“opinionway pour CESIN

Baromètre de la cybersécurité des entreprises

Vague 9 – Janvier 2024

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

afaq ISO 20252 Étude marketing et d'opinion

ESOMAR24 Corporate

Les objectifs

Contexte et objectifs

- Le **Club des Experts de la Sécurité de l'Information et du Numérique** (CESIN) offre un lieu d'échanges aux **experts de la sécurité et du numérique** au sein des entreprises.

- Le CESIN, avec OpinionWay, a lancé en 2015 sa première grande enquête auprès de ses membres pour connaître :
  - la **perception de la cybersécurité et de ses enjeux** au sein des entreprises membres du CESIN
  - **la réalité** concrète de la sécurité informatique des entreprises.

- L'enquête, renouvelée chaque année, met à jour les résultats sur la perception et la réalité de la cybersécurité, et apporte de nouvelles données sur l'impact de la transformation numérique des entreprises.

La méthodologie

La méthodologie

Echantillon de **456 membres du CESIN,** à partir du fichier des membres du CESIN.

Questionnaire

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

Les interviews ont été réalisées **du 27 novembre et le 22 décembre 2023**.

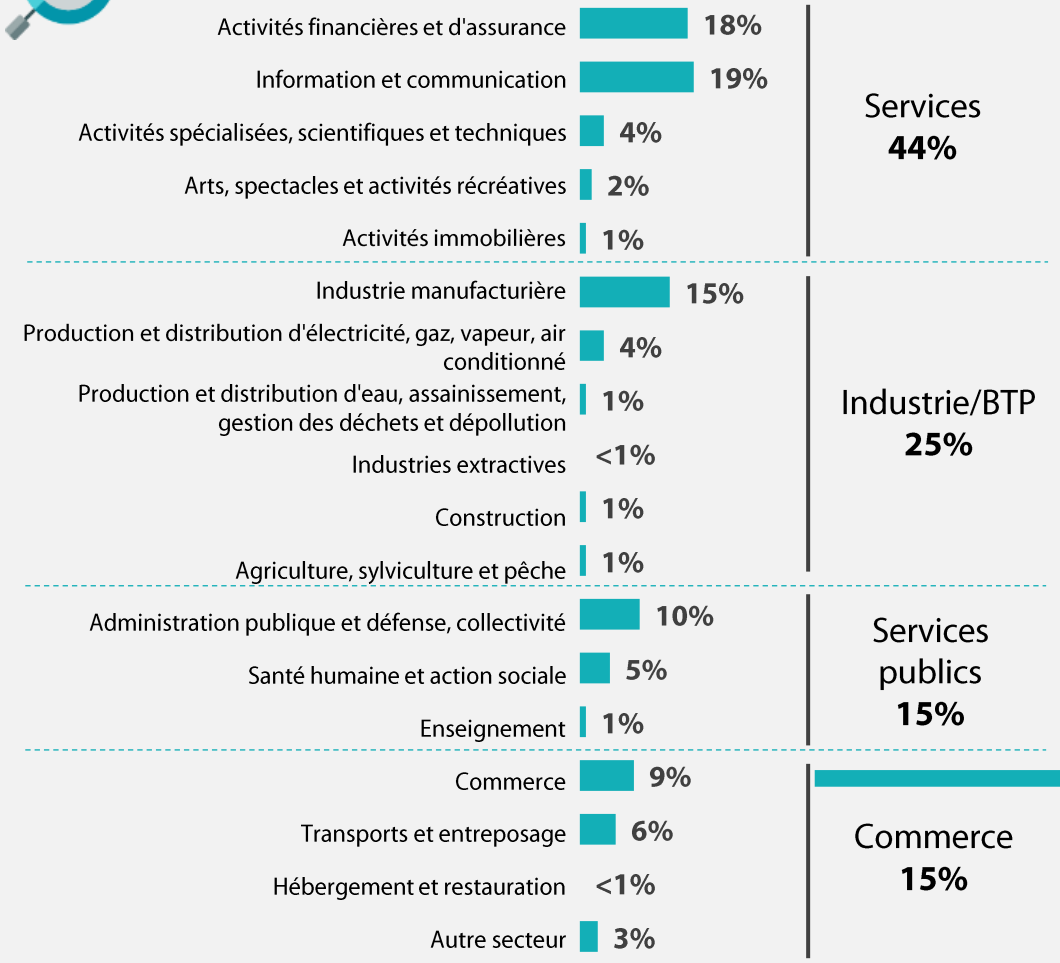
OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la **norme ISO 20252**

Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 4,6 points au plus pour un échantillon de 450 répondants.

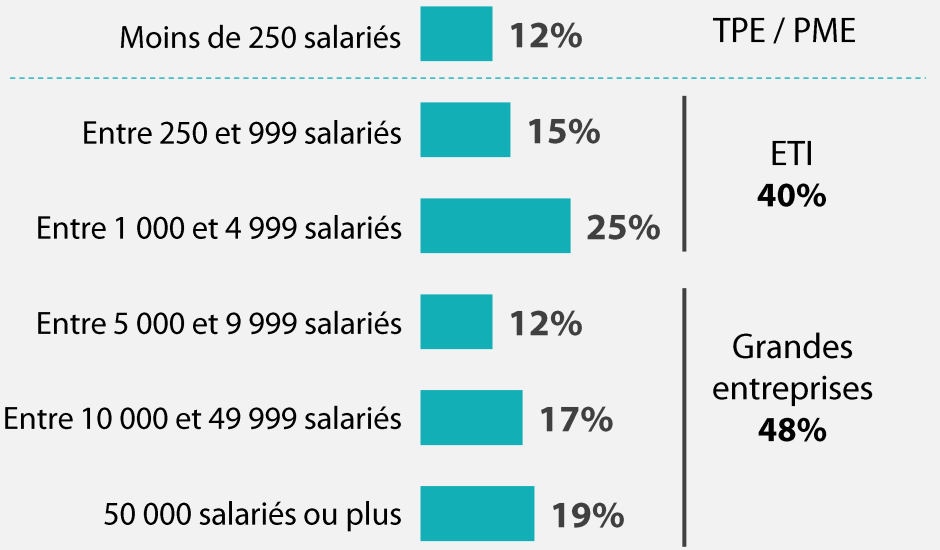
Le profil des répondants

Un échantillon qui reflète parfaitement la diversité de la population interrogée

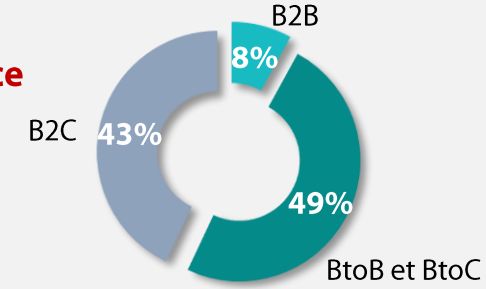
Secteur d'activité de l'entreprise



Nombre de salariés de l'entreprise



Activité Commerce



L’analyse

01

Le nombre de cyberattaques réussies en 2023 reste stable

L’attaque en déni de service prend plus d’importance cette année

Définition d'une cyberattaque

« Une cyberattaque, telle que nous l'entendons dans cette enquête, est le fait de subir un acte malveillant envers un dispositif informatique 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, entraînant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise et/ou des efforts significatifs de défense pour contenir et traiter l'attaque. Nous ne comptons pas là les tentatives d'attaques qui ont été arrêtées par vos systèmes de prévention. »

**** Définition en vague 6** : La cyberattaque, telle que nous l'entendons dans cette enquête, est le fait de subir un acte malveillant envers un dispositif informatique 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, entraînant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise.*

La moitié des entreprises a subi une cyberattaque réussie cette année, si la proportion est orientée à la hausse par rapport à 2022, le nombre d'entreprises ayant subi 15 cyberattaques ou plus diminue

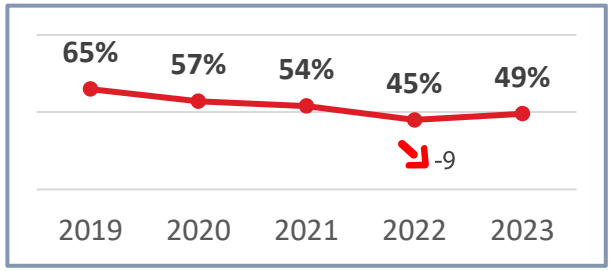
456 personnes

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

49%

des entreprises ont constaté au moins une cyberattaque

Rappel vagues précédentes

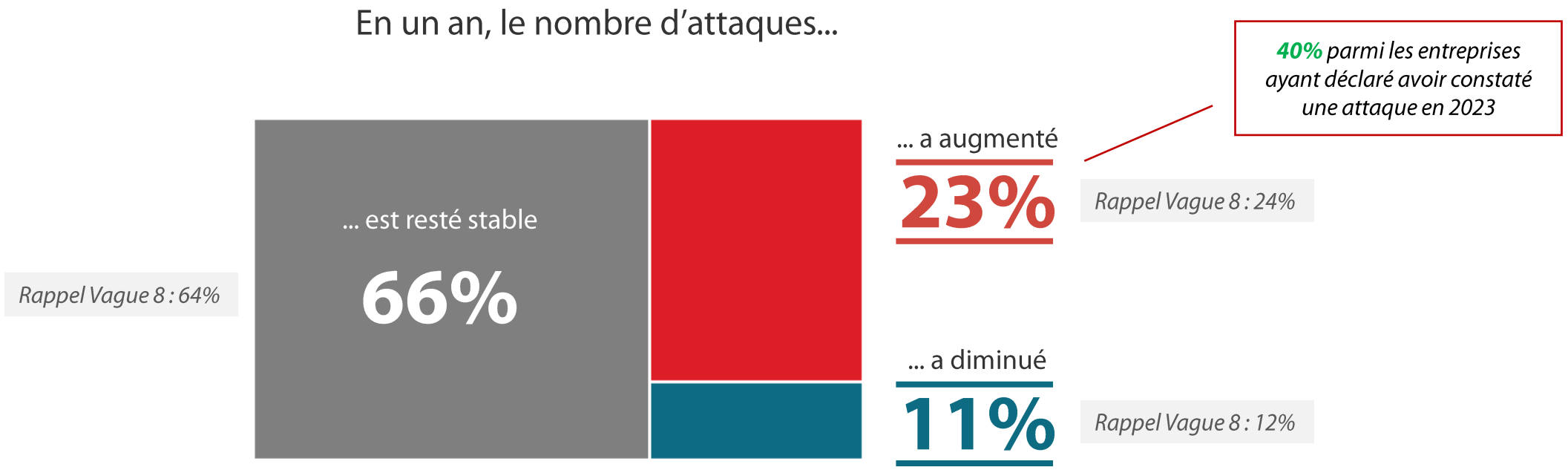


		Rappel Vague 8
Entre 1 et 3	38%	*32%*
Entre 4 et 9	8%	*7%*
Entre 10 et 14	2%	*2%*
15 ou plus	1% ↘ -3	*4%*

Le nombre d'attaques semble se stabiliser, il continue de croître d'une année sur l'autre, même si cette croissance reste limitée

456 personnes

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



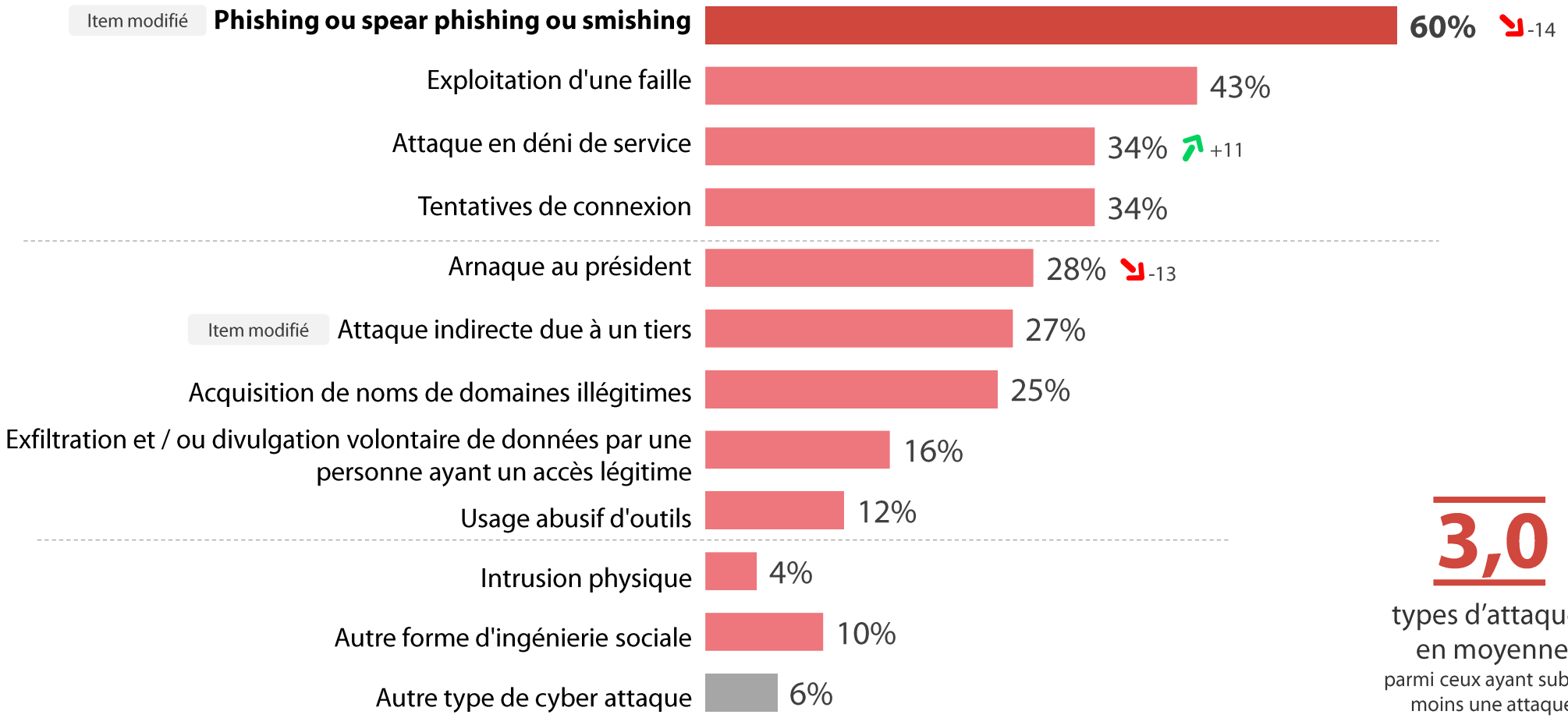
Les entreprises ayant constaté au moins une attaque en ont subi 3 en moyenne, si le phishing ou spear phishing ou smishing reste le principal vecteur, il diminue cette année. A noter, la forte augmentation de l'attaque en déni de service

225 personnes

Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?

Base : ont constaté une attaque - plusieurs réponses possibles

49% des entreprises ont subi au moins une cyberattaque en 2023



3,0

types d'attaques en moyenne

parmi ceux ayant subi au moins une attaque

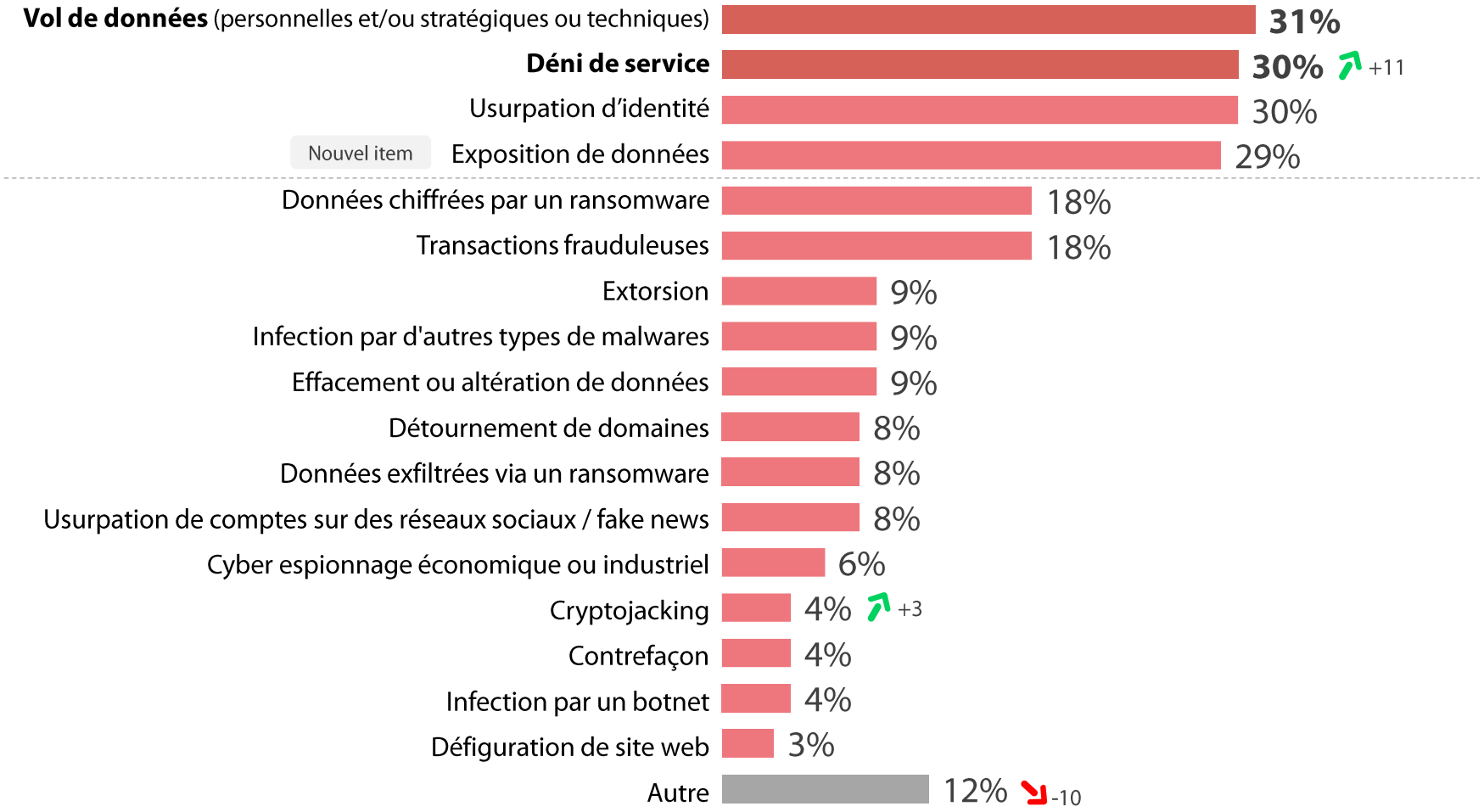
Le vol de données, le déni de service, l'usurpation d'identité et l'exposition de données sont les principales conséquences de ces attaques

225 personnes

Q5B. Et quelles ont été les conséquences de cette/ces attaque(s) ?

