“opinionway pour CESIN

Baromètre de la cyber-sécurité des entreprises

Vague 7 – Janvier 2022

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

afaq ISO 20252 Étude marketing et d'opinion

ESOMAR'21 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 de grandes entreprises.

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

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

La méthodologie

La méthodologie

Echantillon de **282 membres du CESIN,** a 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 24 novembre au 21 décembre 2021**.

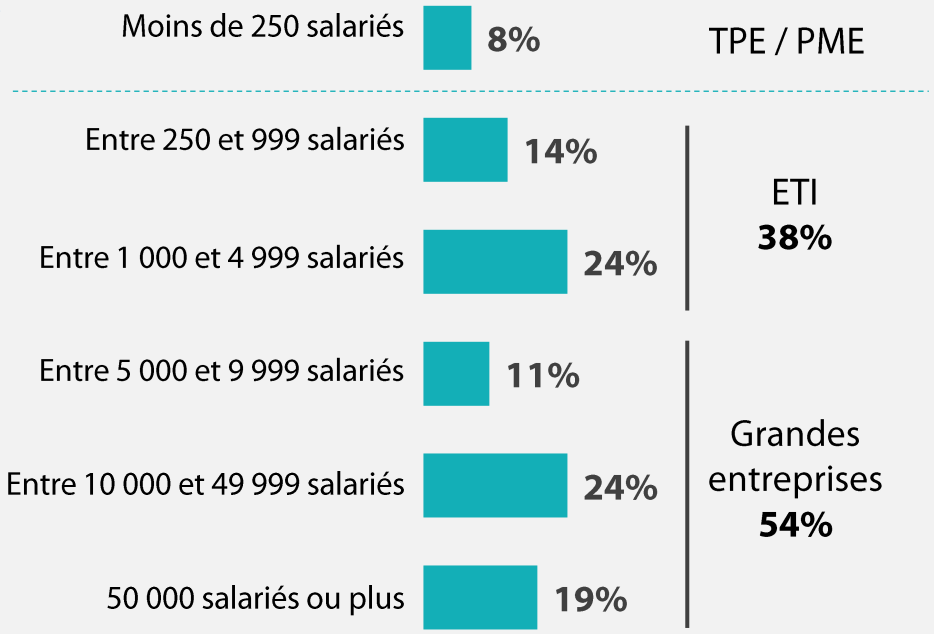
OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la **norme ISO 20252**

Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 1, 6 à 5,9 point au plus pour un échantillon de 280 répondants.

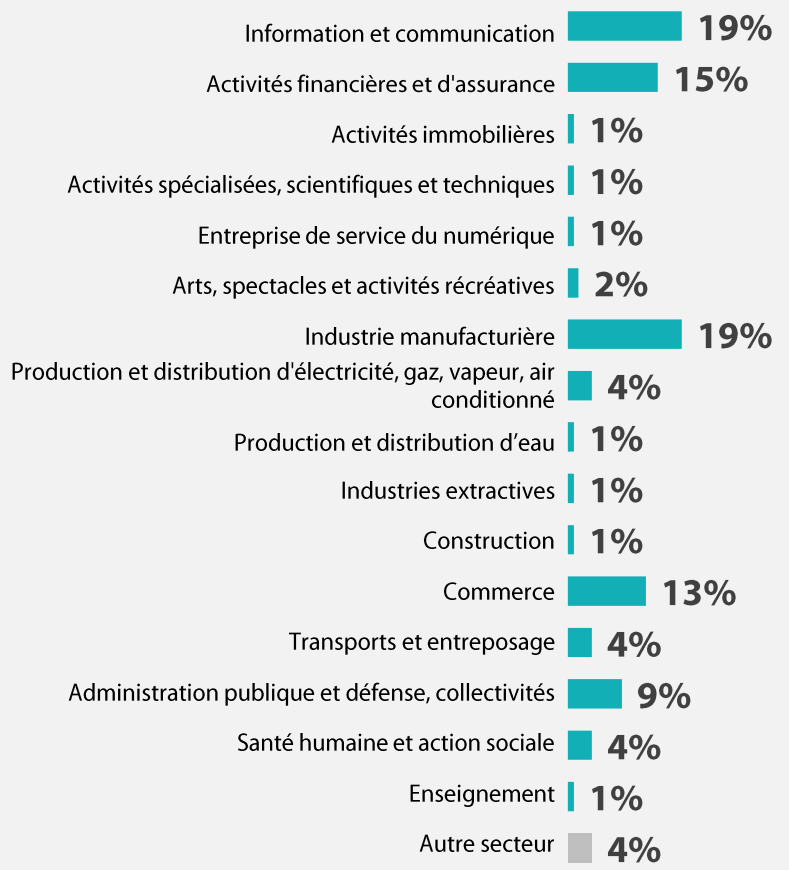
Le profil des répondants

Un échantillon qui reflète la structure réelle des entreprises

Nombre de salariés de l'entreprise



Secteur d'activité de l'entreprise



La synthèse

Des entreprises touchées par les attaques, mais qui ont été très réactives face aux évolutions du monde du travail…

54% des entreprises déclarent avoir subi au moins une attaque en 2021

Plus d'une entreprise sur 2 est donc encore touchée, un chiffre en légère baisse par rapport aux vagues précédentes (57% en 2020 et 65% en 2019), ce qui montre que les dispositifs mis en place progressivement portent leur fruit. **On note pourtant dans la réalité que leur ampleur et leur virulence ne cesse d'augmenter.**

Les vecteurs d'attaques les plus répandues restent **le phishing** (73%) et **l'exploitation des failles** (53%). À noter **l'augmentation année après année des attaques indirectes par rebond via un prestataire** (21% vs 16% en 2019), ce qui souligne la dépendance grandissante des entreprises envers leurs fournisseurs externes. A souligner que l'usurpation d'identité (32%) est cette année la principale conséquence de ces attaques.

Au final, **6 entreprises sur 10 ayant vécu une attaque ont été impactées sur leur business**, principalement en raison d'une perturbation de la production (21%) ou par la compromission d'information (14%).

La crise sanitaire et le développement du télétravail ont conduit les entreprises à revoir les dispositifs de sécurité mis en place. Ainsi, la plupart d'entre elles **ont sensibilisé plus fortement leurs collaborateurs** (70%). Une forte majorité (63%) a également généralisé le recours à **l'authentification multi-facteurs.**

Si le nombre d'entreprises ayant subi une attaque de type ransomware est équivalent à l'année dernière (18% vs 19% en 2020), les entreprises ont décidé de renforcer certains dispositifs, tout d'abord **la sensibilisation**, mais surtout **le déploiement d'un EDR** (+16 pts par rapport à 2020) et **le durcissement de l'AD** (+9 points).

…et qui se protègent mieux et de plus en plus

La grande majorité des entreprises trouvent que **les solutions présentent sur le marché sont adaptées à leur entreprise** (85%). Le nombre moyen de solutions mises en place (+ de 10) reste élevé. Nous retrouvons en tête l'utilisation du **VPN** (91%) et **du proxy** (81%). **À noter la progression importante des solutions d'EDR (68%/+17 pts) et de chiffrement (56%/+7 pts).**

En termes de détection, **les entreprises sont relativement bien dotées en matière de SOC** : qu'il soit interne, externalisé ou hybride, ce service est désormais incontournable dans le dispositif de sécurité des entreprises.

7 entreprises sur 10 estiment être préparées en termes de moyen de prévention et de moyens de détection (+13 pts). Pour autant, 54% seulement, se disent prêtes à répondre à l'attaque et 41% à se reconstruire après.

Des entreprises qui se sentent donc mieux préparés et qui **mettent plus systématiquement en place des programmes d'entraînement** (44% / +11pts).

7 entreprises sur 10 possèdent une cyber-assurance, si plus de la moitié compte la renouveler, une entreprise sur 10 environ hésite à le faire. Par ailleurs, le recours aux agences de notation par les cyber-assureurs est noté négativement par une large majorité des répondants (54%). De plus, il faut souligner, un avis mitigé auprès des entreprises ayant eu recours à la cyber-assurance dans le cadre d'une cyber-attaque.

La moitié des entreprises ayant subi une attaque ont porté plainte et seulement 16% d'entre elles ont vu aboutir leur démarche par l'identification et/ou l'interpellation des attaquants.

Une sensibilisation des salariés toujours accrue

Les collaborateurs sont également mieux sensibilisés (82%, dont 24% qui sont tout à fait sensibilisés/ +11 pts), ils respectent également mieux les recommandations (70%) mais peinent à être proactifs et à prendre des précautions par eux-mêmes.

Au final, **une hausse de la protection des entreprises qui permettent d'atténuer les risques perçus par les usages numériques des salariés** : le recours massif au service cloud non approuvé est perçu comme un risque élevé pour ¾ des entreprises contre 84% en 2020, le risque lié au recours au télétravail est, cette année, jugé moins prégnant : 29% vs 41% en 2020.

Le Cloud, sécurisé, mais nécessitant des outils spécifiques

La non-maîtrise de la chaîne de sous-traitance de l'hébergeur (48%), les difficultés de contrôles des accès par les administrateurs de l'hébergeur (43%) sont les 2 principaux facteurs de risques émis en ce qui concerne l'utilisation du Cloud. On note également le risque important notés pour les nouveaux items : la rareté de l'expertise parmi les architectes et les administrateurs (40%) et la mauvaise visibilité de l'inventaire des ressources dans le cloud (38%)

Plus de 8 RSSI sur 10 estiment encore que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques (86%) et notamment des outils en complément de ceux proposés par le Cloud Provider (63%).

Les entreprises face aux enjeux de demain

Si **8 entreprises sur 10 sont confiantes quant à la prise en compte de la cybersécurité dans la stratégie**, elles ne sont pas pour autant moins inquiètes, la moitié environ est préoccupée par leur capacité à faire face aux cyber-risques.

Il faut souligner que le budget, nerf de la guerre de la lutte contre la cybercriminalité, évolue de manière significative année après année. La proportion d'entreprise consacrant moins de 5% de leur budget est en diminution au profit de celles qui y consacrent plus de 5%.

Autres tendances observées

Les entreprises restent sensibles aux menaces en lien avec le cyber espionnage qui est corroboré cette année par un nouvel item autour de la souveraineté**, 6 entreprises sur 10 se sentent préoccupées par les sujets de souveraineté et de Cloud de Confiance**.

Une tendance encourageante en matière d'innovation : les entreprises sont **de plus en plus nombreuses à faire appel à des solutions issues de start-ups**.

Les nouveaux concepts comme le **Zero Trust** ou encore le **SASE** font de timides entrées pour le moment dans l'agenda du RSSI : à peine un tiers des entreprises (30%) se sont réellement engagées dans une démarche Zero Trust tandis que seulement 13% des répondants ont appréhendé le concept SASE.

Concernant le risque grandissant observé ces dernières années sur la **sécurité de la supply chain**, **6 entreprises sur 10 estiment que ces questions peuvent trouver une issue**, à la condition d'une plus grande garantie du code et des labels

L’analyse

01

Des entreprises touchées par les attaques, mais qui commencent à réagir face aux évolutions du monde du travail…

Définition CESIN précisée de la cyber-attaque sur cette vague *

« La cyber-attaque, 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 cyber-attaque, 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.*

Plus de 5 entreprises sur 10 ont subi au moins une cyber-attaque cette année.

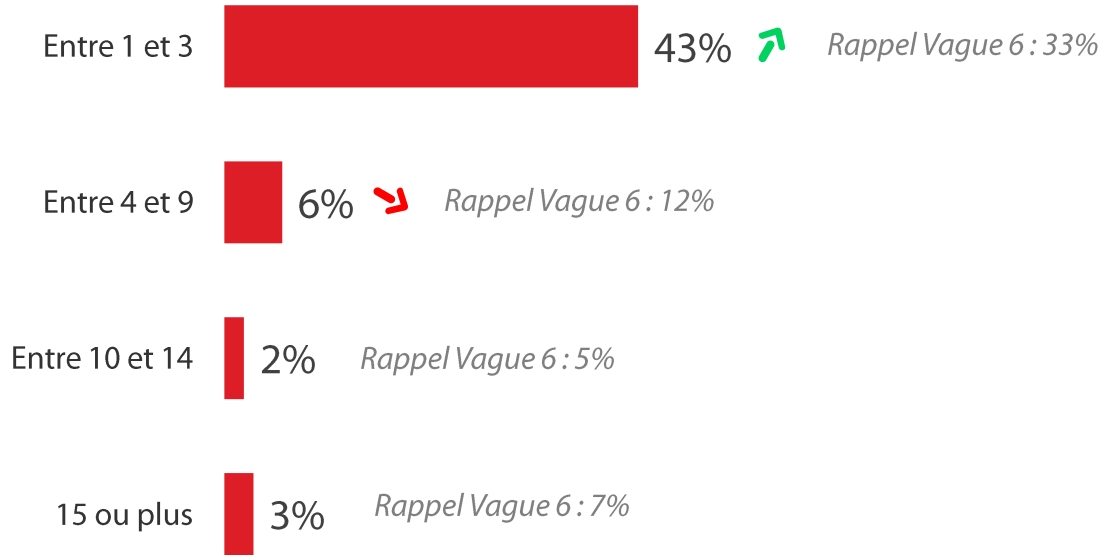
282 personnes

Q4. De façon générale, combien de cyber-attaques significatives ont été subies par votre entreprise au cours des 12 derniers mois ?
Base ensemble

54%

des entreprises ont constaté au moins une cyber-attaque

Rappel vague 5 : 57%
(mais la définition* a été précisée cette année)

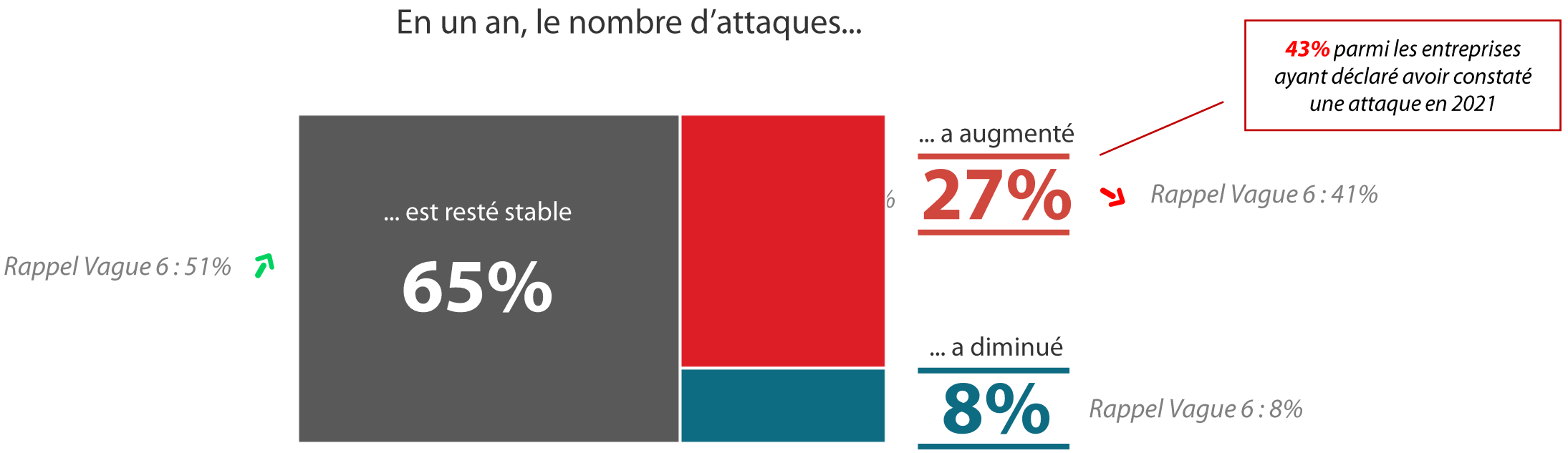


Évolution statistiquement significative par rapport à la vague précédente

Ce qui donne l'impression d'une stabilisation du nombre d'attaques, elles sont pourtant de plus en plus virulentes dans la réalité

