponses possibles

40% des entreprises ont subi au moins une cyberattaque en 2025

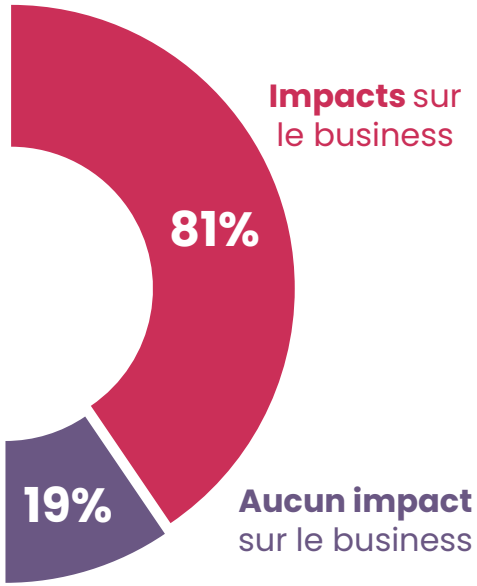


En 2025, les cyberattaques significatives ont eu un impact important sur les business des entreprises, atteignant 4 entreprises sur 5. Il s'agit le plus souvent d'une perturbation de la production ou la perte d'image.

Q7 : Quel a été **l'impact des cyberattaques sur votre business** ?

Base : ont constaté une attaque et / ou une cause d'incidents de sécurité (159)

Plusieurs réponses possibles



Impacts sur le business

Aucun impact sur le business

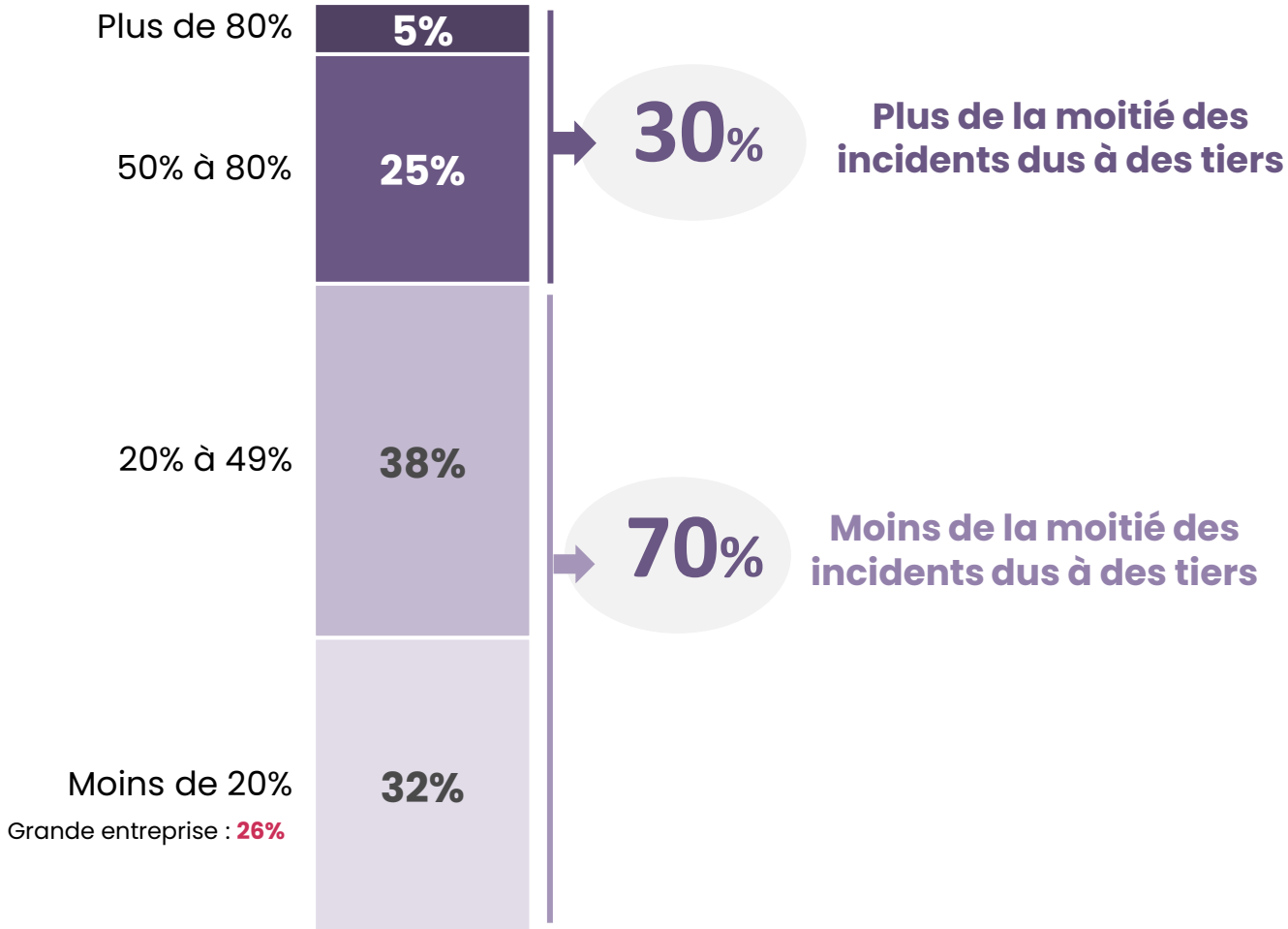
Perturbation de la production pendant une période significative (impactant le business)	**28%**
Perte d'image, impact médiatique	**26%** GE : 36% ETI : 14%!
Compromission d'information / élément de processus et savoir-faire de l'entreprise	**18%**
Perte de CA	18%
Indisponibilité du site web pendant une période significative (visible par le client)	17%
Arrêt de la production pendant une période significative (impactant le business)	14% Grandes entreprises : 20%
Perte financière directe liée à des transactions frauduleuses	14%
Déconnexion par les tiers (mise en quarantaine)	12%
Retard sur la livraison auprès des clients	8%
Nouvel item Impact sur les biens et personnes	8%
Sanction par une autorité	3%
Contrefaçon	1%
Autre impact	8%

Près d'un tiers des entreprises estiment que plus de la moitié des incidents de cybersécurité sont dus à des tiers.

Nouvelle question en 2025

Q52 : A combien estimez-vous **le ratio d'incidents de cybersécurité dus à des tiers** (tiers informatiques et non informatiques) ?

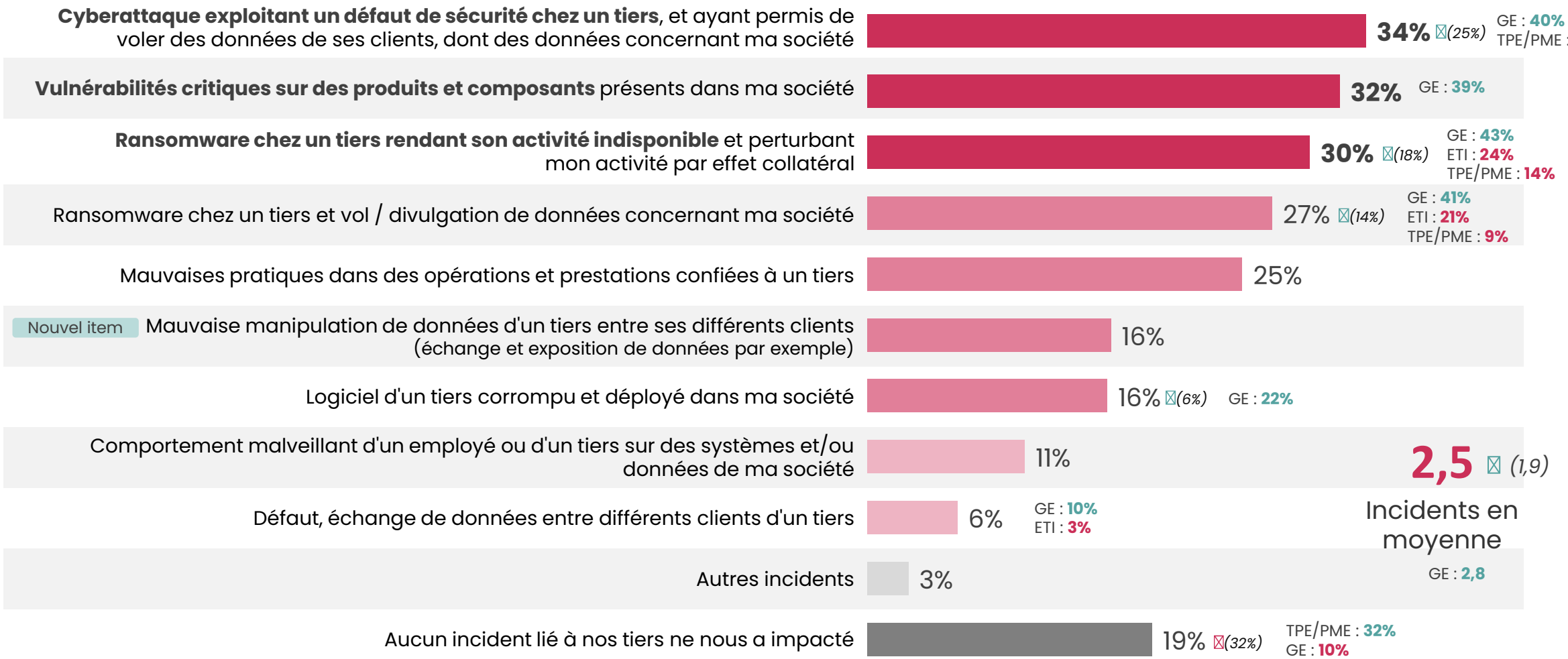
Base : ensemble (397)



De façon générale, les entreprises identifient de plus en plus d'incidents liés à des tiers par rapport aux années précédentes. Parmi eux, les cyberattaques exploitant un défaut de sécurité chez un tiers sont les plus régulières.

Q40 : Quels **incidents liés à vos tiers vous ont impactés** ?

Base : ensemble (397) – Plusieurs réponses possibles

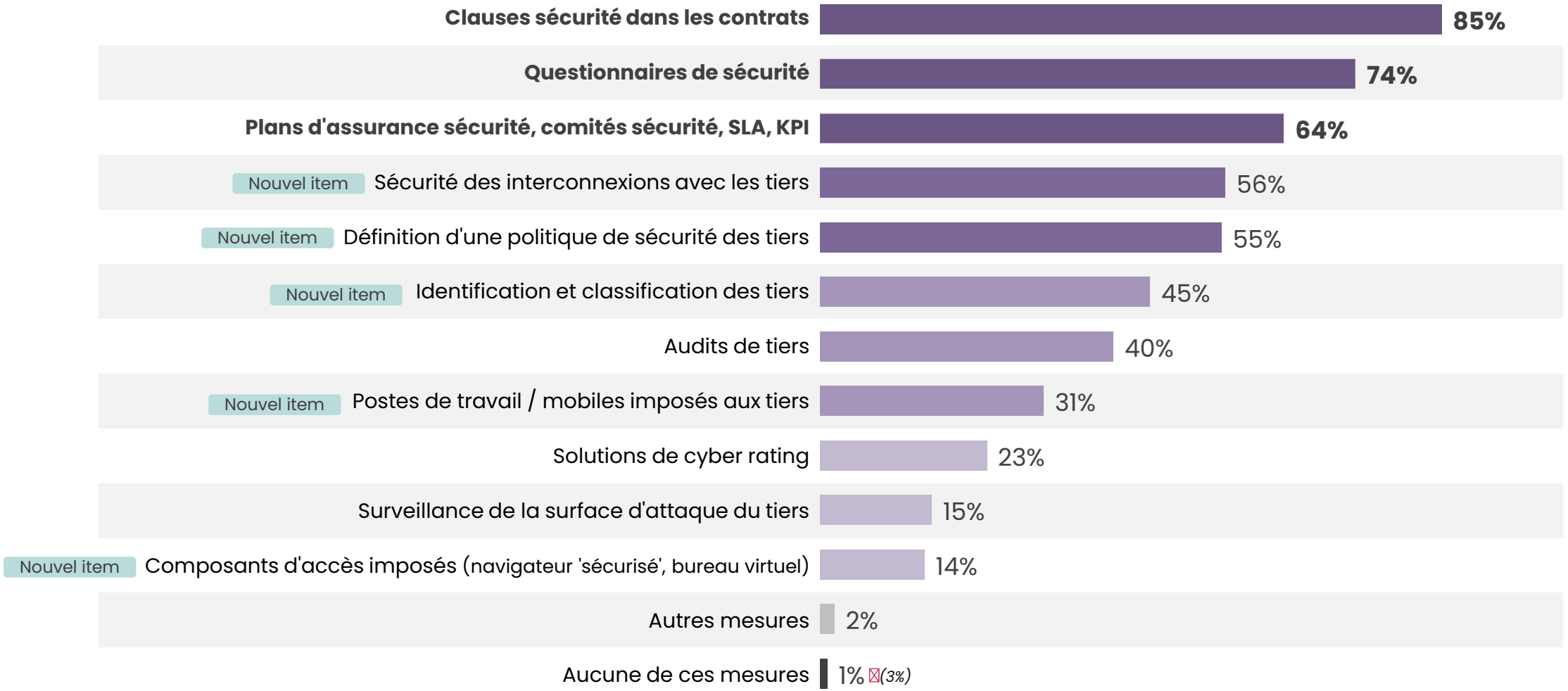


⊠⊠ significativement supérieur/ inférieur par rapport à la vague précédente

Pour limiter ces risques, les clauses de sécurité dans les contrats, les questionnaires de sécurité et les plans d'assurance sécurité sont les principales mesures mises en place.

Q43 : Quelles **mesures** avez-vous entreprises **pour adresser le risque lié aux tiers** ?

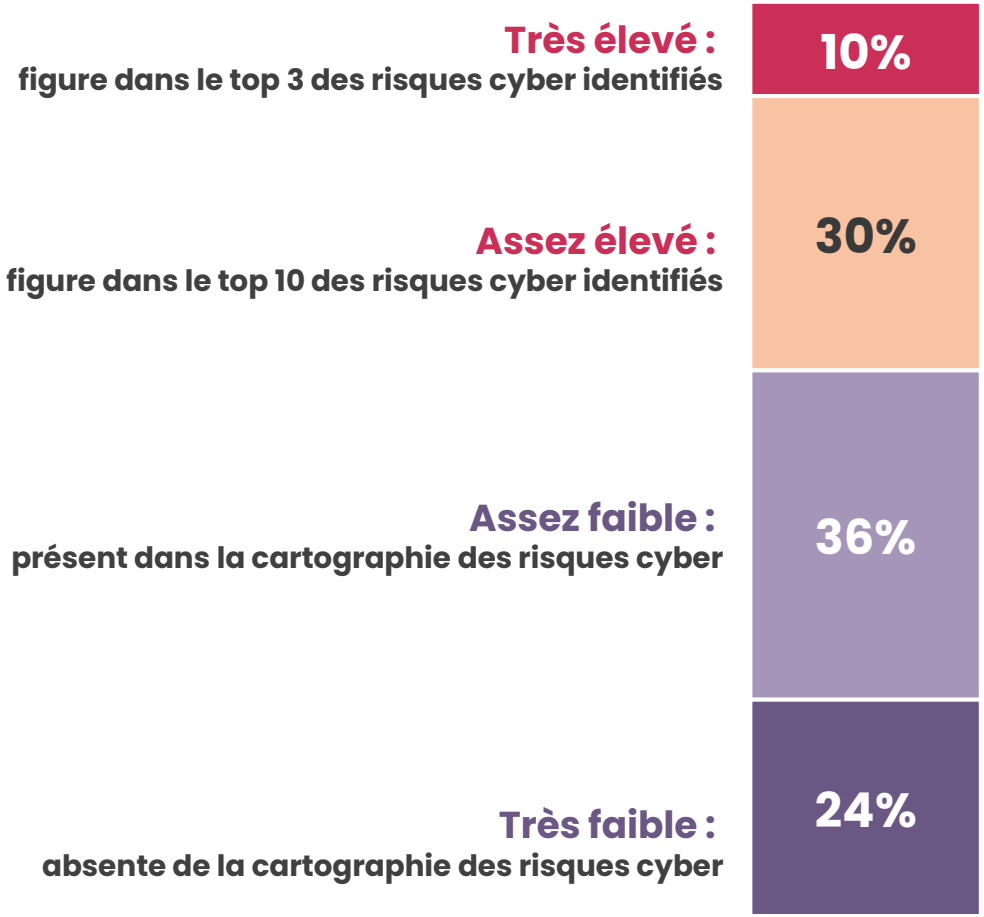
Base : ensemble (397) – Plusieurs réponses possibles



En 2025, 4 entreprises sur 10 estiment élevé le niveau des menaces relatives au cyber espionnage, et ce, quelle que soit leur structure.