Base : ont constaté une attaque - plusieurs réponses possibles

49% des entreprises ont subi au moins une cyberattaque en 2023



Évolution statistiquement significative par rapport à la vague précédente

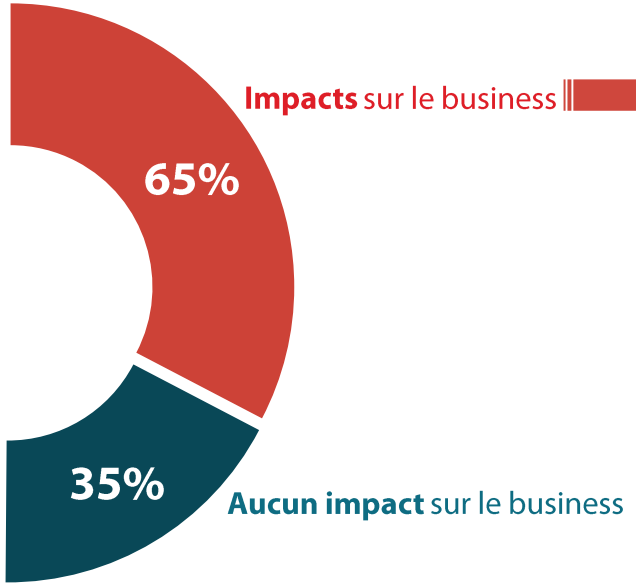
L'impact des cyberattaques est légèrement plus important sur le business cette année, outre la perturbation de la production, l'indisponibilité du site web pendant une période significative est en hausse, en lien avec l'augmentation des attaques en déni de service

420 personnes

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

Base : ont constaté une attaque et / ou une cause d'incidents de sécurité - Plusieurs réponses possibles

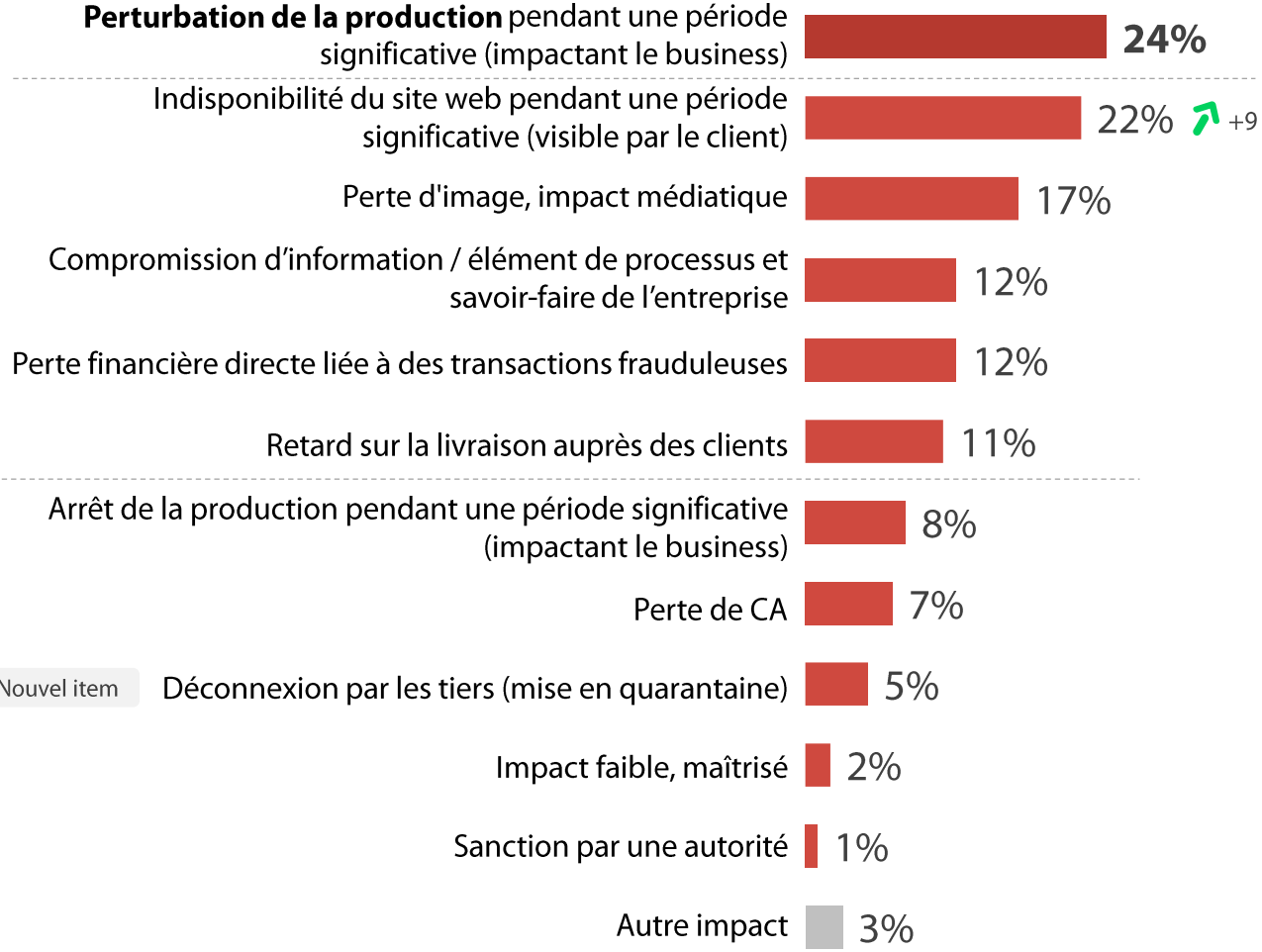
Rappel Vague 8 : 60%



Impacts sur le business

Rappel Vague 8 : 40%

Aucun impact sur le business

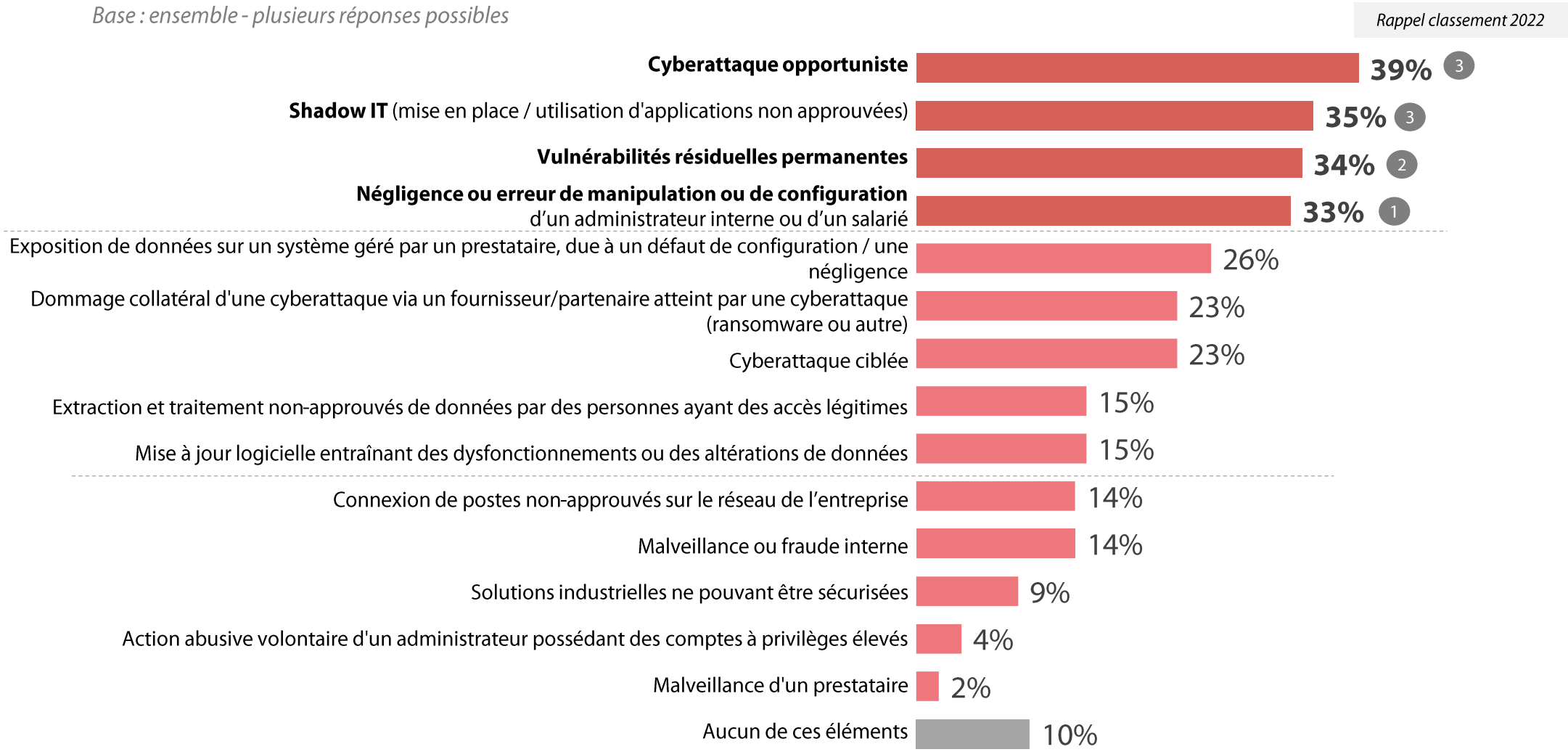


La place des mauvaises pratiques, incluant les opérations IT et le Shadow IT, à la source des incidents est toujours importante. On comprend mieux les origines des attaques et on observe que les attaques opportunistes occupent une place relativement importante

456 personnes

Q6. Parmi les causes des incidents de sécurité rencontrées par l'entreprise, cyberattaques incluses, quelles sont celles auxquelles votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?

Base : ensemble - plusieurs réponses possibles



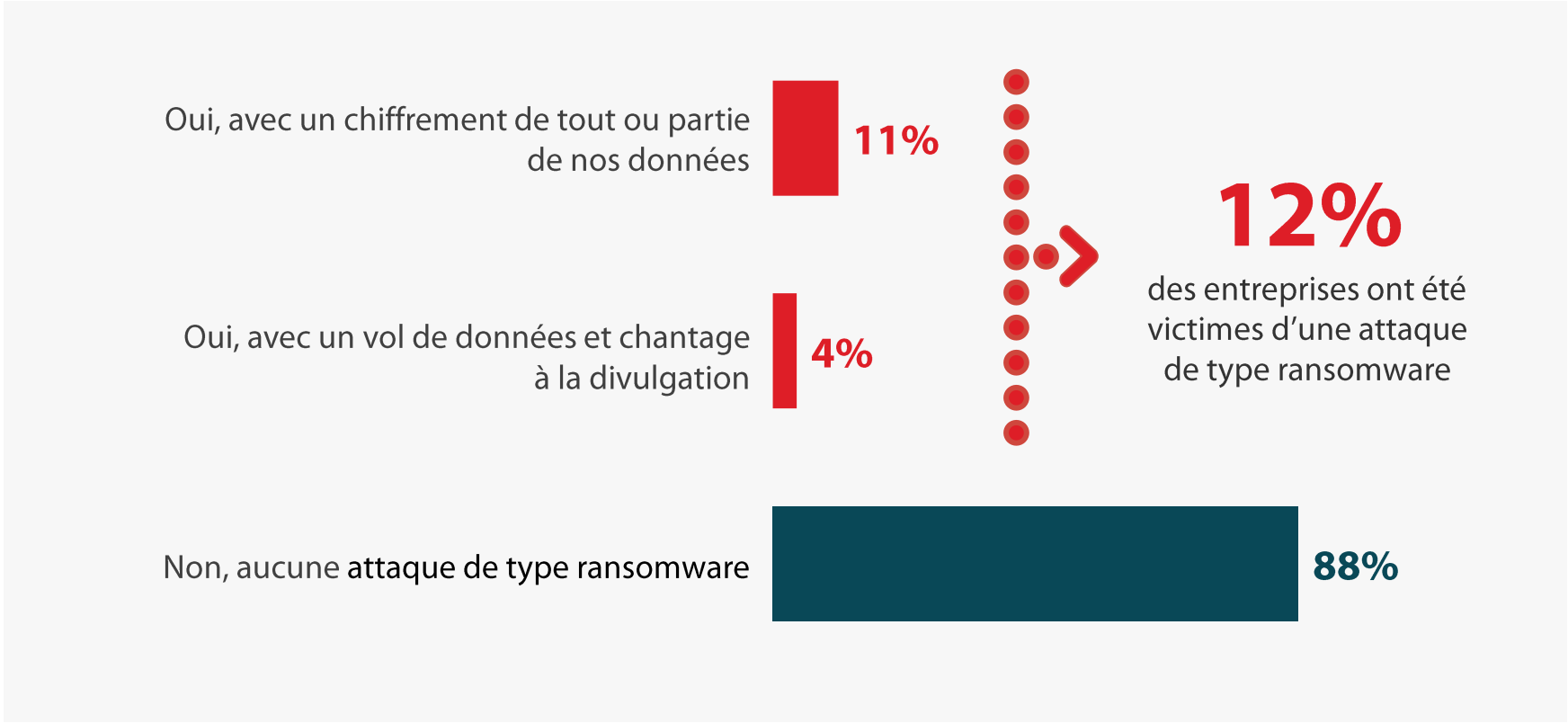
Les attaques par ransomware se stabilisent et touchent environ 10% des entreprises

456 personnes

L'année passée a à nouveau été marquée par le renforcement de la menace par ransomware. Outre la vague d'attaques réussies dans certains cas, les attaquants ont exercé un chantage à la divulgation de données.

Q10. Avez-vous été victime d'une attaque de type ransomware ?

Base : ensemble - Plusieurs réponses possibles



Rappel Vague 8 : 14%

Le risque de cyberespionnage est un risque élevé pour 2 entreprises sur 5, ce qui constitue un élément important compte tenu du fait que certaines entreprises ne sont pas, du fait de leur activité, très concernées par ce type de risque

456 personnes

Q9. Aujourd'hui, comment évaluez-vous le niveau des menaces relatives au cyberespionnage pour votre entreprise ?