282 personnes

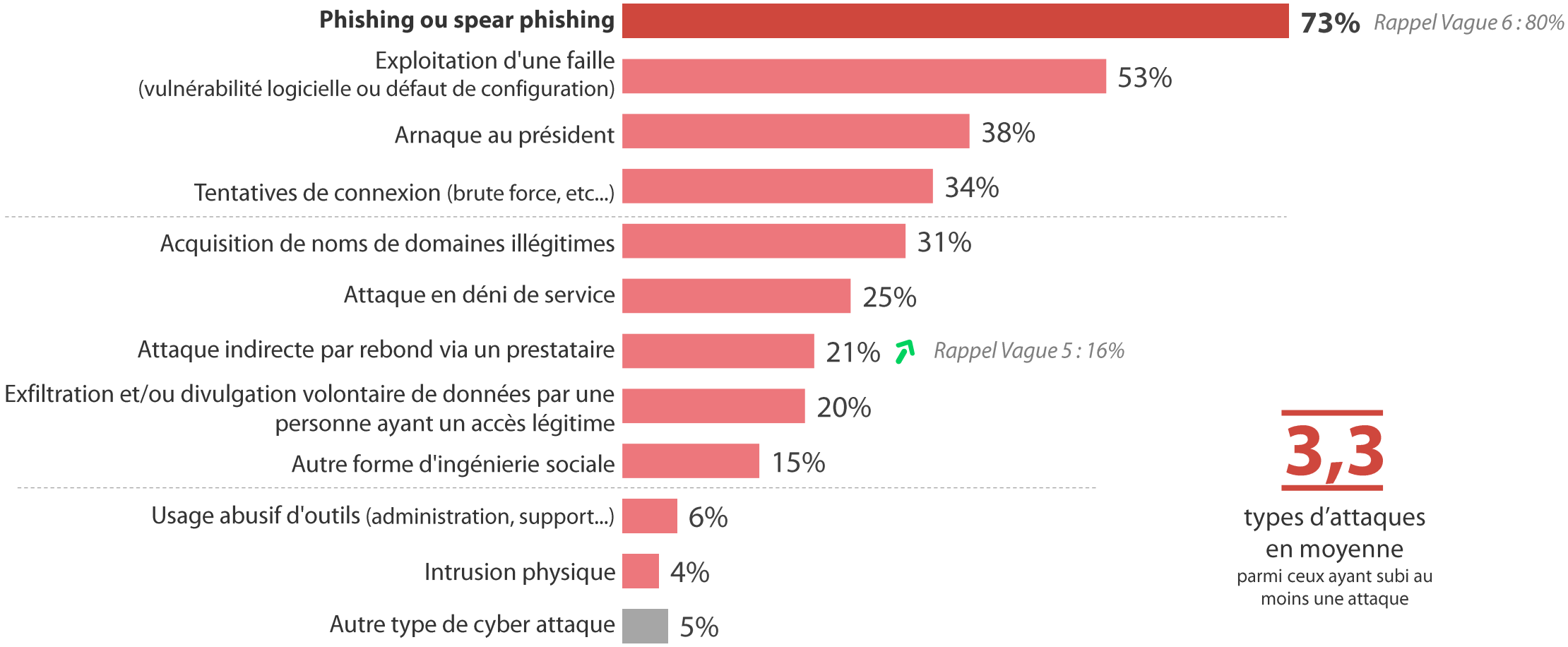
Q4bis. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ?
Base ensemble



Le phishing, reste le premier vecteur d'attaque dans les entreprises malgré une légère baisse. A noter, l'augmentation des attaques indirectes via un prestataire

152 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



3,3

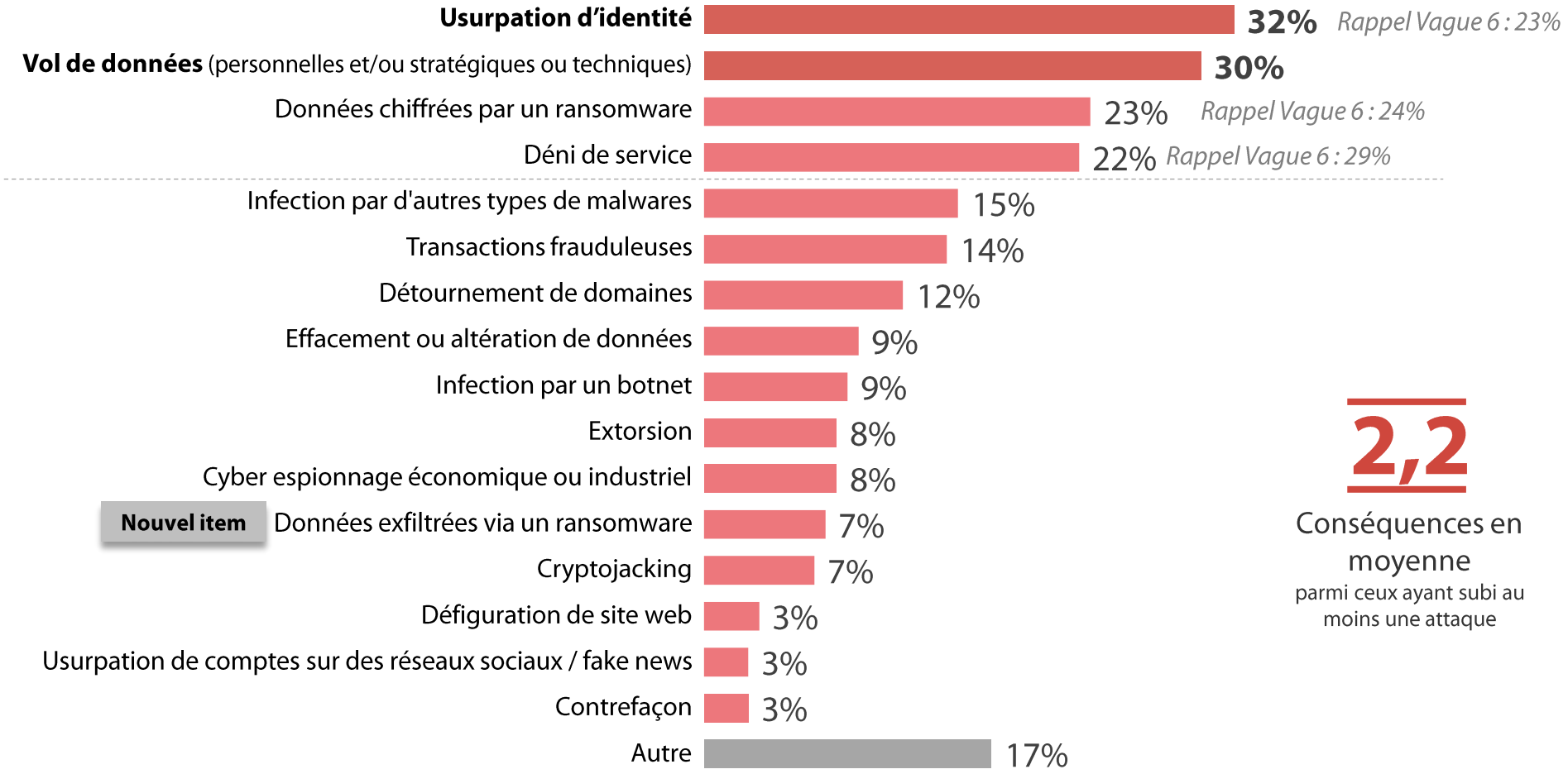
types d'attaques en moyenne
parmi ceux ayant subi au moins une attaque

L'usurpation d'identité est, cette année, la première conséquence des attaques. Le chiffrement des données par ransomware se stabilise

152 personnes

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

Base ont constaté une attaque / Plusieurs réponses possibles



2,2

Conséquences en moyenne

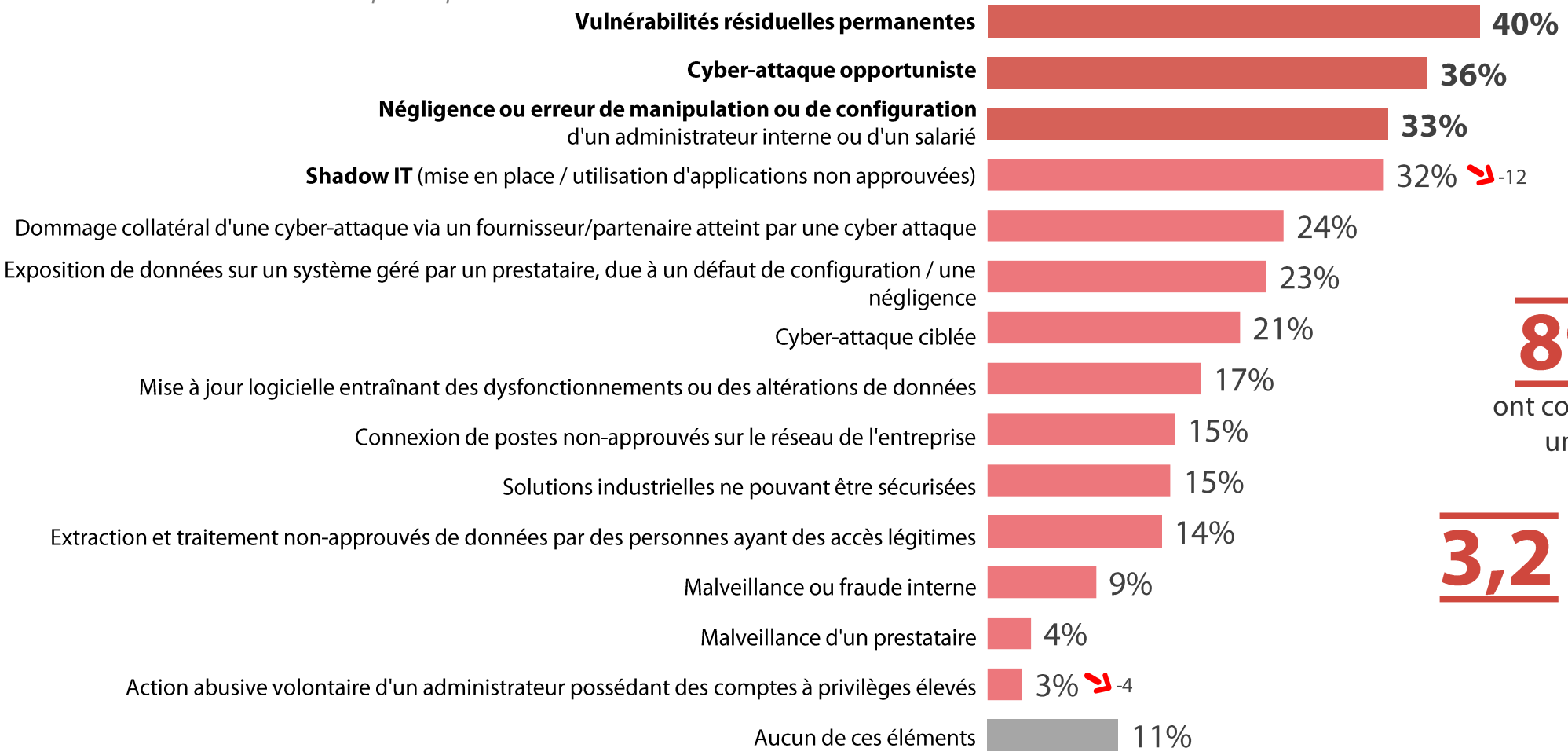
parmi ceux ayant subi au moins une attaque

Les efforts de sensibilisation au Shadow IT semblent porter leurs fruits cette année, les vulnérabilités résiduelles et les cyber-attaques opportunistes en tête des causes d'incidents

282 personnes

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

Base ensemble / Plusieurs réponses possibles



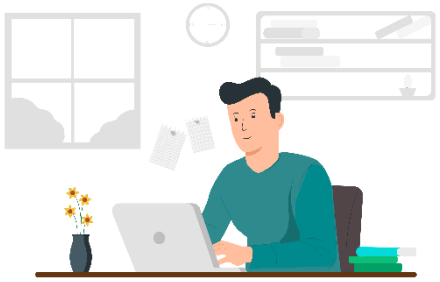
89%
ont connu au moins un élément

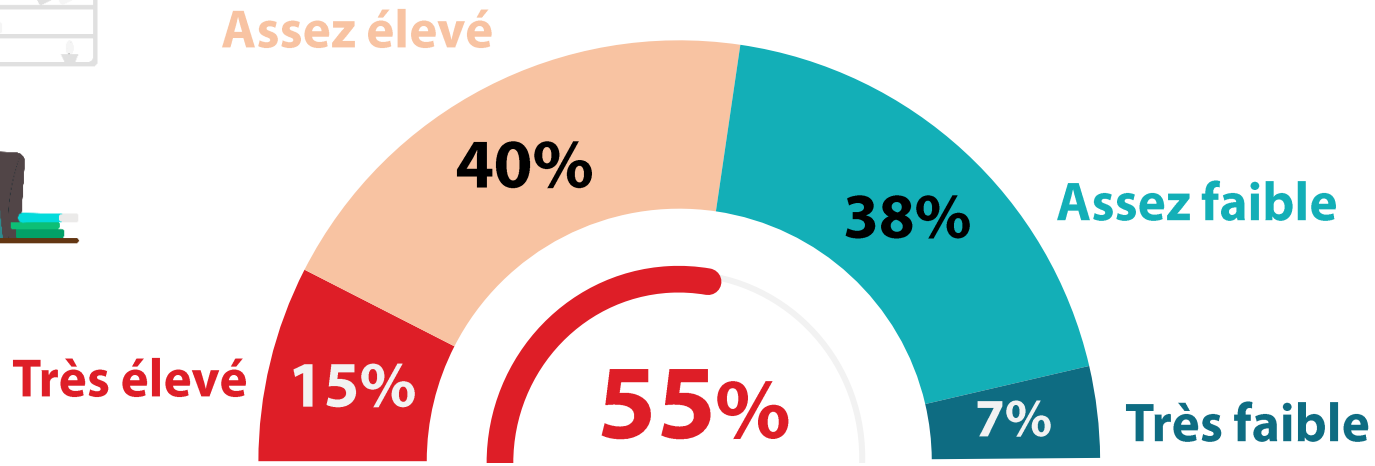
3,2 éléments en moyenne

Plus de la moitié des entreprises estiment que les menaces en lien avec le cyber-espionnage sont élevées, une opinion similaire à 2020