Q9 : Aujourd'hui, comment évaluez-vous **le niveau des menaces relatives au cyberespionnage** pour votre entreprise, parmi tous vos risques cyber ?

Base : ensemble (397)



40% **Estiment un niveau élevé des menaces relatives au cyberespionnage**

Rappel Vague 10 *37%*

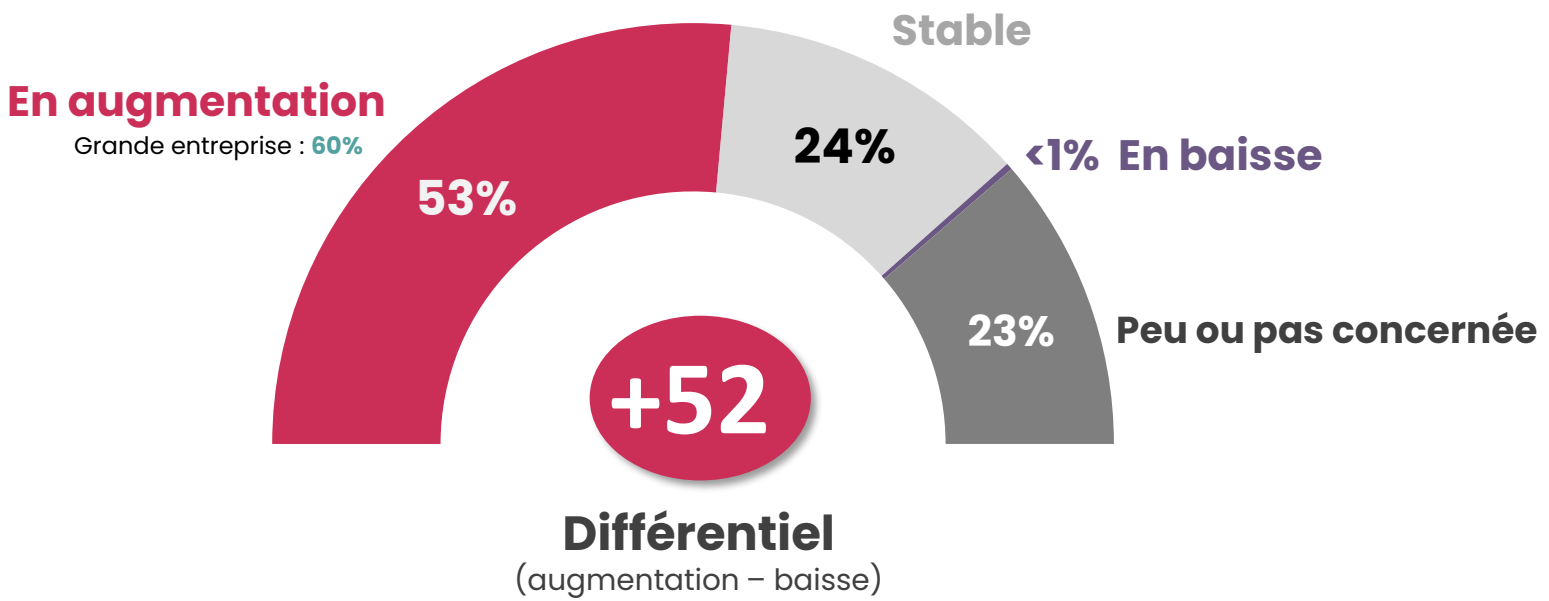
Crédits : Icone de Storyset.com

La menace d'origine étatique, en lien avec le contexte géopolitique mondial est jugée en augmentation par la moitié des entreprises.

Nouvelle question en 2025

Q51 : Dans un contexte géopolitique en tension, comment jugez-vous **l'évolution de la menace d'origine étatique** sur votre entreprise ?

Base : ensemble (397)



Crédits : Icone de Storyset.com

02

Des entreprises bien équipées et proactives face aux menaces cyber

Les solutions de sécurité sur le marché sont adaptées aux besoins de la grande majorité des entreprises. C'est d'autant plus le cas pour les grandes entreprises.

Q25 : Pensez-vous que **les solutions et services de sécurité disponibles sur le marché sont adaptés** à votre entreprise ?

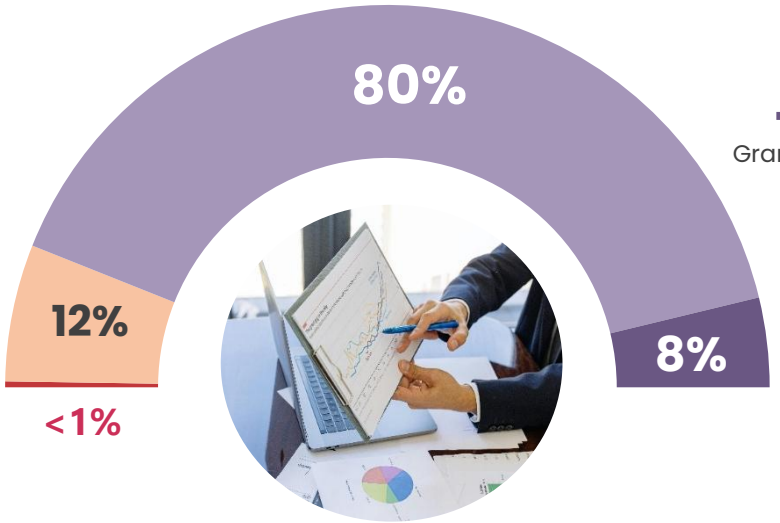
Base : ensemble (397)

Rappel Vague 10

Pas du tout adaptés | Plutôt pas adaptés | Plutôt adaptés | Tout à fait adaptés

% Inadaptés

16% **12%**

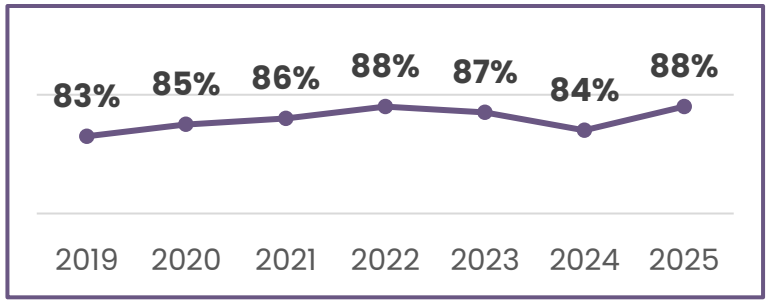


% Adaptés

88%

Grandes entreprises : **92%**

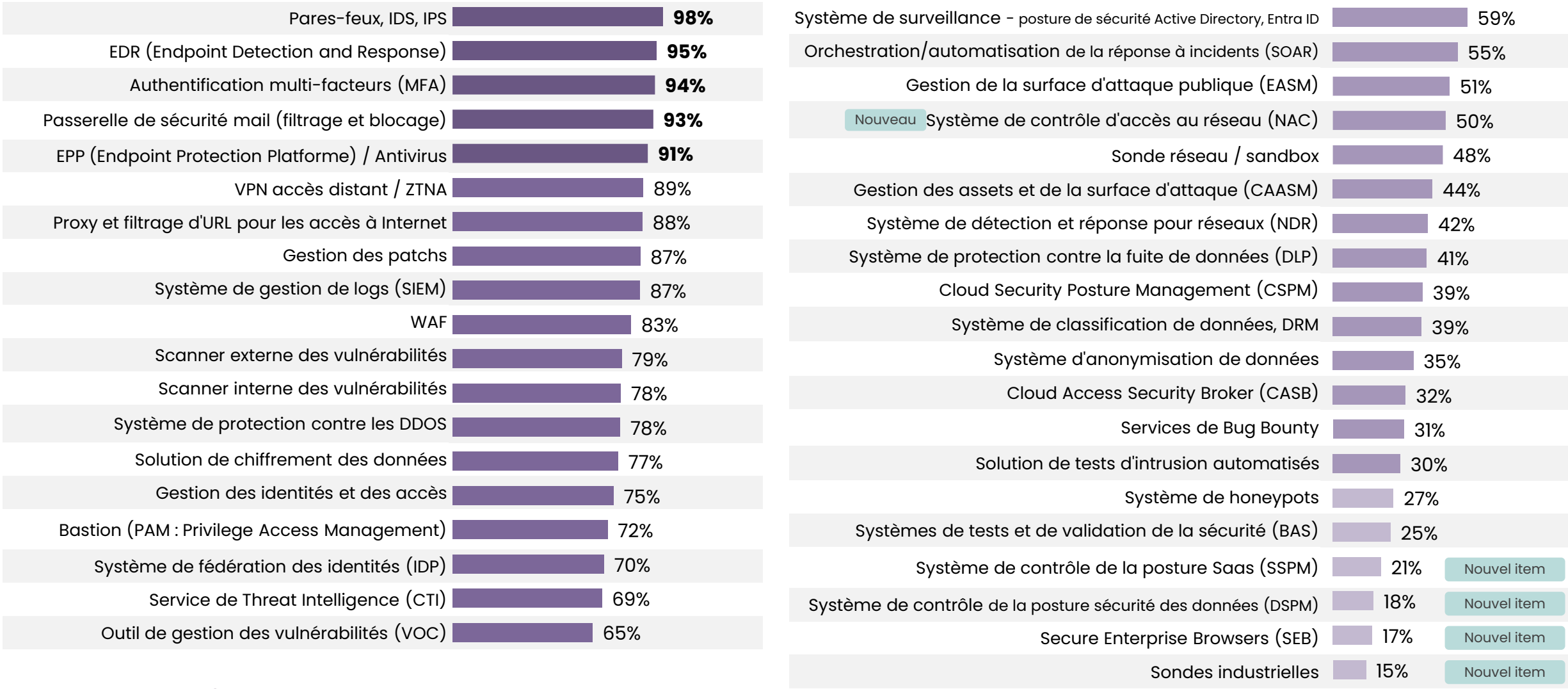
Rappel vagues précédentes



Crédits : Photo de Anthony Shkraba sur Pexels.com

Le trio Pare-feu, EDR et MFA restent les solutions les plus utilisées dans les entreprises.

Q13 : Les **solutions de sécurité** suivantes sont-elles **en place dans votre stratégie de défense** ? *Base : ensemble (397) – Plusieurs réponses possibles*



Détail de la mise en place des solutions de sécurité

Question modifiée en 2025

Q13 : Les **solutions de sécurité** suivantes sont-elles **en place dans votre stratégie de défense** ?

Base : ensemble (397)

	Total Déployé dans l'entreprise	Oui et elle a une valeur élevée	Oui et elle a une valeur moyenne	Oui mais elle a une valeur faible ou nulle	Cette solution n'est pas déployée	Cette solution est en projet
Pares-feux, IDS, IPS	***98%***	76%	19%	3%	2%	0%
EDR (Endpoint Detection and Response)	***95%***	87%	7%	1%	1%	4%
Authentification multi-facteurs (MFA)	***94%***	85%	8%	1%	1%	5%
Passerelle de sécurité mail (filtrage et blocage)	***93%***	72%	18%	3%	5%	2%
EPP (Endpoint Protection Platforme) / Antivirus	***91%***	73%	15%	3%	9%	-
VPN accès distant / ZTNA (Zero Trust Network Access)	***89%***	63%	23%	3%	4%	7%
Proxy et filtrage d'URL pour les accès à Internet (SWG : Secure Web Gateway)	***88%***	59%	25%	4%	9%	3%
Gestion des patchs	***87%***	58%	26%	3%	7%	6%
Système de gestion de logs (SIEM)	***87%***	64%	19%	4%	5%	8%
WAF (Web Application Firewall)	***83%***	50%	27%	6%	13%	4%
Scanner externe des vulnérabilités	***79%***	44%	30%	5%	16%	5%
Scanner interne des vulnérabilités	***78%***	43%	28%	7%	13%	9%
Système de protection contre les DDOS	***78%***	38%	30%	10%	19%	3%
Solution de chiffrement des données	***77%***	37%	30%	10%	17%	6%
Gestion des identités et des accès (gouvernance des identités)	***75%***	52%	20%	3%	9%	16%
Bastion (PAM : Privilege Access Management)	***72%***	48%	20%	4%	12%	16%
Système de fédération des identités (IDP)	***70%***	49%	19%	2%	20%	10%
Service de Threat Intelligence (CTI)	***69%***	32%	28%	9%	20%	11%
Outil de gestion des vulnérabilités (VOC)	***65%***	37%	23%	5%	21%	14%

Détail de la mise en place des solutions de sécurité

Question modifiée en 2025

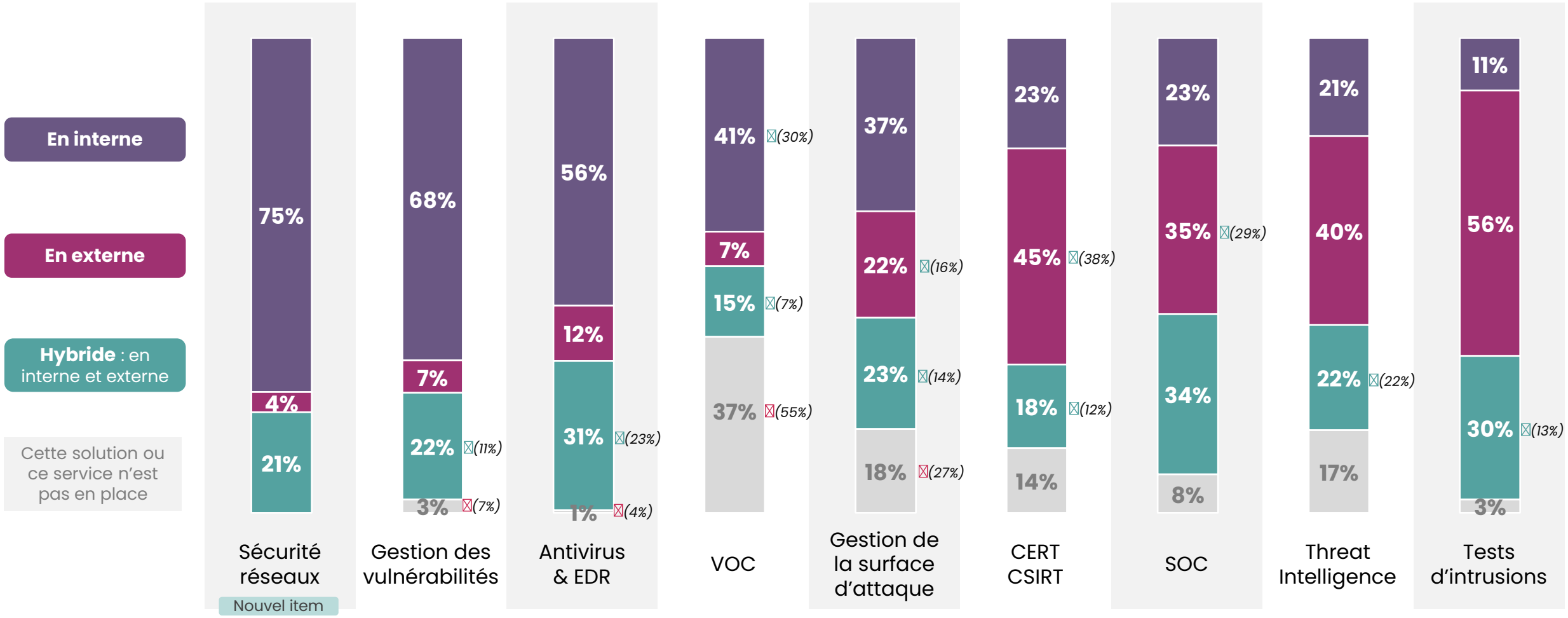
Q13 : Les **solutions de sécurité** suivantes sont-elles **en place dans votre stratégie de défense** ?