Base : ensemble

Très élevé : figure dans le top 3 des risques identifiés — **13%**

Assez élevé : figure dans le top 10 des risques identifiés — **28%**

Assez faible : présent dans la cartographie des risques — **39%**

Très faible : absente de la cartographie des risques — **20%**

41% Estiment un niveau élevé des menaces relatives au cyber-espionnage

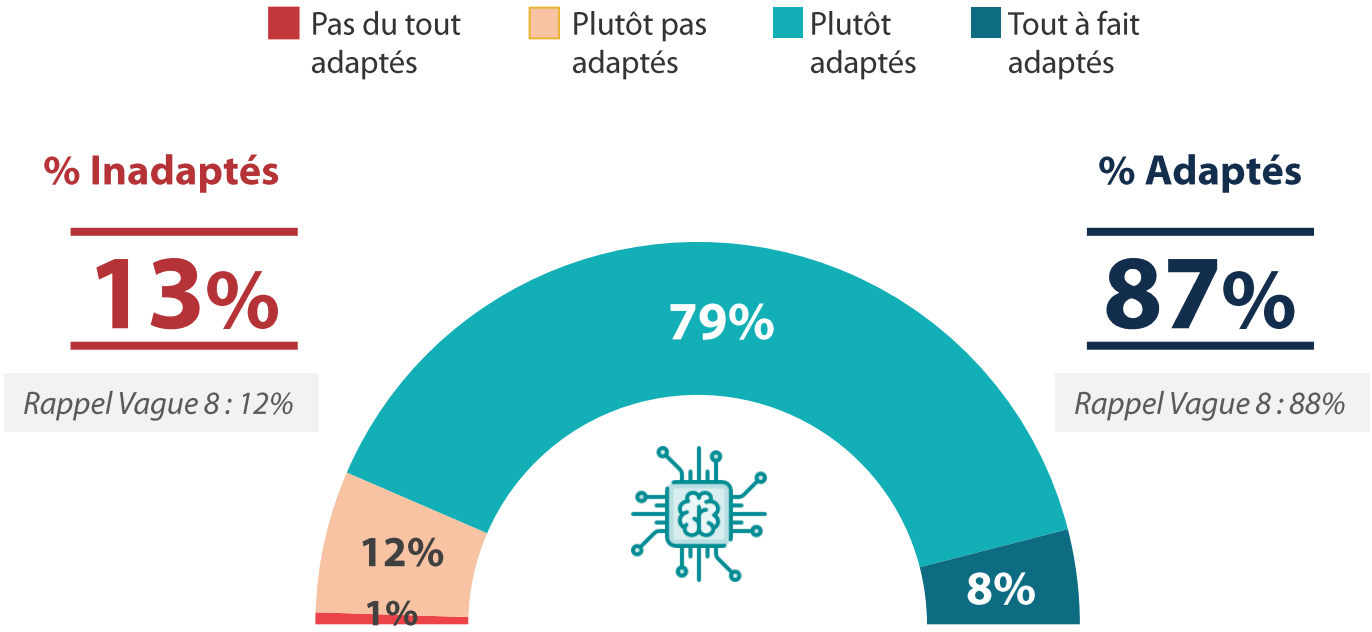
02

La protection des entreprises reste stable. L'efficacité et l'utilisation de l'EDR se confirment cette année encore

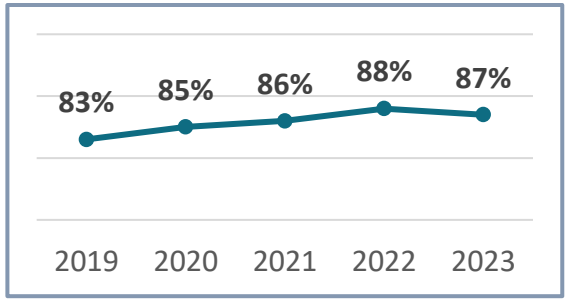
Le niveau de confiance envers les solutions et services de sécurité disponibles sur le marché reste toujours élevé comme l'année dernière

456 personnes

Q25. Pensez-vous que les solutions et services de sécurité disponibles sur le marché ne sont tout à fait, plutôt, plutôt pas ou pas du tout adaptés à votre entreprise ?
Base : ensemble



Rappel vagues précédentes

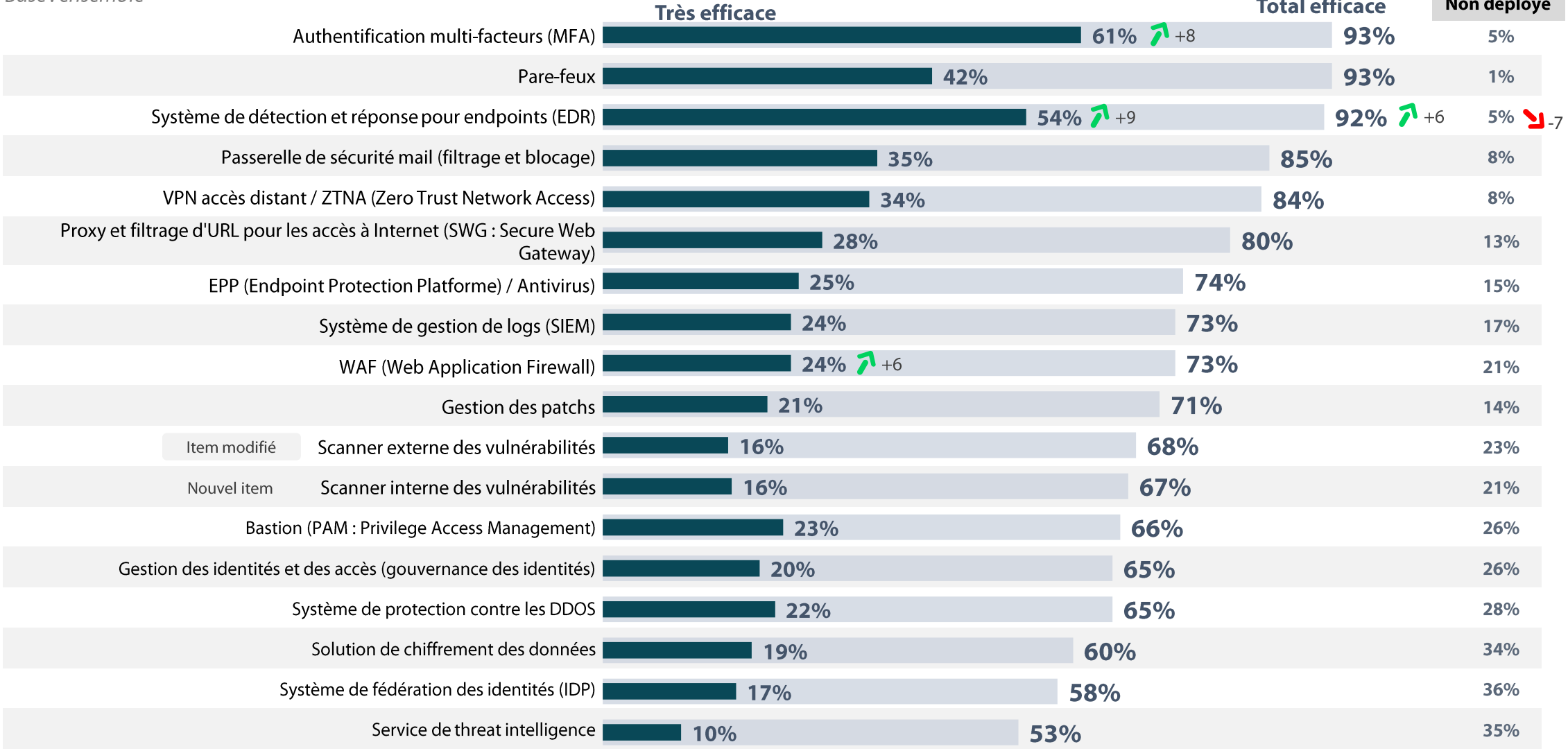


Dans le détail, la confiance envers le couple MFA/EDR se renforce avec des niveaux de très efficace avoisinant les 60%

456 personnes

Q13. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ?

Base : ensemble

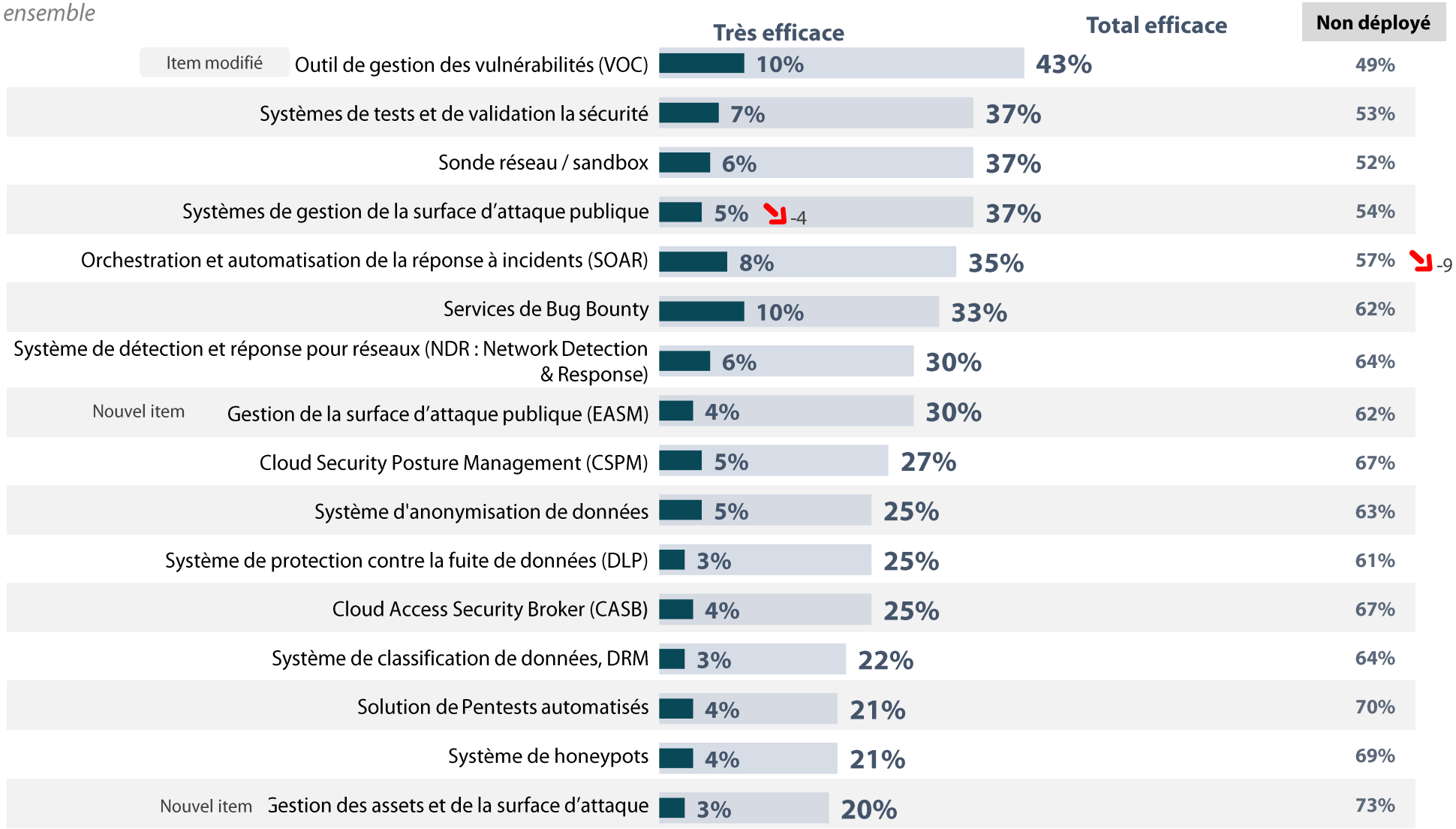


Les autres solutions sont moins déployées dans les entreprises

456 personnes

Q13. Pour chacune des solutions suivantes, estimez-vous qu'elle est très efficace, plutôt efficace, plutôt pas efficace ou pas du tout efficace ?

Base : ensemble



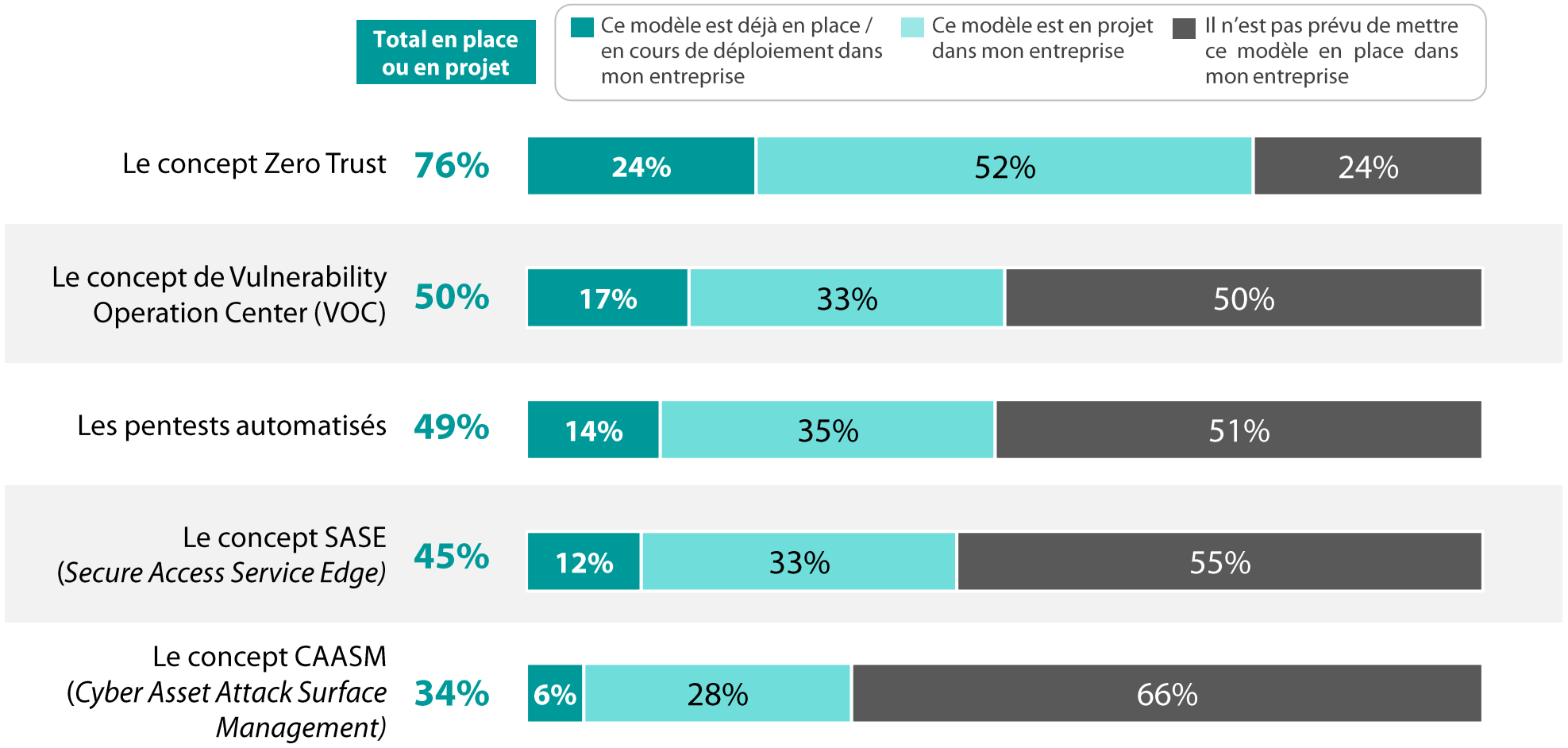
Le Zero Trust commence à acquérir une certaine maturité, alors que le concept plus récent de CAASM commence tout juste à être repéré dans les entreprises mais fait une petite percée à suivre

456 personnes

Nouvelle question en 2023

Q28b. Quelle est votre vision des concepts suivants ?

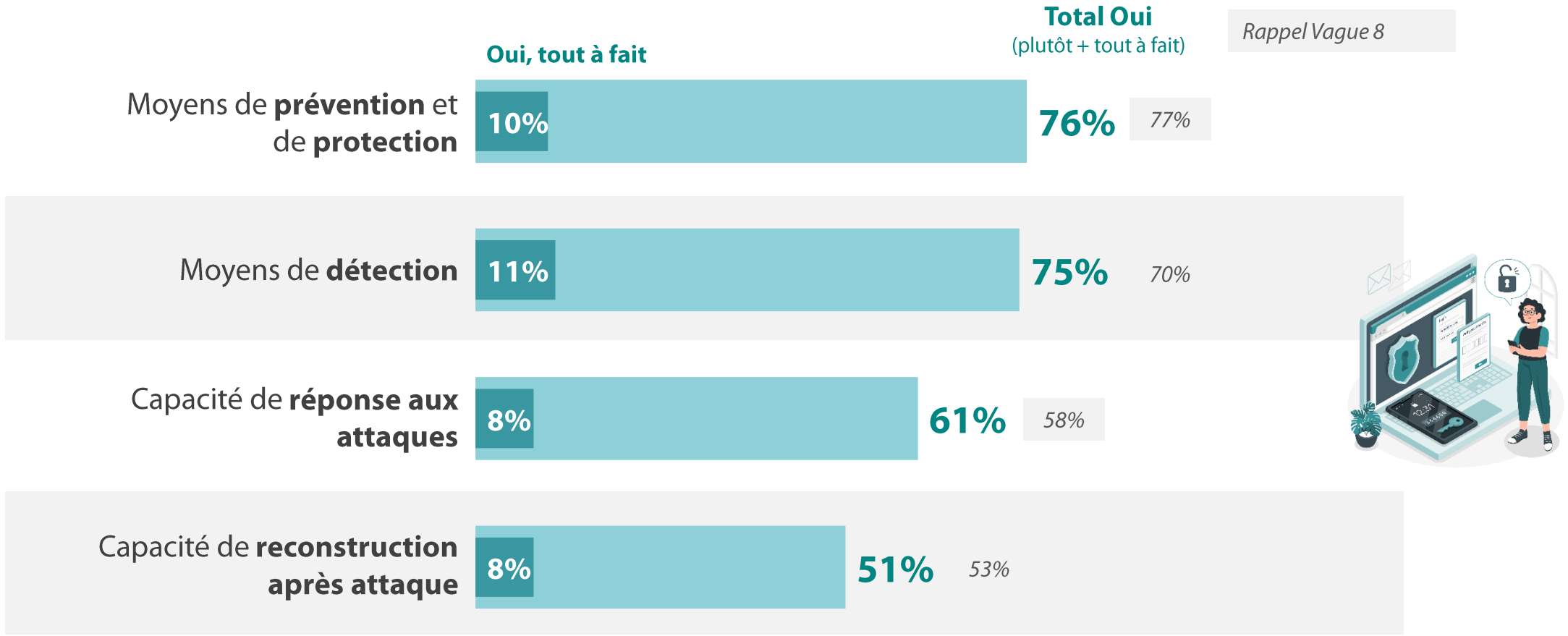
Base : ensemble



Similairement à l'année dernière, les entreprises sont davantage confiantes dans leur préparation pour faire face à une attaque que pour y répondre