282 personnes

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





ESTIMENT UN NIVEAU ÉLEVÉ DES MENACES RELATIVES AU CYBER-ESPIONNAGE

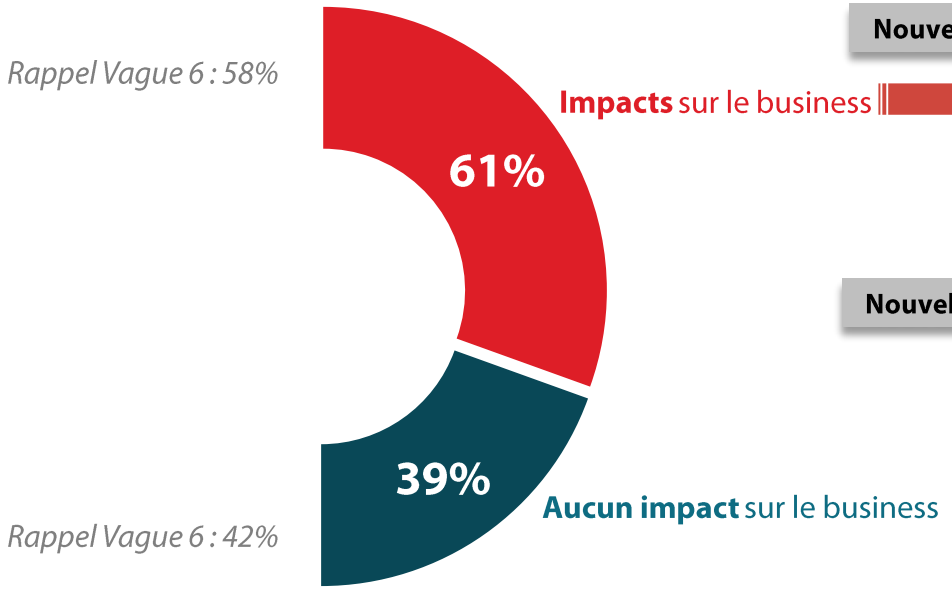
Rappel Vague 6 : 56%

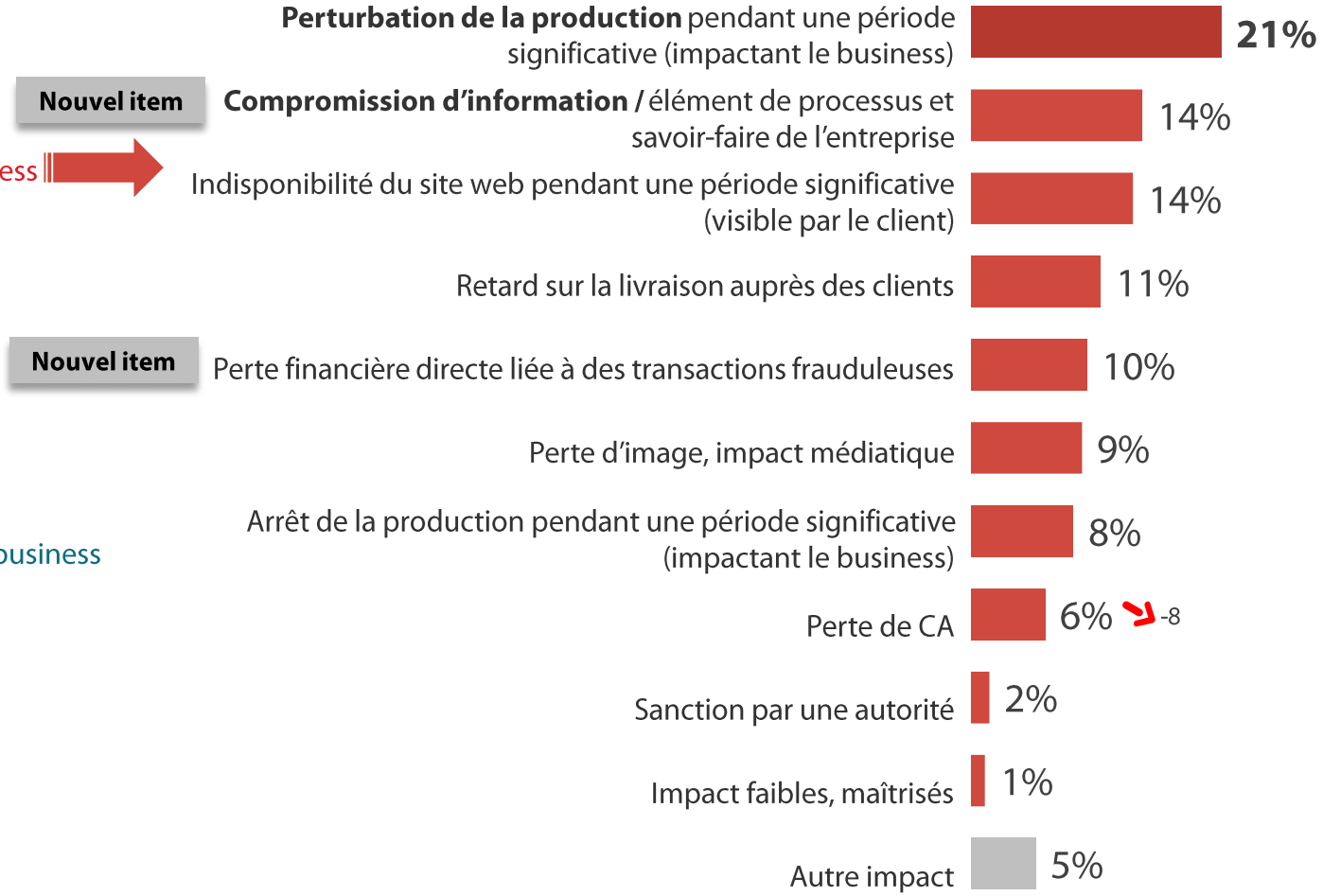
Comme les années précédentes, 6 entreprises sur 10 ayant constatées une attaque ont vu leur business directement impacté. A noter que la compromission d'information est l'un des impacts les plus importants

259 personnes

Q7. Quel a été l'impact des cyber-attaques sur votre business ?

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





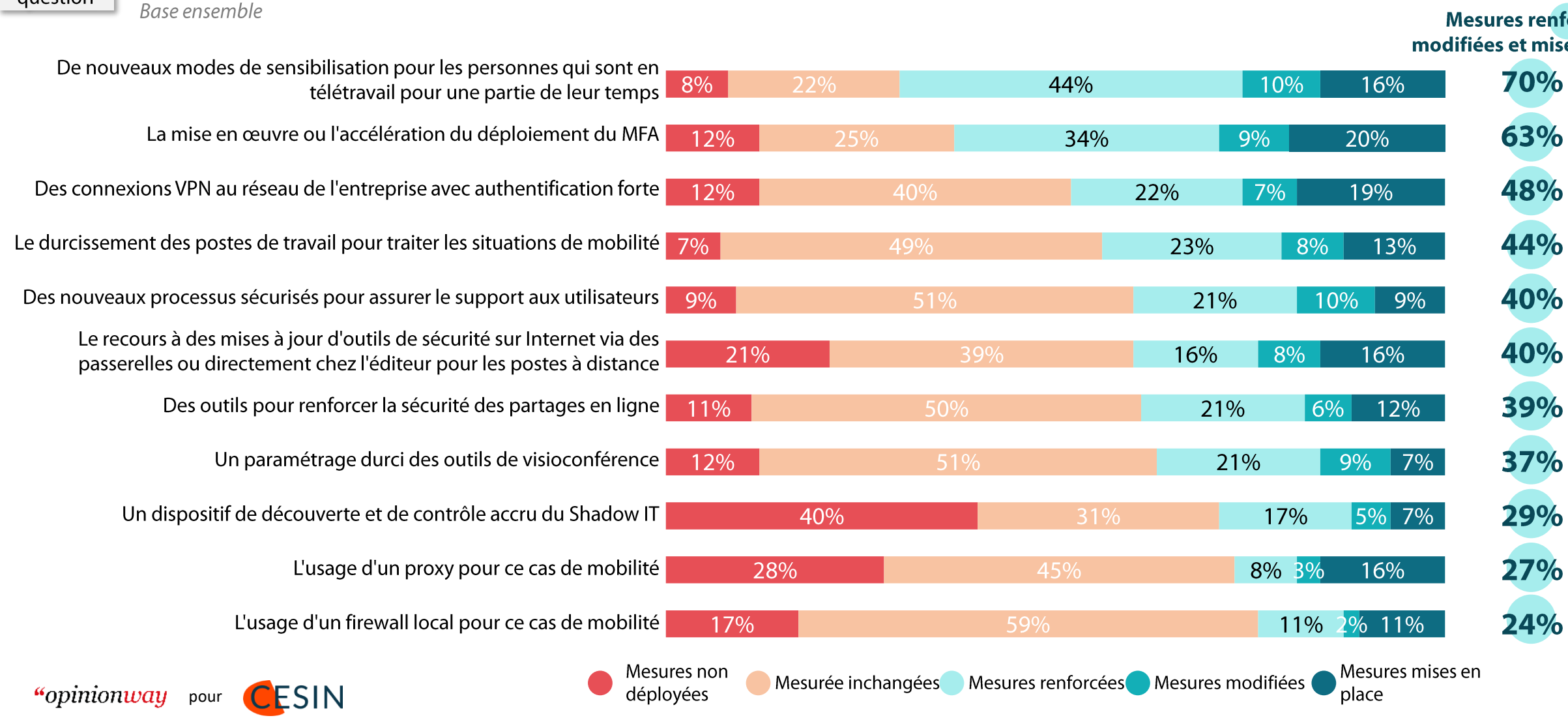
La sensibilisation et l'authentification multi-facteurs ont été les premiers recours au développement du télétravail, à noter qu'un grand nombre des autres mesures ont été renforcées

282 personnes

Nouvelle question

Q29. La crise sanitaire a installé durablement des nouveaux modes de travail qui ont conduit les entreprises à mettre en place, à renforcer ou à modifier certains dispositifs de sécurité. Quelles mesures ont été mises en place, modifiées ou renforcées, dans le contexte de votre entreprise ?

Base ensemble



Zoom sur…

Le ransomware

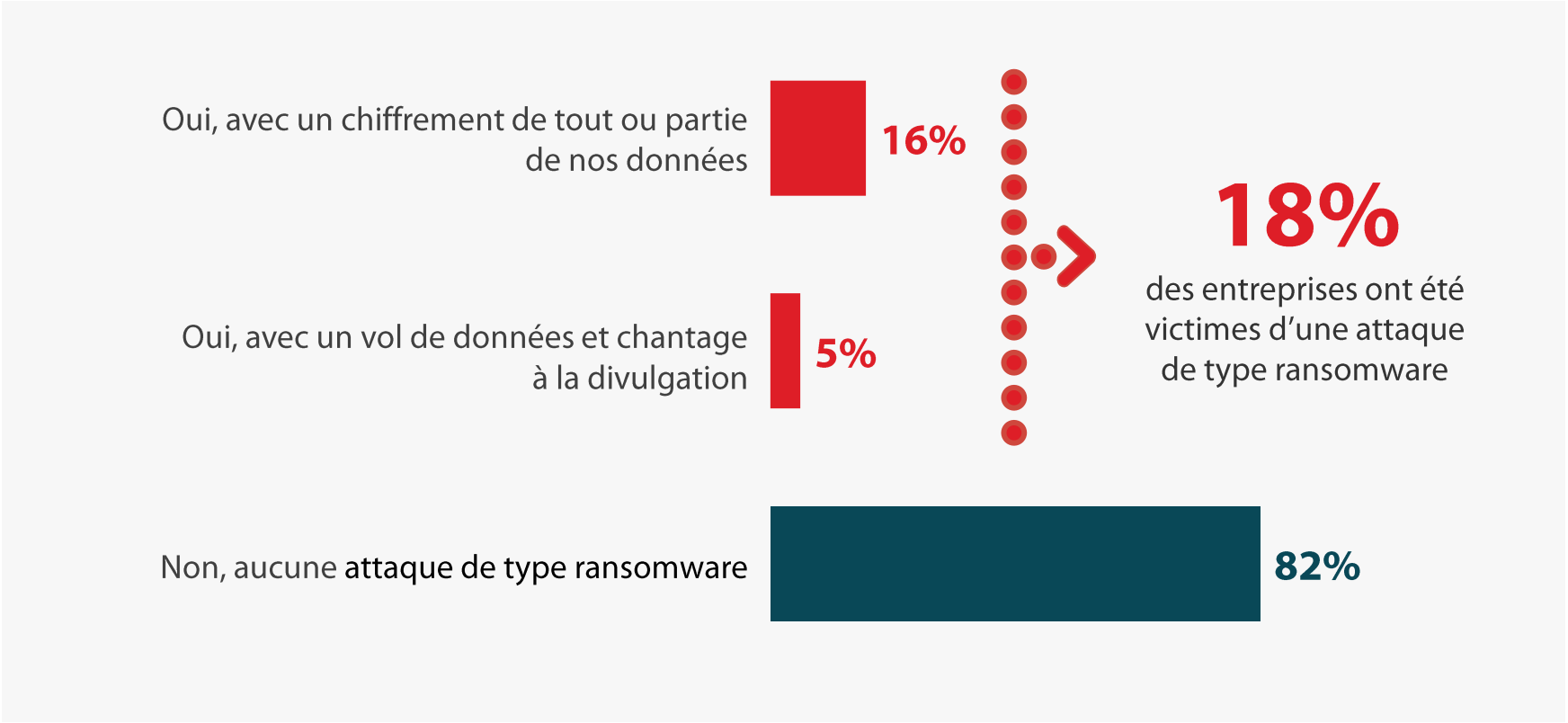
Similairement à 2020, 1 entreprise sur 5 a subi une attaque de type ransomware

282 personnes

L'année 2021 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



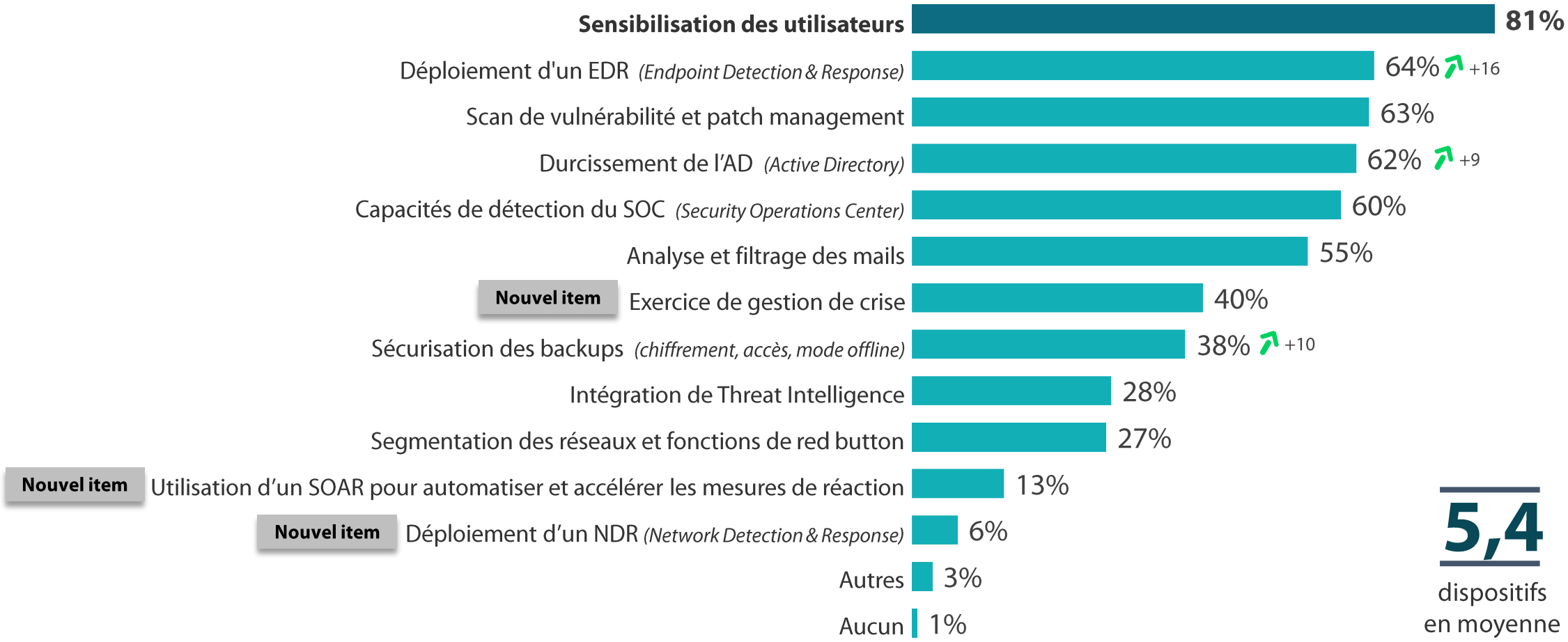
Rappel Vague 6 : 19%

Les entreprises, plus conscientes de la menace du ransomware, se préparent mieux, notamment avec le déploiement des EDR et le durcissement de l'AD