Base : ensemble (397)

	Total Déployé dans l'entreprise	Oui et elle a une valeur élevée	Oui et elle a une valeur moyenne	Oui mais elle a une valeur faible ou nulle	Cette solution n'est pas déployée	Cette solution est en projet
Système de surveillance de la posture de sécurité Active Directory, Entra ID (ISPM)	***59%***	35%	20%	4%	30%	11%
Orchestration et automatisation de la réponse à incidents (SOAR)	***55%***	31%	18%	6%	29%	16%
Gestion de la surface d'attaque publique (EASM)	***51%***	21%	23%	7%	38%	11%
Système de contrôle d'accès au réseau (NAC)	***50%***	27%	18%	5%	33%	17%
Sonde réseau / sandbox	***48%***	17%	22%	9%	44%	8%
Gestion des assets et de la surface d'attaque (CAASM)	***44%***	15%	20%	9%	46%	10%
Système de détection et réponse pour réseaux (NDR : Network Detection & Response)	***42%***	19%	17%	6%	43%	15%
Système de protection contre la fuite de données (DLP)	***41%***	15%	17%	9%	33%	26%
Cloud Security Posture Management (CSPM)	***39%***	20%	13%	6%	45%	16%
Système de classification de données, DRM	***39%***	10%	16%	13%	41%	20%
Système d'anonymisation de données	***35%***	8%	17%	10%	53%	12%
Cloud Access Security Broker (CASB)	***32%***	12%	15%	5%	54%	14%
Services de Bug Bounty	***31%***	14%	12%	5%	57%	12%
Solution de tests d'intrusion automatisés	***30%***	11%	14%	5%	53%	17%
Système de honeypots	***27%***	6%	11%	10%	63%	10%
Systèmes de tests et de validation de la sécurité (BAS)	***25%***	9%	13%	3%	64%	11%
Système de contrôle de la posture Saas (SSPM)	***21%***	7%	11%	3%	65%	14%
Système de contrôle de la posture sécurité des données (DSPM)	***18%***	5%	9%	4%	68%	14%
Secure Enterprise Browsers (SEB)	***17%***	5%	9%	3%	71%	12%
Sondes industrielles	***15%***	6%	6%	3%	73%	12%

Si le mode de gestion varie selon les solutions, les tests d'intrusions, threat intelligence, SOC et CERT/CSIRT sont surtout gérés en externe.

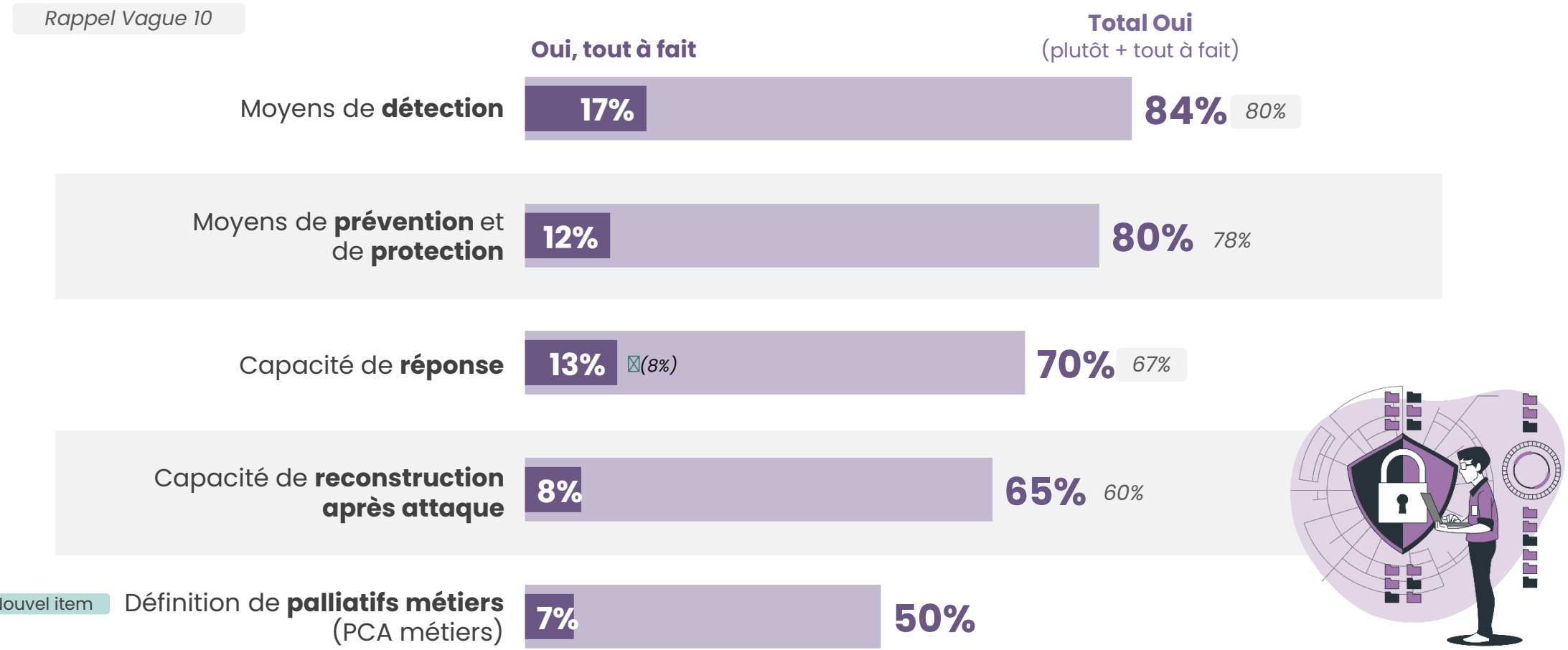
Q30b : **Comment opérez-vous les solutions et services de cybersécurité** ci-dessous ? *Base : ensemble (397)*



Comme lors de la mesure précédente, les entreprises se disent davantage prêtes à gérer les cyberattaques en amont qu'en aval. Pour autant, la définition de palliatifs métiers, nouvellement évaluée cette année, est bien moins développée.

Q14 : Selon vous, votre entreprise est-elle **préparée à gérer une cyberattaque de grande ampleur** en termes de… ?

Base : ensemble (397)



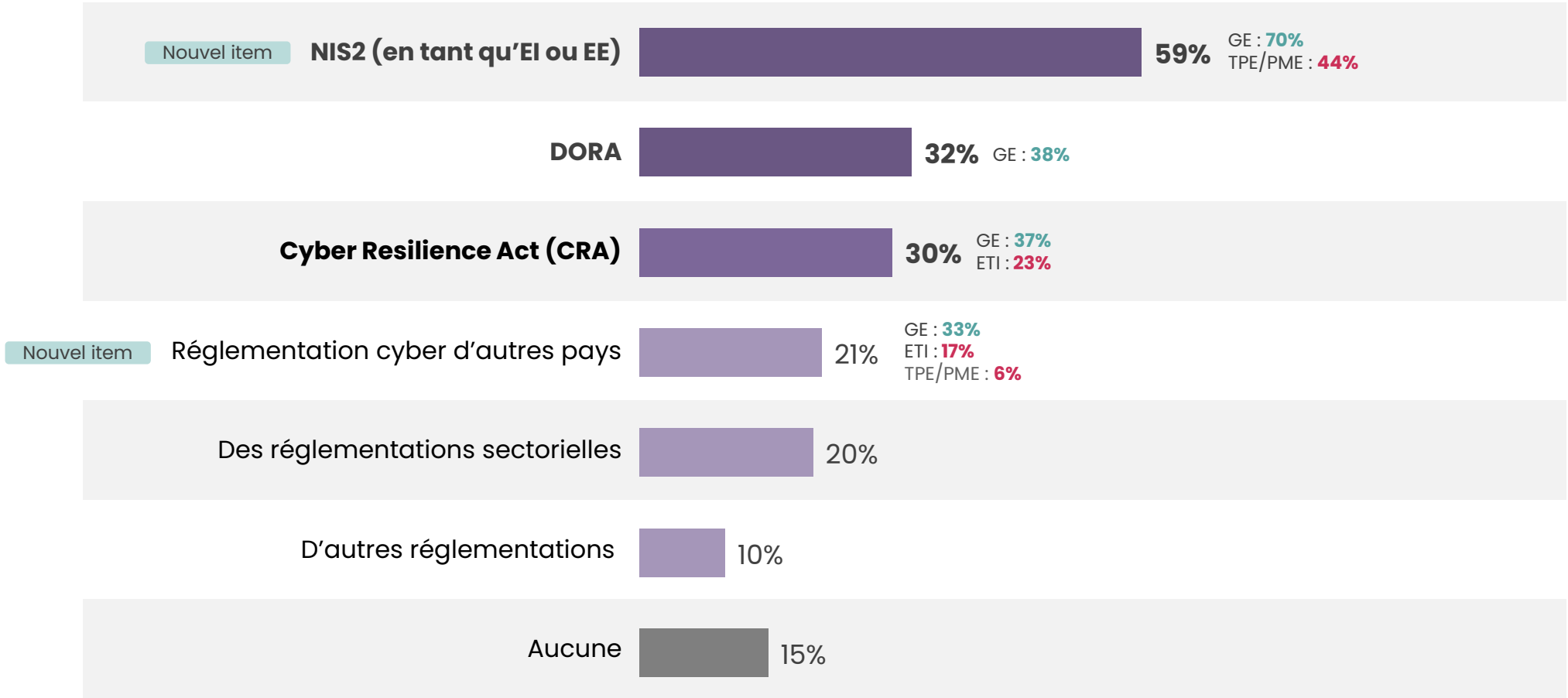
Crédits : Icone de Storyset.com

Sans surprise, la réglementation NIS2 est la plus répandue, arrivant en tête devant DORA et le CRA.

Question modifiée en 2025

Q47 : Par lesquelle(s) de ces **réglementation(s) cyber** votre société est-elle impactée ?

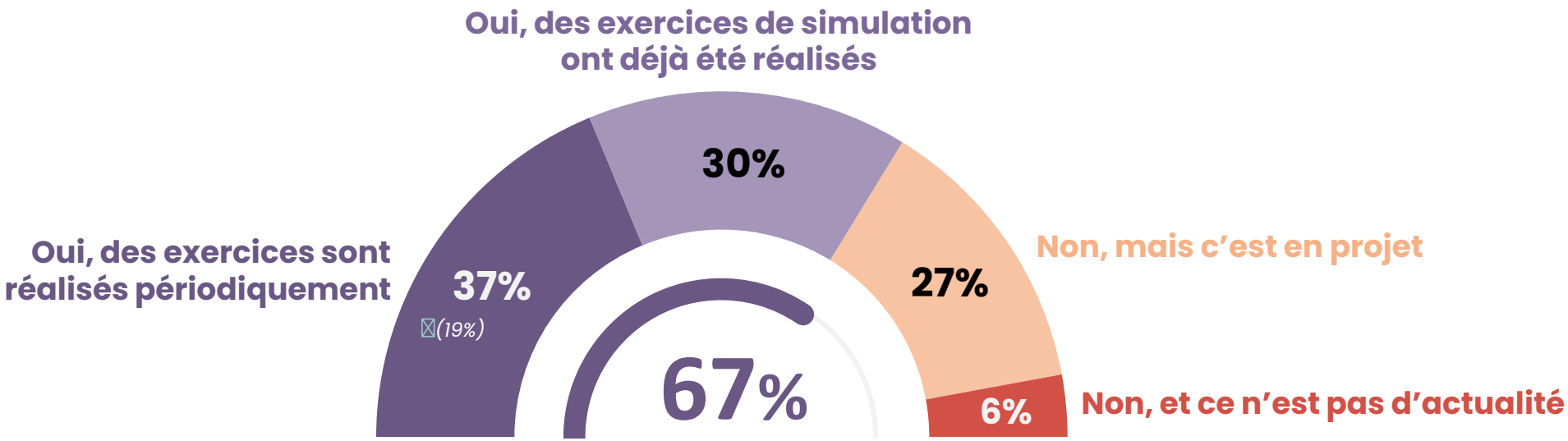
Base : ensemble (397) – Plusieurs réponses possibles



Deux tiers des entreprises ont mis en place un programme d'entraînement à la crise cyber, elles sont plus nombreuses à avoir mis en place des exercices périodiques.

Q15 : Votre entreprise a-t-elle mis en place **un programme d'entraînement à la gestion de crise cyber** ?

Base : ensemble (397)



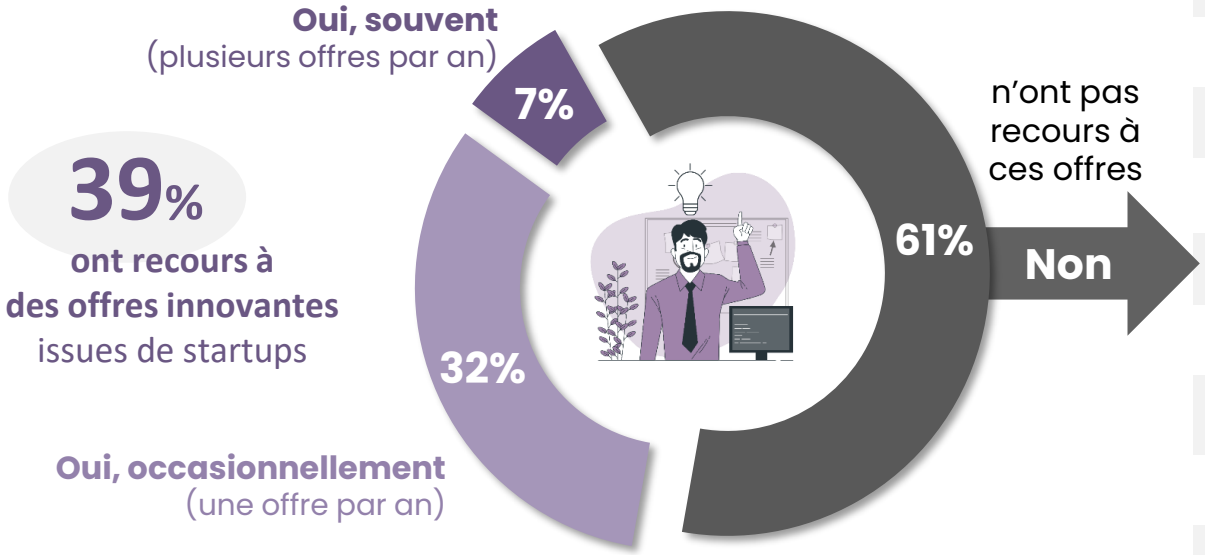
ONT MIS EN PLACE UN PROGRAMME D'ENTRAÎNEMENT À LA CRISE CYBER

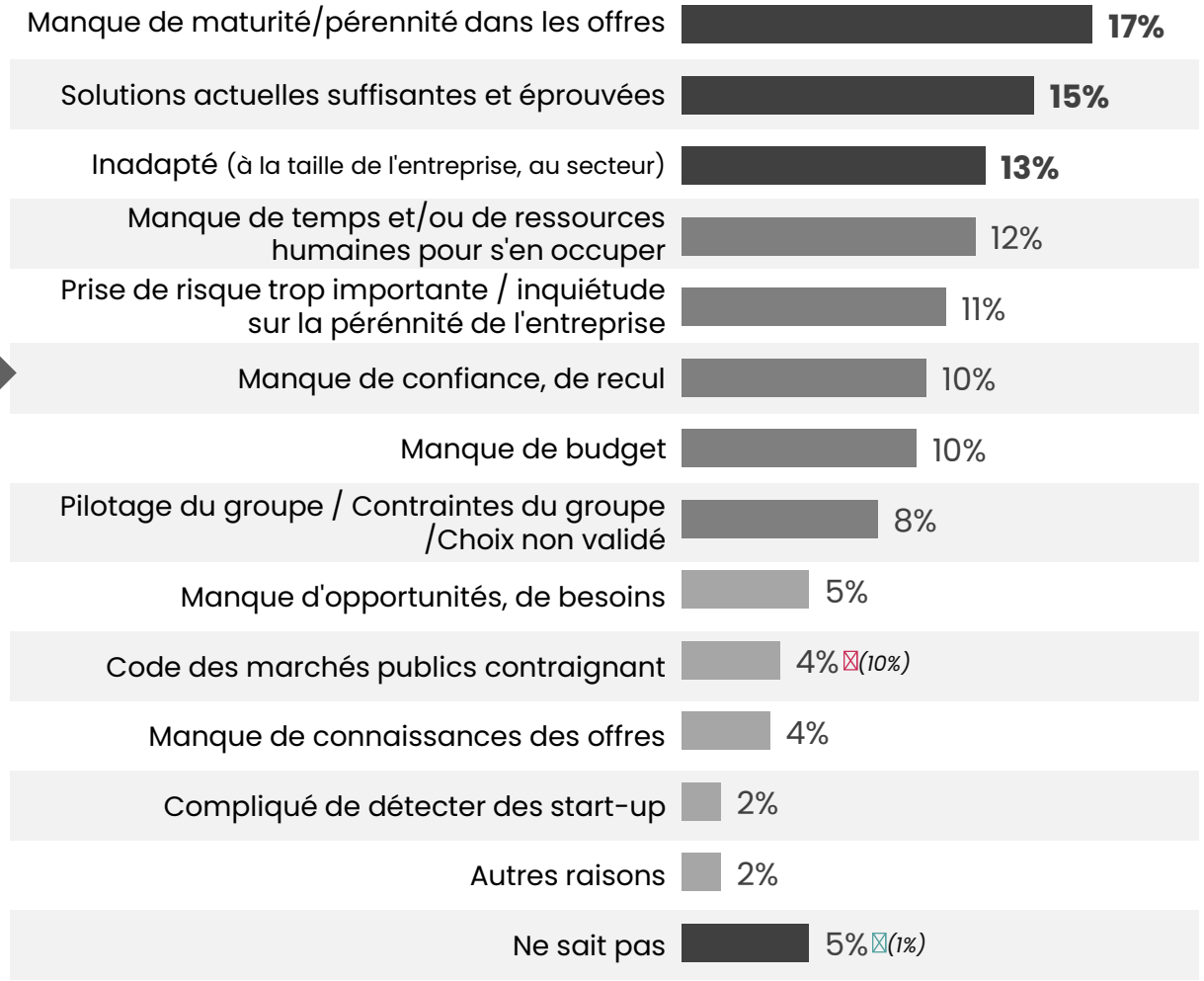
Rappel Vague 10 : 62%

Crédits : Icone de Storyset.com

4 entreprises sur 10 ont recours à des offres innovantes issues de start-ups. Pour celles ne le faisant pas, c'est le plus souvent dû à un manque de maturité de l'offre ou à une satisfaction des solutions actuelles.

Q26 : En matière de cybersécurité, recourrez-vous à **des offres innovantes issues de start-up** ? *Base : ensemble (397)*
Q26b : Pour quelle(s) raison(s) ne le faites-vous pas ? *Base : ne font pas appel à des offres issues de start-up – hors non-répondant (242)*





La majorité des entreprises pense avoir une vision complète et à jour de ses actifs numériques.

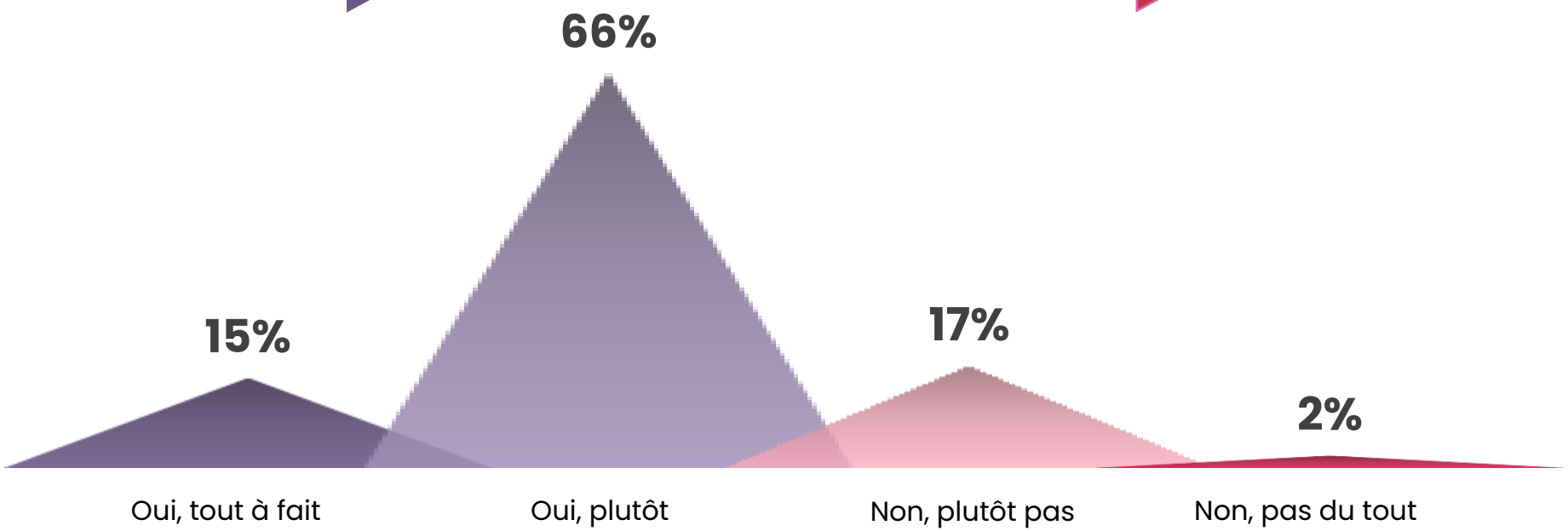
Question modifiée en 2025

Q41 : Avez-vous **une vision complète et à jour de vos actifs numériques** (applications, infrastructure, endpoints, réseaux, etc.) ?

Base : ensemble (397)

81% **ont une vision complète et à jour** de leurs actifs numériques

N'ont pas une vision complète et à jour de leurs actifs numériques **19%**

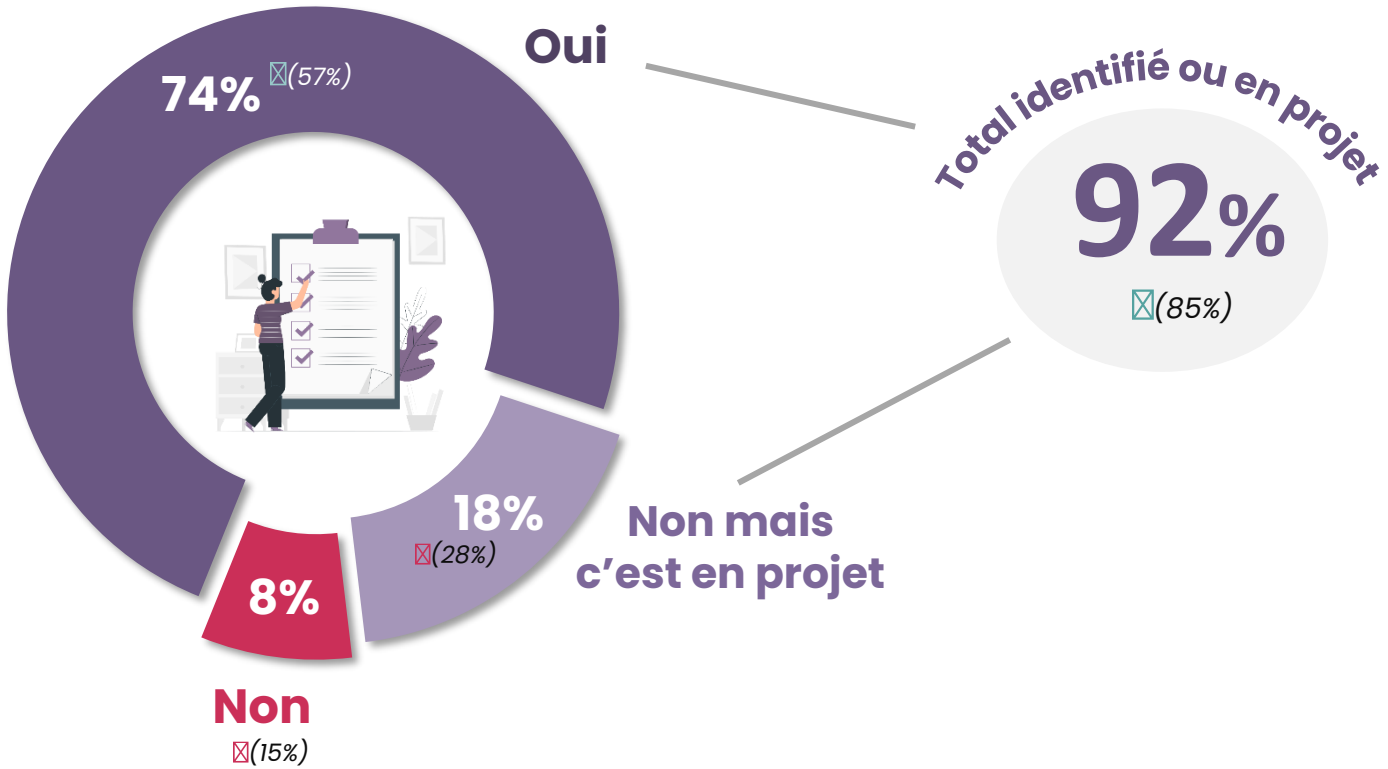


Depuis l’an dernier, le nombre d’entreprises ayant identifié ses actifs numériques a très largement augmenté.

Question modifiée en 2025

Q42 : Avez-vous **clairement identifié vos actifs numériques critiques** (« crown jewels ») ?

Base : ensemble (397)



Attention à l’interprétation car on parlait jusqu’à présent d’identification des « assets » donc le changement de formulation peut induire un biais.

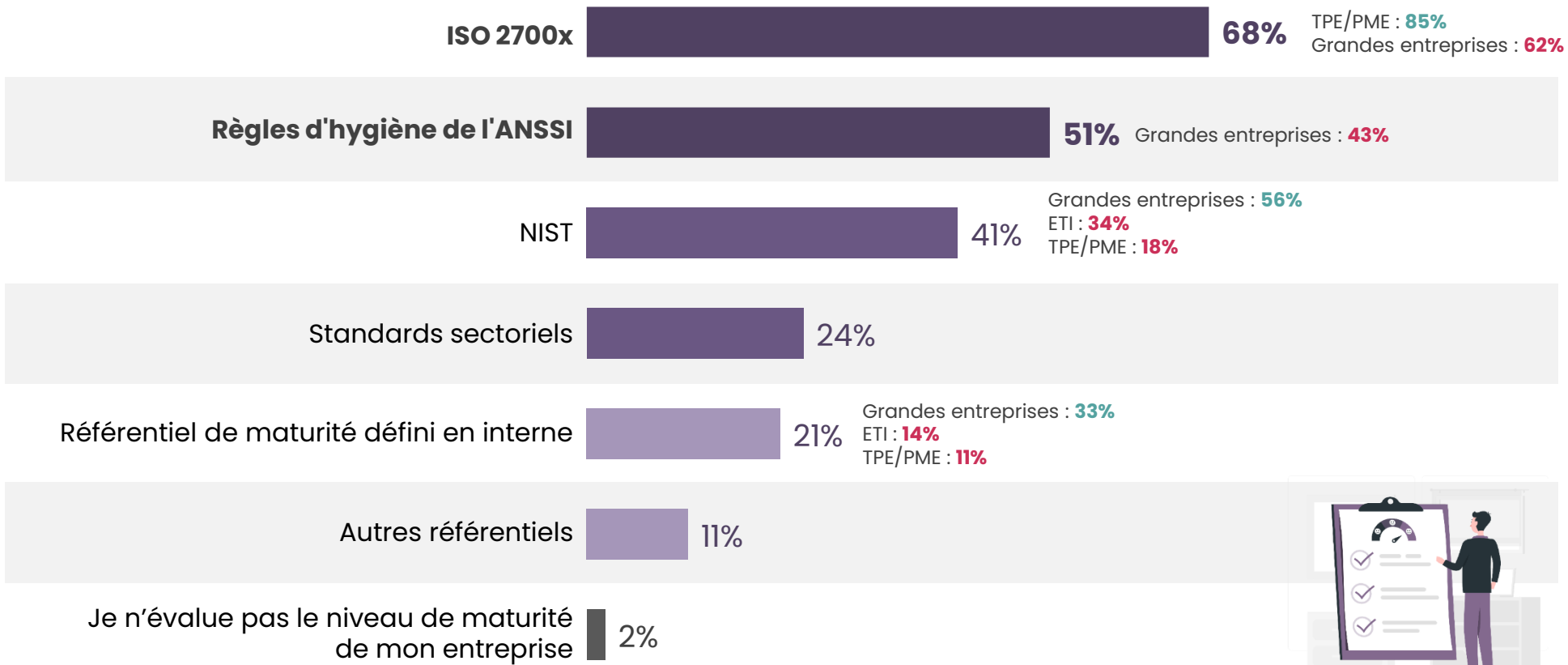
Crédits : Icone de Storyset.com

La quasi-totalité des entreprises évaluent leur niveau de maturité, le plus souvent via la norme ISO 2700x. Les grandes entreprises, qui consultent plus de référentiels, s'appuient notamment sur le NIST ou des référentiels définis en interne.

Nouvelle question en 2025

Q54 : Selon quel(s) référentiel(s) évaluez-vous **le niveau de maturité** de votre entreprise ?

Base : ensemble (397) – Plusieurs réponses possibles



Nombre moyen de réponses citées : **2,2**

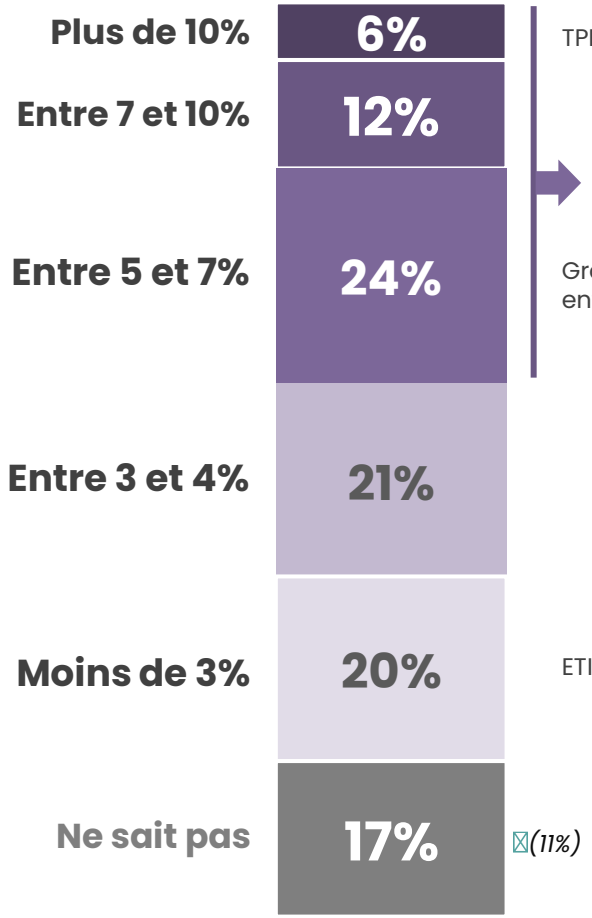
Grandes entreprises : **2,3**

Crédits : Icone de Storyset.com

Pour la première fois depuis trois ans, on observe une tendance baissière des entreprises consacrant 5% ou plus de leur budget IT/digital à la cybersécurité.

Q18 : Dans votre entreprise, **quelle part du budget IT/numérique est consacrée à la sécurité** ?

Base : ensemble (397)



TPE/PME : **13%**

5% ou plus du budget IT/digital est consacrée à la sécurité :

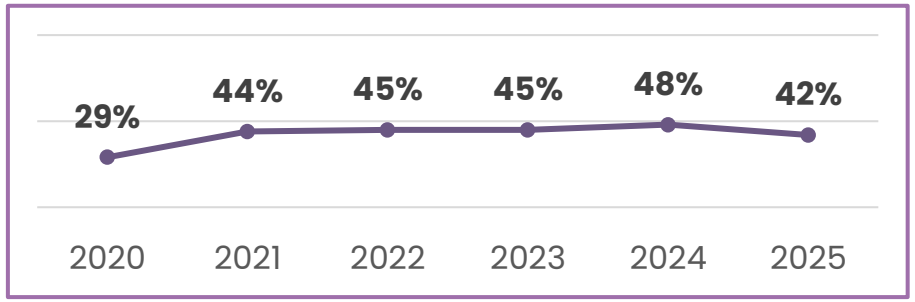
Grandes entreprises : **31%**

ETI : **25%**

Rappel Vague 10 : 48%

42%

Rappel vagues précédentes



03

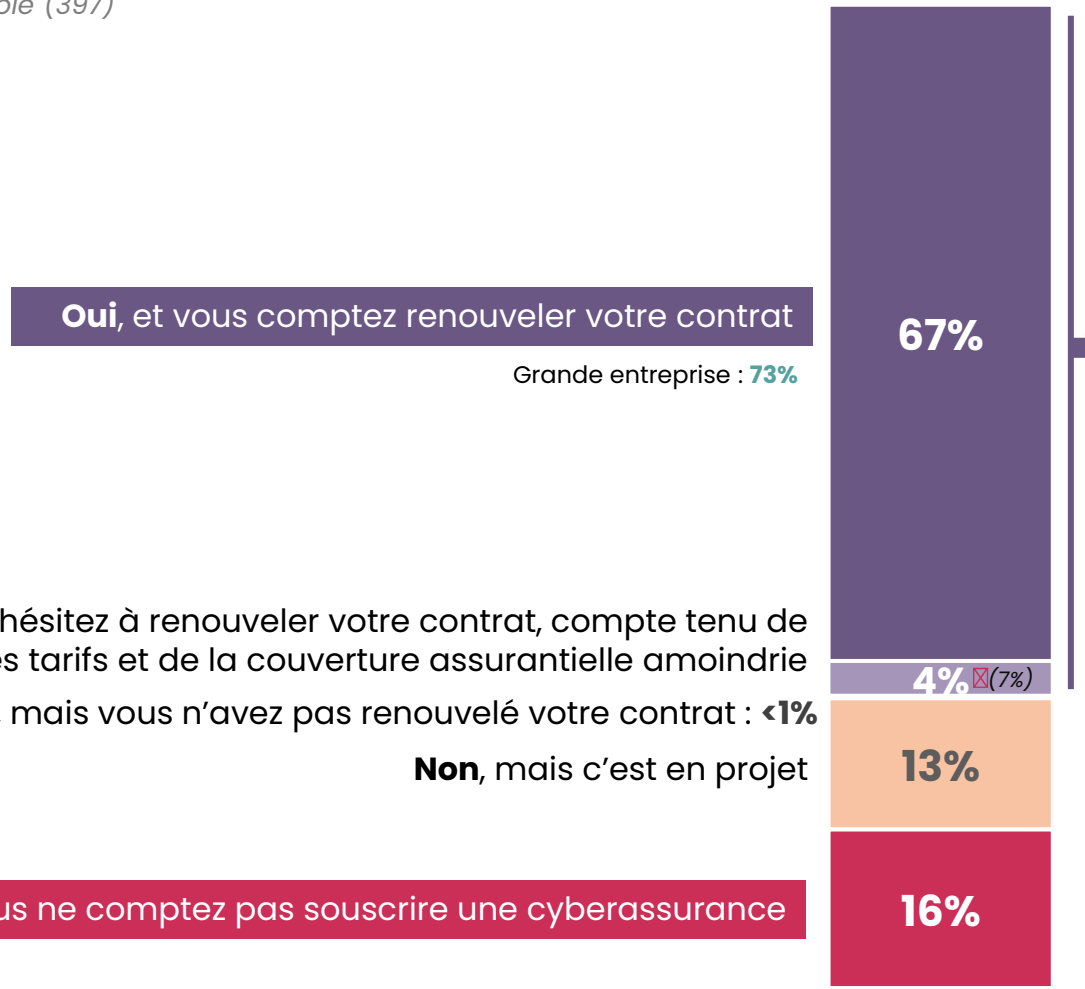
Focus sur …

La cyberassurance

7 entreprises sur 10 ont souscrit une cyberassurance, et la quasi-totalité d'entre elles prévoit de renouveler son contrat.

Q31 : Avez-vous **souscrit une cyber-assurance** ?

Base : ensemble (397)



71%

Grande entreprise : 78%

Rappel Vague 10 : 72%

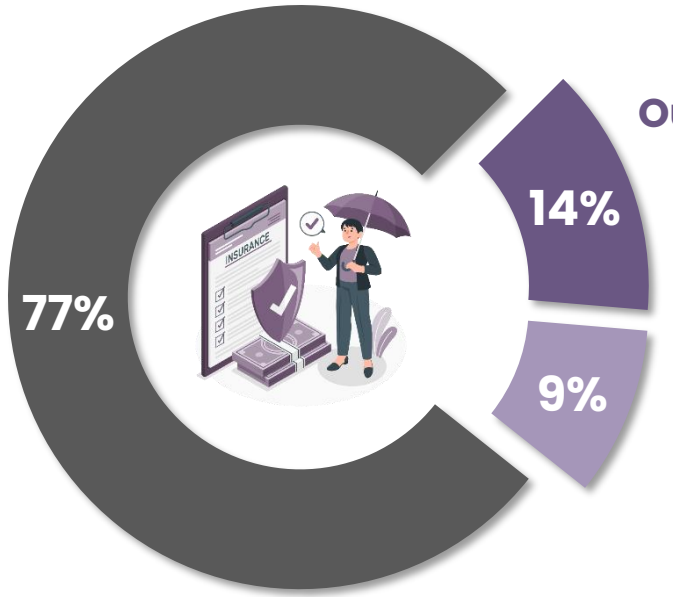
Ont souscrit une cyberassurance

Crédits : Icone de Storyset.com

Et comme en 2025, près d'1 entreprise sur 4 possédant une cyberassurance a fait appel à elle.

Q32 : Votre entreprise a-t-elle **déjà fait appel à sa cyber-assurance** dans le cadre d'une cyberattaque ?
Base : possèdent une cyberassurance (280)

Utilisation de la cyberassurance



Non 77%

14% **Oui, et cela s'est bien passé**
Grande entreprise : **19%**

9% **Oui, mais ça a été compliqué**

Total oui

23%

Rappel Vague 10 : 23%

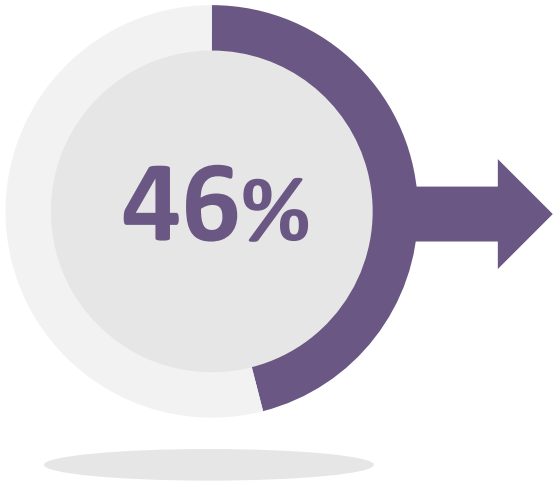
Grande entreprise : **32%**

Crédits : Icone de Storyset.com

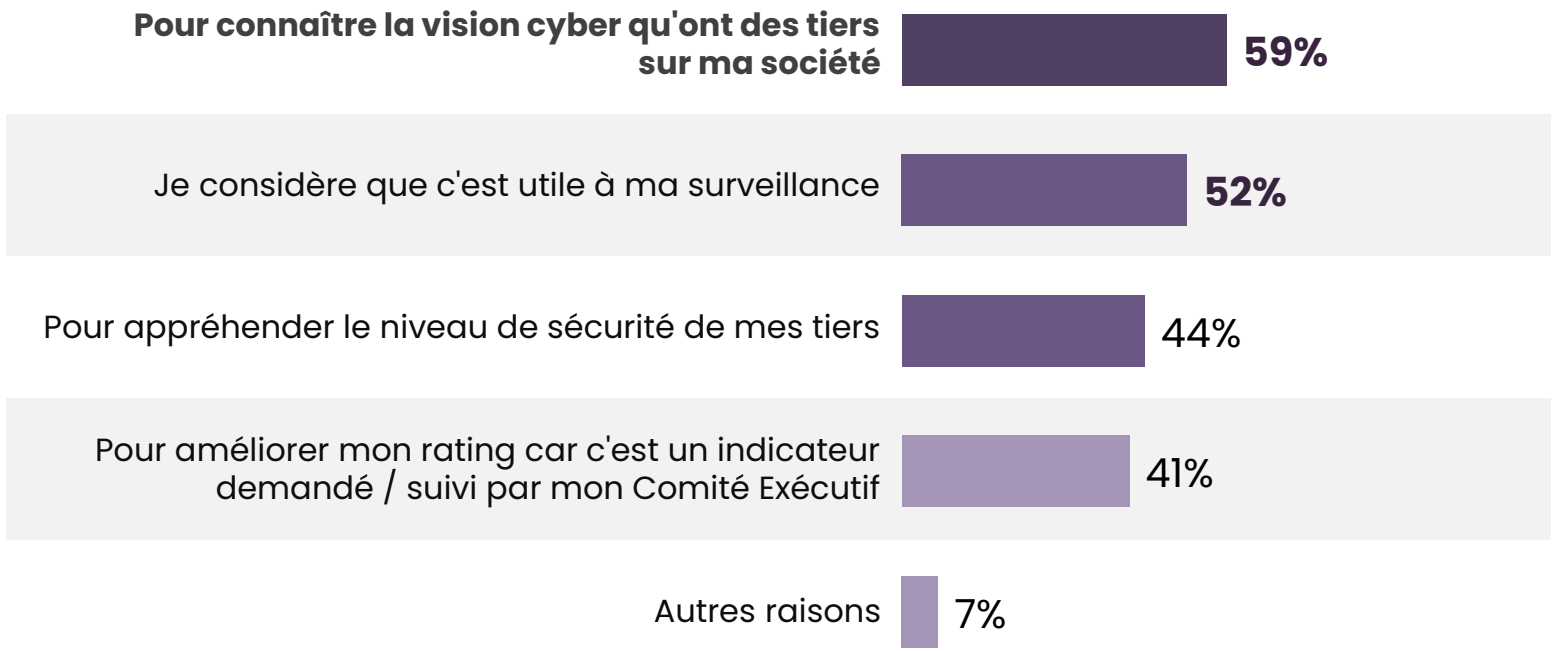
Le cyber-rating devient un outil incontournable, avec près de la moitié des entreprises utilisant ce service. Le plus souvent, l'objectif est de connaître la vision cyber qu'ont des tiers à leur sujet, mais également car cela est utile à leur surveillance.

Q33b : Si vous utilisez **un service de cyber-rating**, quelle en est la raison ?

Base : Utilisent un service de cyber-rating (181) – Plusieurs réponses possibles



Utilisent un service de cyber-rating



54% n'ont pas de contrat de cyber-rating

Les raisons de la méfiance des entreprises non équipées de services de cyber-rating diminuent cette année, démontrant une confiance en progression.

Q33bis : Pour quelle(s) raison(s) n'avez-vous pas de services de cyber-rating ?

Base : n'ont pas de contrat de cyber-rating (216) – Plusieurs réponses possibles

N'ont pas de contrat de cyber-rating

	Parce que ces plateformes **ne font par construction qu'une analyse très partielle du niveau de sécurité** et fournissent un score par extrapolation	**41%** ⊠(68%)
	Parce que les critères et le mode de **calcul des scores sont contestables** du point de vue des priorités définies	**36%** ⊠(63%)
	Parce que **les résultats ne sont pas fiables** dans l'identification et l'assignation des assets	28% ⊠(53%)
	Parce que ces services constituent une forme de vente forcée de solution	27% ⊠(38%)
	Parce qu'il y a trop d'opacité et d'instabilité dans les calculs de scores	26% ⊠(55%)
Nouvel item issu du poste ***Autre raison***	Parce que les coûts sont trop élevés/pas de budget alloué	6%
Nouvel item issu du poste ***Autre raison***	Parce que nous n'avons pas considéré cette éventualité	4%
Nouvel item issu du poste ***Autre raison***	Parce que ce n'est pas une priorité pour nous	2%
Nouvel item issu du poste ***Autre raison***	C'est en projet	2%
	Autre raison	16% ⊠(3%)

Comme l’an dernier, plus de la moitié des entreprises victimes de cyberattaque ont porté plainte. Cependant, seulement 1/3 l’a fait lors de toutes les attaques.

Q8 : **Avez-vous porté plainte** à la suite de la cyberattaque / des cyberattaques dont votre entreprise a été victime ?

Base : ont constaté une attaque (159)

Rappel : **40%** des entreprises ont subi au moins une cyberattaque en 2024

N’ont pas porté plainte **42%**

58% **Ont porté plainte**

Rappel Vague 10 : 62%

Grande entreprise : **68%**

pour **toutes les attaques** : **35%**

pour **certaines attaques** : **23%**

Crédits : Icone de Storyset.com

04

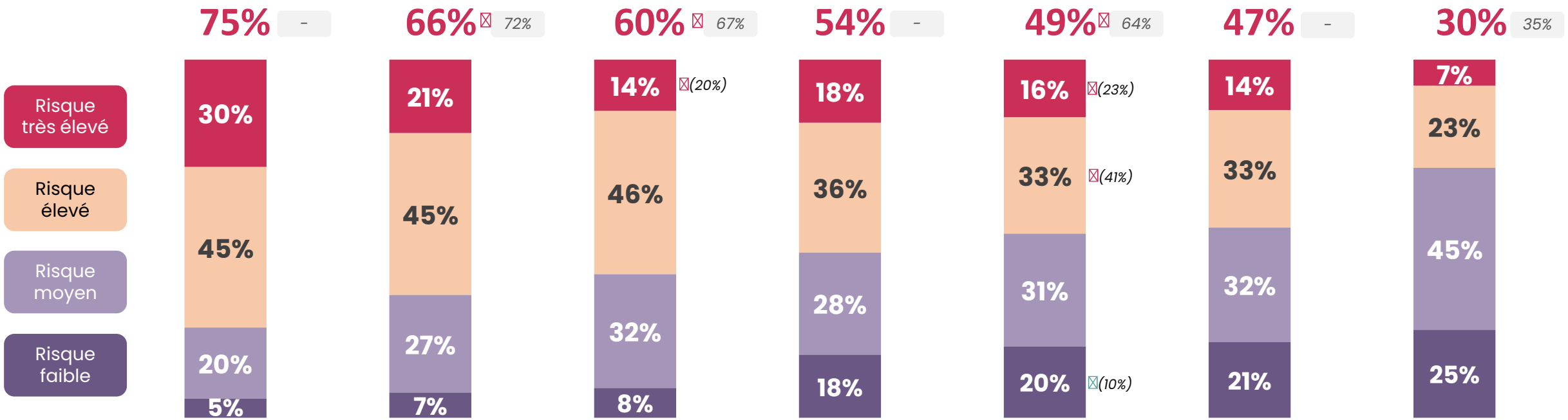
De nouveaux risques voient le jour en lien avec l’évolution des habitudes de travail des salariés

Cette année, le recours à des IA non approuvées par les salariés est devenu le comportement jugé le plus risqué.

Q23 : Comment évaluez-vous **le niveau de risque induit par les usages suivants** du numérique par les salariés ?

Base : ensemble (397)

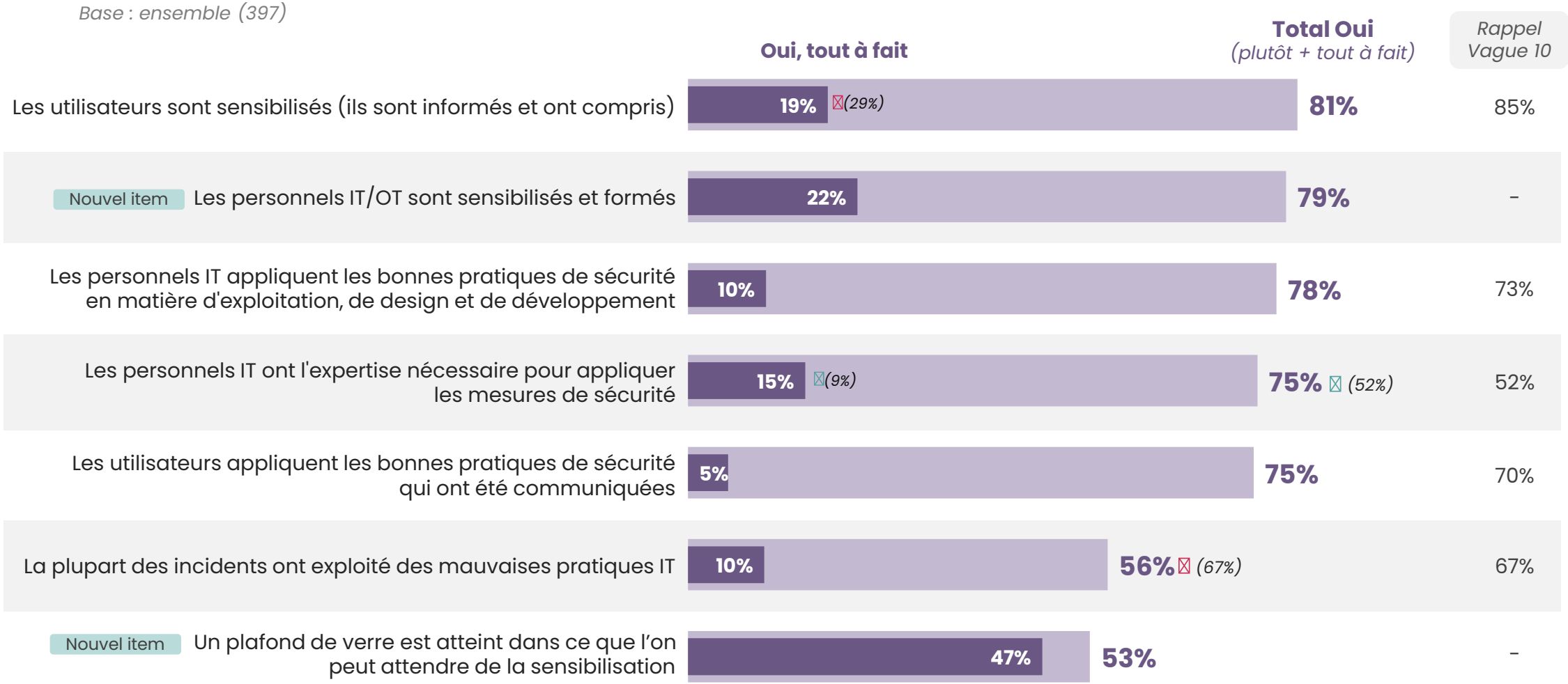
Rappel Vague 10



Concernant la sensibilisation et la formation, la moitié des entreprises estiment qu'un plafond de verre est atteint, et la plupart d'entre elles y sont tout à fait convaincues. Globalement, les utilisateurs et les personnels IT/OT sont bien sensibilisés selon 4 entreprises sur 5.

Q19 : En ce qui concerne **la sensibilisation et la formation à la cybersécurité**, pensez-vous que … ?

Base : ensemble (397)



05

Focus sur …

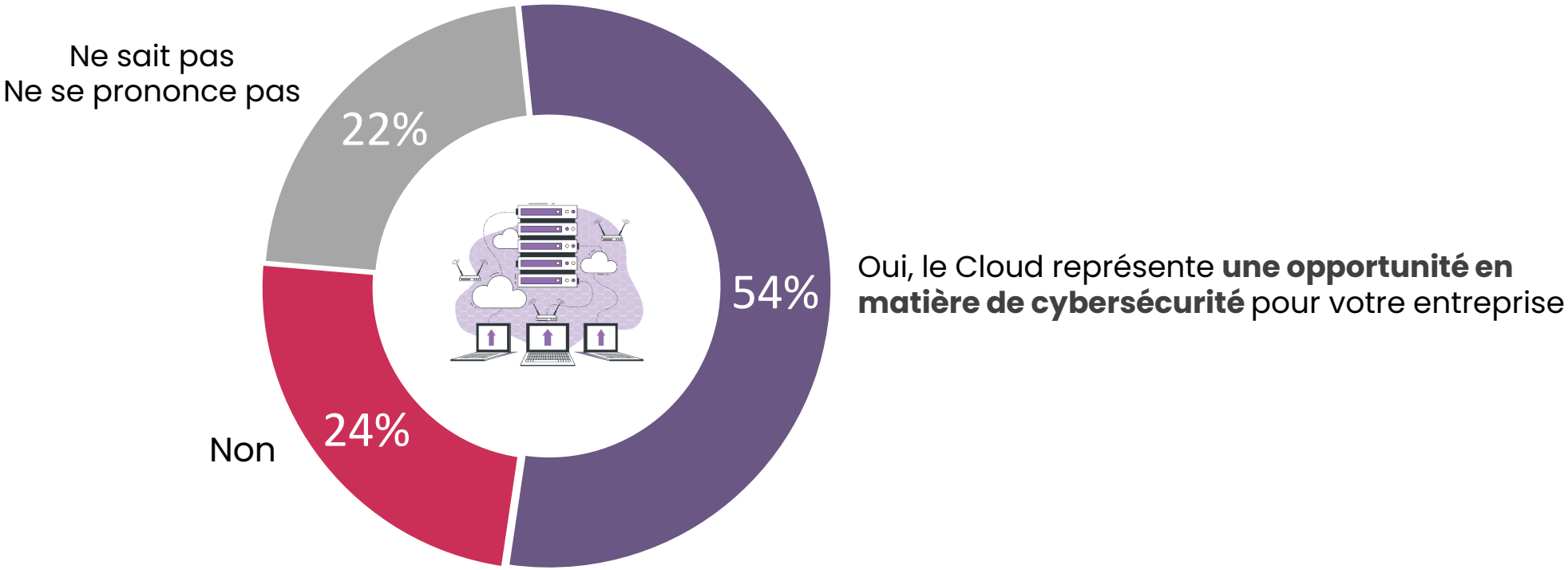
Le Cloud

Bien qu'un quart des entreprises ne se prononcent pas ou ne savent pas quoi en penser, le Cloud est tout de même identifié comme une opportunité en matière de cybersécurité par plus de la moitié.

Nouvelle question en 2025

Q57 : Selon vous, le Cloud représente-t-il **une opportunité en matière de cybersécurité** pour votre entreprise ?

Base : ensemble (397)

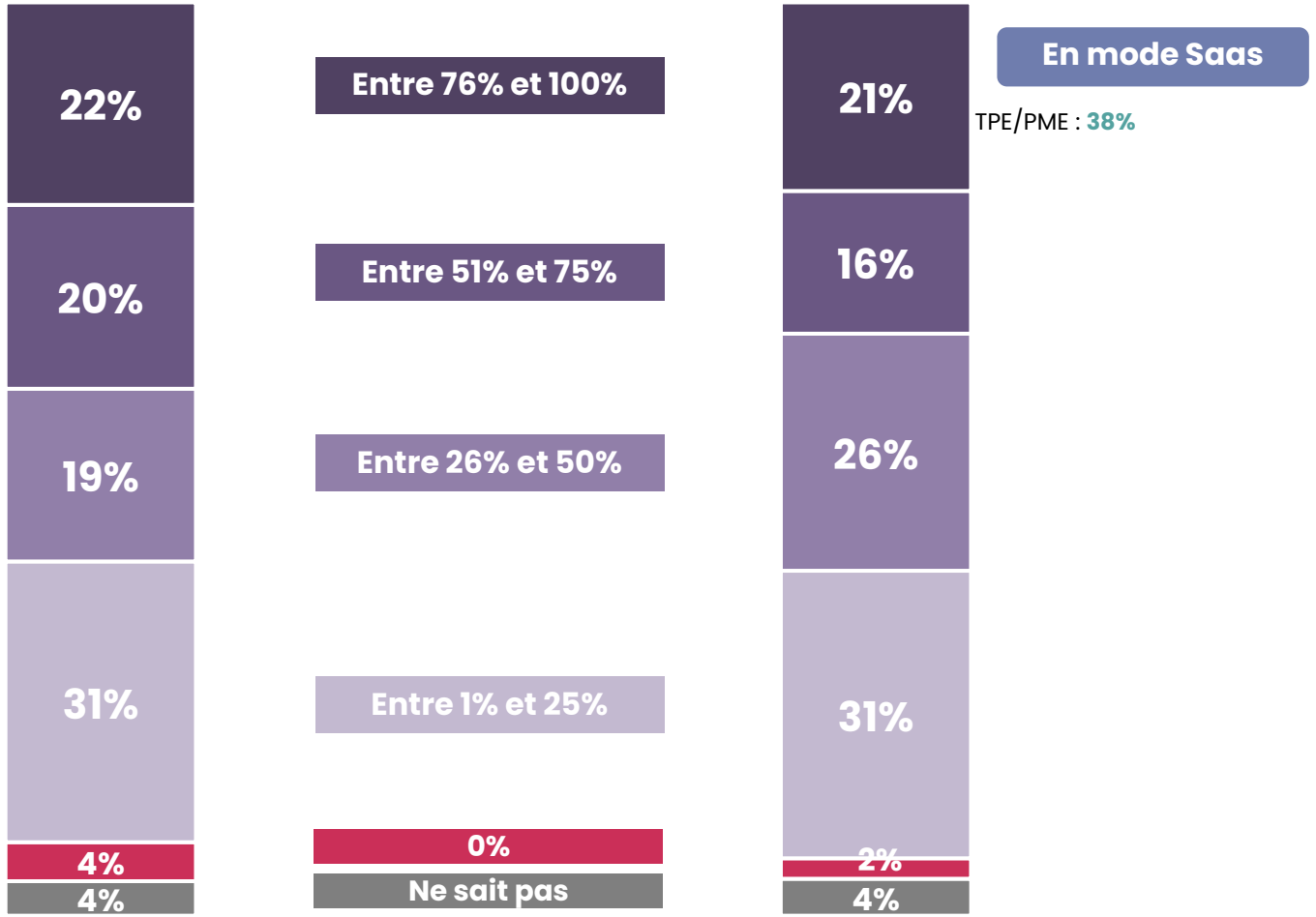


Crédits : Icone de Storyset.com

Comme lors de la dernière mesure, la part d'adoption du cloud entre les modes Iaas, Paas et Saas est plutôt similaire, bien que les TPE & PME semblent davantage adopter du cloud en Saas.

Q20b : Quelle est **la part d'adoption du Cloud dans votre SI**, que ce soit en mode IaaS, PaaS ou SaaS ?

Base : ensemble (397)



Crédits : Icone de Storyset.com

Concernant justement l'utilisation du Cloud, le fort risque de l'hébergement des données soumis à des lois extraterritoriales progresse cette année et est mentionné par 1 entreprise sur 2, de même que la rigidité de négociation des clauses contractuelles.

Q21 : Selon vous, les facteurs suivants représentent-ils **un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud** ?

Base : ensemble (397)

Rappel classement 2024	% Un risque fort	
	52%	**Clauses contractuelles très difficilement négociables** Nouvel item
↗(34%)	48%	**Hébergement des données soumis à des lois extraterritoriales y compris en France et en Europe**
1	44%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
↗(15%)	37%	Compromission d'une plateforme SaaS
	35%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur
2	34%	Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
	34%	Confidentialité des données vis-à-vis de l'hébergeur
	34%	Compétences insuffisantes dans mon entreprise sur la sécurité du Cloud Nouvel item
3	33%	Difficulté de contrôler les accès à ses données par les administrateurs de l'hébergeur
	32%	Non-maîtrise du niveau de sécurité de l'hébergeur
	29%	Risque systémique
	28%	Non-effacement des données par l'hébergeur durant ou en fin de contrat (normal ou anticipé) Nouvel item
	27%	Défaut de cloisonnement entre les différents clients de l'hébergeur
	24%	Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant d'un service SaaS
	23%	Forte fréquence des nouvelles versions mises en ligne avec des potentielles évolutions non contrôlées des principes ou paramètres de sécurité
	21%	Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé)
	21%	Traitement et exploitation des données par l'hébergeur, problème de propriété de la donnée

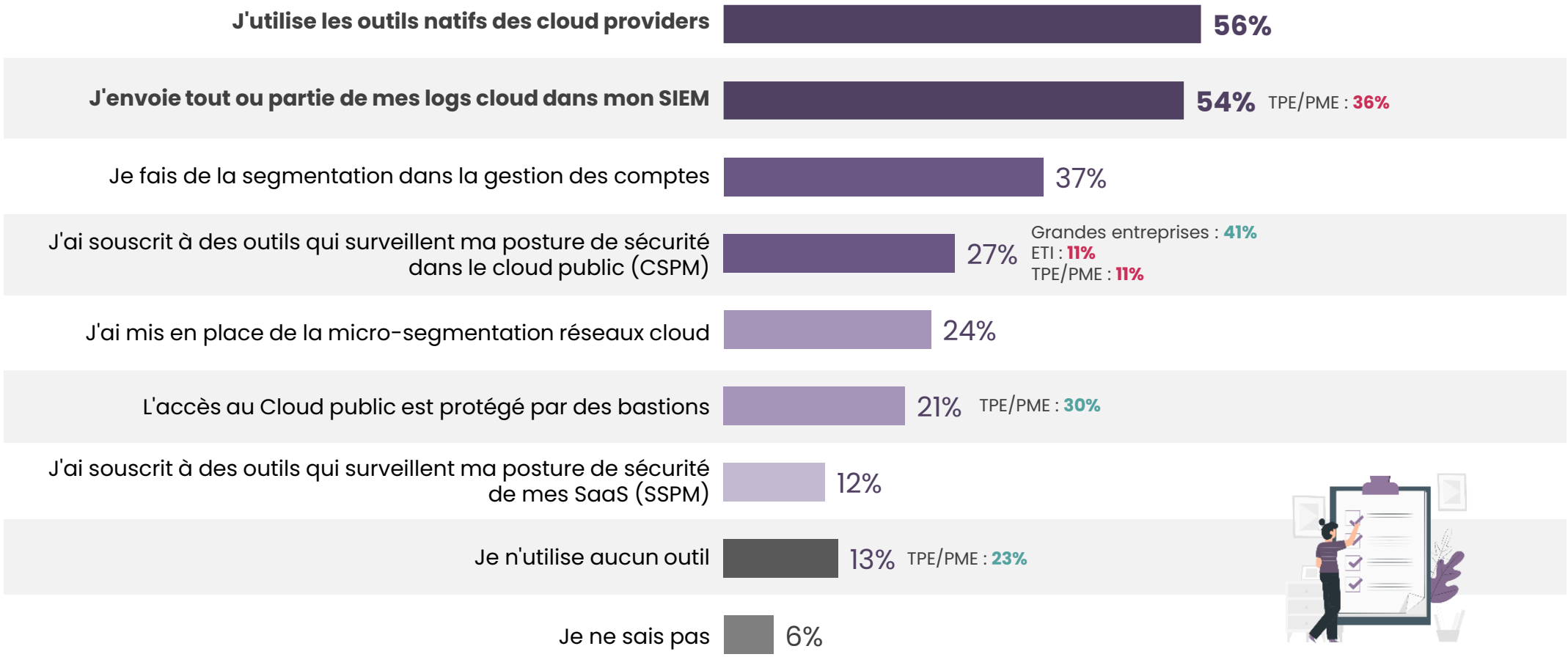
Crédits : Icone de Storyset.com

Pour sécuriser leur Cloud, les entreprises privilégient deux solutions : l'utilisation des outils natifs des cloud providers et l'envoi des logs dans le SIEM.

Nouvelle question en 2025

Q58 : Quels outils utilisez-vous **pour sécuriser votre Cloud** ?

Base : ensemble (397) – Plusieurs réponses possibles



Nombre moyen d'outils citées : **2,9**

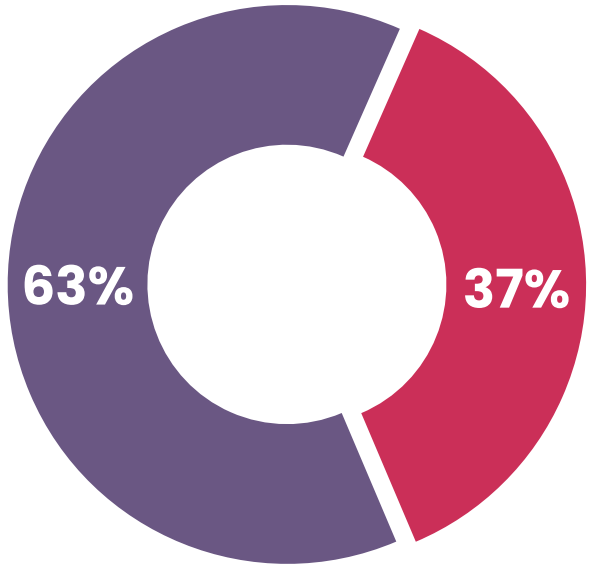
Crédits : Icone de Storyset.com

Près de 2 entreprises sur 3 se sentent concernées par les enjeux de souveraineté et de Cloud de confiance, un constat en augmentation de +11 points depuis l'an dernier.

Q35 : De nombreuses initiatives ont récemment vu le jour en matière de souveraineté et de Cloud de confiance. **Vous sentez-vous concerné par ces sujets** ?

Base : ensemble (397)

Souveraineté & Cloud de Confiance



Oui, c'est un sujet de préoccupation pour mon entreprise

(52%)

Non, mon entreprise ne se sent pas concernée par ces sujets

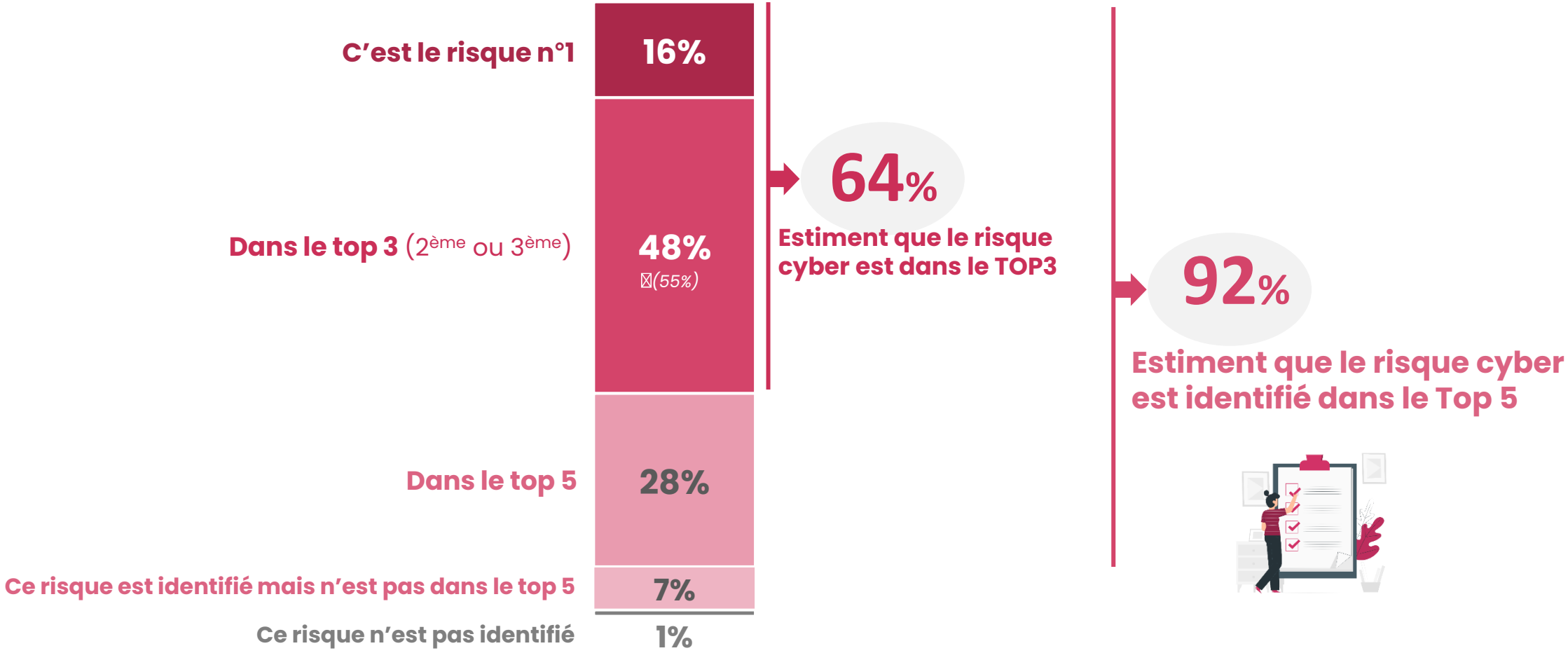
(48%)

06

Cybersécurité en entreprise : Une fonction stratégique en constante adaptation

Le risque cyber est identifié dans le TOP5 par les entreprises, pour près de 2/3, il est même identifié dans le TOP 3.

Q48 : **Comment le risque cyber est-il positionné dans la cartographie des risques** de votre entreprise ?
Base : ensemble (397)



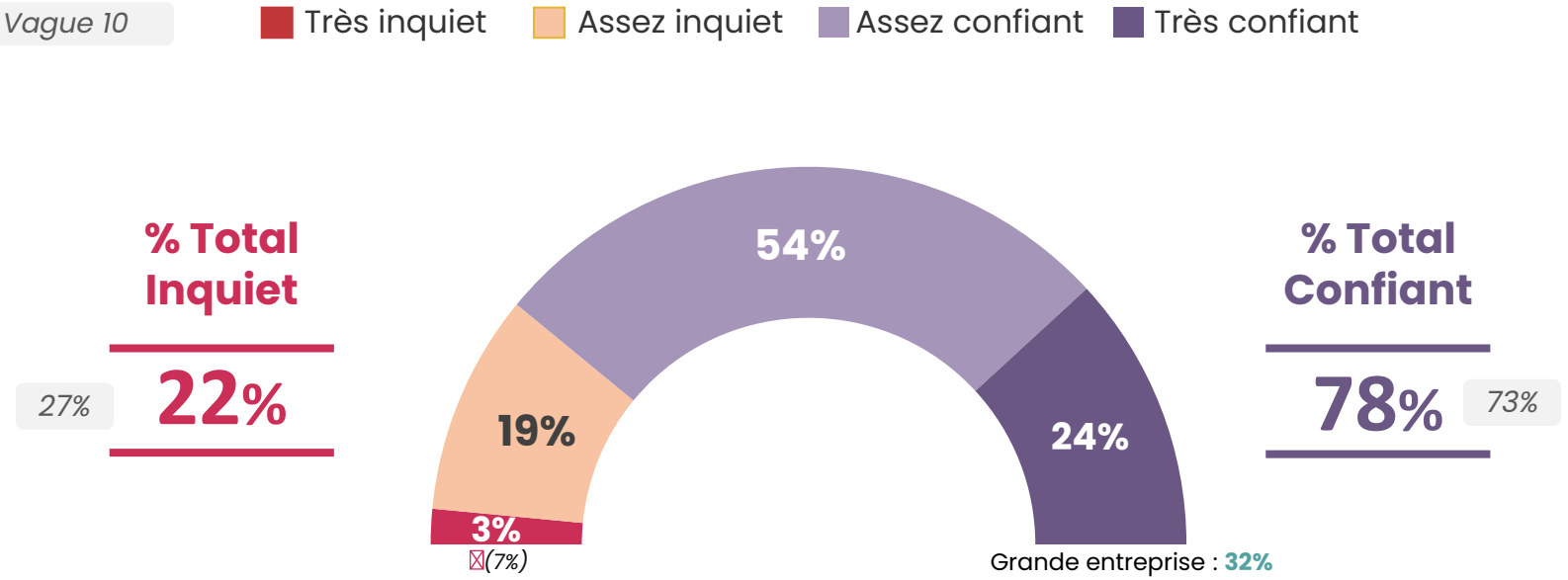
Crédits : Icone de Storyset.com

Alignée avec la vague précédente, la prise en compte de la cybersécurité au sein du COMEX n'est pas une inquiétude.

Q24 : Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (397)

La **prise en compte des enjeux** de la cybersécurité au sein du COMEX de votre entreprise

Rappel Vague 10

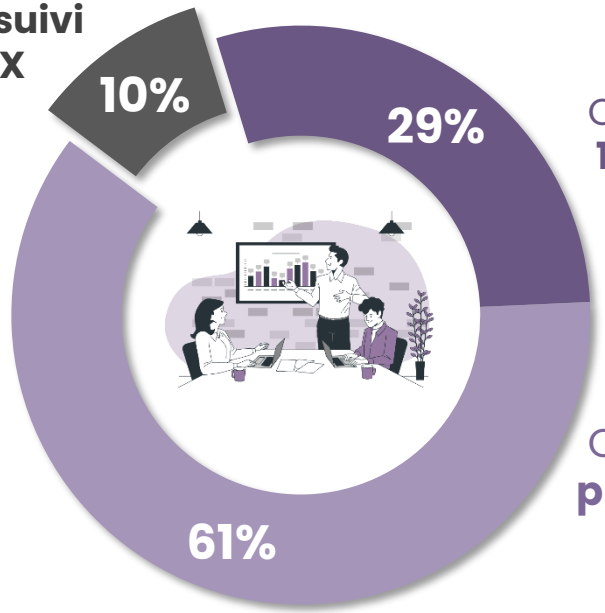


Pour cause, le suivi du risque cyber par les instances dirigeantes (COMEX/CODIR) est une pratique régulière et institutionnalisée

Nouvelle question en 2025

Q50 : Ce risque fait-il **l'objet d'un suivi régulier** en comité de direction (CODIR) ou en comité exécutif (COMEX) ?

Base : ensemble (397)



Crédits : Icone de Storyset.com

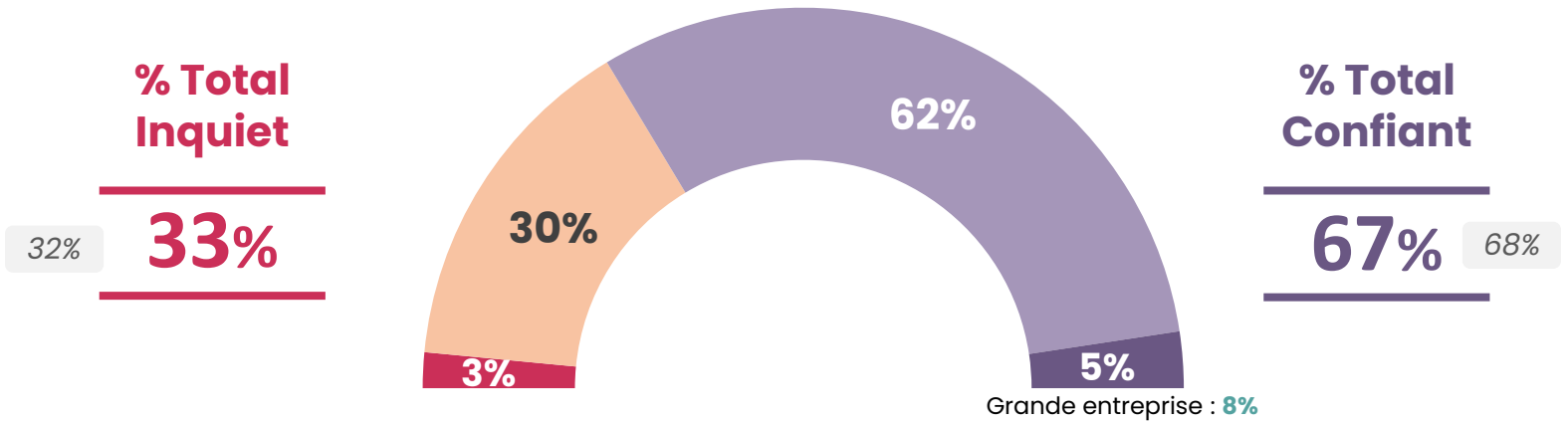
Bien que les entreprises se sentent capables de faire face aux cyber-risques, cette confiance est plus souvent modérée que totale.

Q24 : Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?

Base : ensemble (397)

La capacité de votre entreprise à faire face aux cyber-risques

Rappel Vague 10

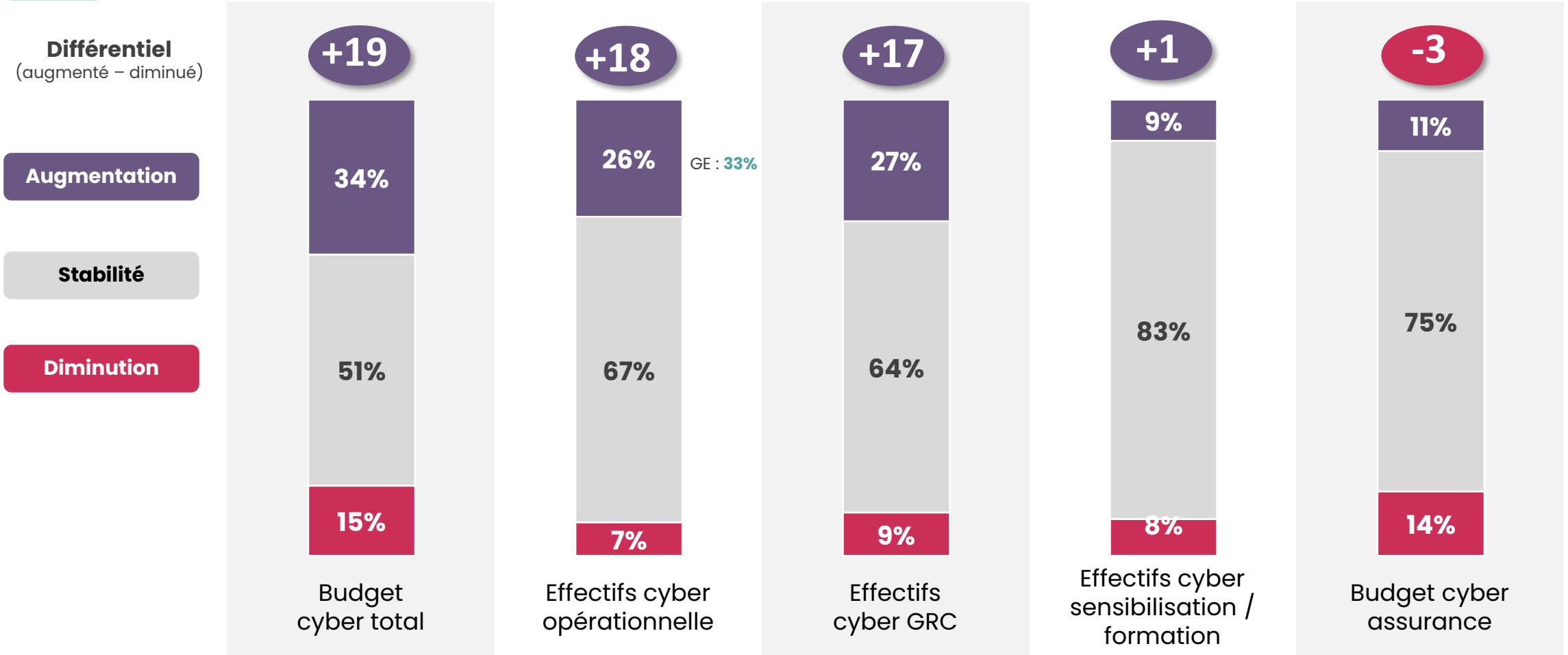


Les prévisions de ressources cyber pour 2026 montrent une priorisation du budget et des effectifs opérationnels et GRC, potentiellement au détriment de la cyberassurance.

Nouvelle question en 2025

Q55 : Au cours de 12 prochains mois, **comment vos ressources cyber vont-elles évoluer** ?

Base : ensemble (397)



Une dynamique positive puisque deux tiers des entreprises estiment ne pas disposer actuellement des ressources humaines et financières nécessaires pour répondre aux différents enjeux actuels.

Nouvelle question en 2025

Q56 : A votre avis, disposez-vous **des ressources humaines et financières suffisantes** pour répondre aux enjeux actuels ?

Base : ensemble (397)

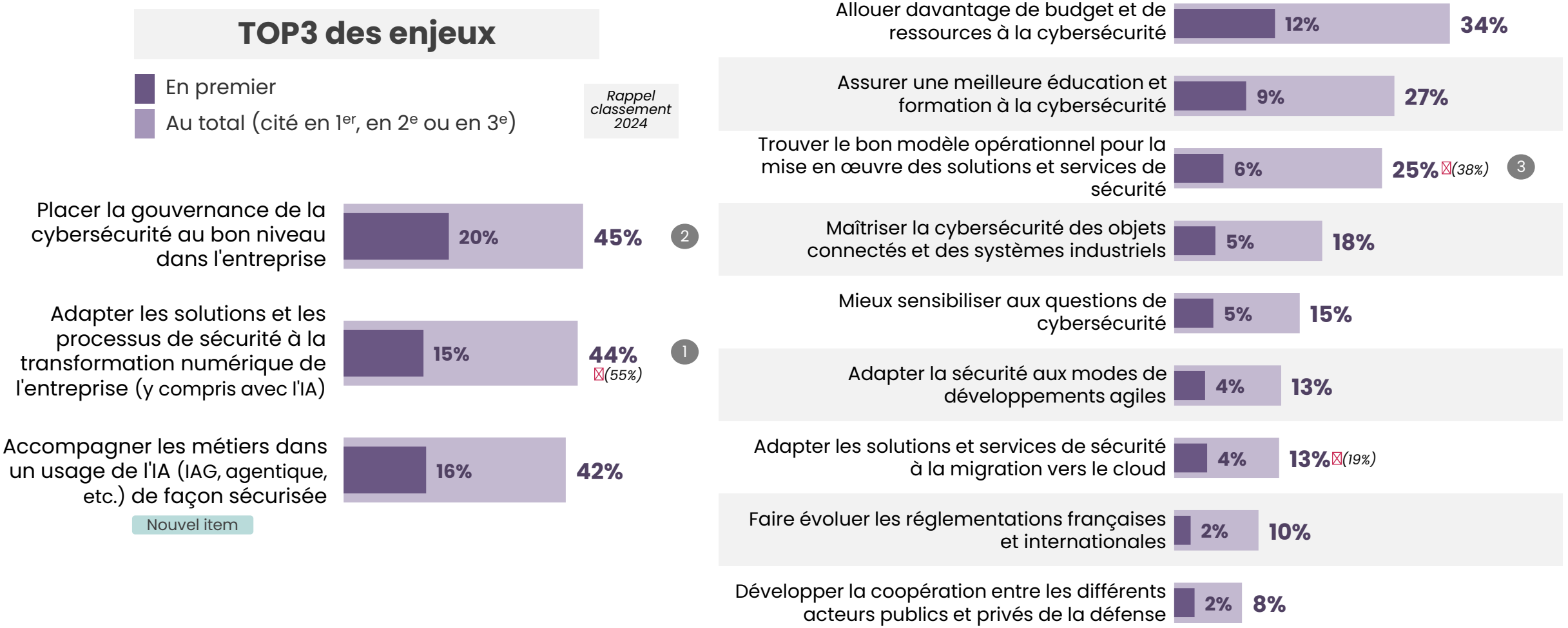
31% estiment disposer des ressources humaines et financières suffisantes pour répondre aux enjeux actuels

Crédits : Photo de Pavel Danilyuk sur Pexels.com

La place de la cybersécurité dans la gouvernance, l'adaptation des solutions en fonction des transformations numériques et l'accompagnement des métiers à l'usage de l'IA représentent les principaux enjeux cybers de demain identifiés par les entreprises.

Q27. Parmi les enjeux suivants, quels sont selon vous **les trois enjeux de demain pour l'avenir de la cybersécurité** des entreprises ?