456 personnes

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

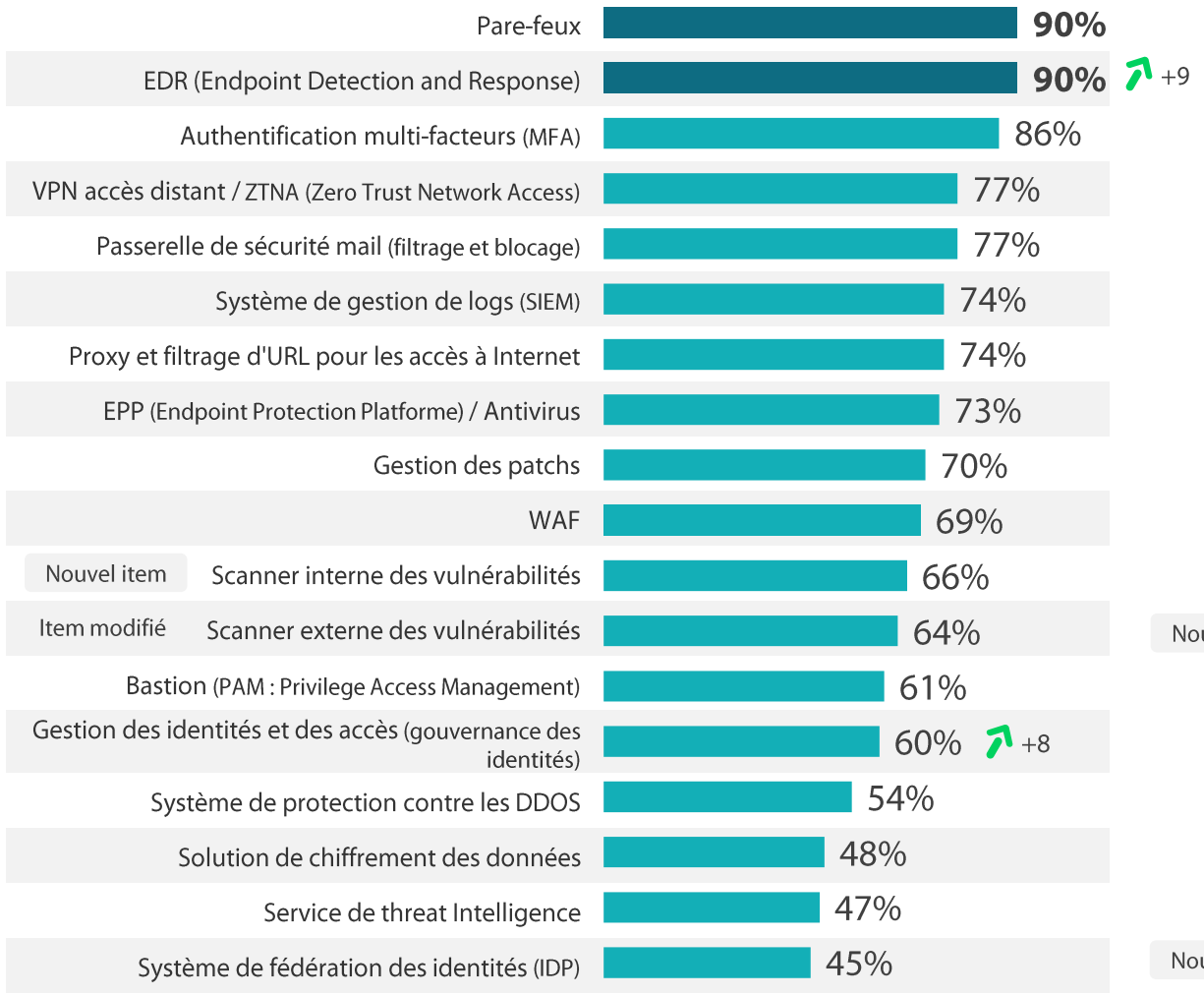


Au global, plus de 15 solutions ou services en moyenne mis en place dans les entreprises. L'EDR rejoint les pare-feux en tête des solutions déployées, avec le MFA qui est complété par une belle croissance de la gestion des identités

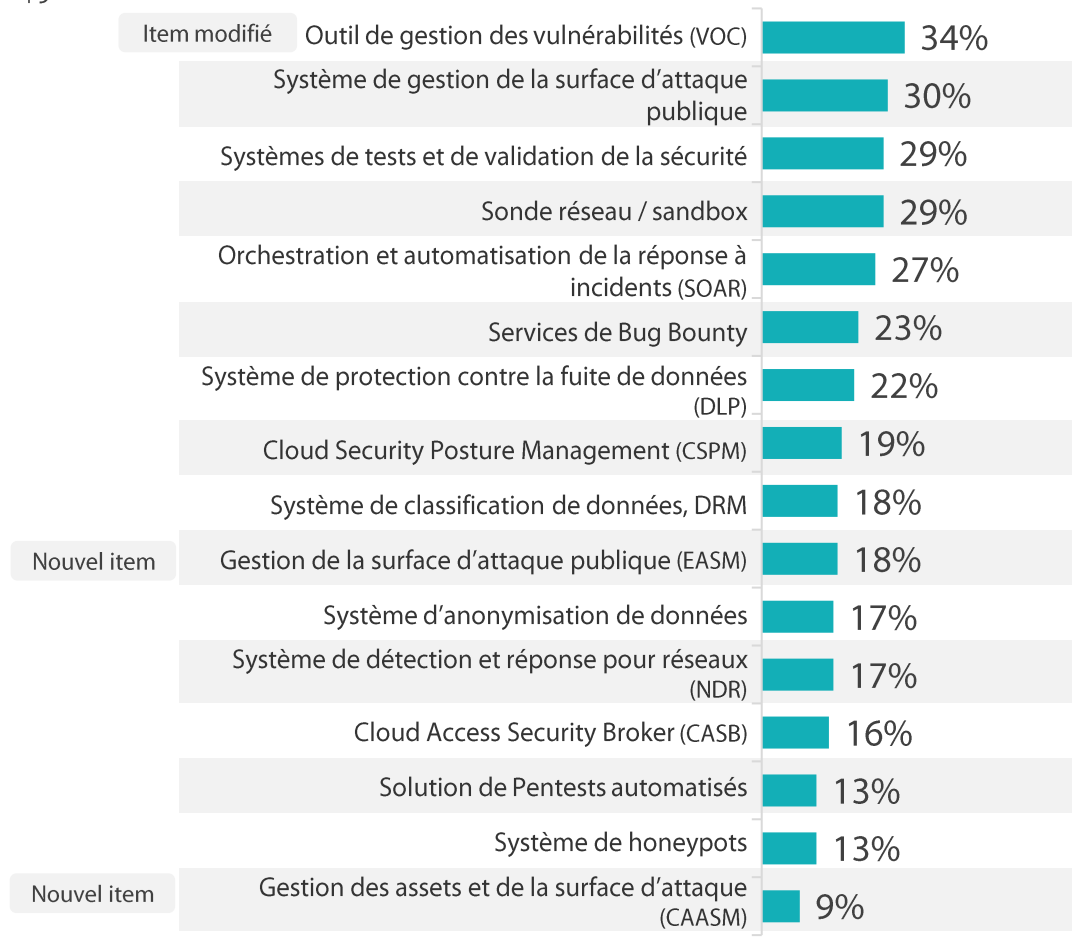
456 personnes

Q12. D'une manière plus générale, parmi les solutions et services suivants, quels sont ceux qui sont en place dans votre entreprise ?

Base : ensemble - plusieurs réponses possibles



15,6 solutions en moyenne



*Nouvel item
** item modifié

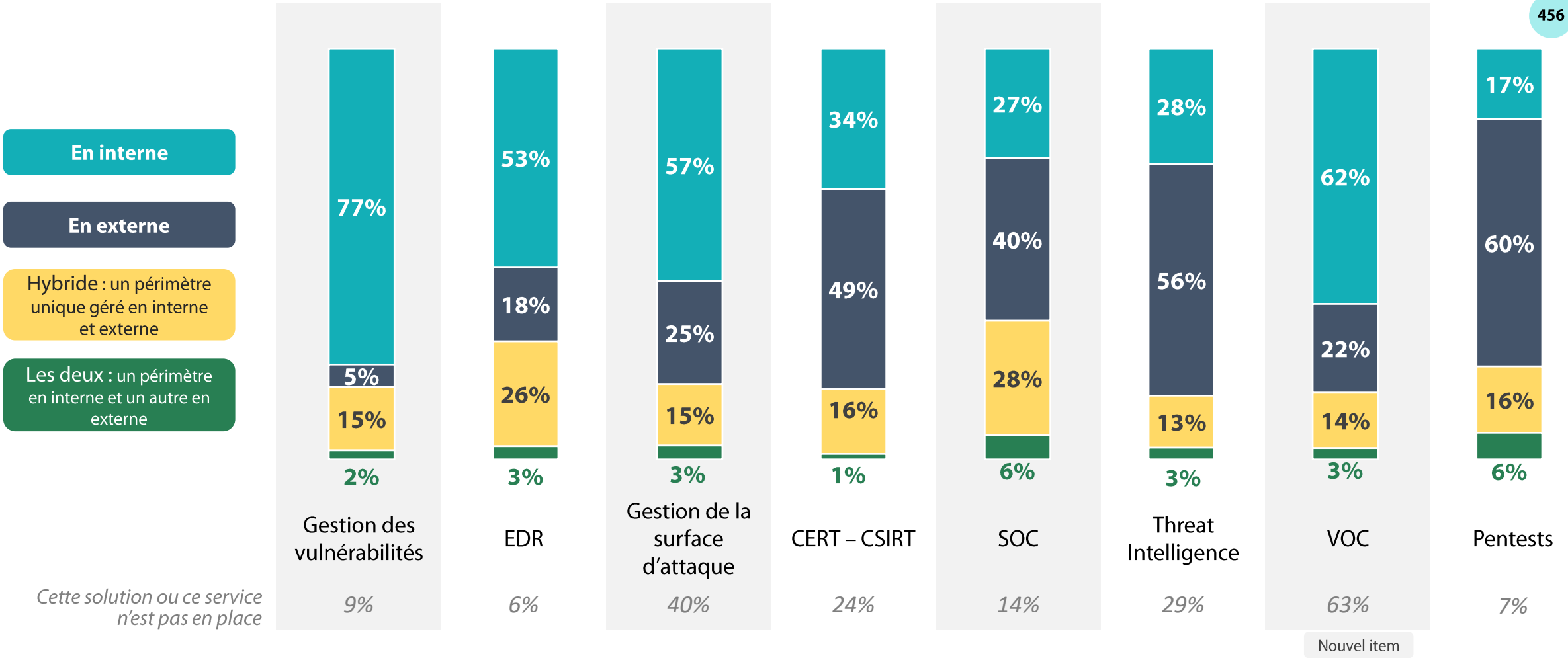
Évolution statistiquement significative par rapport à la vague précédente
Évolution à interpréter avec prudence au vu de l'ajout d'items

La gestion des vulnérabilités, le VOC et la gestion de la surface d'attaque sont majoritairement traités en interne, à l'inverse des Pentests, de la Threat Intelligence ou du CERT-CSIRT. Il faut noter la part non négligeable des EDR et des SOC traités de manière hybride

Q30b. Comment opérez-vous les solutions et services ci-dessous ?

Base : ensemble – résultats hors solution non mise en place

456 personnes



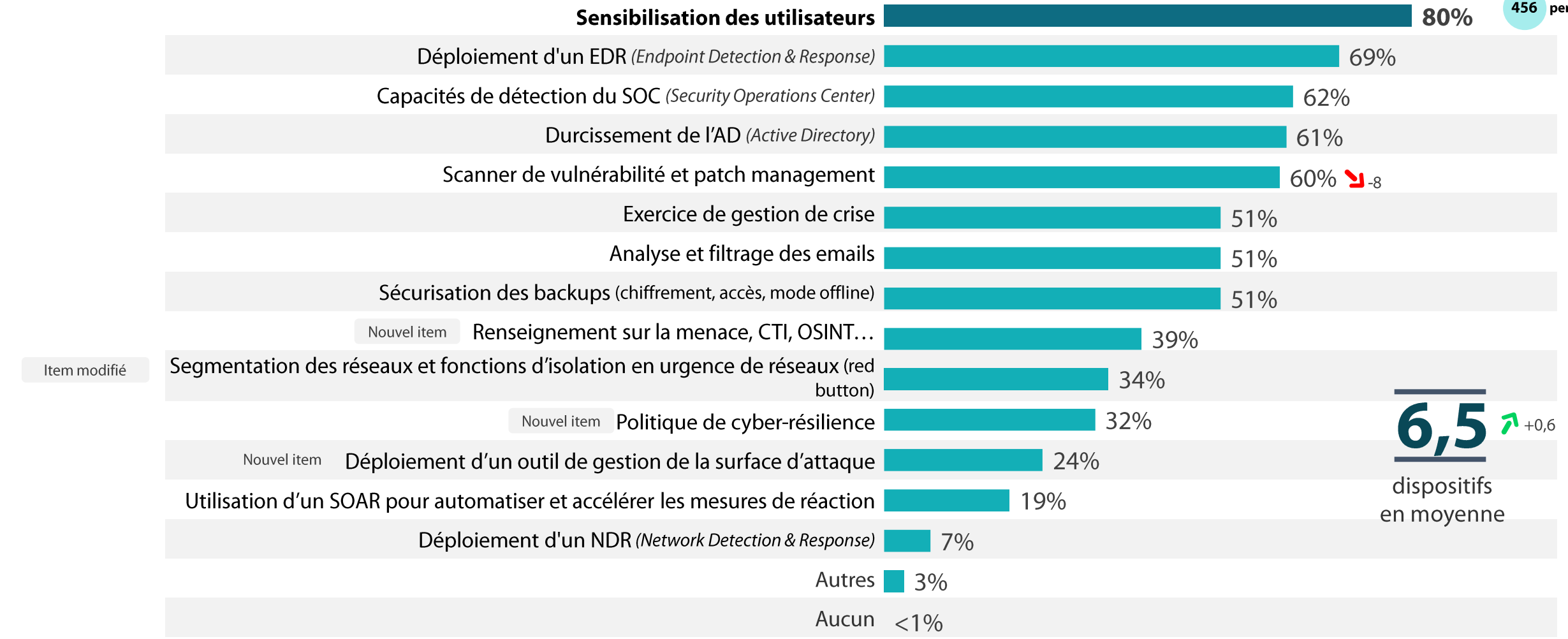
Nouvel item

Les entreprises ont, cette année, renforcé plus de dispositifs (plus de 6 en moyenne). Avec toujours la sensibilisation des utilisateurs et l'EDR qui prédominent

Q11. Face à cette vague de cyberattaque dominée par le ransomware, quels dispositifs avez-vous renforcés ?