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

Base ensemble / Plusieurs réponses possibles

282 personnes



5,4
dispositifs
en moyenne

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

02

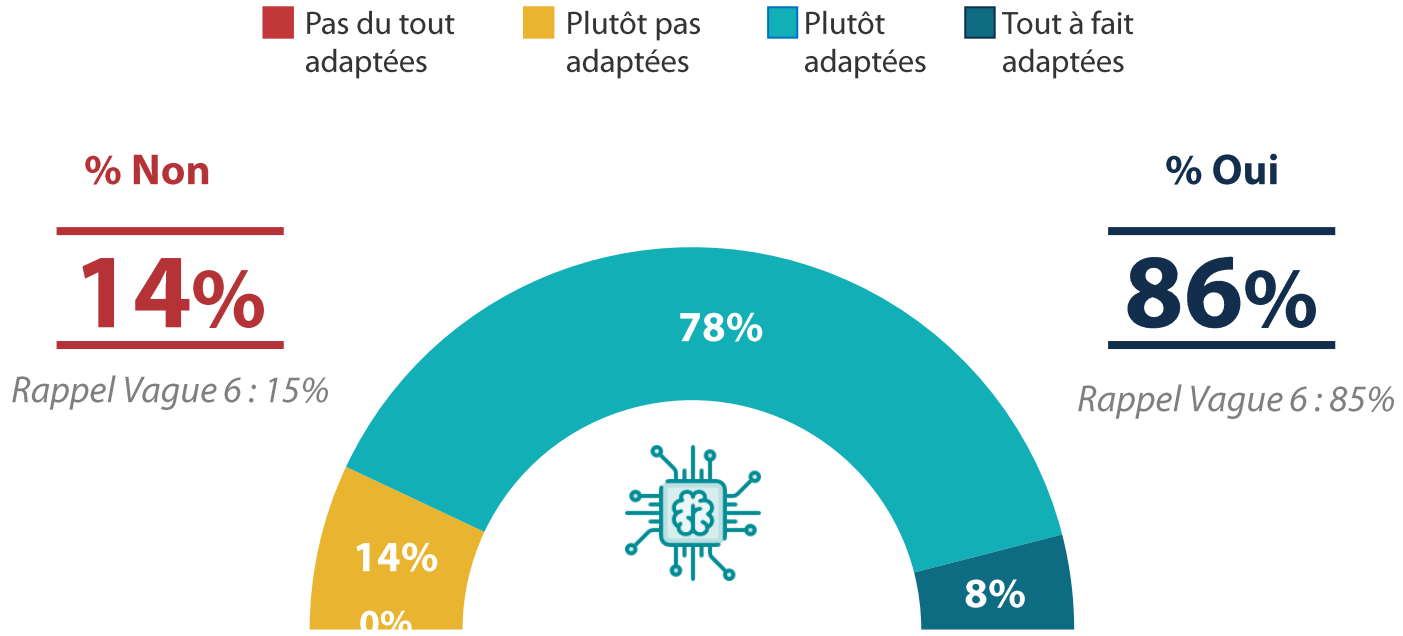
…et qui se protègent mieux et de plus en plus

Toujours un haut niveau de satisfaction des RSSI envers les solutions présentes sur le marché

Q25. Pensez-vous que les solutions de sécurité disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptées à votre entreprise ?

Base ensemble

282 personnes

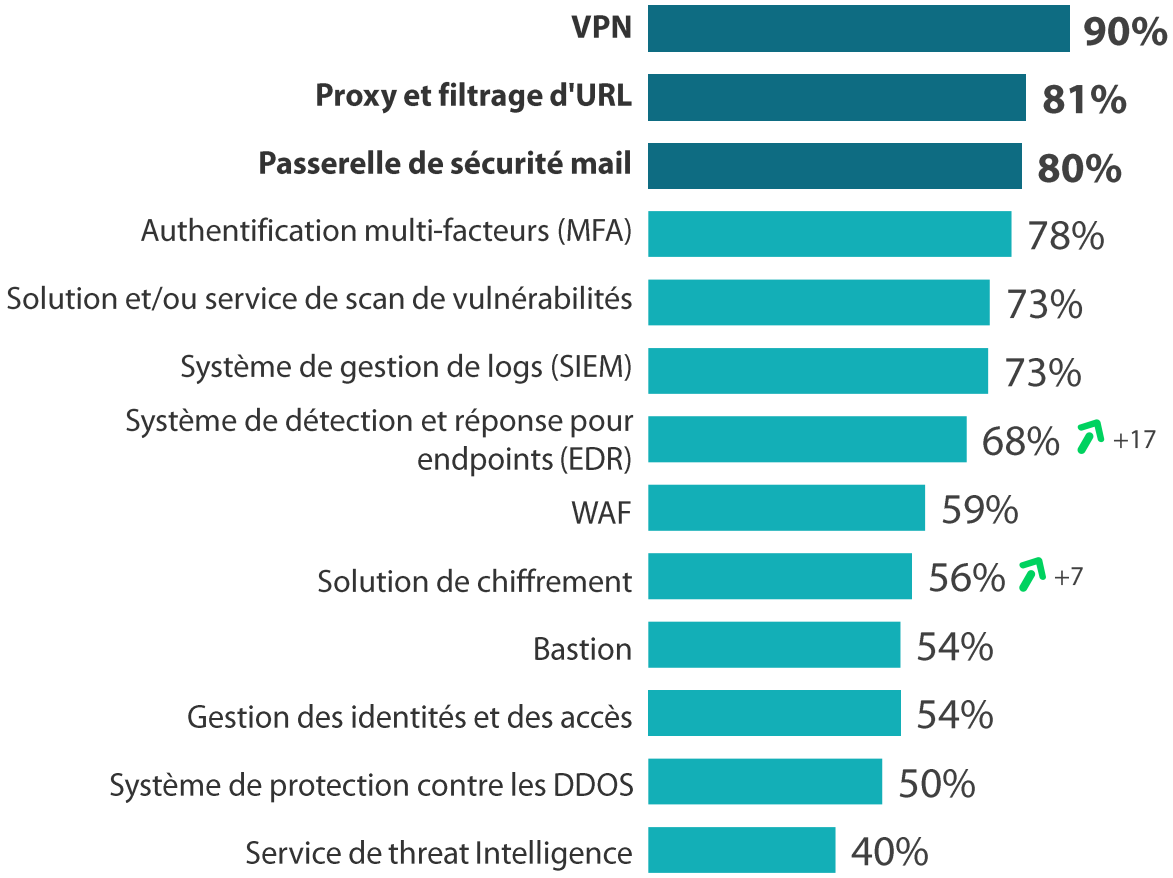


Une dizaine de dispositifs mis en place en moyenne dans les entreprises. À noter l'augmentation de l'usage des solutions EDR et de chiffrement

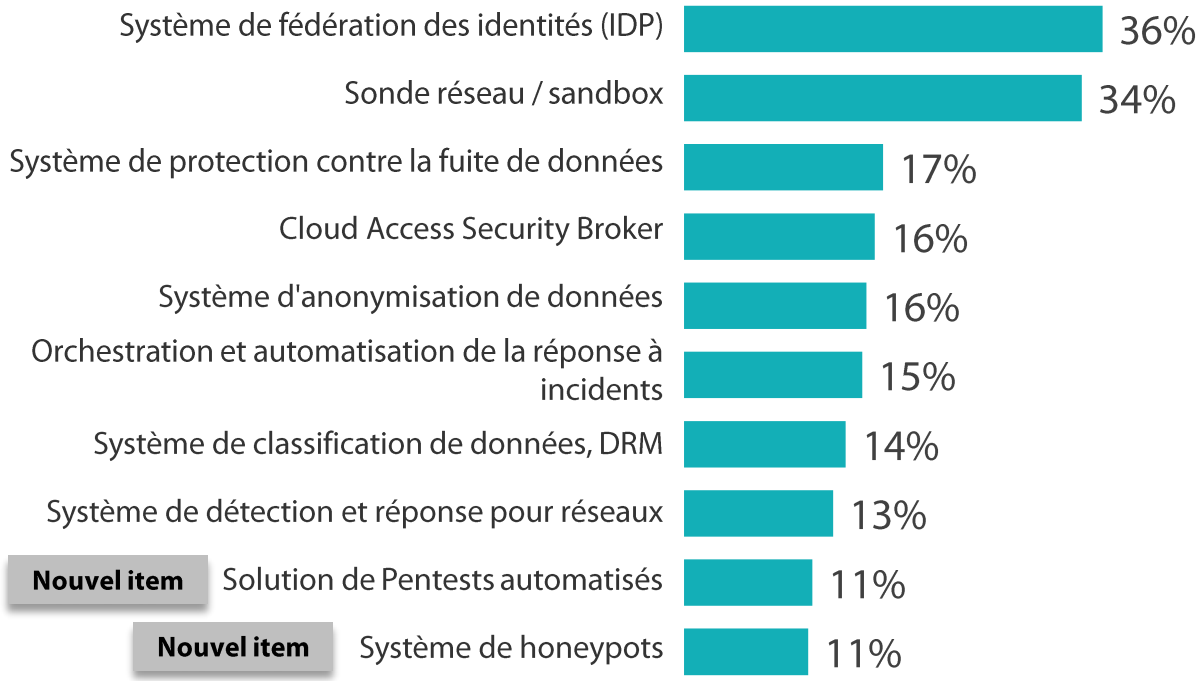
282 personnes

Q12. D'une manière plus générale, parmi les solutions de protection suivantes, quelles sont celles qui sont en place dans votre entreprise, en plus des classiques antivirus et pare-feu ?

Base ensemble /plusieurs réponses possibles



10,4 solutions en moyenne



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

…ce qui peut expliquer que les entreprises se sentent mieux préparées notamment au niveau des moyens de détection, elles reconnaissent tout de même manquer d'expertise sur les réponses et la reconstruction après attaques

282 personnes

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

72%
Moyens de prévention

Rappel Vague 6 : 69%

72% +13
Moyens de détection

Rappel Vague 6 : 59%

54%
Réponse à l'attaque

Rappel Vague 6 : 46%

Nouvel item

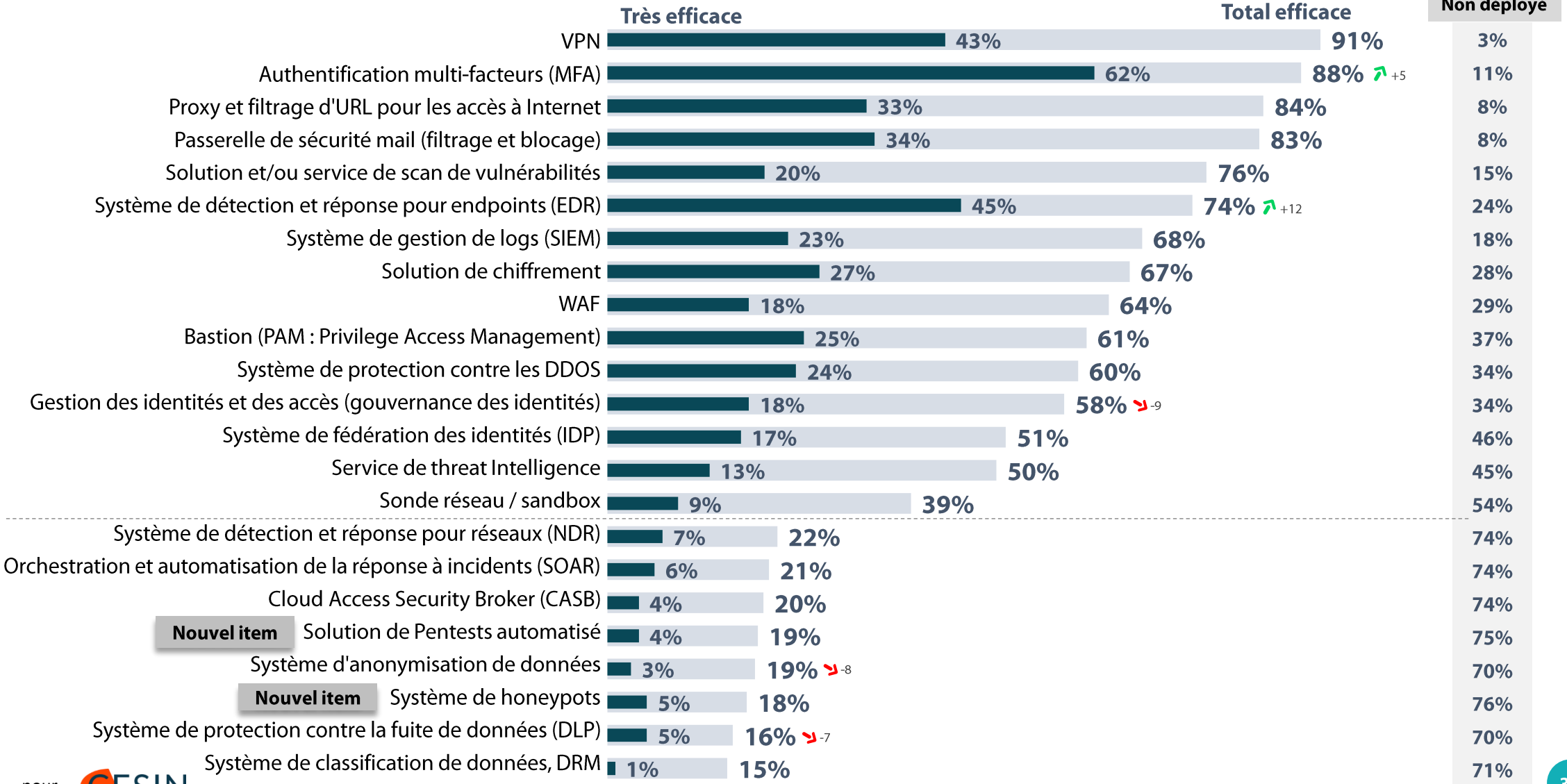
51%
Reconstruction après l'attaque

L'authentification multi-facteurs est l'une des solutions jugées très efficaces par les entreprises, suivi par les EDR et le VPN