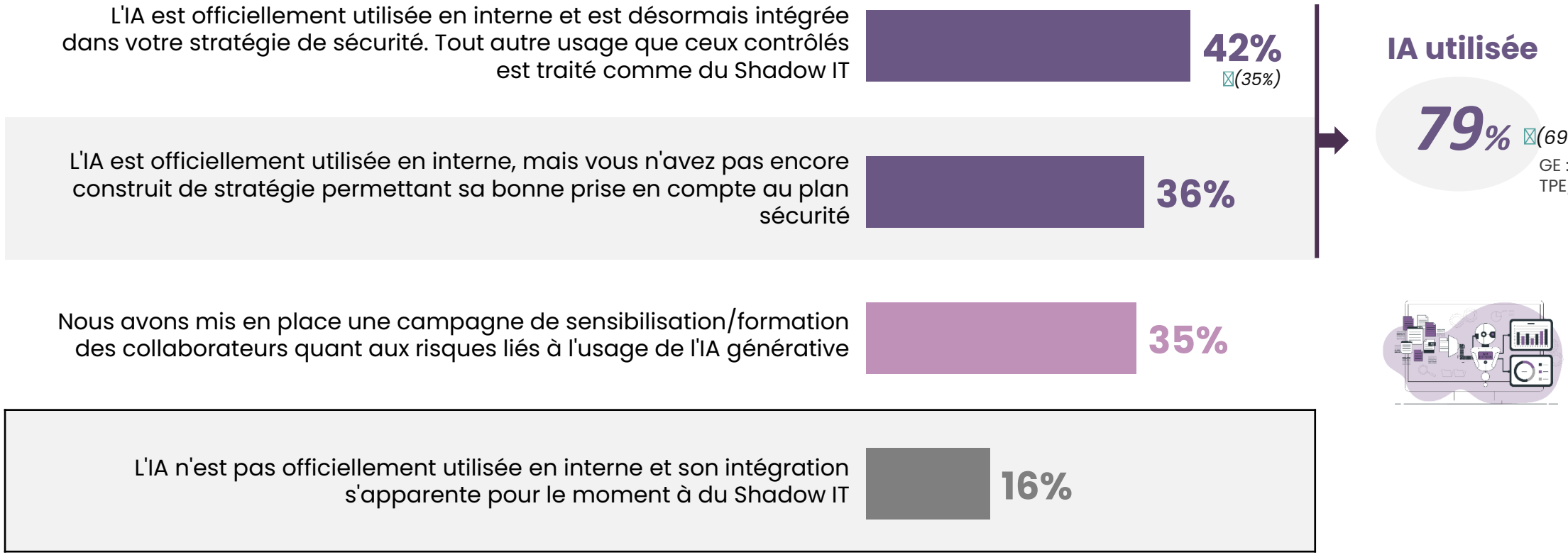
Base : ensemble (397) – Trois réponses possibles



L’intelligence artificielle est dorénavant très utilisée en interne.

Q39 : L’IA, déjà plus ou moins utilisée dans certaines solutions cyber, s’est imposée dans nos SI avec notamment un grand nombre d’initiatives autour de l’IA générative. **Quelle est la place de l’IA aujourd’hui dans votre organisation** ?

Base : ensemble (397) – Plusieurs réponses possibles



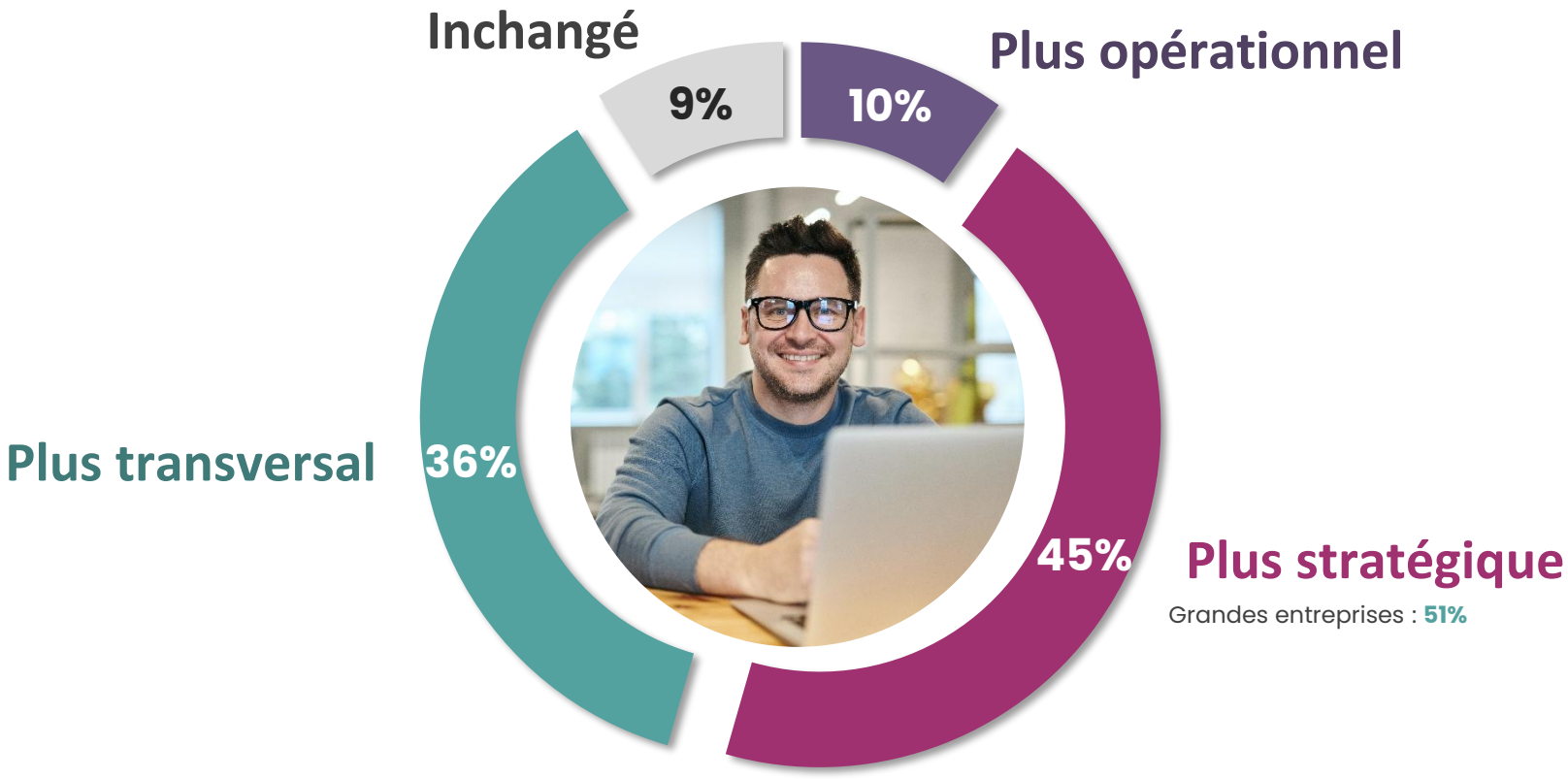
Crédits : Icone de Storyset.com

Le rôle des RSSI évolue significativement vers des fonctions plus transversales et stratégiques au sein des organisations.

Nouvelle question en 2025

Q59 : Comment avez-vous vu évoluer **votre rôle** ces dernières années ?

Base : ensemble (397)



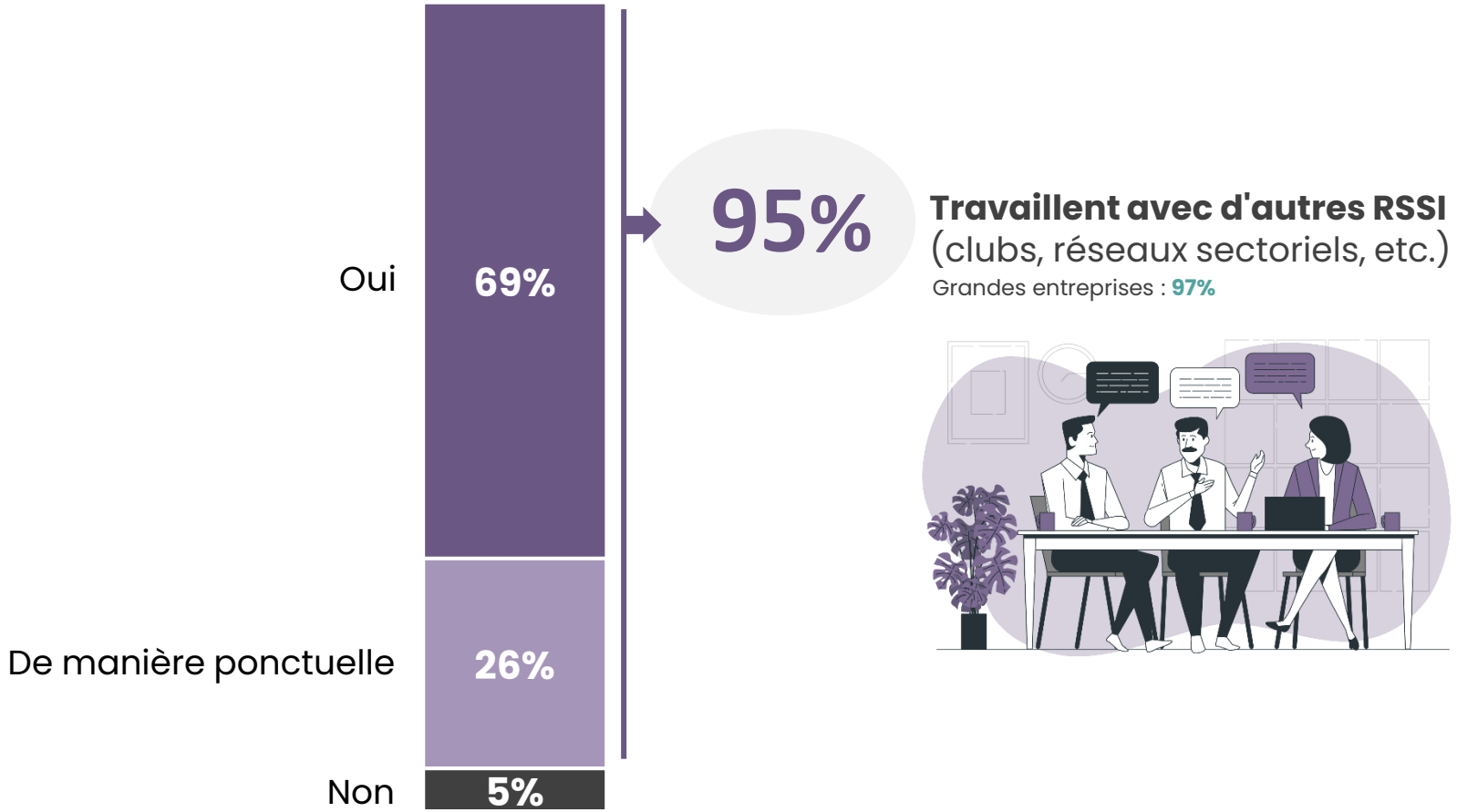
Crédits : Photo de Fauxels sur Pexels.com

La collaboration entre RSSI est une pratique très courante.

Nouvelle question en 2025

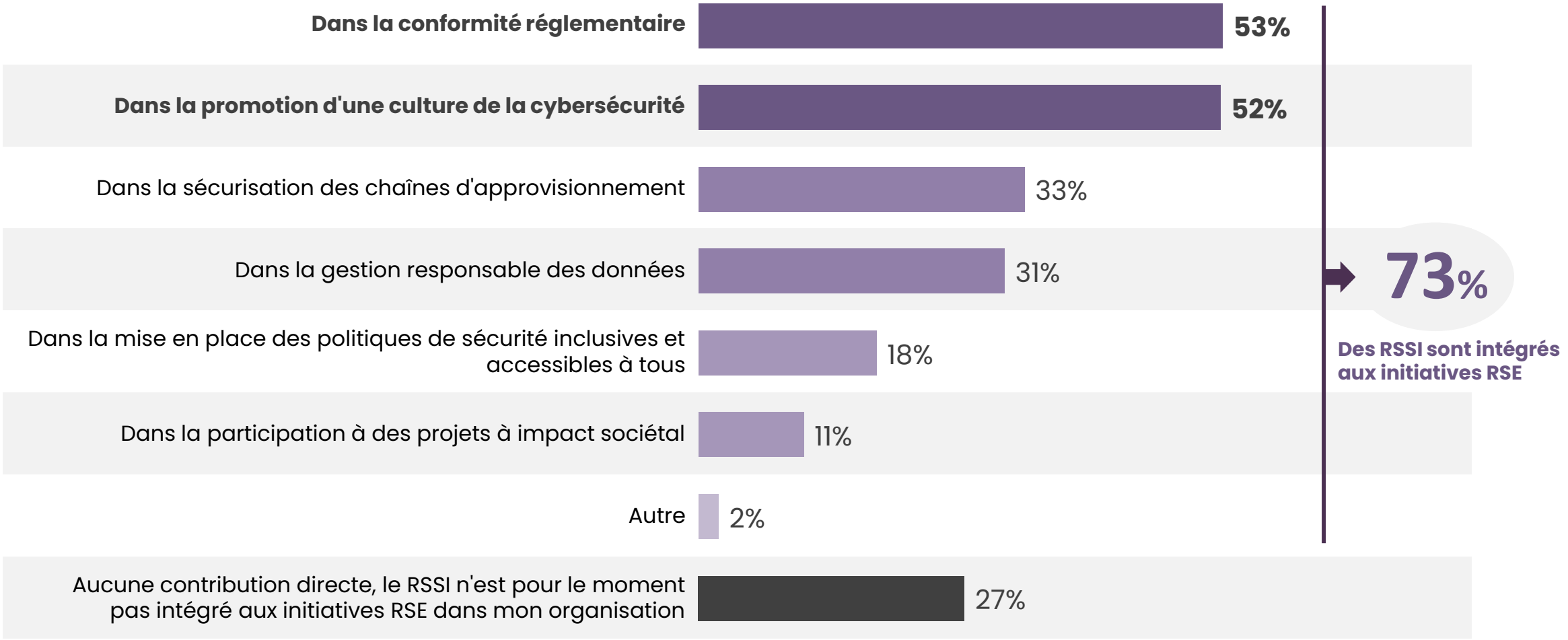
Q60 : **Travaillez-vous régulièrement avec d'autres RSSI** (clubs, réseaux sectoriels, etc.) ?

Base : ensemble (397)



3 RSSI sur 4 se sentent intégrés aux objectifs de responsabilité sociétale et environnementale, elle se manifeste le plus souvent par la conformité réglementaire et la promotion d'une culture de la cybersécurité.

Q49 : Dans quelle mesure votre rôle contribue, ou pourrait contribuer aux objectifs de **responsabilité sociétale et environnementale (RSE)** de votre organisation ? *Base : ensemble (397) – Plusieurs réponses possibles*



opinionway

PARIS ⊠ BORDEAUX ⊠ VARSOVIE ⊠ CASABLANCA ⊠ ABIDJAN

Fondé en 2000 sur cette idée radicalement innovante pour l'époque, OpinionWay a été précurseur dans le renouvellement des pratiques de la profession des études marketing et d'opinion.

Forte d'une croissance continue depuis sa création, l'entreprise n'a eu de cesse de s'ouvrir vers de nouveaux horizons pour mieux adresser toutes les problématiques marketing et sociétales, en intégrant à ses méthodologies le Social Média Intelligence, l'exploitation de la smart data, les dynamiques créatives de co-construction, les approches communautaires et le storytelling.

Aujourd'hui OpinionWay poursuit sa dynamique de croissance en s'implantant géographiquement sur des zones à fort potentiel que sont l'Europe de l'Est et l'Afrique.

C'est la mission qui anime les collaborateurs d'OpinionWay et qui fonde la relation qu'ils tissent avec leurs clients.

Le plaisir ressenti à apporter les réponses aux questions qu'ils se posent, à réduire l'incertitude sur les décisions à prendre, à tracker les insights pertinents et à co-construire les solutions d'avenir, nourrit tous les projets sur lesquels ils interviennent.

Cet enthousiasme associé à un véritable goût pour l'innovation et la transmission expliquent que nos clients expriment une haute satisfaction après chaque collaboration - 8,9/10, et un fort taux
de recommandation – 3,88/4.

Le plaisir, l'engagement et la stimulation intellectuelle sont les trois mantras de nos interventions.

ESOMAR 25 Corporate

afaq ISO 20252 Étude marketing et d'opinion AFNOR CERTIFICATION

Restons *connectés* !

Recevez chaque semaine nos derniers résultats d'études dans votre boite mail en vous abonnant à notre newsletter !

Je m'abonne

Vos contacts OpinionWay

Stéphane Lefebvre-Mazurel
Directeur Général Adjoint
Tel. +33 1 81 81 83 48
slefebvre@opinion-way.com

Valentin Heritier
Directeur d'études
Tel. +33 1 81 81 83 63
vheritier@opinion-way.com