Base : ensemble - plusieurs réponses possibles

456 personnes

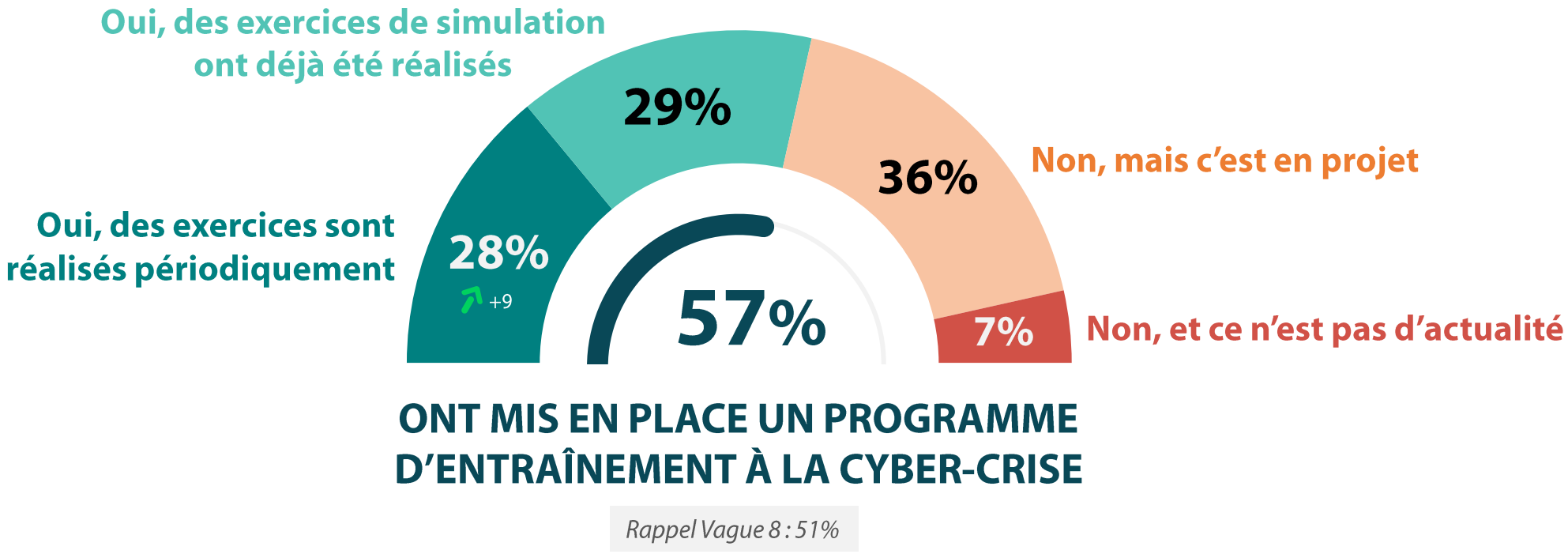


6,5 +0,6
dispositifs en moyenne

La part d'entreprises ayant mis en place un programme d'entraînement à la cyber-crise est orientée à la hausse. Les exercices se déroulent par ailleurs plus fréquemment

456 personnes

Q15. Votre entreprise a-t-elle mis en place un programme d'entraînement à la crise cyber ?
Base : ensemble



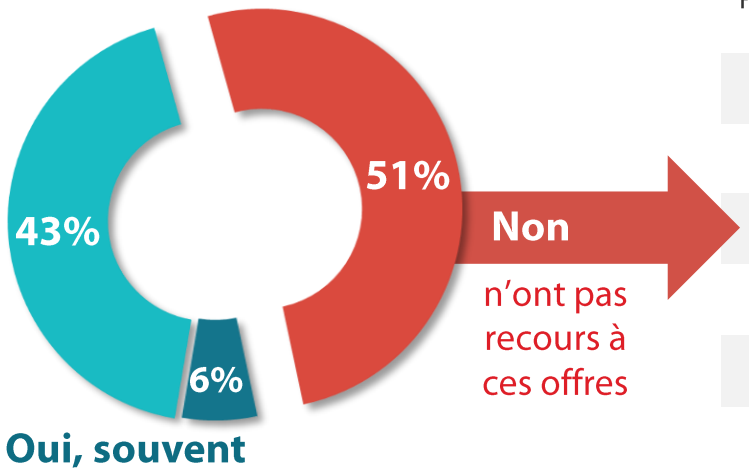
Rappel Vague 8 : 51%

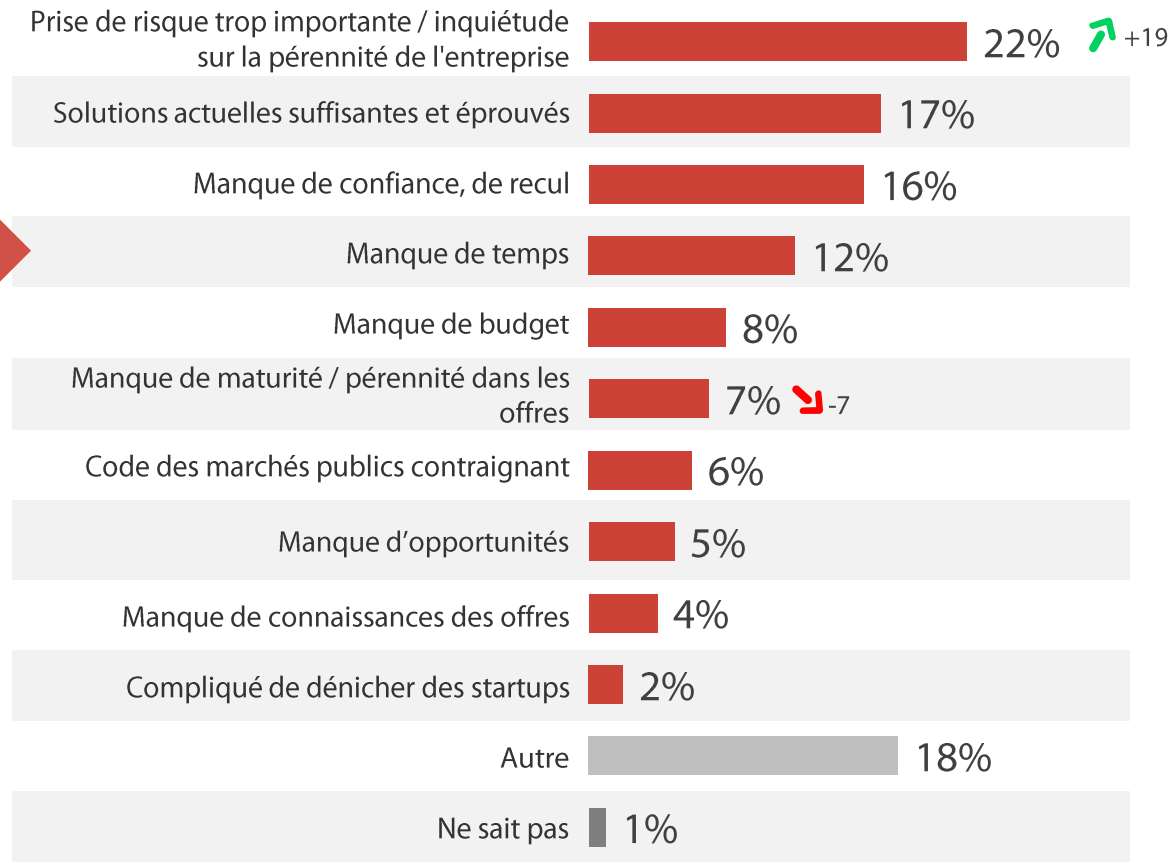
La moitié des entreprises ont recours à des offres innovantes issues des startups, celles qui ne le font pas mettent en avant la prise de risque trop importante

456 personnes

Q26. En matière de cybersécurité, recourrez-vous à des offres innovantes issues de startups ? *Base : ensemble*
Q26bis. Pour quelle(s) raison(s) ne le faites-vous pas ? *Base : ne fait pas appel à des offres issues de start-up (153)*

49% ont recours à des offres innovantes issues de startups

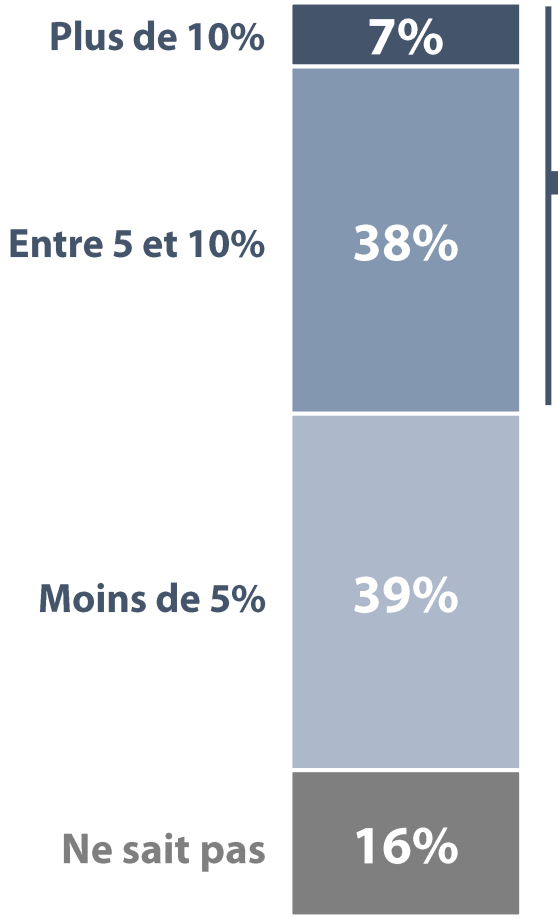




Au final, les budgets cyber se maintiennent au même niveau que l'année dernière

456 personnes

Q18. Dans votre entreprise, quelle part du budget IT/digital est consacrée à la sécurité ?
Base : ensemble



5% ou plus du budget IT/digital est consacrée à la sécurité : 45%

Rappel Vague 8 : 45%

Focus sur…

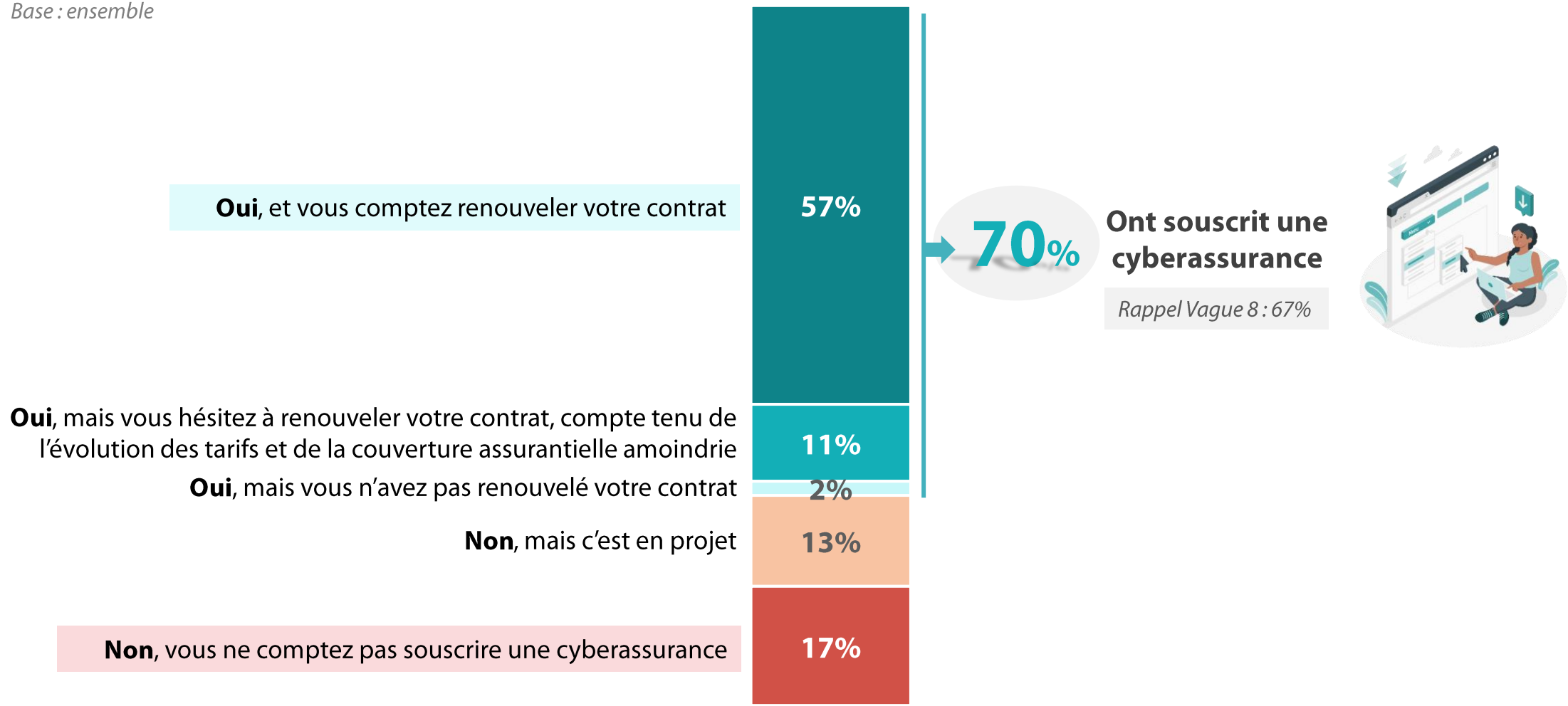
La cyberassurance

7 entreprises sur 10 ont souscrit à une cyberassurance et la majorité compte renouveler ce contrat, le périmètre des entreprises assurées se stabilise

456 personnes

Q31. Avez-vous souscrit une cyberassurance ?

Base : ensemble

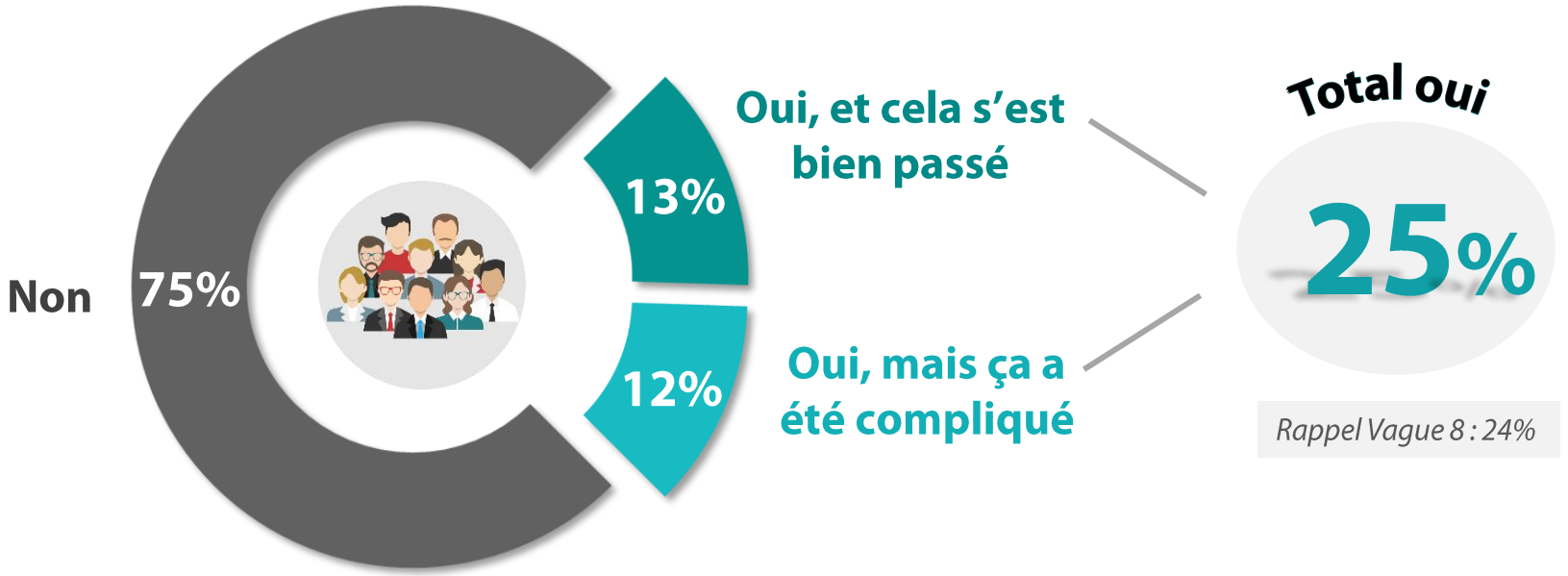


Similairement à l'année dernière, trois quarts des entreprises assurées n'ont jamais fait appel à leur cyberassurance

320 personnes

Q32. Votre entreprise a-t-elle déjà fait appel à sa cyberassurance dans le cadre d'une cyberattaque ?
Base : possède une cyberassurance ou projette d'en posséder une

Utilisation de la cyberassurance



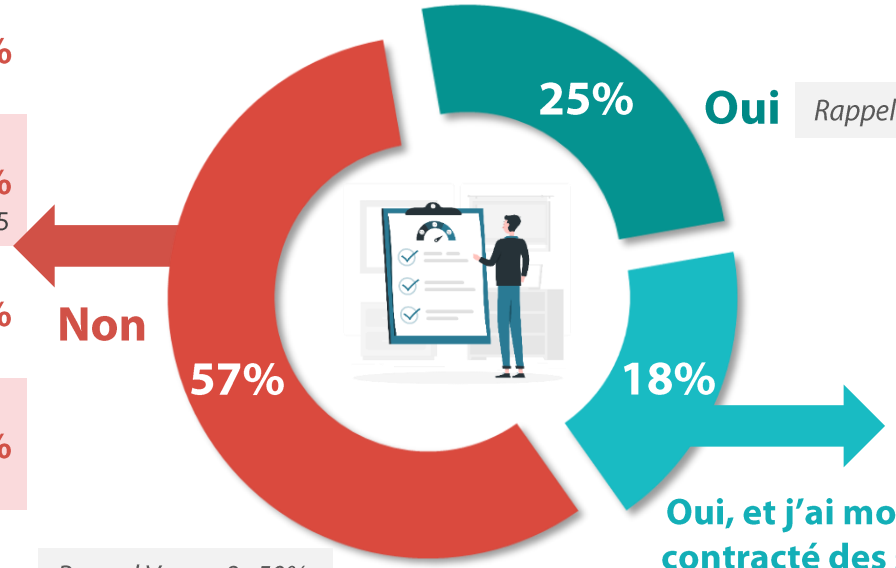
Plus de la moitié des entreprises estime que le recours des cyber-assureurs aux agences de notation n'est pas une bonne chose considérant que l'analyse reste très partielle

456 personnes

Nouvelle question en 2023

Q33. Les cyber-assureurs ont de plus en plus recours au service d'agences de notation. Est-ce une bonne chose selon vous ? *Base : ensemble*
Q33b. Et pour quelle raison avez-vous contracté les services de cyber-rating ? *Base : ont contracté des services de cyber-rating (81)*
Q33bis. Pour quelles raisons ? *Base : ce n'est pas une bonne chose (259)*