282 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



Évolution statistiquement significative par rapport à la vague précédente

Évolution à interpréter avec prudence au vu de l'ajout d'items

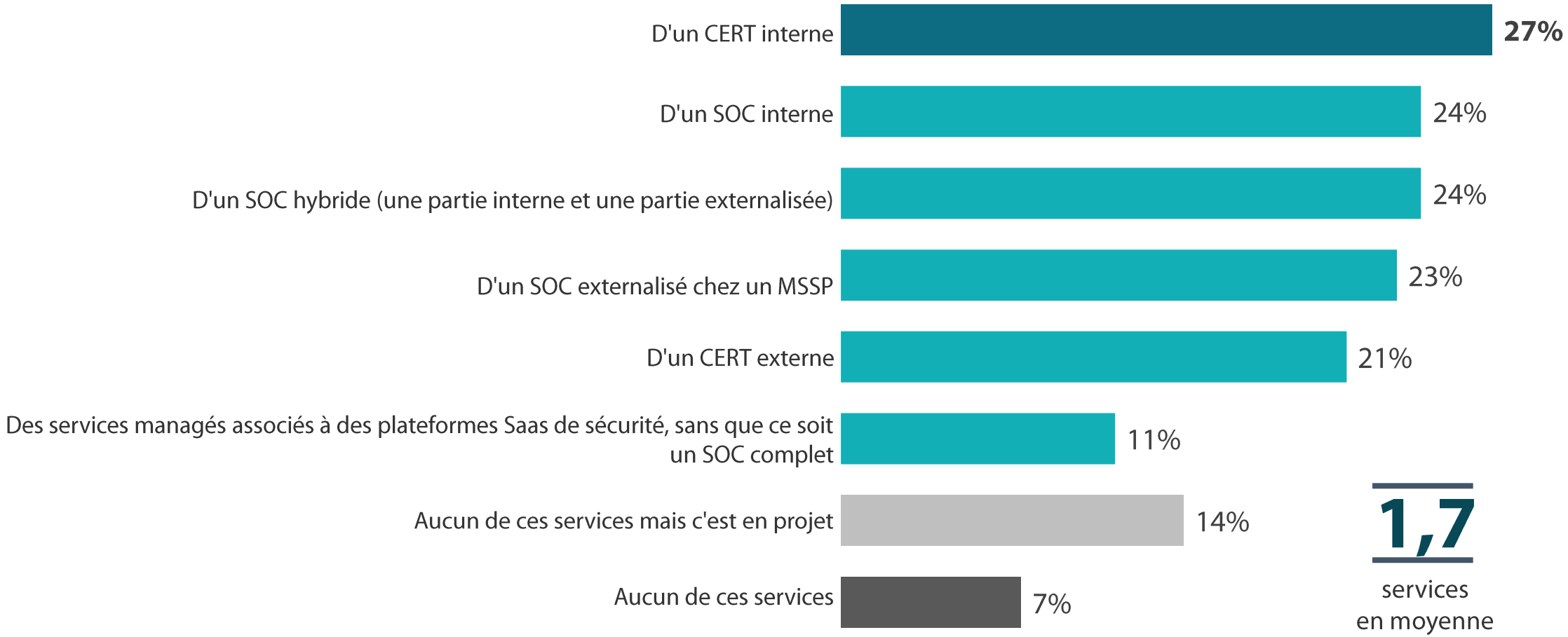
Des entreprises qui ne mettent pas forcément en place les mêmes services pour assurer les fonctions de détection et de réponse

282 personnes

Nouvelle question

Q30. Quels services avez-vous mis en place pour assurer les fonctions de détection et réponse à incidents ?

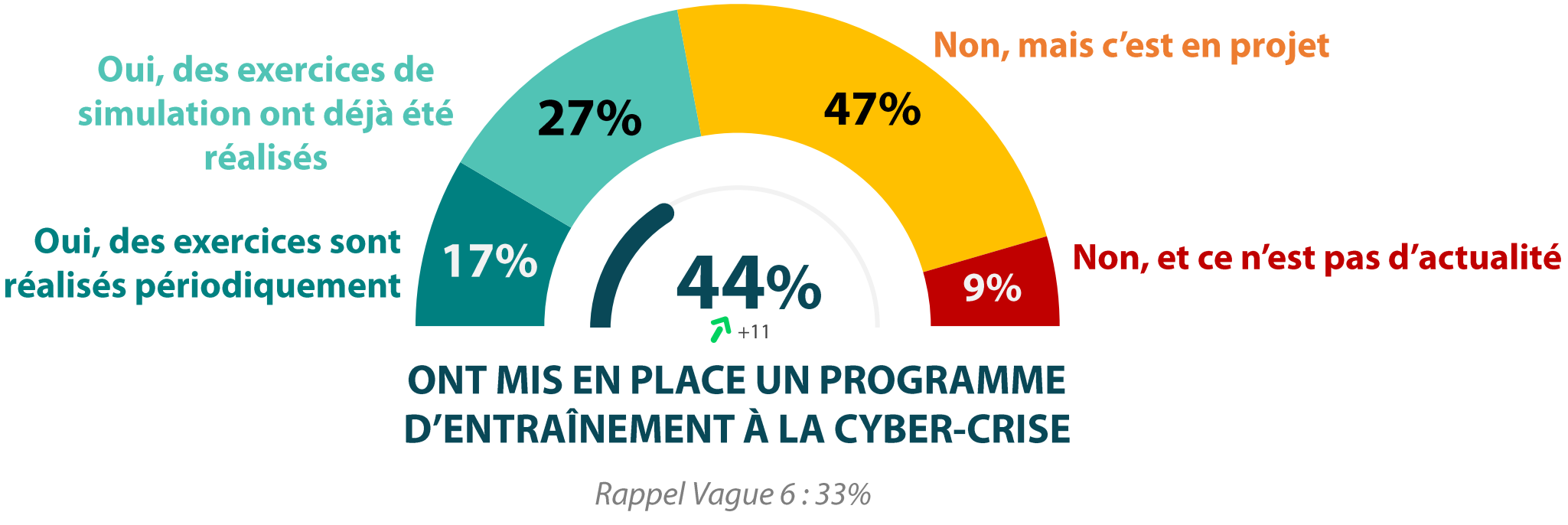
Base ensemble / Plusieurs réponses possibles



Plus de 4 entreprises sur 10 ont mis en place un programme d'entraînement à la cyber crise, c'est largement plus qu'en 2020

282 personnes

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



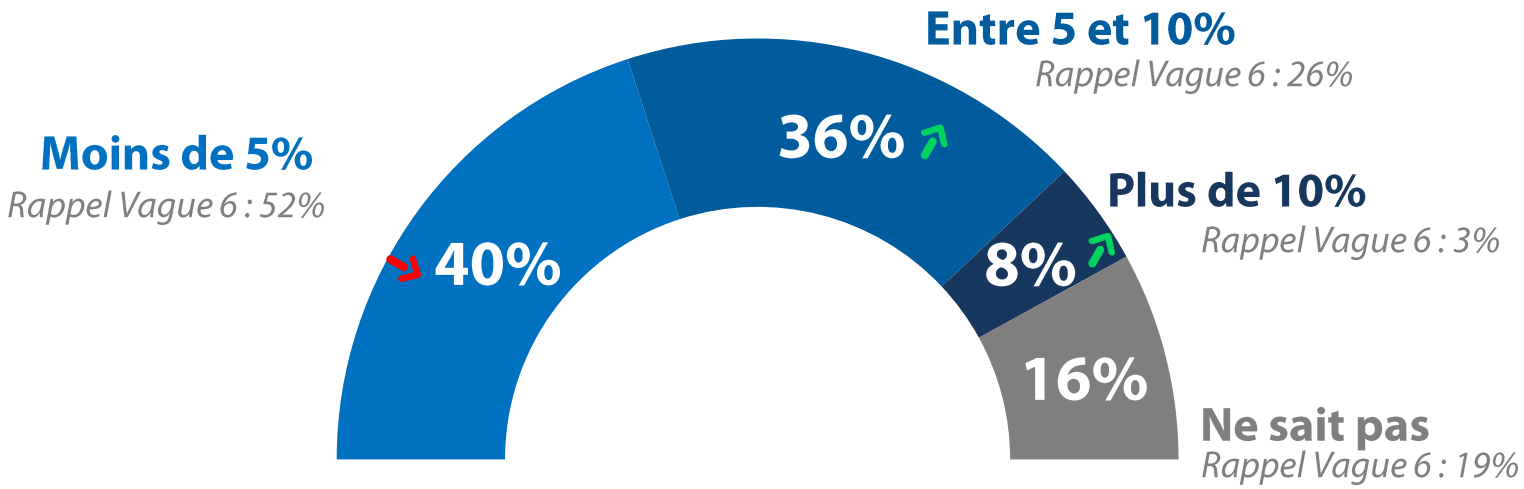
Rappel Vague 6 : 33%

Un budget sécurité de l'IT/digital en augmentation significative cette année. La proportion d'entreprise consacrant moins de 5% de leur budget en diminution au profit de celles qui y consacrent plus de 5%.

282 personnes

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

Base ensemble

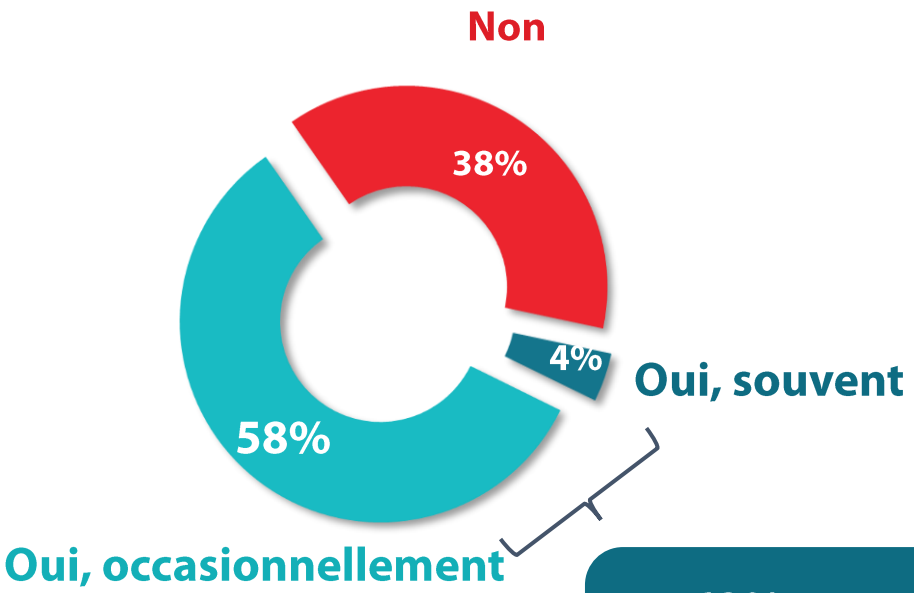


Modification de la question en vague 7

Les entreprises sont de plus en plus nombreuses à faire appel à des solutions issues de start-ups

282 personnes

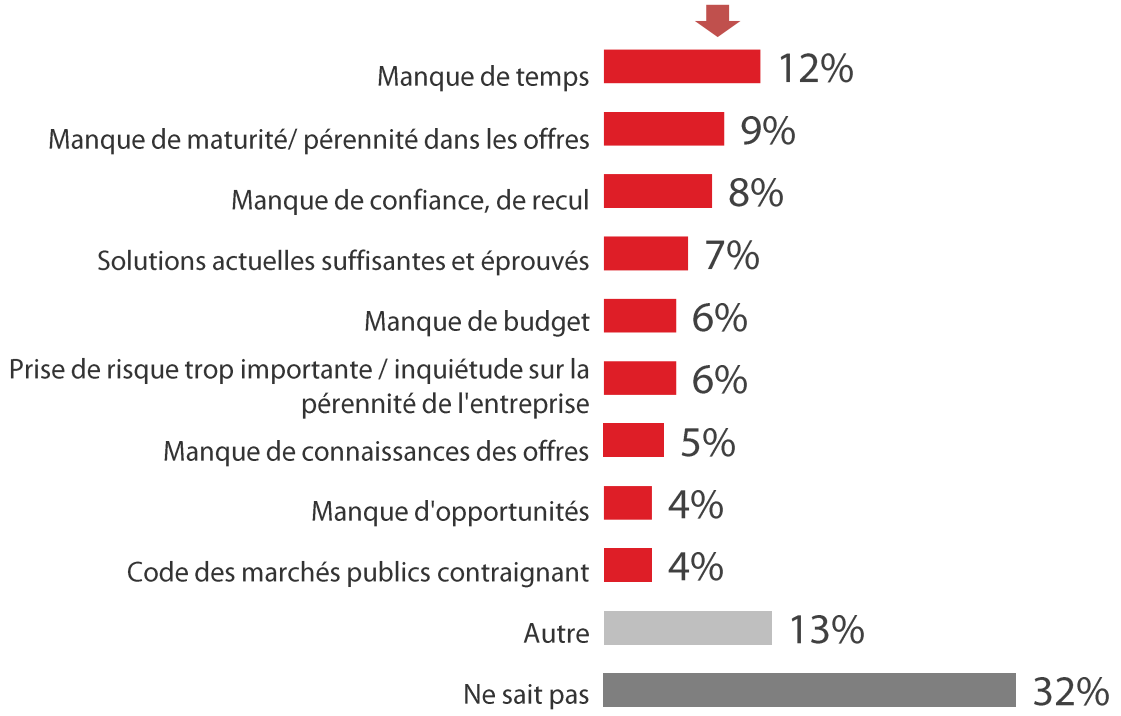
Q26. En matière de cybersécurité, recourrez-vous à des offres innovantes issues de start-up ? *Base ensemble*
Q26bis. Pour quelle(s) raison(s) ne le faites-vous pas ? *Base : ne fais pas appel à des offres issues de start-up (107)*



62% ont recours à des offres innovantes issues de start-up

Rappel Vague 6 : 55%

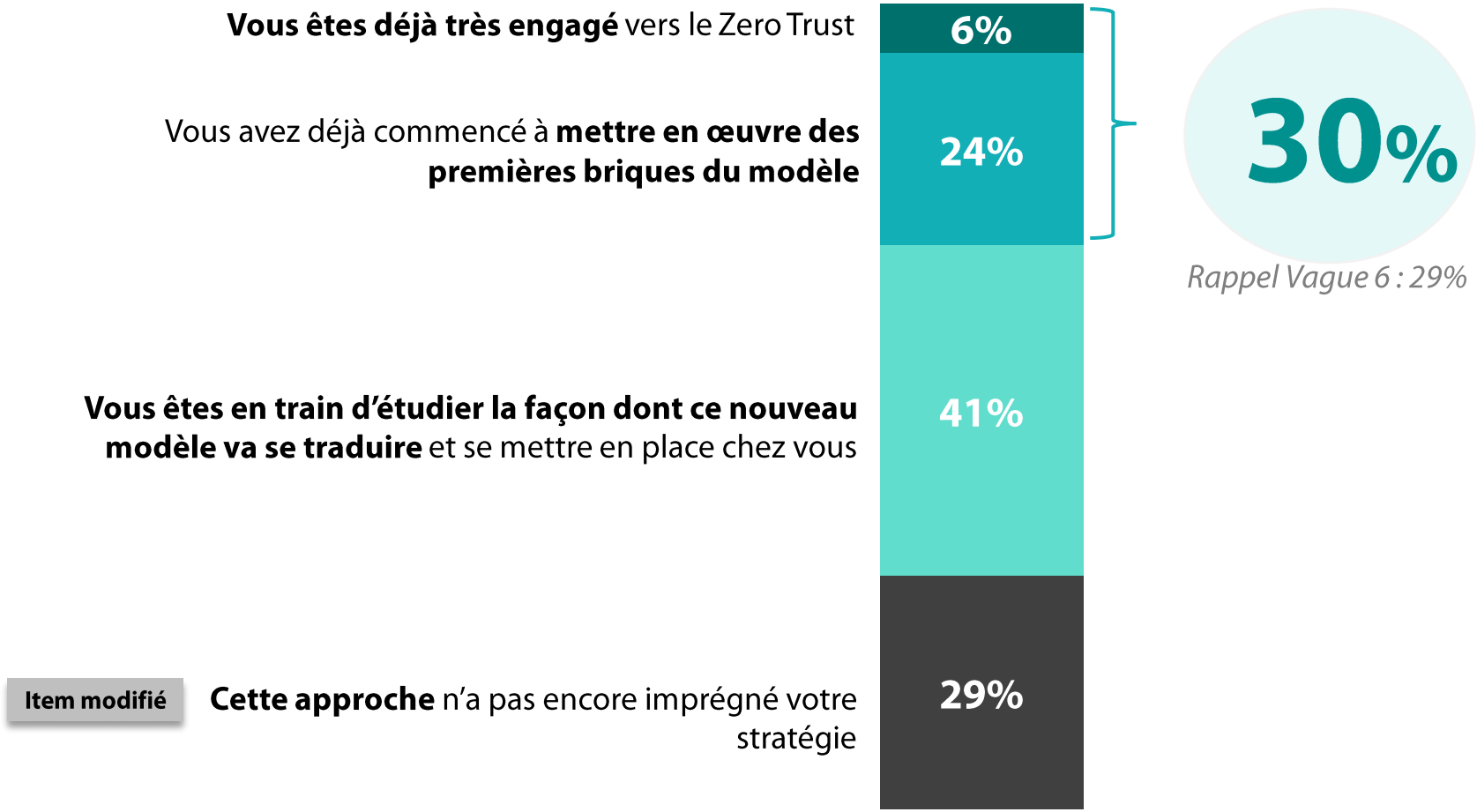
38% n'ont pas recours à ces offres



Similairement à 2020, 3 entreprises sur 10 ont déjà mis en place le concept Zero Trust

282 personnes

Q28. Quelle est votre opinion et votre appétence pour le concept Zero Trust ?
Base ensemble



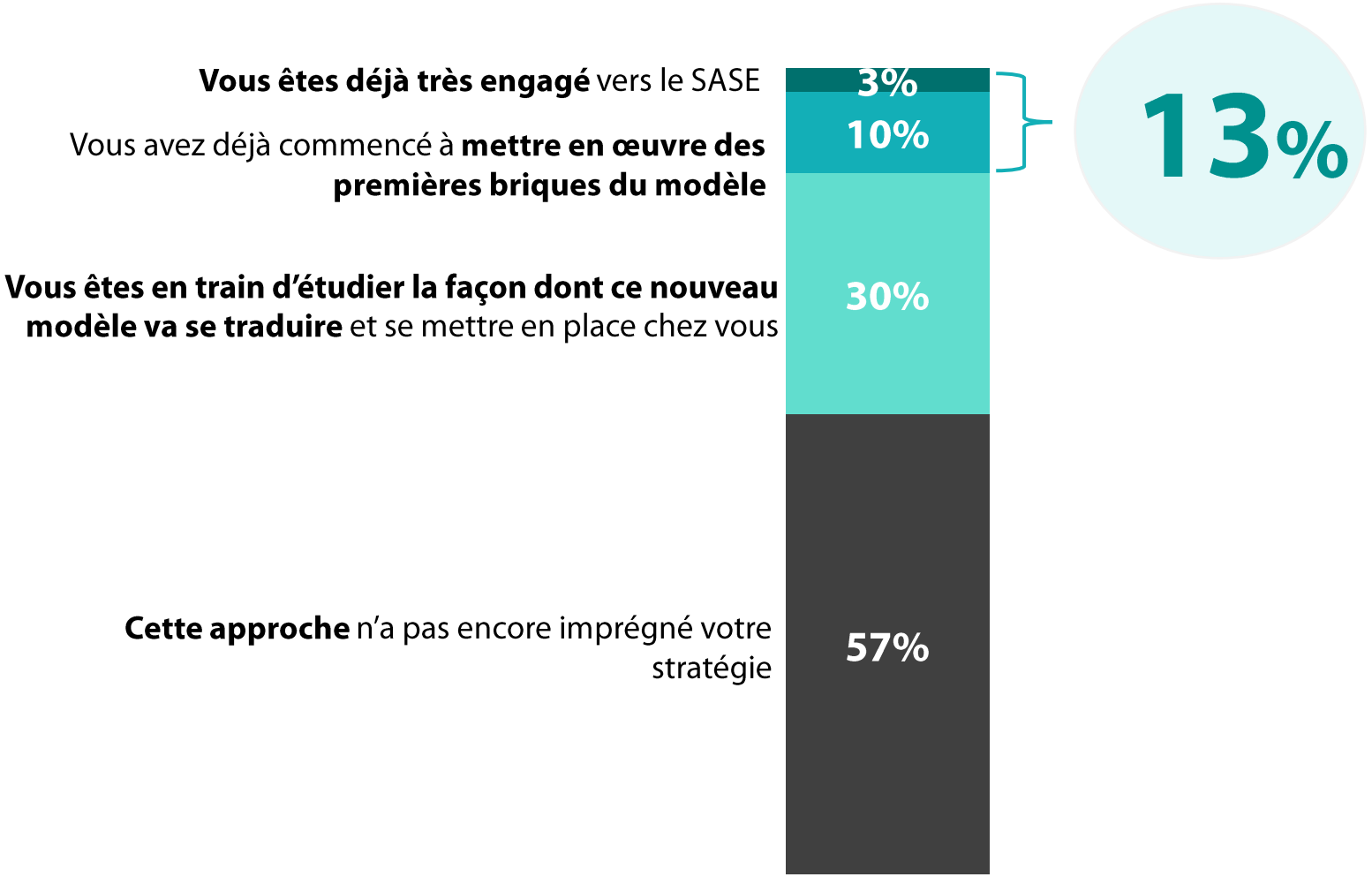
Le concept SASE n'a pas encore imprégné la stratégie sécurité des entreprises

282 personnes

Nouvelle question

Q34. Quelle est votre opinion et votre appétence pour le concept SASE ?

Base ensemble



Focus sur…

La cyber-assurance

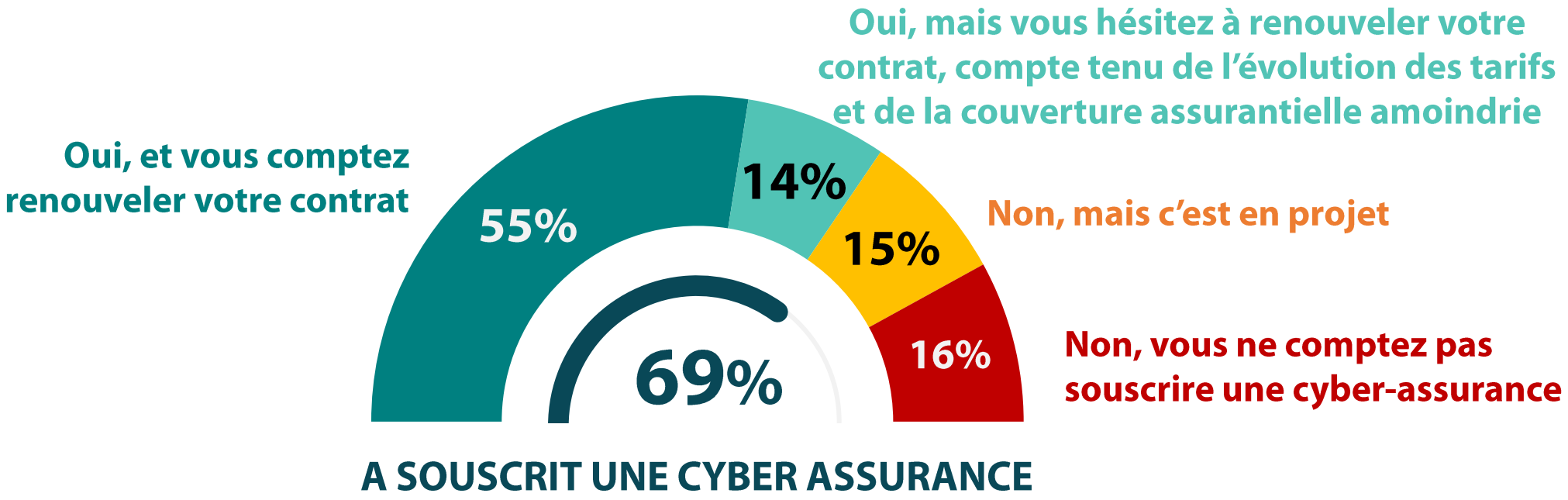
Une majorité d'entreprises détiennent aujourd'hui une cyber-assurance, à noter que plus d'une entreprise sur 10 hésite à renouveler son contrat

282 personnes

Nouvelle question

Q31. Avez-vous souscrit une cyber-assurance ?

Base ensemble



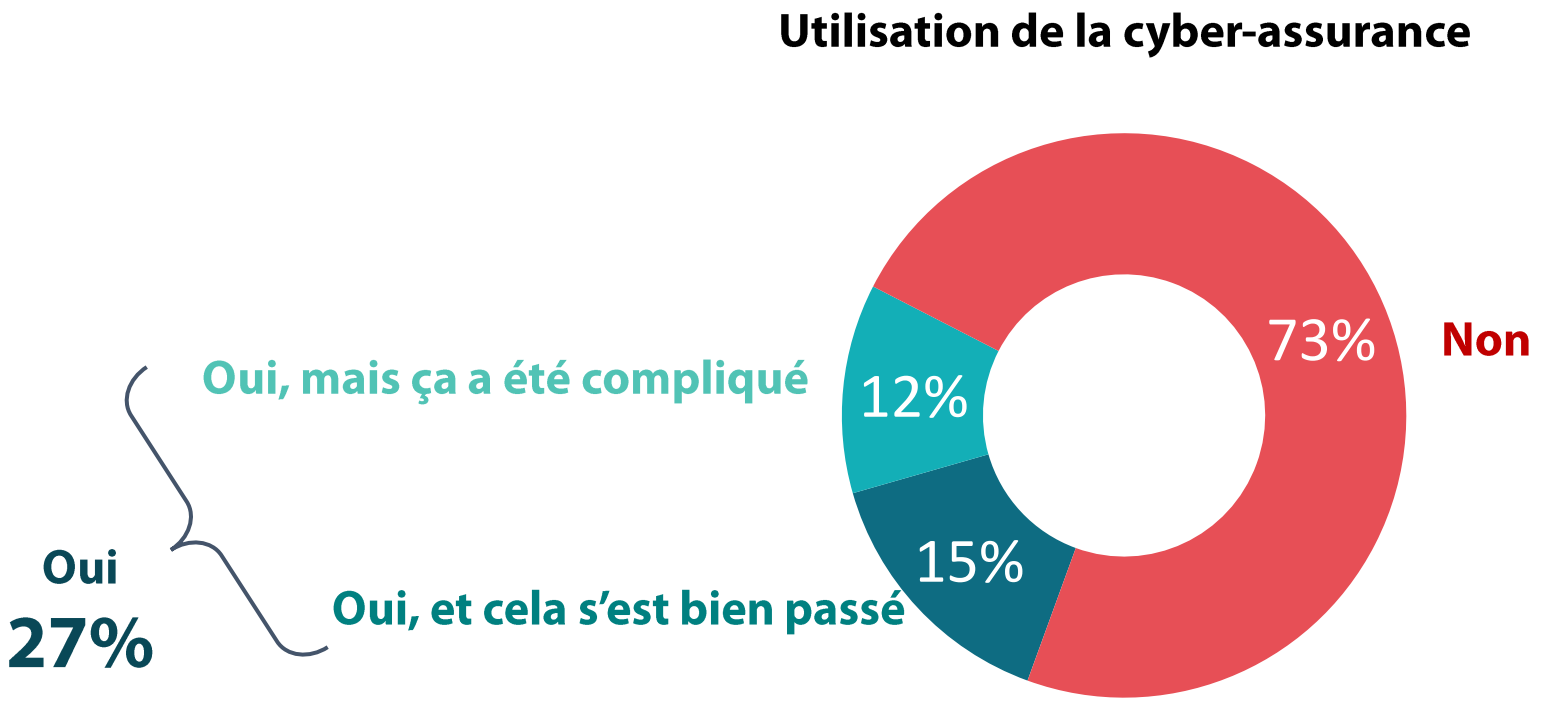
Un niveau de satisfaction suite au recours à la cyber-assurance toujours mitigé

194 personnes

Nouvelle question

Q32. Votre entreprise a-t-elle déjà fait appel à sa cyber-assurance dans le cadre d'une cyber-attaque ?

Base possède une cyber-assurance



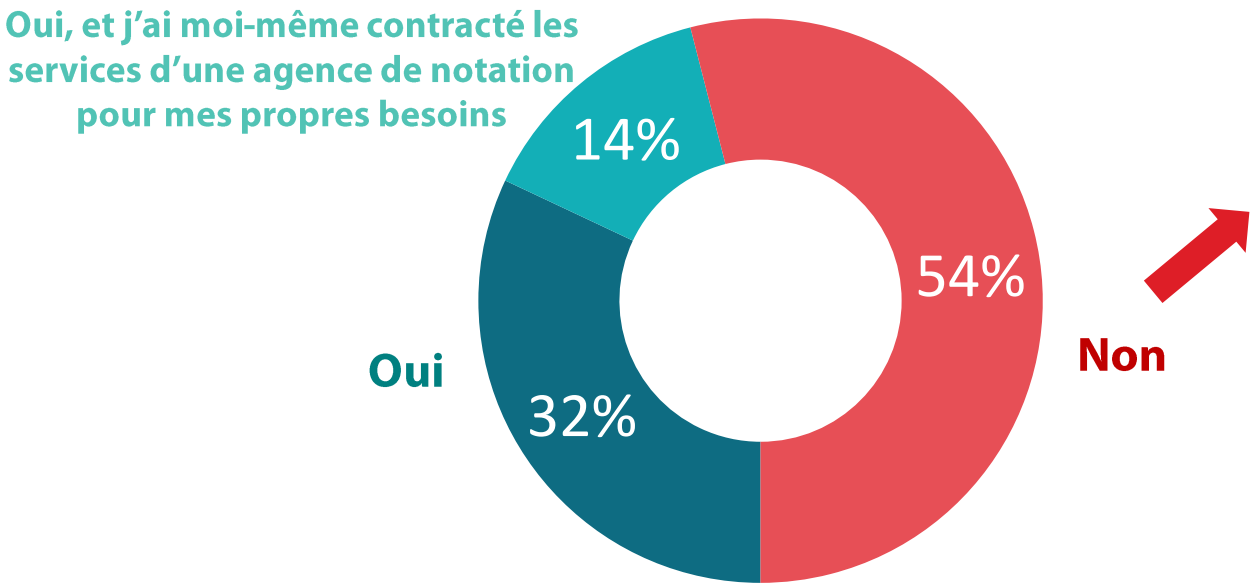
La majorité des entreprises ont un avis négatif sur le recours au service d'agences de notation pour la cyber-assurance

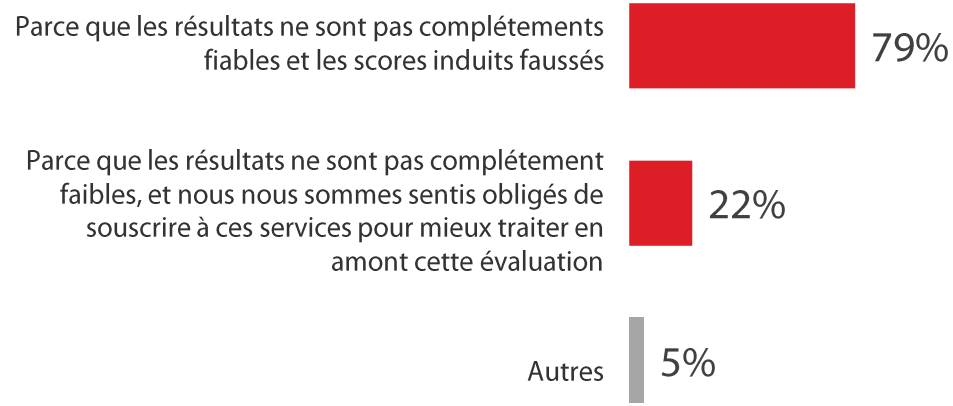
282 personnes

Nouvelle question

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*
Q33bis. Pour quelles raisons ? *Base ce n'est pas une bonne chose (153)*