Le recours au service d'agences de notation



Rappel Vague 8 : 29%

Rappel Vague 8 : 50%

Rappel Vague 8 : 21%

Item modifié

- Parce que ces plateformes ne font par construction qu'une analyse très partielle du niveau de sécurité et fournissent un score par extrapolation — **71%**
- Parce que les résultats ne sont pas fiables dans l'identification et l'assignation des assets — **58%** +15

Item modifié

- Parce que les critères et le mode de calcul des scores sont contestables du point de vue des priorités définies — **69%**
- Parce que ces services constituent une forme de vente forcée de solution — **37%**
- Pour une autre raison — **3%**

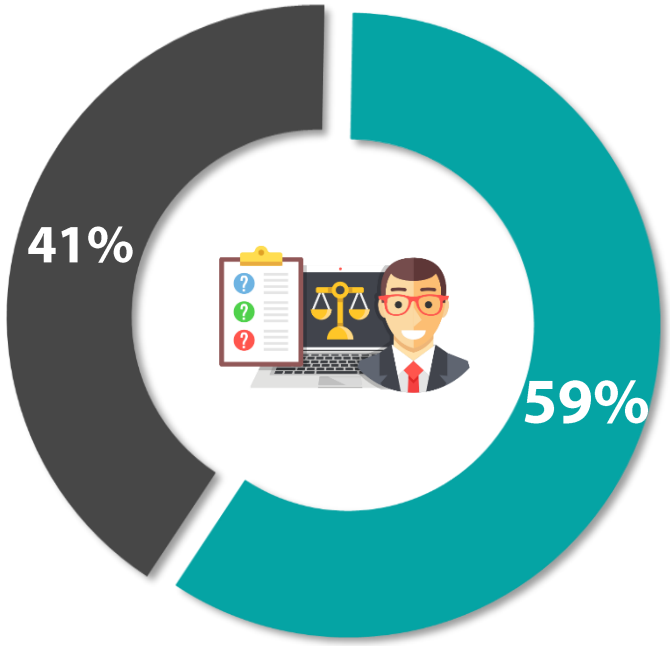
- **64%** En complément de ma gestion des risques cyber
- **30%** Pour comprendre et améliorer la note qui m'a été imposée
- **6%** Autre raison

Près de 6 entreprises sur 10 ont déjà porté plainte suite à une cyberattaque…

225 personnes

Q8. Avez-vous porté plainte à la suite de la cyberattaque / des cyberattaques dont votre entreprise a été victime ?
Base : ont constaté une attaque

49% des entreprises ont subi au moins une cyberattaque en 2023



N'ont pas porté plainte

Ont porté plainte

Rappel Vague 8 : 54%

pour **toutes les attaques** : **32%**

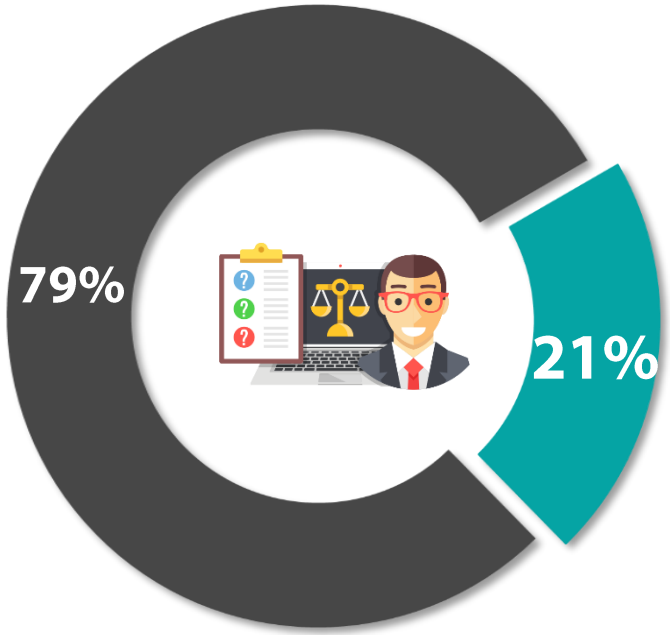
pour **certaines attaques** : **27%**

…et l'identification/l'interpellation des attaquants s'est produit 1 fois sur 5, un score qui tend à augmenter

132 personnes

Q8bis. Suite à votre ou vos plainte(s), l'enquête a-t-elle permis d'identifier et/ou d'interpeller le ou les attaquant(s) ?
Base : ont porté plainte

59% des entreprises ont porté plainte



Oui, l'enquête a permis une identification

Rappel Vague 8 : 16%

pour **toutes les plaintes**: **5%**

pour **certaines plaintes** : **16%**

03

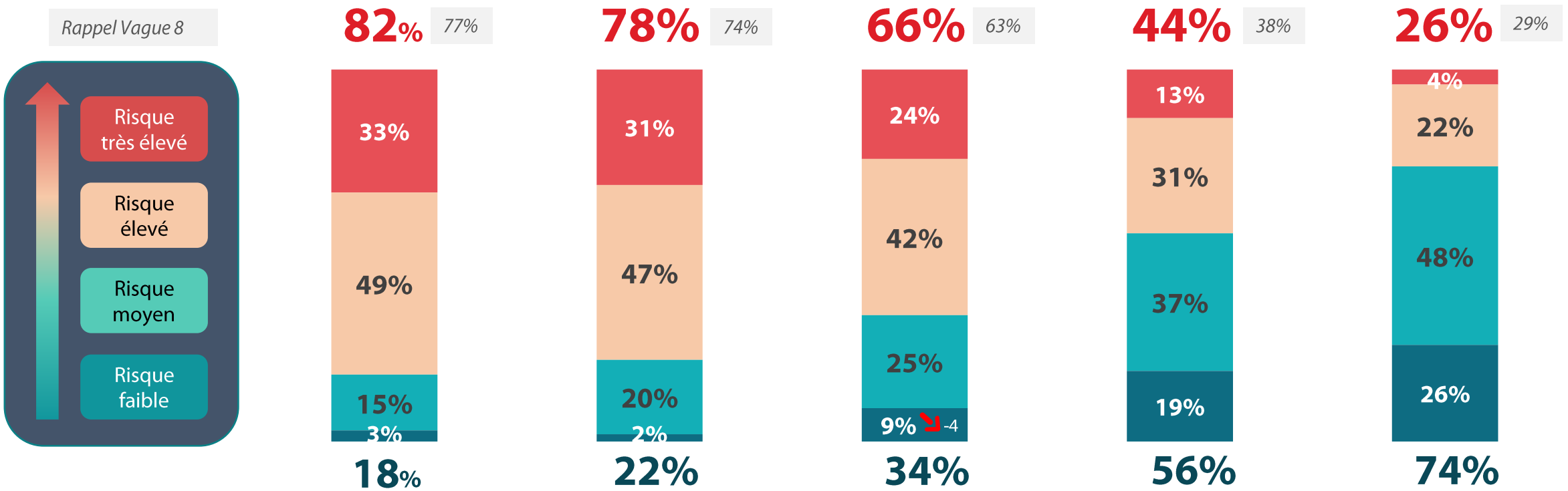
Des usages numériques qui présentent toujours autant de risques, même si les salariés se montrent plus conscients des enjeux

A l'exception des risques induits par le télétravail, les RSSI voient le niveau de risques des usages numériques des salariés orientés à la hausse, notamment dans les usages du cloud illégitime ou Shadow IT

456 personnes

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

Base : ensemble



Le recours massif aux services cloud non approuvés (Shadow IT)

La gestion des partages de données par les utilisateurs eux-mêmes dans le cas du collaboratif cloud

L'utilisation de devices personnels pour se connecter aux applications de l'entreprise (BYOD)

L'usage à des fins personnelles des devices fournis par l'entreprise

Le télétravail, l'accès au réseau en mobilité

Si les métriques permettant de mesurer la participation des salariés aux formations / sensibilisations sont largement déployés dans les entreprises, cela est largement moins le cas pour mesurer la connaissance des salariés en matière de cybersécurité

456 personnes

Nouvelle question en 2023

Q19b. Et toujours en ce qui concerne la sensibilisation et la formation à la cybersécurité, avez-vous mis en place les métriques suivants ?

Base : ensemble

Des métriques pour mesurer **la participation aux formations/ sensibilisations**

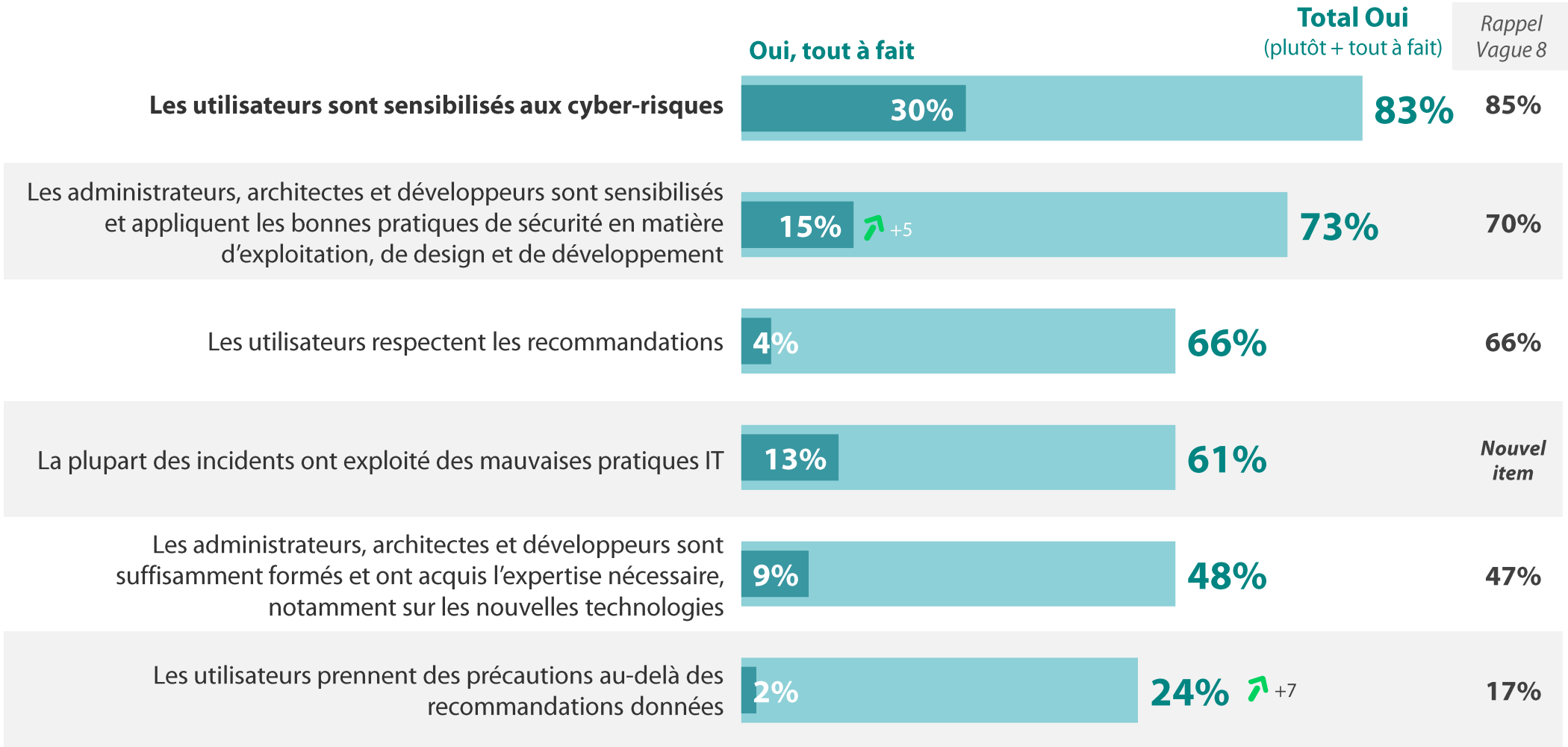
Des métriques pour mesurer **la connaissance des collaborateurs en matière de cybersécurité**

La sensibilisation et la formation des salariés à la cybersécurité est équivalente à 2022 selon les RSSI, il est à noter que les utilisateurs prennent davantage de précaution, même si cela n'est pas toujours suffisant

456 personnes

Q19. En ce qui concerne la sensibilisation et la formation des salariés à la cybersécurité, pensez-vous que ?

Base : ensemble



Focus sur…

Le Cloud

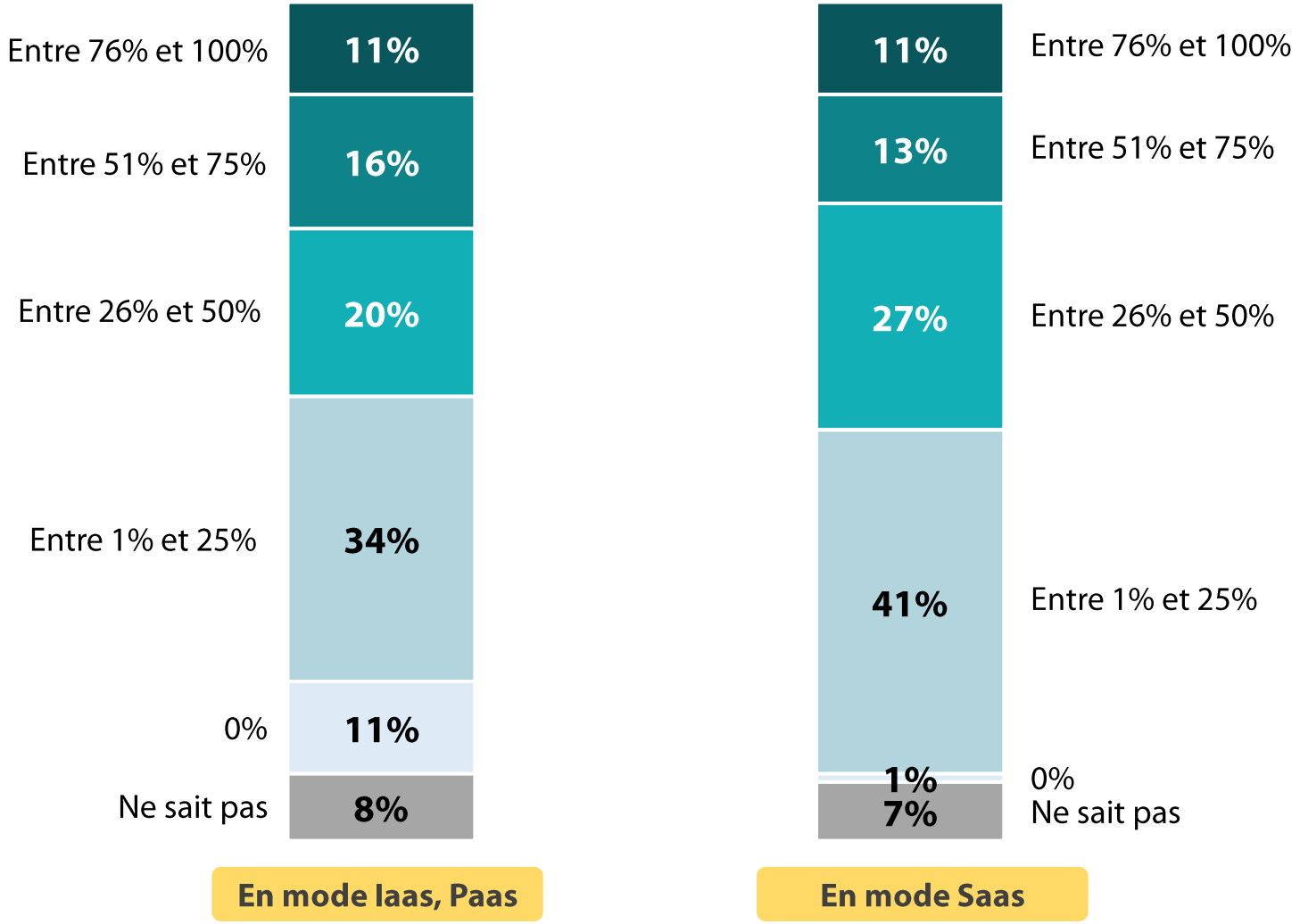
Que ce soit en mode Iaas / Pass ou en mode Saas, le cloud représente moins de 50% du SI dans la majorité des entreprises (65% pour le mode Iaas / Pass et 69% pour le mode Saas)

456 personnes

Nouvelle question en 2023

Q20b. Quelle est la part d'adoption du Cloud dans votre SI, que ce soit en mode Iaas, Paas ou Saas ?

Base : ensemble



Les risques sur le contrôle des sous-traitants et des accès par les administrateurs restent les plus importants, les défauts de cloisonnement entre les différents clients de l'hébergeur sont de plus en plus problématiques, heureusement le niveau d'expertise augmente

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

Base : ensemble

Rappel classement 2022		% Un risque fort	
1		48%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
2		43%	**Difficulté de contrôler les accès par des administrateurs de l'hébergeur**
		40%	Mauvaise visibilité de l'inventaire des ressources qu'il y a dans le cloud
4		39%	Stockage des données en France/Europe mais assuré et/ou opéré par des prestataires étrangers où la loi du pays d'origine s'applique également
		37%	Stockage des données dans des datacenters à l'étranger, hors du droit français
	+10	37%	Défaut de cloisonnement entre les différents clients de l'hébergeur
5		36%	Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
Item modifié		36%	Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur (l'hébergeur gère les clés de déchiffrement)
3	-9	34%	Expertise encore trop rare, attendue de la part des architectes et des administrateurs
		33%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur
		33%	Non-effacement des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
		32%	Confidentialité des données vis-à-vis de l'hébergeur
		32%	Maîtrise difficile de l'utilisation qui en est faite par les salariés de votre entreprise
		30%	Forte fréquence des nouvelles versions mises en ligne avec des potentielles évolutions non contrôlées des principes ou paramètres de sécurité
		30%	Attaque par rebond depuis l'hébergeur
		29%	Non-effacement des données au cours de l'usage, les suppressions et purges opérées par le client n'étant pas réellement effectives
		27%	Propagation systémique des attaques et erreurs humaines qui surviendraient au niveau de l'hébergeur
		27%	Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant du Cloud
		25%	Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
		23%	Traitement et exploitation des données par l'hébergeur à l'insu de ses clients
		16%	Piégeage d'une application hébergée

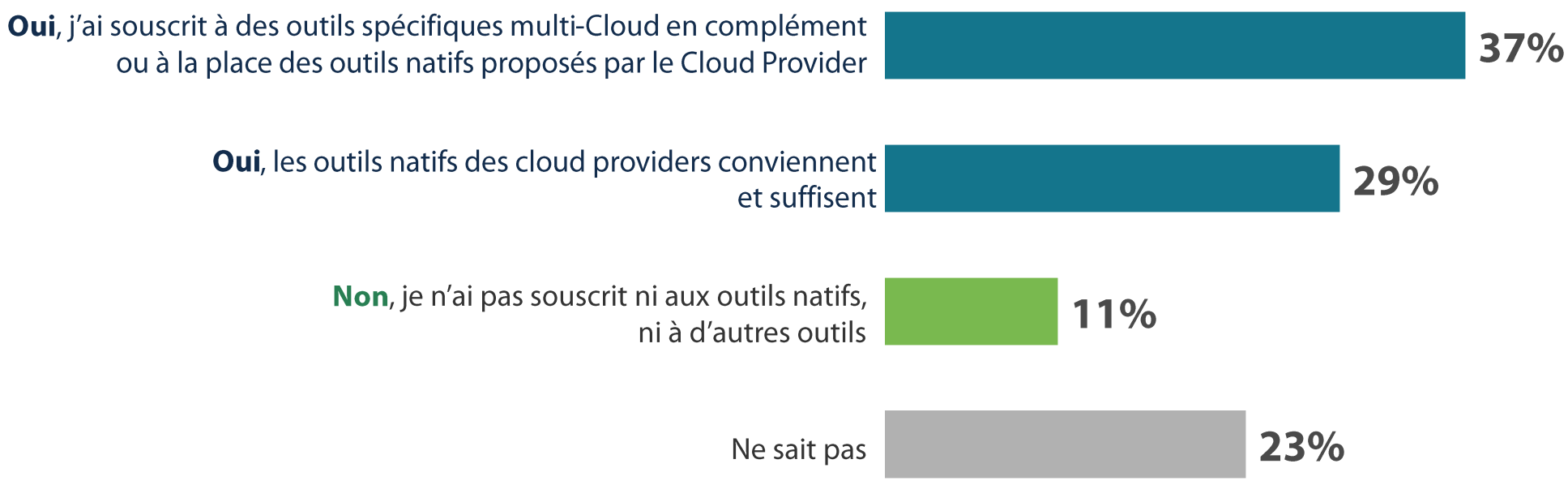
Deux tiers des RSSI estiment que la sécurisation des données dans le Cloud nécessite des outils spécifiques

456 personnes

Nouvelle question en 2023

Q22b. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble

… 66% estiment que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques



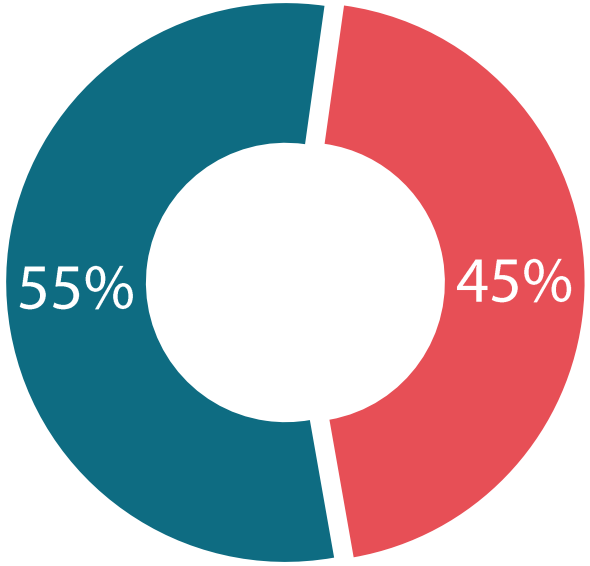
Une entreprise sur deux (55%) s'intéresse aux initiatives en matière de souveraineté et de Cloud de Confiance

456 personnes

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

Souveraineté et Cloud de Confiance



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

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

04

Le développement de l’IA et le renforcement de la réglementation obligent les entreprises à s’adapter

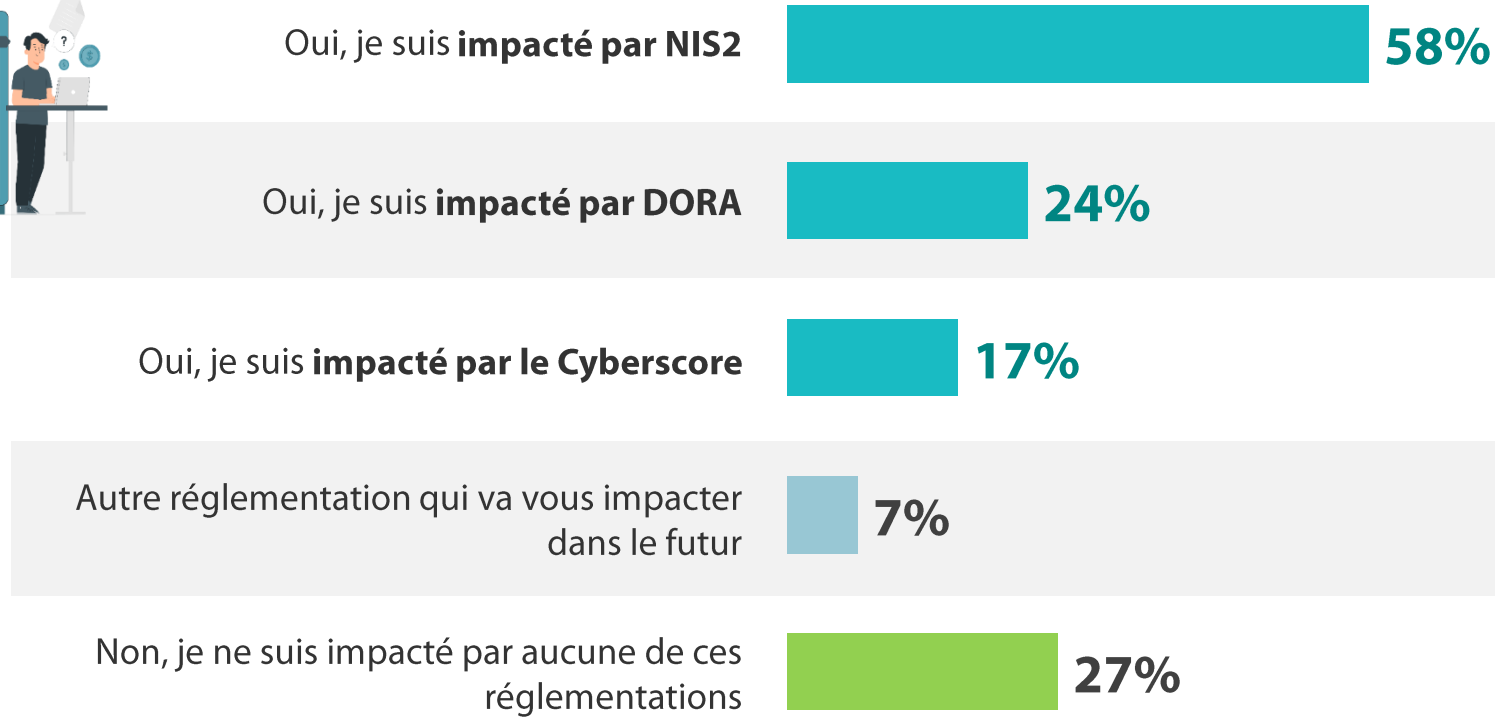
La grande majorité des entreprises se retrouve impactée par le renforcement de la réglementation, et plus particulièrement par la directive NIS2

456 personnes

Nouvelle question en 2023

Q37. La réglementation se renforce. Etes-vous impactés ?

Base : ensemble – Plusieurs réponses possibles



72%

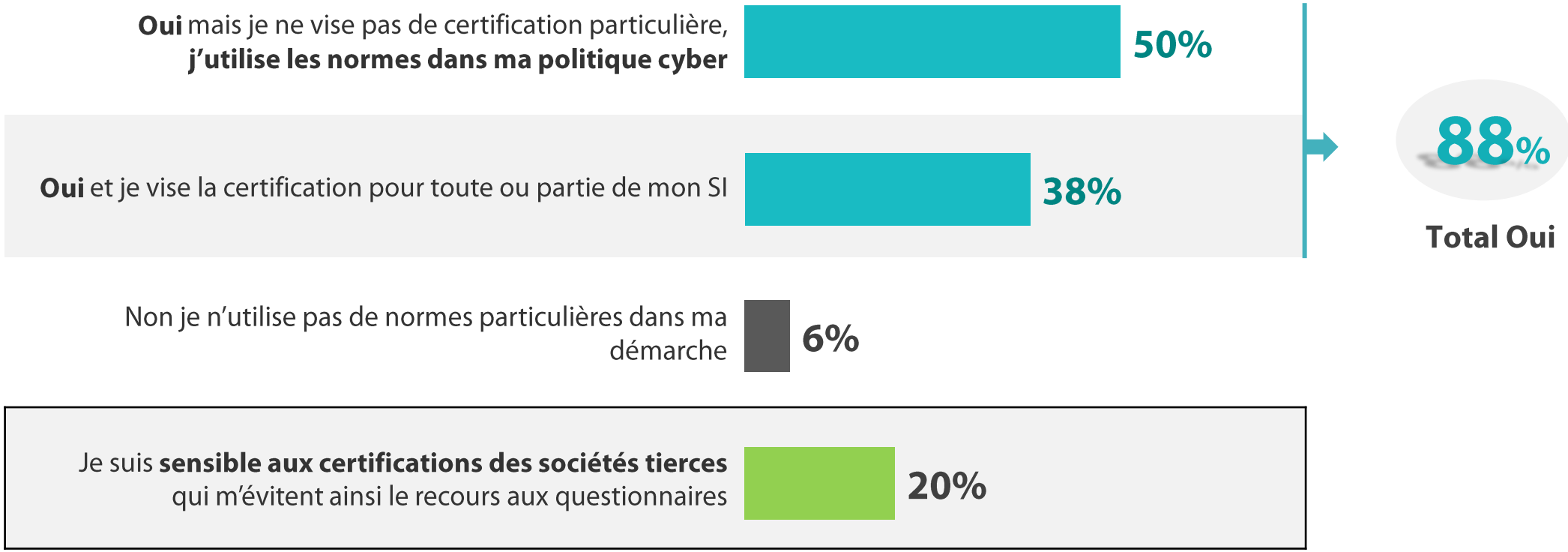
Impactés par au moins une réglementation

La très grande majorité des entreprises intègre les normes dans le quotidien de leur métier, et les certifications sont relativement recherchées en interne comme pour les tiers

456 personnes

Nouvelle question en 2023

Q38. Les normes font parties intégrantes du paysage cyber. Y êtes-vous sensibles ?
Base : ensemble



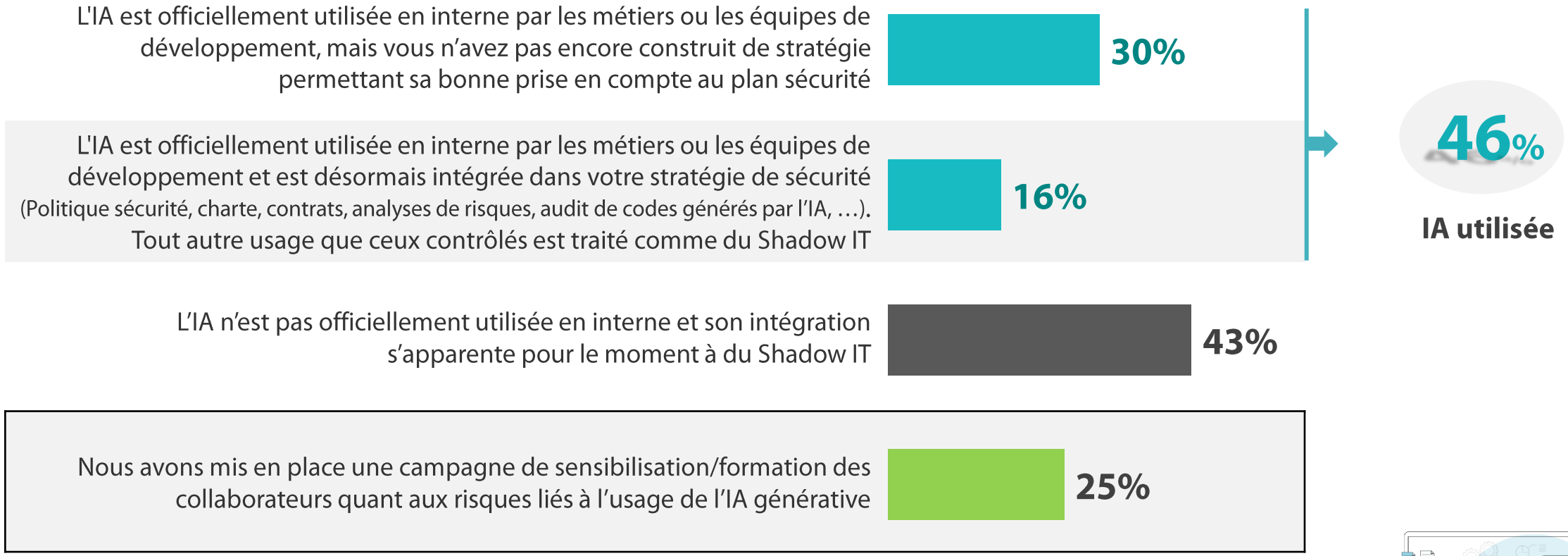
L’IA est désormais utilisée dans la moitié des SI, pour autant l’intégration de l’IA dans la stratégie de sécurité est encore peu développée (16%)

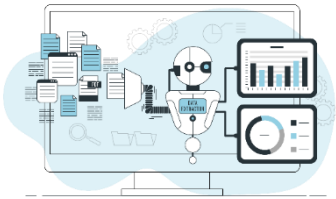
456 personnes

Nouvelle question en 2023

Q39. L’IA, déjà plus ou moins utilisée dans certaines solutions cyber, a fait une entrée fracassante 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