Le recours au service d'agence de notation

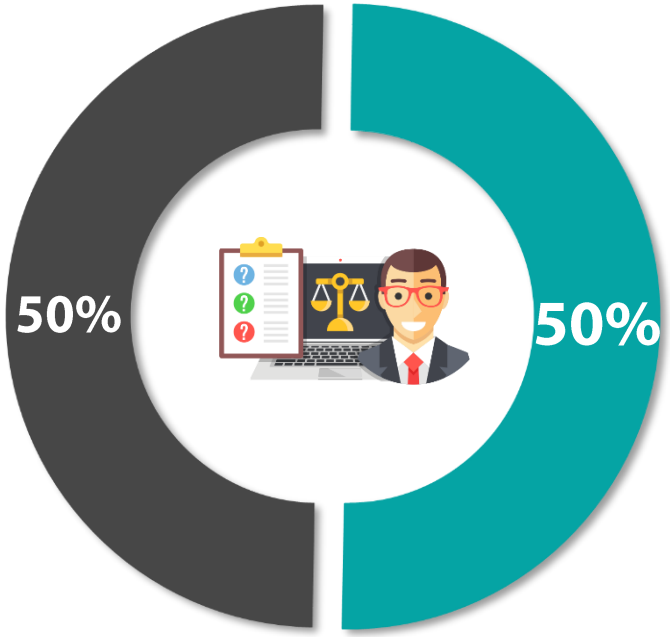




La moitié des entreprises ayant subi une attaque ont déjà porté plainte, en légère hausse par rapport à 2020

152 personnes

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



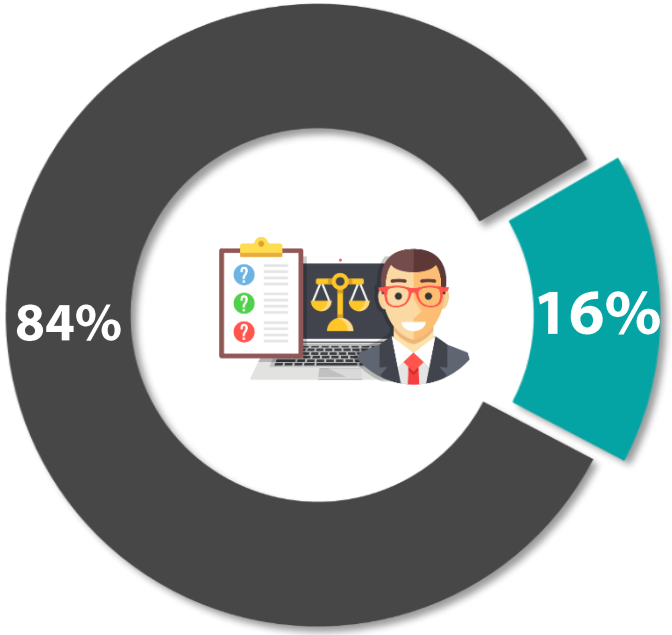
pour **toutes les attaques** : **21%**

pour **certaines attaques** : **29%**

Mais l'enquête a permis l'identification/l'interpellation des attaquants dans un peu plus d'1 cas sur 10

76 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



Oui, l'enquête a permis une identification
Rappel Vague 6 : 15%

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

pour **certaines plaintes** : **11%**

03

Une sensibilisation des salariés toujours accrue

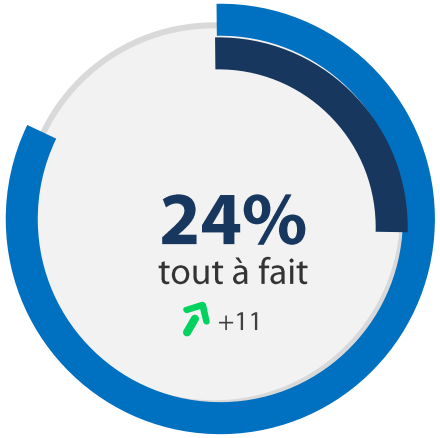
Des utilisateurs qui sont sensibilisés et qui respectent mieux les recommandations, mais qui ne prennent pas suffisamment de précautions

282 personnes

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

82%

Les utilisateurs **sont sensibilisés** aux cyber-risques



Rappel Vague 6 : 77%

70%

Les utilisateurs **respectent les recommandations**

Rappel Vague 6 : 63%

18%

Les utilisateurs **prennent des précautions au-delà des recommandations** données

Rappel Vague 6 : 16%

Modification de la question et des items en vague 7

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

Les administrateurs, architectes et développeurs pourraient également être plus sensibilisés et formés

282 personnes

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

68%

Les administrateurs, architectes et développeurs sont sensibilisés et appliquent les bonnes pratiques de sécurité en matière d'exploitation, de design et de développement

Nouvel item

44%

Les administrateurs, architectes et développeurs sont suffisamment formés et ont acquis l'expertise nécessaire, notamment sur les nouveaux sujets

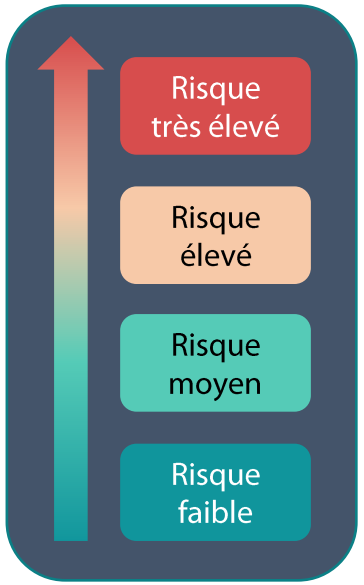
Nouvel item

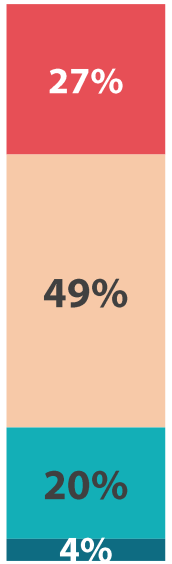
Modification de la question et des items en vague 7

Au final, des usages numériques perçus comme moins risqués cette année, notamment sur le recours au Shadow IT et le télétravail

282 personnes

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



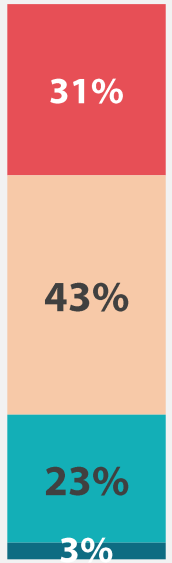


76%

Rappel Vague 6 : 80%

24%

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

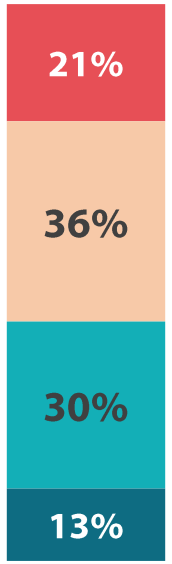


74% ↘

Rappel Vague 6 : 84%

26%

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

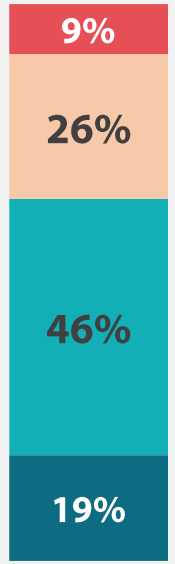


57%

Rappel Vague 6 : 61%

43%

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

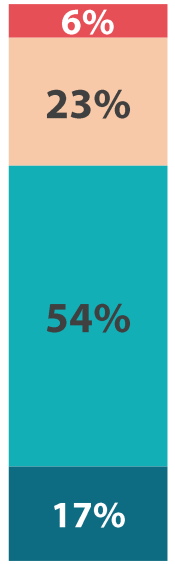


35%

Rappel Vague 6 : 41%

65%

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



29% ↘

Rappel Vague 6 : 41%

71%

Le télétravail, l'accès au réseau en mobilité

04

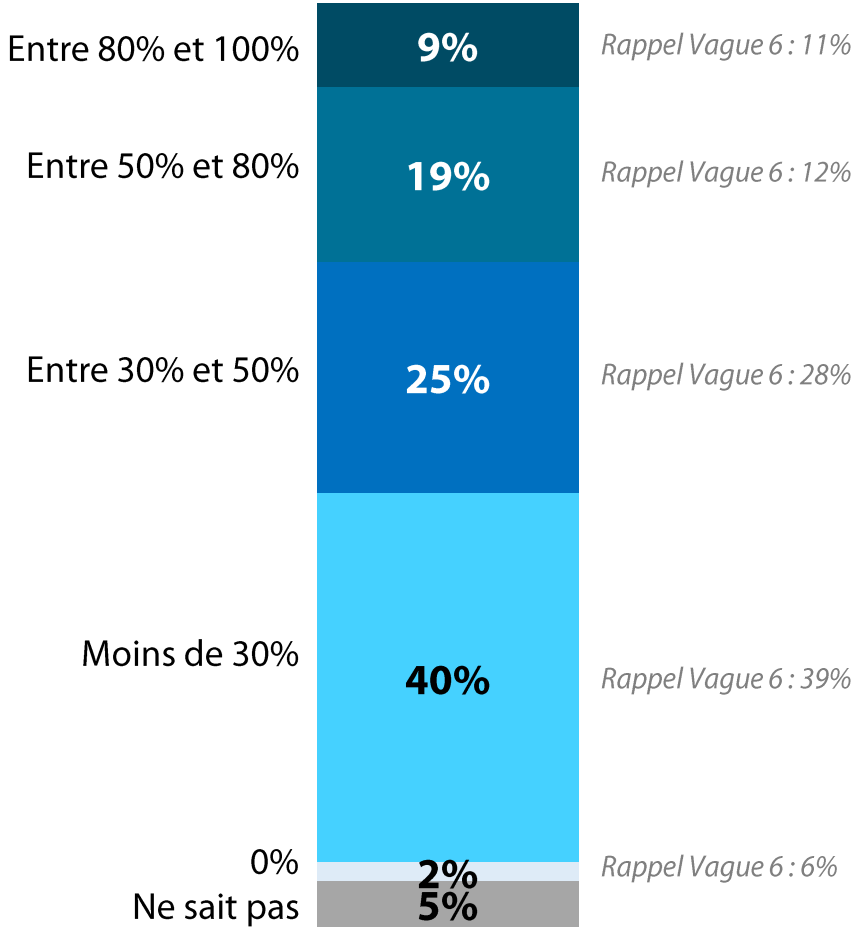
Le cloud, sécurisé, mais nécessitant des outils spécifiques

Similairement à 2020, la pénétration du cloud est effective dans la plupart des entreprises

282 personnes

Q20. Quel est le degré de pénétration de votre SI dans le cloud, que ce soit en mode Iaas, Paas ou Saas ?

Base ensemble



La non-maîtrise de la chaîne de sous-traitance de l'hébergeur, en tête des risques liés à l'utilisation du Cloud, comme en 2020. A noter que la rareté de l'expertise et la mauvaise visibilité de l'inventaire, nouveaux items cette année, présentent un risque fort

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

Base ensemble

	% Un risque fort
	48% Non maîtrise de la chaîne de sous-traitance de l'hébergeur
	43% Difficulté de contrôler les accès par des administrateurs de l'hébergeur
Nouvel item	**40% Expertise encore trop rare, attendue de la part des architectes et des administrateurs**
Nouvel item	38% Mauvaise visibilité de l'inventaire des ressources qu'il y a dans le cloud
Rappel Vague 6 : 41%	36% Confidentialité des données vis-à-vis de l'hébergeur
	36% Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
	35% 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
	33% Stockage des données dans des datacenters à l'étranger, hors du droit français
Rappel Vague 6 : 44%	33% Maîtrise difficile de l'utilisation qui en est faite par les salariés de votre entreprise
	31% Défaut de cloisonnement entre les différents clients de 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
Item modifié	29% Propagation systémique des attaques et erreurs humaines qui surviendraient au niveau de l'hébergeur
Rappel Vague 6 : 36%	28% Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur
	28% Non-effacement des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
Item modifié	28% Forte fréquence des nouvelles versions mises en ligne avec des potentielles évolutions non contrôlées des principes ou paramètres de sécurité
	27% Attaque par rebond depuis l'hébergeur
	26% Traitement et exploitation des données par l'hébergeur à l'insu de ses clients
Rappel Vague 6 : 31%	25% Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant du Cloud
	25% Indisponibilité des données / de l'application due à une attaque de l'hébergeur
	23% Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
	18% Piégeage d'une application hébergée

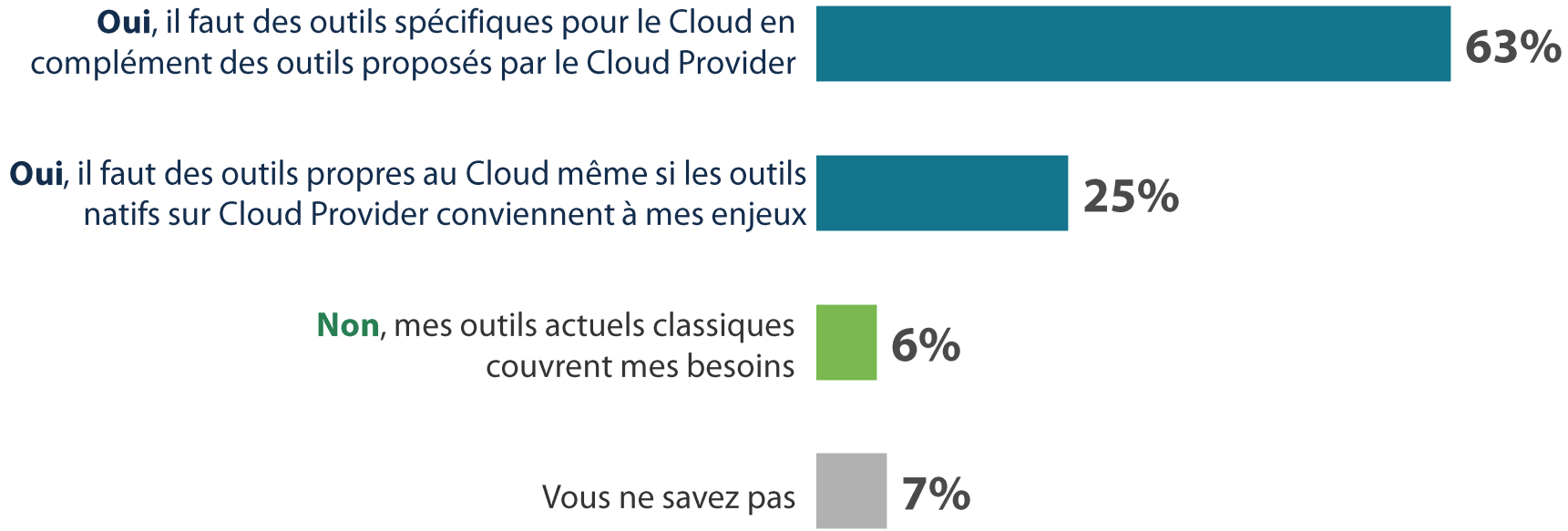
Modification de la liste en vague 7

Près de 9 entreprises sur 10 estiment que sécuriser des données dans le cloud nécessite des outils spécifiques, et la grande majorité avec d'autres outils que ceux proposés par le Cloud Provider

282 personnes

Q22. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base ensemble

… 86% estiment que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques



Modification des items en vague 7

6 entreprises sur 10 se sentent préoccupées par les sujets de souveraineté et de Cloud de Confiance

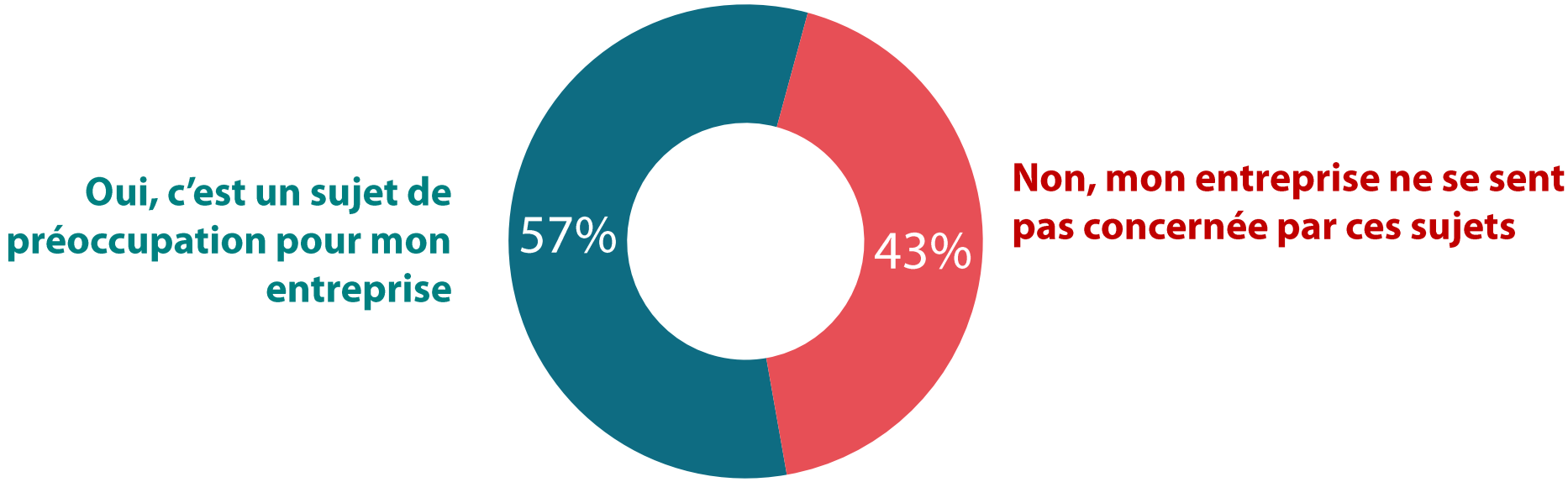
282 personnes

Nouvelle question

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



05

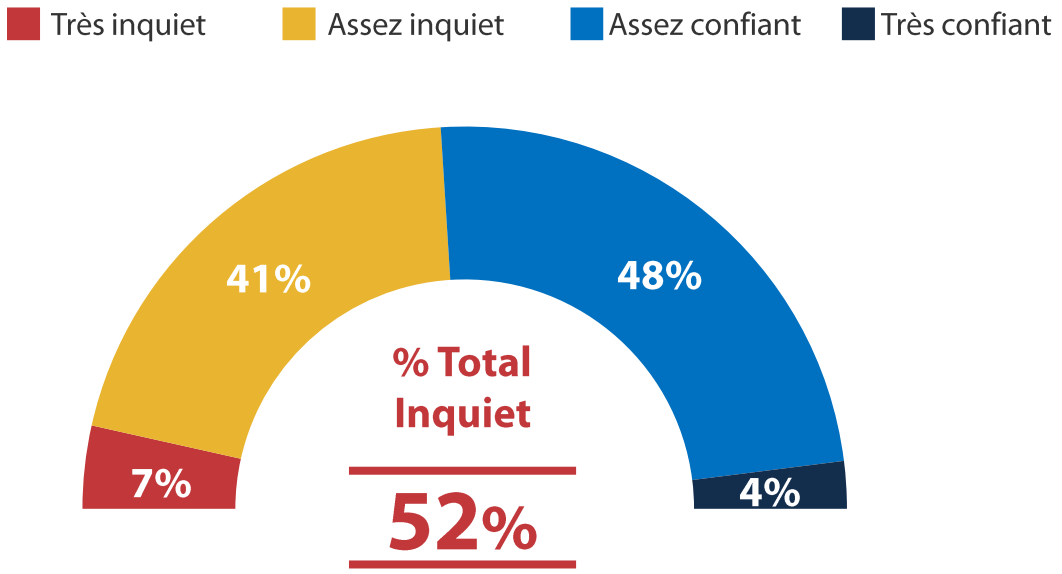
Les entreprises face aux enjeux de demain

Comme en 2020, 1 entreprise sur 2 se dit inquiète sur sa capacité à lutter contre les cyber-risques

282 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



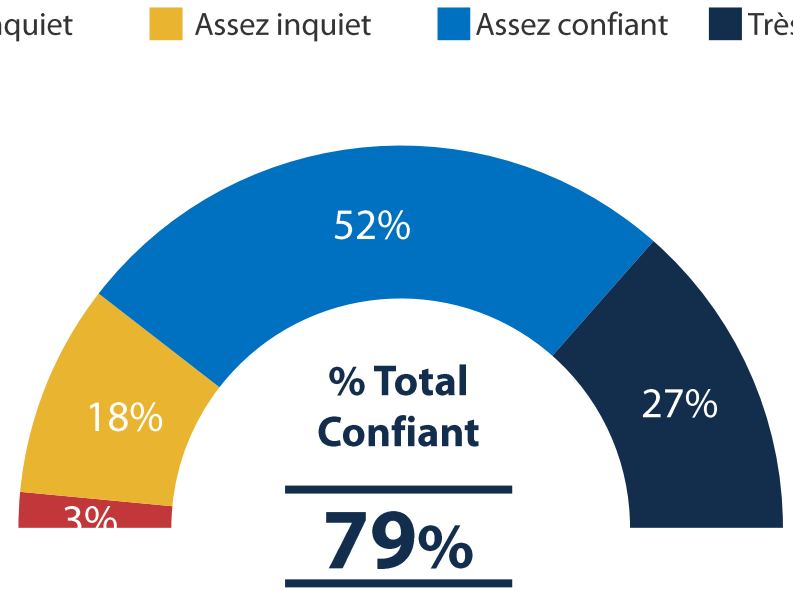
Rappel Vague 5 : 50%

Même si le COMEX prend de plus en plus en compte les enjeux représentés par la cybersécurité

282 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 votre entreprise



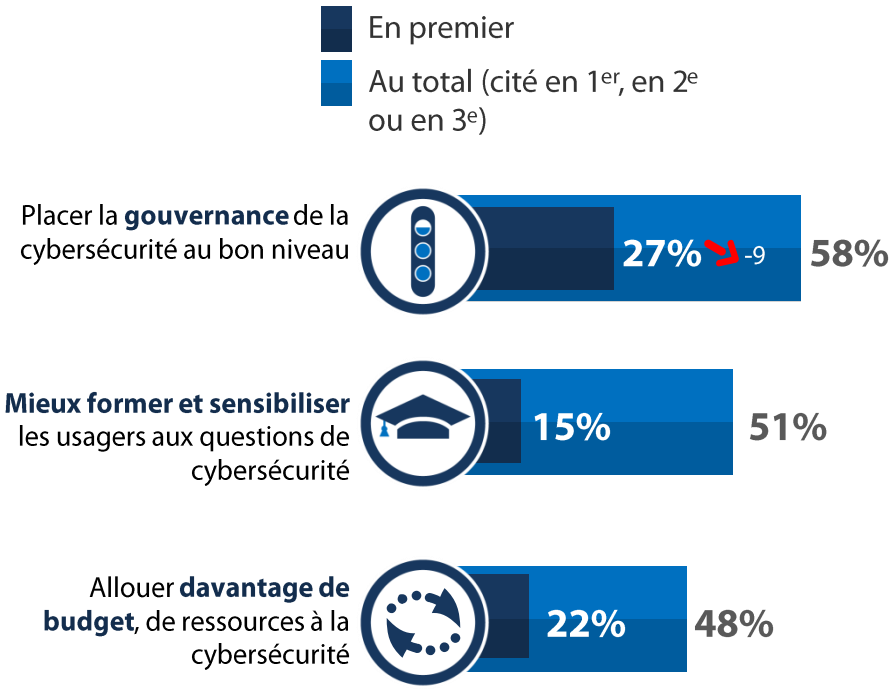
Rappel Vague 5 : 72%

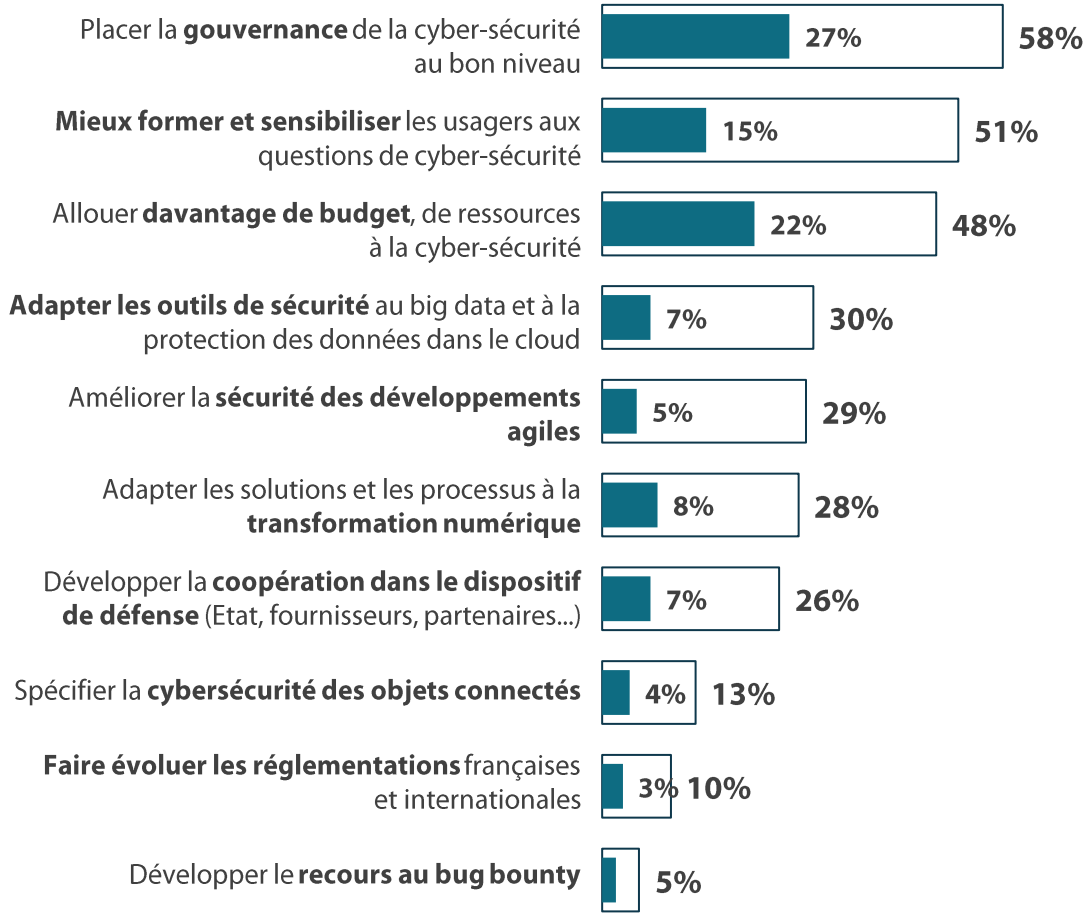
Les enjeux humains et budgétaires restent les priorités de demain

282 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





En lien avec les enjeux, une large augmentation des budgets est prévue au cours des prochains mois…

282 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

Rappel Vague 6 : 57%

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

Rappel Vague 6 : 52%

… de même, plus de 8 entreprises sur 10 ont prévu d'acquérir de nouvelles solutions de protection

282 personnes

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

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

Rappel Vague 6 : 85%

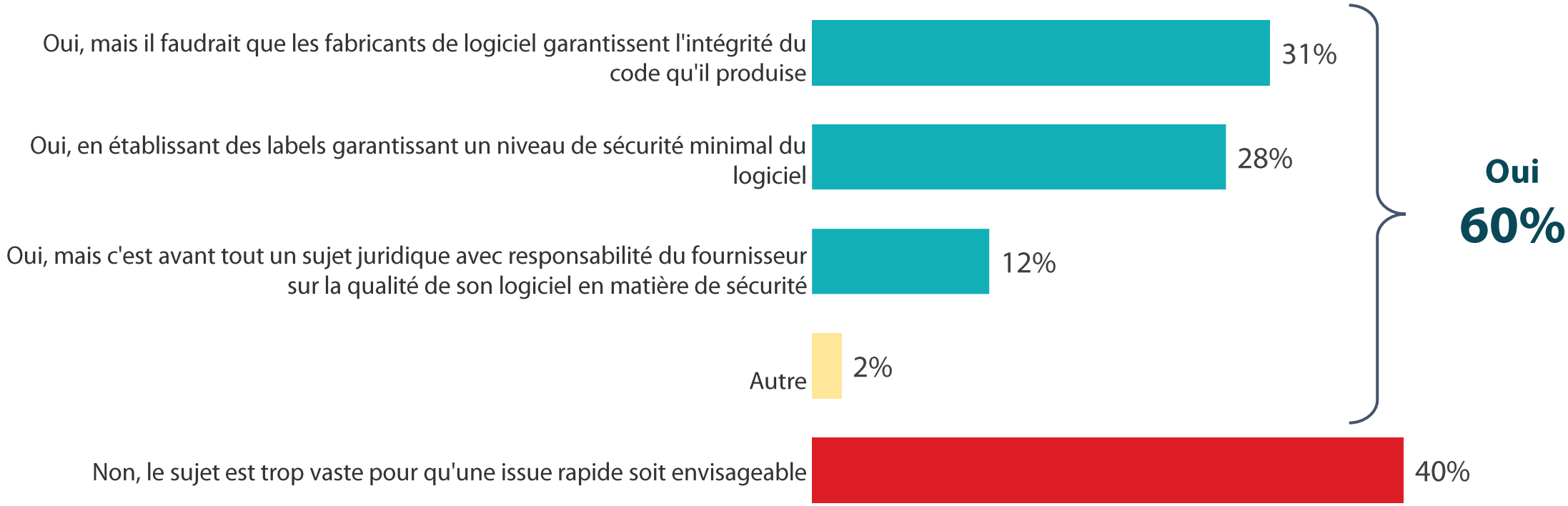
6 entreprises sur 10 estiment que les questions de sécurité de la supply chain peuvent trouver une issue, à la condition d'une plus grande garantie du code et des labels

Nouvelle question

Q36. Les attaques de type Solarwinds posent la question de la sécurité logicielle. Pensez-vous que ces questions de sécurité de la supply chain peuvent trouver une issue ?

Base ensemble / plusieurs réponses possibles

282 personnes



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.

15 place de la République
75003 Paris

PARIS
CASABLANCA
ALGER
VARSOVIE
ABIDJAN

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 !