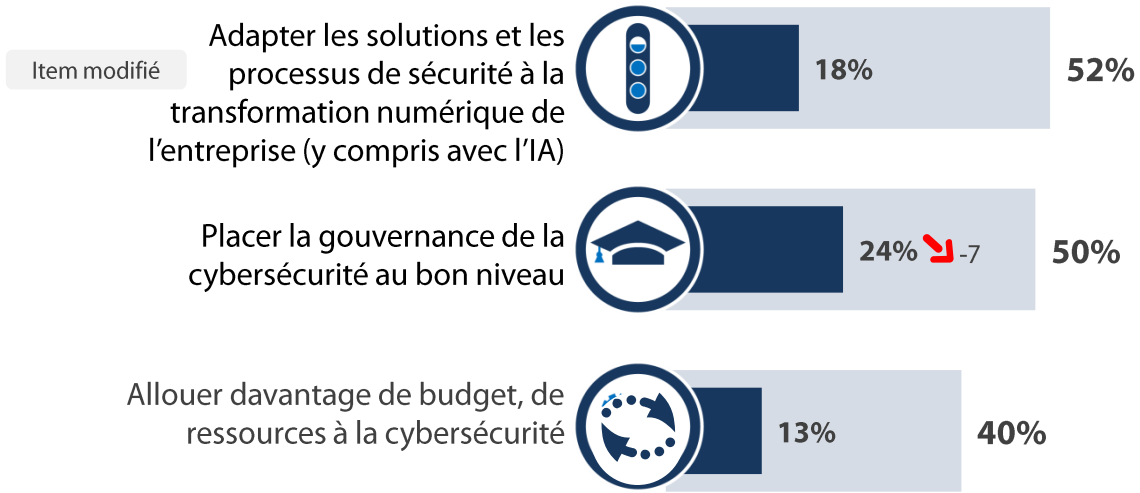


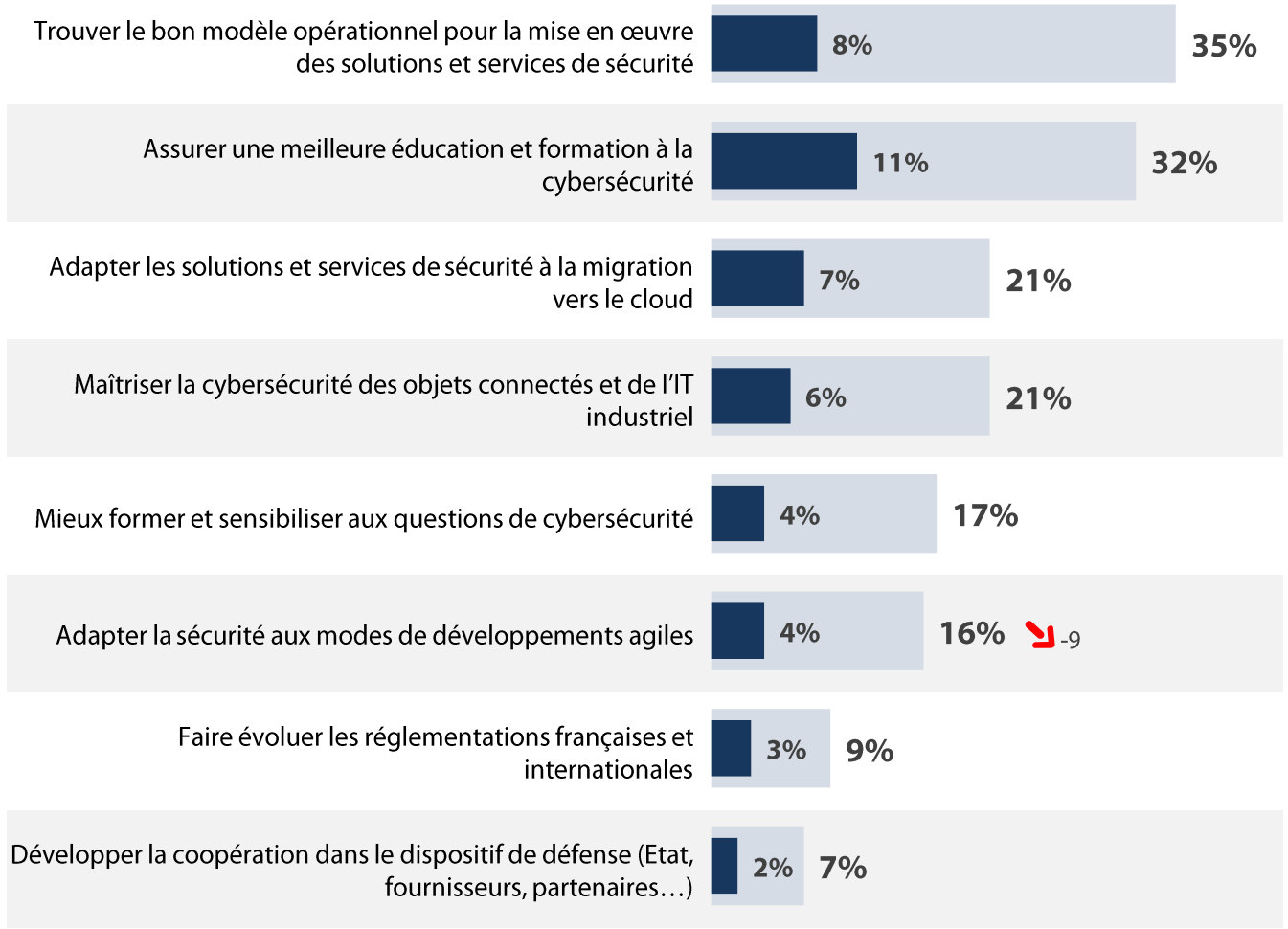
Le développement de l'IA fait de l'adaptation des solutions et des processus de sécurité le premier enjeu des entreprises

456 personnes

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

TOP3 des enjeux



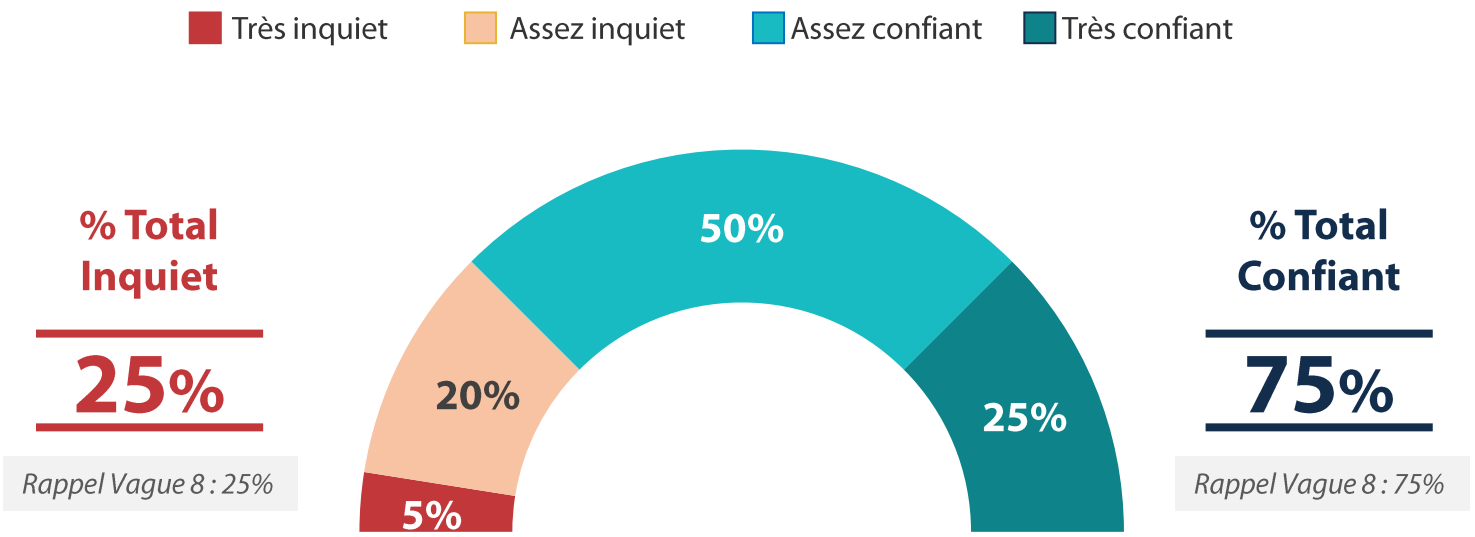


La cybersécurité est perçue comme un sujet important, pris en compte au sein du COMEX est à un niveau identique à 2022

456 personnes

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

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

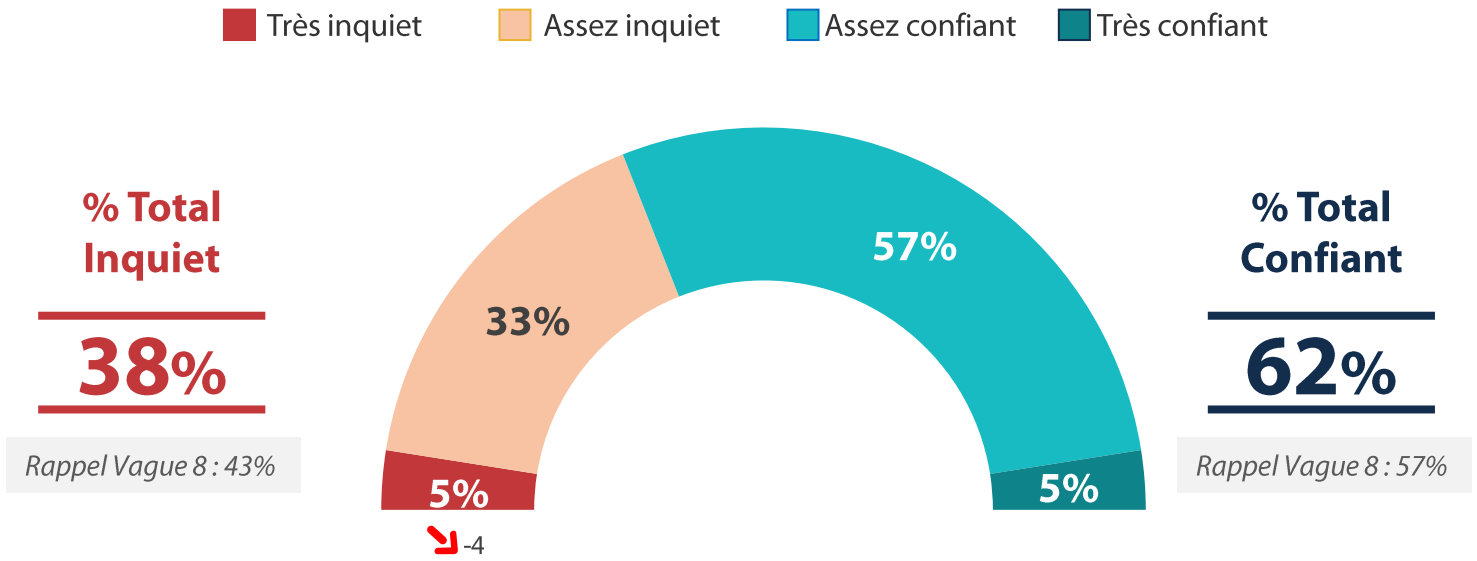


Les entreprises se sentent davantage préparées pour faire face aux cyber-risques, la part de « très inquiets » diminue cette année

456 personnes

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

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



Plus de la moitié des entreprises prévoit d'augmenter les effectifs pour lutter contre les cyber-risques, ces effectifs seront principalement destinés à la cybersécurité opérationnelle

456 personnes

Q17. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?
Base : ensemble

53% prévoient d'augmenter les effectifs alloués à la protection contre les cyber-riques

d'**augmenter les effectifs** alloués à la gouvernance de la protection contre les cyber-risques

Item modifié

d'**augmenter les effectifs** alloués à la cybersécurité opérationnelle de la protection contre les cyber-risques

Nouvel item

Et si la grande majorité des entreprises compte acquérir de nouvelles solutions techniques destinées à la cybersécurité, elles sont moins nombreuses à avoir l'intention d'augmenter les budgets

456 personnes

Q17. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ?
Base : ensemble

d'**augmenter les budgets** alloués à la protection contre les cyber-risques

d'**acquérir de nouvelles solutions techniques** destinées à la cybersécurité

La synthèse

Synthèse (1/3)

Un nombre de cyberattaques orienté à la hausse, boosté par une augmentation des dénis de service

Pour la première fois depuis 4 ans, le nombre d'entreprises ayant constaté une cyberattaque est orienté à la hausse (49%, +4 points).

Les scénarios reposant sur la manipulation sont en baisse. Le phishing, spear phishing et smishing réunis restent le principal vecteur d'attaque, mais diminuent sensiblement (60%, -14 points), tout comme l'arnaque au président (28%, - 13 pts).

A l'inverse, il est à noter l'augmentation des attaques en déni de service cette année (34%, +11 pts) faisant du déni de service (30%, +11 pts) l'une des principales conséquences des cyberattaques avec le vol de données (31%). En lien avec cela, l'indisponibilité du site web a été l'un des principaux impacts des cyberattaques sur le business des entreprises (22%, +9 pts) avec une perturbation de la production (24%).

Il est à noter une stabilisation des ransomwares et un risque jugé significatif de cyberespionnage.

L'EDR plébiscité et plus généralement des solutions du marché jugées efficaces pour des entreprises qui développent également un peu plus leur préparation à la réponse aux incidents.

87% des RSSI trouvent que les solutions de sécurité disponibles sur le marché sont adaptées à leur entreprise. Plus de 15 solutions ou services de sécurité sont déployés en moyenne dans les entreprises selon des modèles opérationnels variables entre l'interne, l'externe ou un mode hybride.

En parallèle, 57% des entreprises ont mis en place un programme d'entraînement à la cyber-crise avec des exercices qui sont réalisés périodiquement (28%, +9 pts).

L'EDR est la solution de sécurité la plus déployée dans les entreprises (90%, +9 points), avec les pare-feux, leur efficacité est davantage confirmée cette année par les RSSI (92%, +6 pts).

Les entreprises restent ouvertes à l'innovation dans le domaine cyber.

Synthèse (2/3)

Des usages numériques risqués, malgré des salariés plus conscients des enjeux

Les différents usages numériques des salariés représentent toujours autant un risque selon les RSSI, en particulier le Shadow IT (82%) et la gestion des partages de données par les utilisateurs eux-mêmes (78%).

La mise en place de métriques pour mesurer la participation aux formations / sensibilisations (84%) est largement déployée, mais on ne sait toujours pas bien en mesurer l'efficacité et évaluer la maturité des salariés sur le sujet de la cybersécurité, bien que ceux-ci semblent prendre plus de précautions que celles recommandées a minima (24%, +7 pts).

Un quart des entreprises assurées a déjà fait appel à leur cyberassurance

7 entreprises sur 10 ont aujourd'hui souscrit à une cyberassurance et un quart d'entre elles l'ont déjà utilisé dans le cadre d'une cyberattaque.

Par ailleurs, 59% des entreprises ont déjà porté plainte suite à une cyberattaque, parmi elles 1 plainte sur 5 a permis d'identifier et/ou d'interpeller les attaquants (un score en légère augmentation de 5%).

La confiance a baissé envers les agences de notation dont il est estimé que les résultats sont très partiels.

Des données Cloud à sécuriser

Les usages numériques autour du Cloud constituent un risque important selon les RSSI, même si la part d'adoption du Cloud dans le SI est encore minoritaire, mais commence à être significative, que ce soit en mode Iaas / Paas ou en mode Saas. Heureusement, l'expertise sur la sécurité du cloud s'est développée.

Deux tiers des RSSI estiment ainsi que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques.

Synthèse (3/3)

La réglementation, les normes et l'utilisation de l'IA poussent les entreprises à agir

7 entreprises sur 10 se disent aujourd'hui impactées par au moins une réglementation (NIS2, DORA, Cyberscore).

88% des entreprises estiment que les normes font partie intégrante du paysage cyber et se tournent volontiers vers des certifications en interne ou qu'elles demandent à leurs tiers.

Près de la moitié (46%) des RSSI constatent une utilisation de l'IA en interne, mais seulement 16% l'ont déjà intégrée dans leur stratégie de sécurité. Une utilisation qui les pousse à définir comme premier enjeu pour l'avenir, l'adaptation de leurs solutions à la transformation numérique de l'entreprise (52%).

Les entreprises se montrent légèrement moins inquiètes, quant à leur capacité à faire face aux cyber-risques (38%, - 5 pts), la part des « très inquiets » est pratiquement divisée par deux passant de 9% à 5%.

Au final, plus de la moitié des entreprises prévoit d'augmenter les effectifs alloués à la protection contre les cyber-risques et la très grande majorité (78%) compte acquérir de nouvelles solutions techniques. Enfin, les budgets pour faire face aux cyber-risques devraient rester stables.

WE ARE DIGITAL !

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.

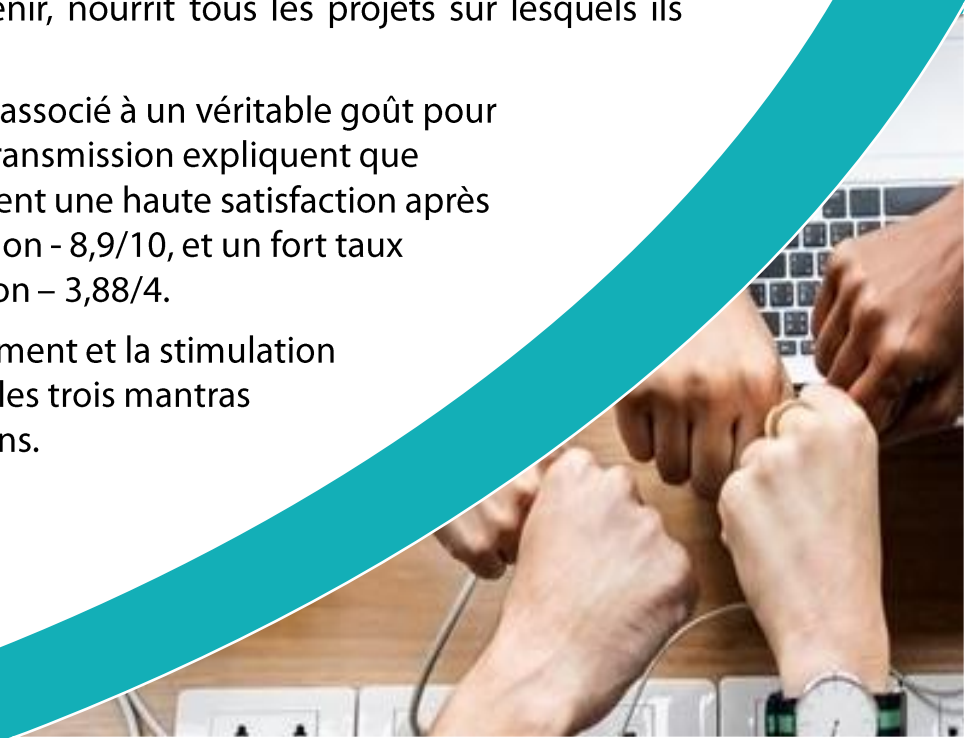
RENDRE LE MONDE INTELLIGIBLE POUR AGIR AUJOURD'HUI ET IMAGINER DEMAIN

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.



RESTONS CONNECTÉS !

www.opinion-way.com

Envie d'aller plus loin ?

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

newsletter !

"opinionway

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN