“opinionway pour CESIN

Baromètre de la cybersécurité des entreprises

Vague 8 – Janvier 2023

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 cybersécurité 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 cybersécurité, et apporte de nouvelles données sur l'impact de la transformation numérique des entreprises.

La méthodologie

La méthodologie

Echantillon de **328 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 8 décembre 2023 au 10 janvier 2023**.

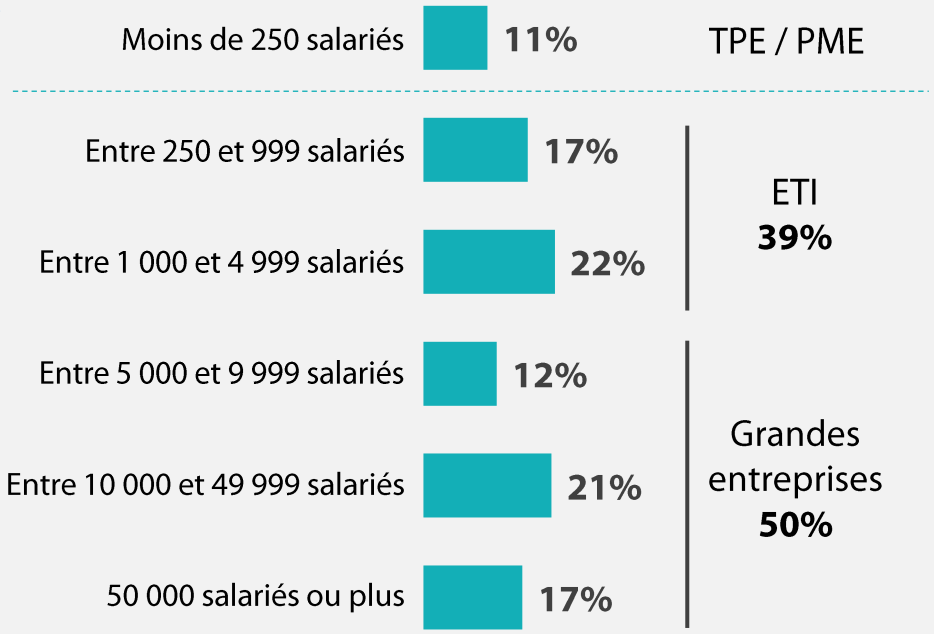
OpinionWay a réalisé cette enquête en appliquant les procédures et règles de la **norme ISO 20252**

Les résultats de ce sondage doivent être lus en tenant compte des marges d'incertitude : 5,5 points au plus pour un échantillon de 330 répondants.

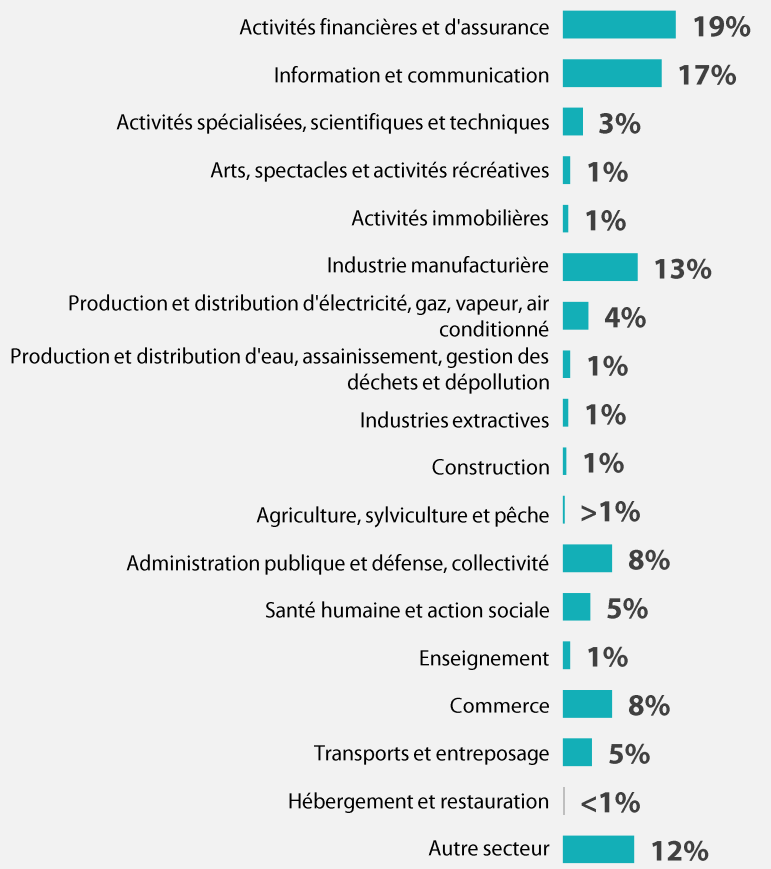
Le profil des répondants

Un échantillon qui reflète parfaitement la diversité de la population interrogée

Nombre de salariés de l'entreprise



Secteur d'activité de l'entreprise



L’analyse

01

Une baisse du nombre de cyberattaques réussies en 2022…

Définition d'une cyberattaque

« 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 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.*

Moins d'1 entreprise sur 2 a subi une cyberattaque réussie cette année, une proportion en baisse par rapport à 2021 (-9pts)

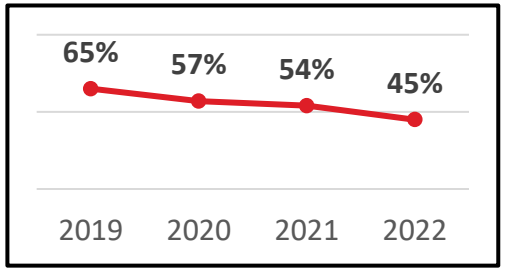
328 personnes

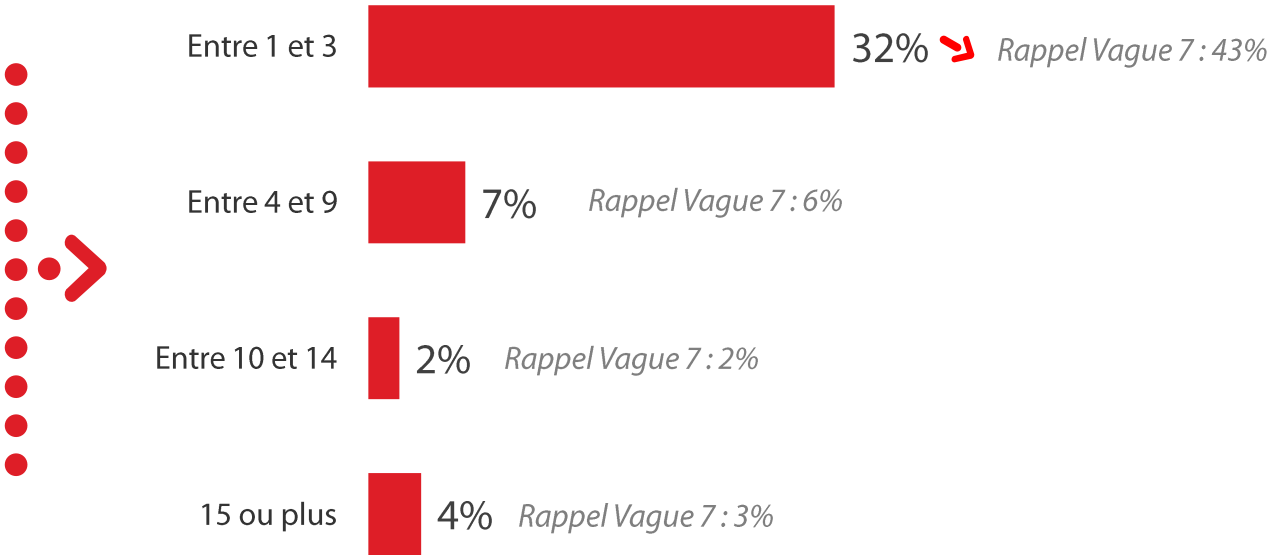
Q4. De façon générale, combien de cyberattaques significatives ont été subies par votre entreprise au cours des 12 derniers mois ?
Base ensemble

45% ↘ -9

des entreprises ont constaté au moins une cyberattaque

Rappel vagues précédentes





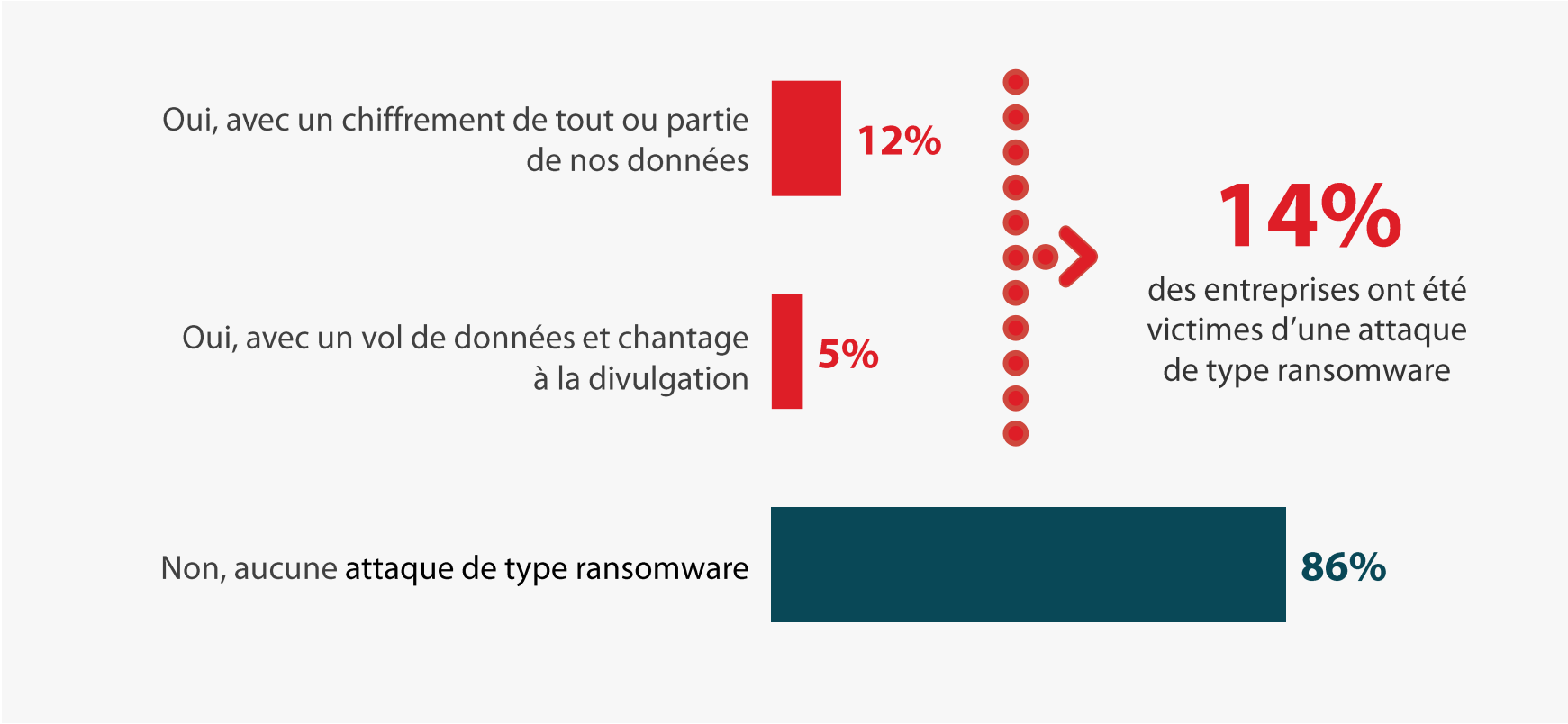
Moins d'1 entreprise sur 5 a été victime de ransomware, un chiffre orienté à la baisse par rapport à 2021

328 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

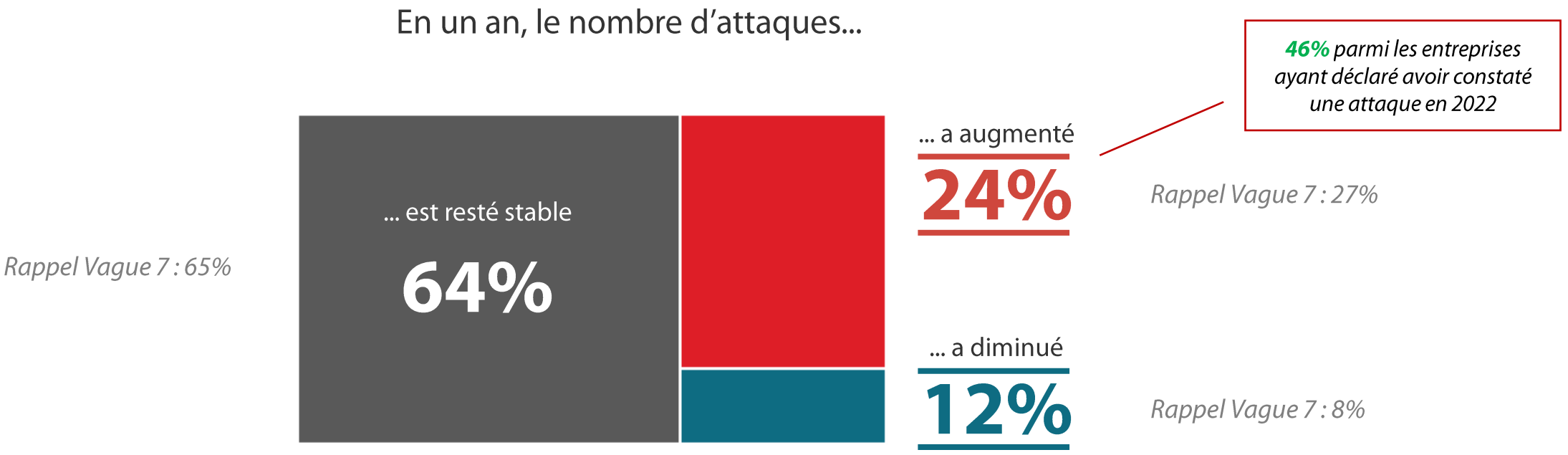


Rappel Vague 7 : 18%

Si le nombre d'attaques par rapport à l'année dernière semble rester stable, une part non-négligeable estime toujours qu'elles ont augmentées

328 personnes

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

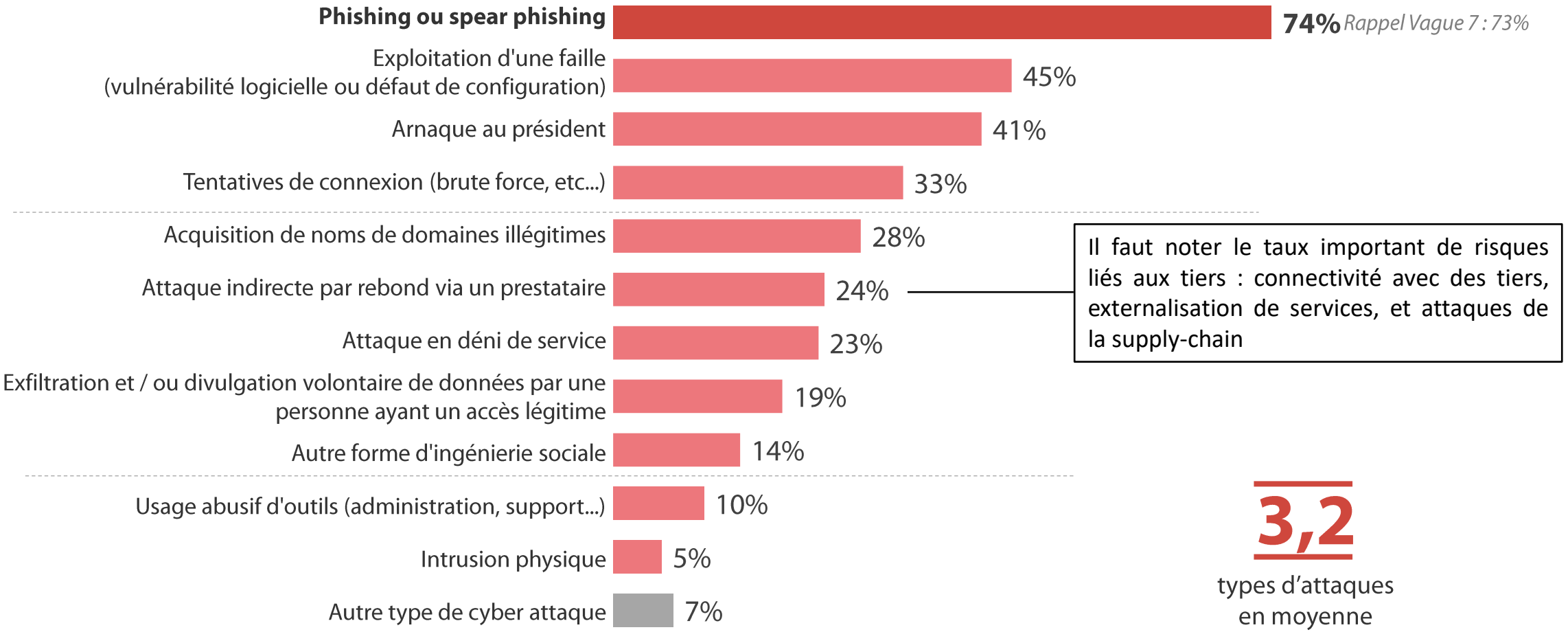


Les entreprises ayant constatées au moins une attaque, en ont subi 3 en moyenne, le phishing ou spear phishing demeurant très nettement le principal vecteur

147 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

45% des entreprises ont subi au moins une cyberattaque en 2022



Il faut noter le taux important de risques liés aux tiers : connectivité avec des tiers, externalisation de services, et attaques de la supply-chain

3,2
types d'attaques en moyenne
parmi ceux ayant subi au moins une attaque

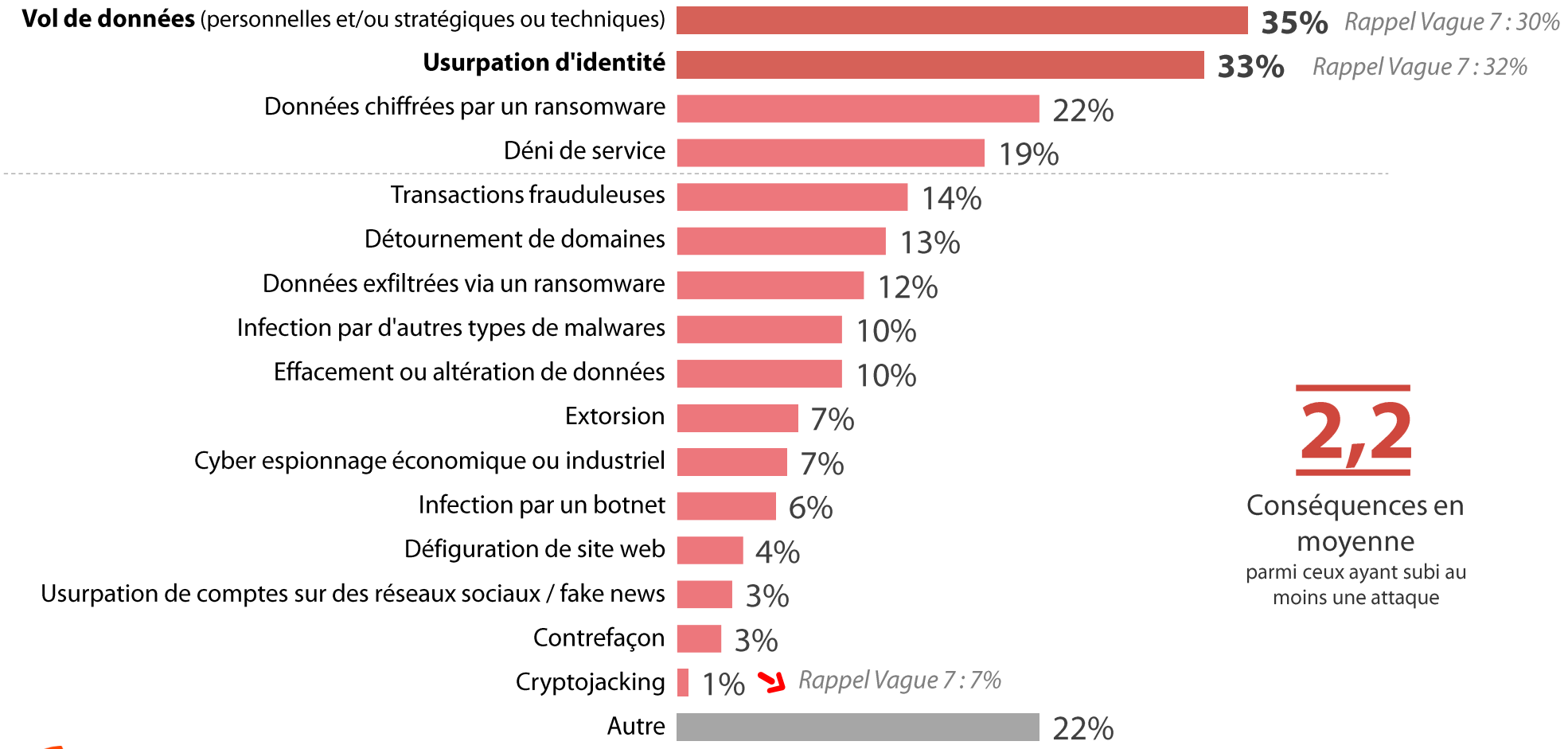
Le vol de données et l'usurpation d'identité restent les conséquences majeures pour les entreprises

147 personnes

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

Base ont constaté une attaque / Plusieurs réponses possibles

45% des entreprises ont subi au moins une cyberattaque en 2022



2,2

Conséquences en moyenne

parmi ceux ayant subi au moins une attaque

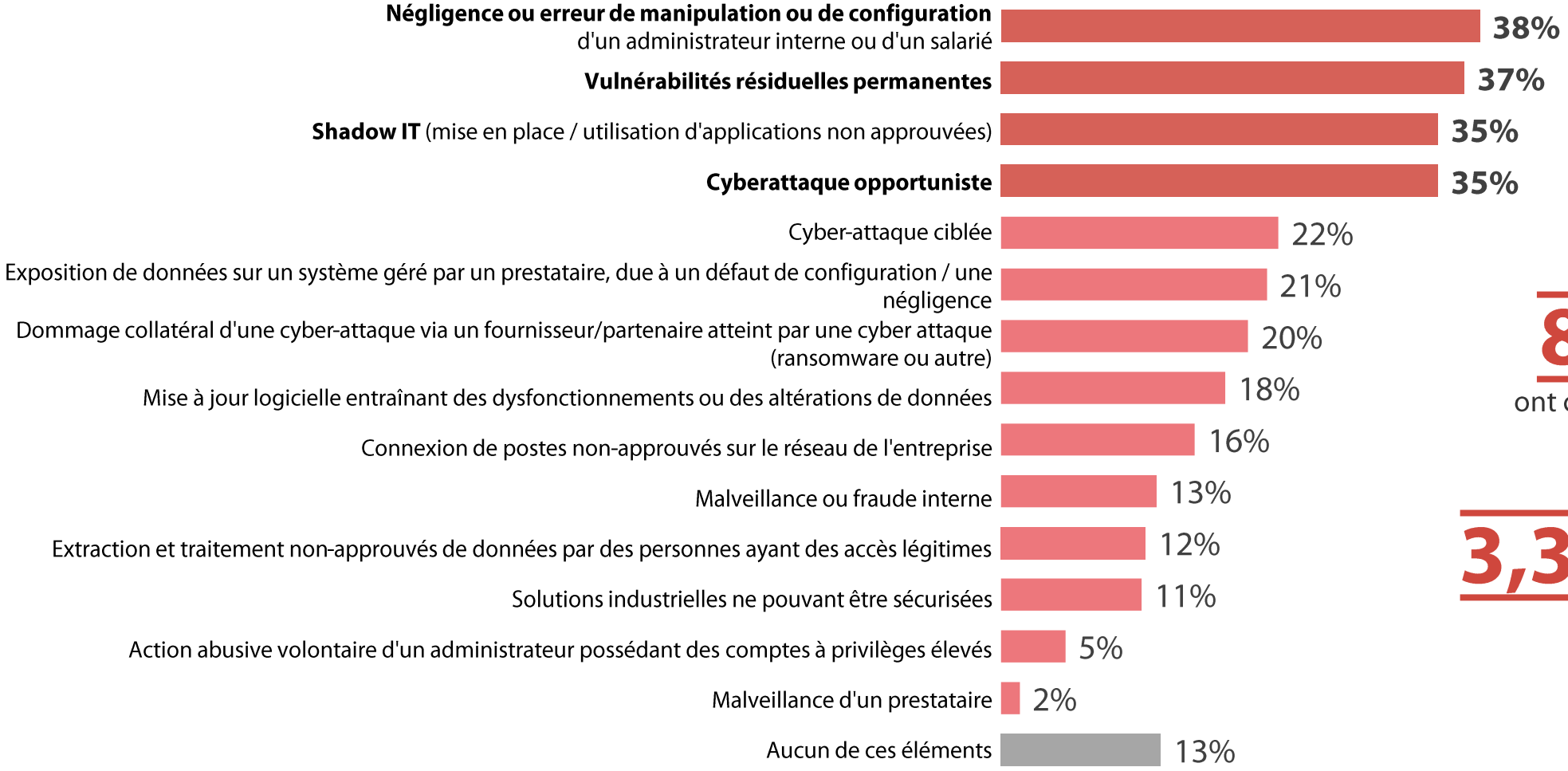
Évolution statistiquement significative par rapport à la vague précédente

Les principales causes des incidents de sécurité résident dans le non-respect des fondamentaux dans les pratiques IT, la gestion des vulnérabilité et le Shadow IT

328 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



87%
ont connu au moins un élément

3,3 éléments en moyenne

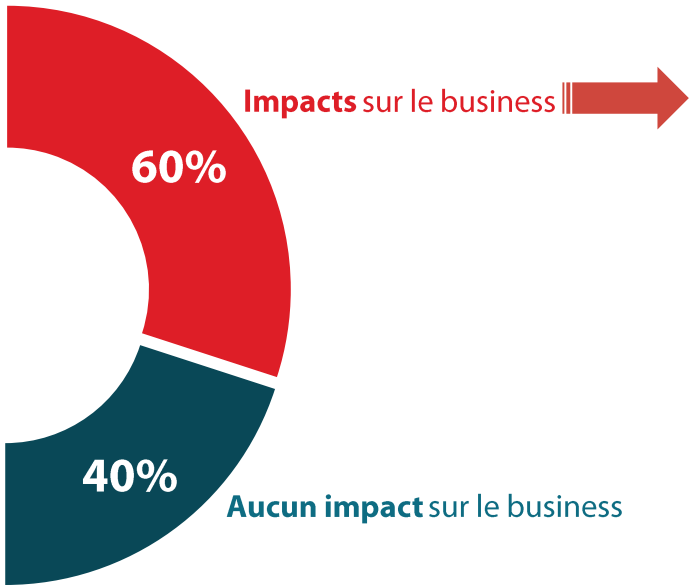
Et comme en 2021, 6 entreprises sur 10 ont noté un impact des cyberattaques sur leur business avec notamment une perturbation de leur production

292 personnes

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

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

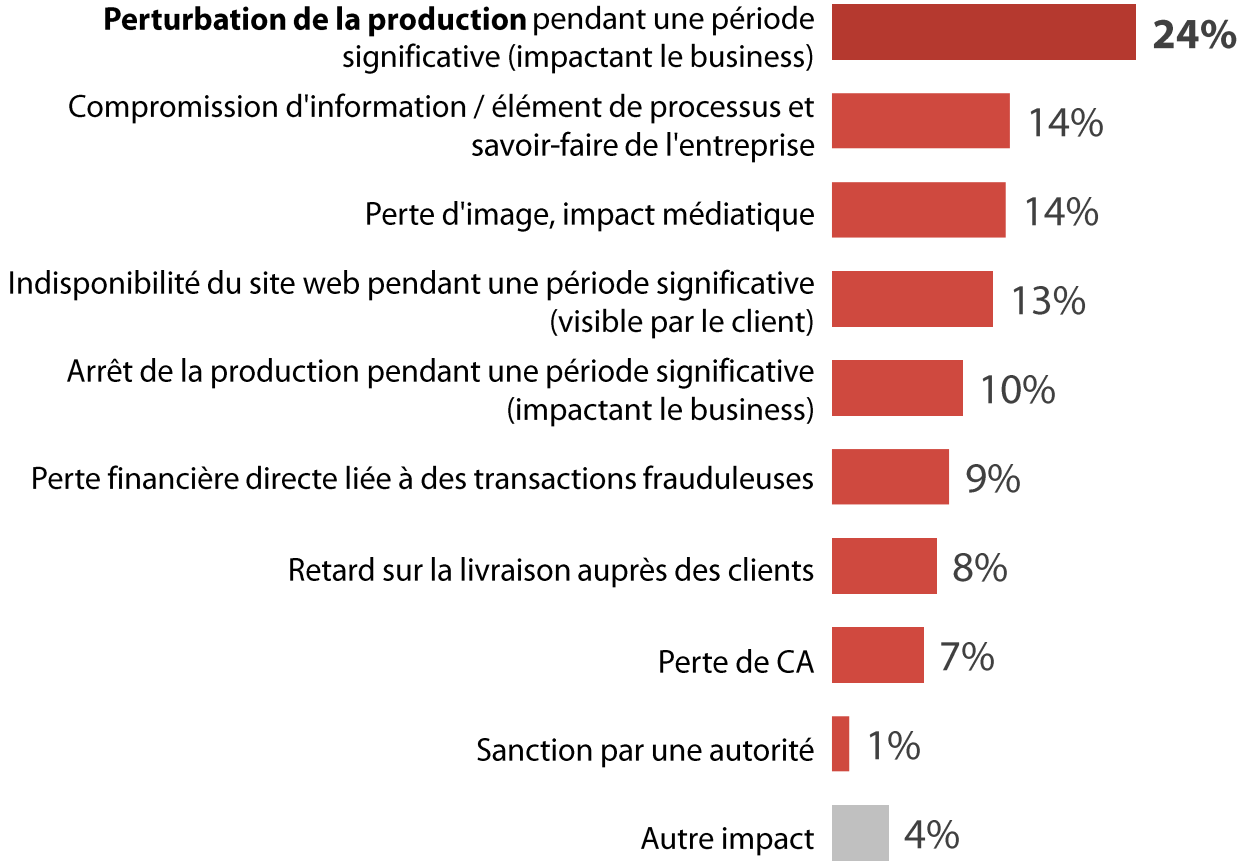
Rappel Vague 7 : 61%



Impacts sur le business

Aucun impact sur le business

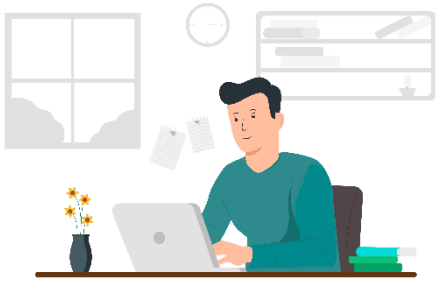
Rappel Vague 7 : 39%

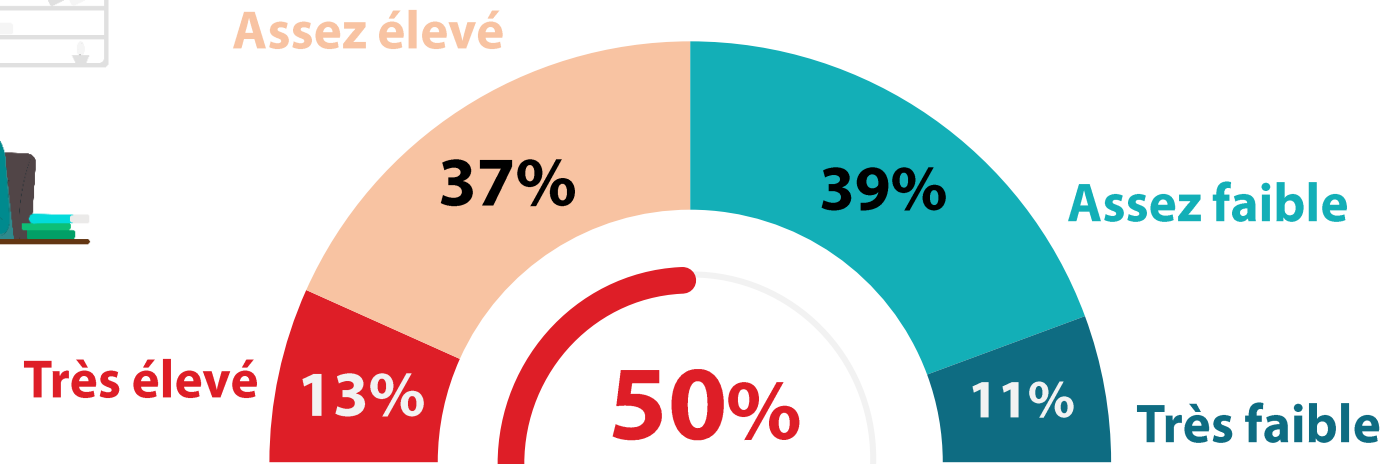


Le niveau des menaces relatives au cyberespionnage est perçu comme élevé par une entreprise sur 2, un chiffre stable par rapport à l'année dernière

328 personnes

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





ESTIMENT UN NIVEAU ÉLEVÉ DES MENACES RELATIVES AU CYBER-ESPIONNAGE

Rappel Vague 7 : 55%

02

…qui peut s’expliquer par une plus grande protection des entreprises

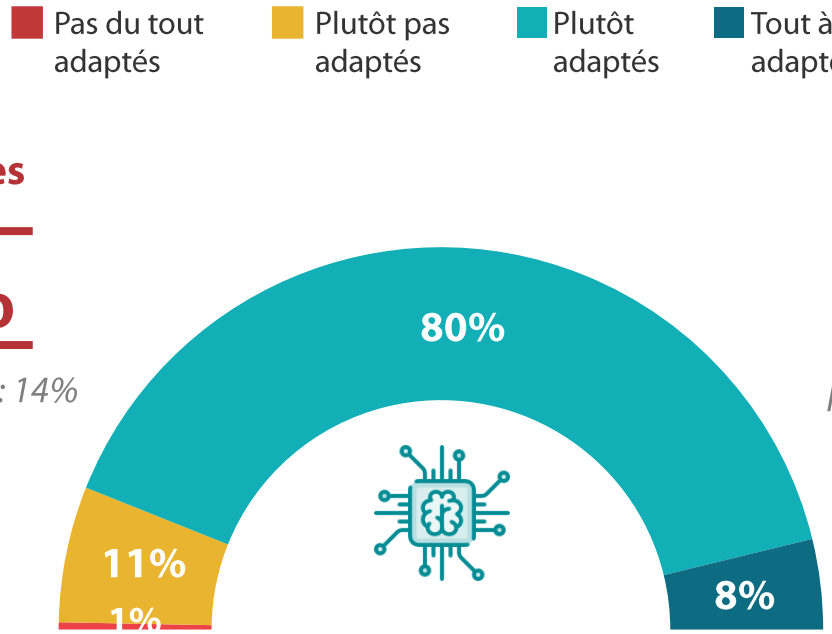
La confiance envers les solutions et services disponibles sur le marché s'intensifie au fil des années

328 personnes

Question modifiée

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

Base ensemble



% Inadaptées

12%

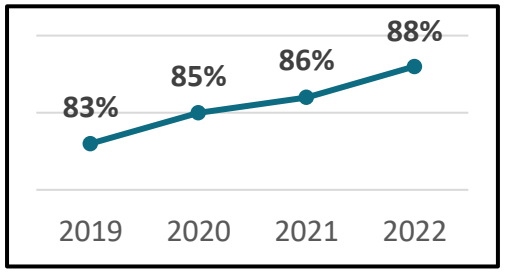
Rappel Vague 7 : 14%

% Adaptées

88%

Rappel Vague 7 : 86%

Rappel vagues précédentes



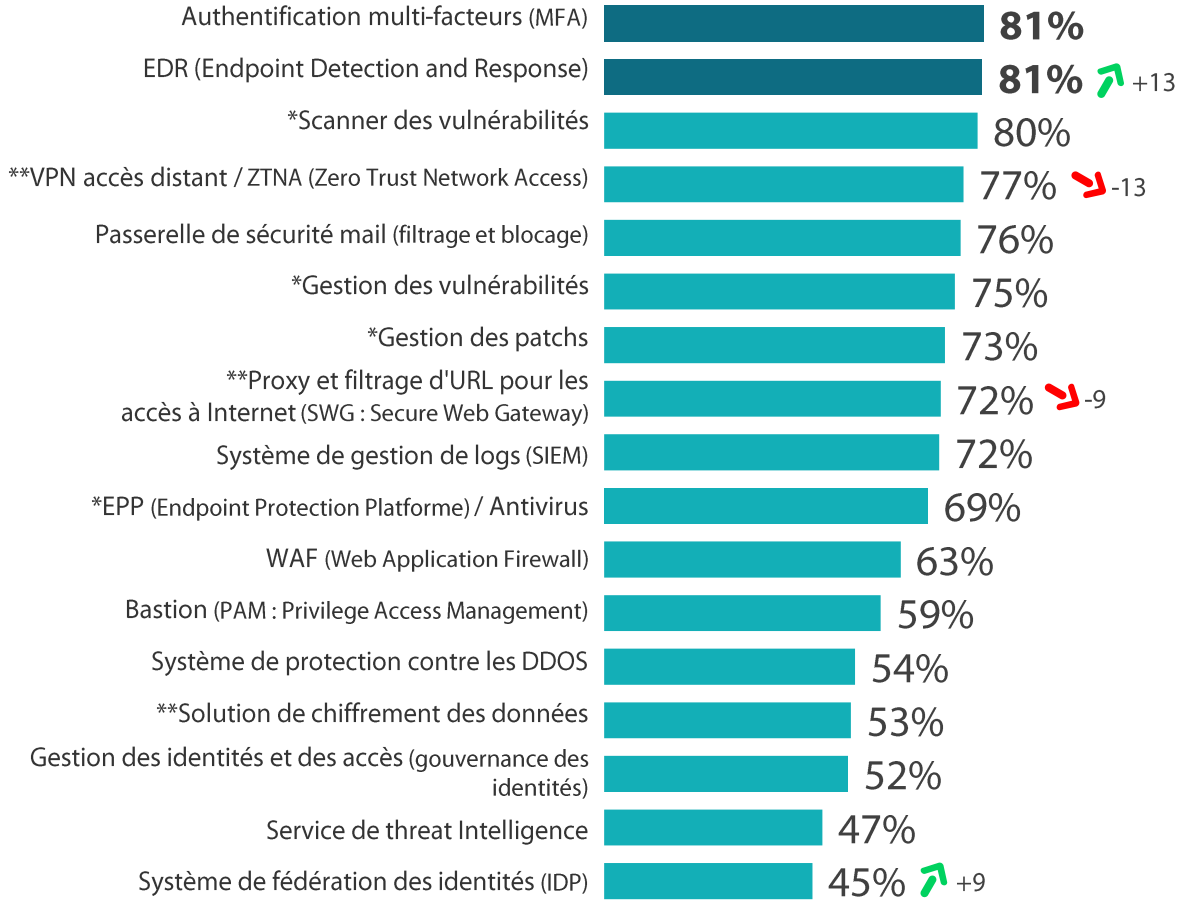
Près de 15 solutions ou services mis en place en moyenne dans les entreprises. On note la place croissante accordée aux outils de détection et de réponse rapide (EDR/NDR) et des outils d'orchestration (SOAR)

328 personnes

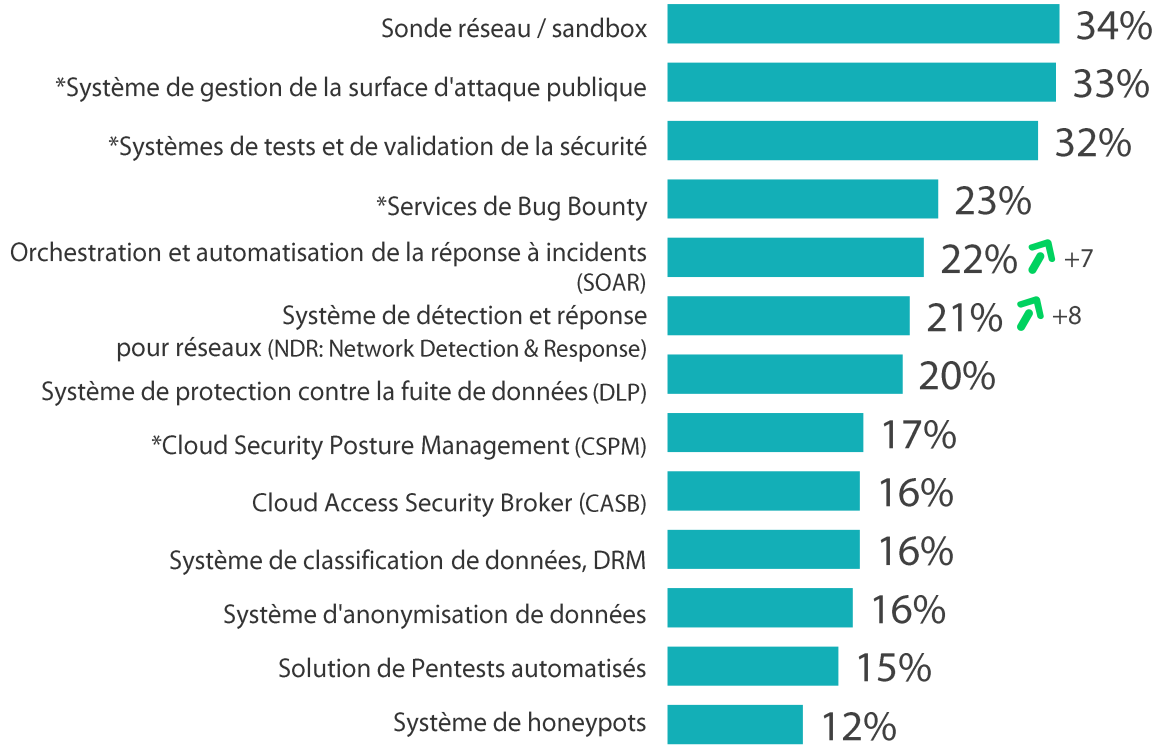
Question modifiée

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



14,9 solutions en moyenne



"opinionway pour CESIN

*Nouvel item
** item modifié

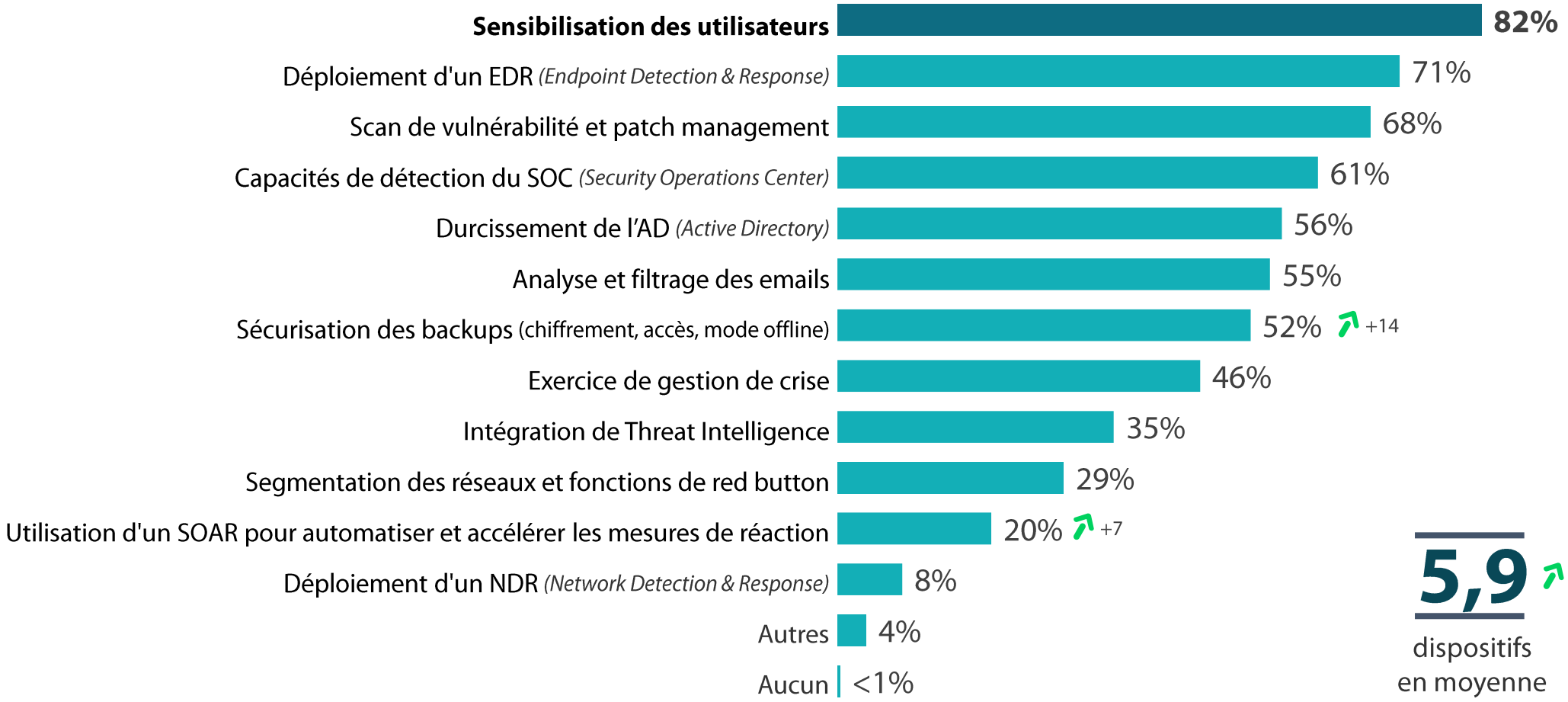
Évolution statistiquement significative par rapport à la vague précédente
Évolution à interpréter avec prudence au vu de l'ajout d'items

Outre le renforcement de la sensibilisation, les RSSI déploient massivement les dispositifs jugés les plus efficaces : l'EDR, les outils de gestion des vulnérabilités et les services de SOC. On note également les efforts en matière de résilience notamment sur la sécurisation des backups

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

Base ensemble / Plusieurs réponses possibles

328 personnes



5,9 +0,4
dispositifs
en moyenne

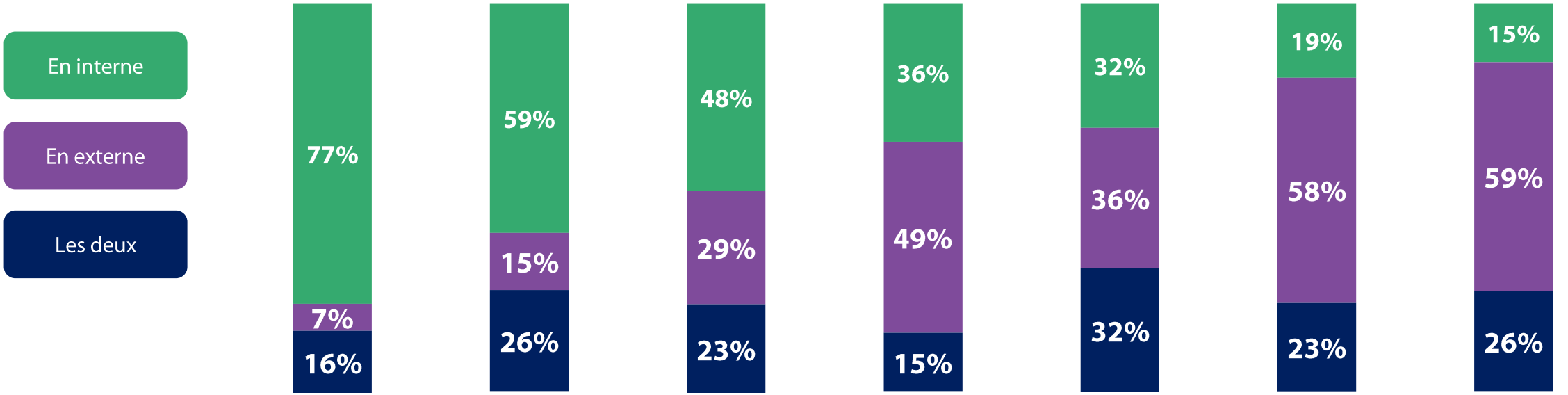
Si la gestion des vulnérabilités est encore majoritairement interne, il faut noter la part significative de l'externalisation des services notamment pour l'EDR ou la gestion de la surface d'attaque qui sont des solutions souvent acquises avec les services opérationnels associés

Nouvelle question

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

Base : solution en place dans l'entreprise

328 personnes



	Gestion des vulnérabilités	EDR	Gestion de la surface d'attaque	CERT – CSIRT	SOC	Threat Intelligence	Pentests
Service pas en place	7%	12%	42%	27%	20%	37%	7%

Les entreprises pensent avoir les moyens de se prémunir d'une cyberattaque de grande ampleur à l'aide de moyens de protection et de détection. En revanche, elles demeurent limitées dans leur capacité de réponse ou de reconstruction post attaque

328 personnes

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

Item modifié

77%

Moyens de prévention et de protection

70%

Moyens de détection

Rappel Vague 7 : 72%

Item modifié

58%

Capacité de réponse aux attaques

Item modifié

53%

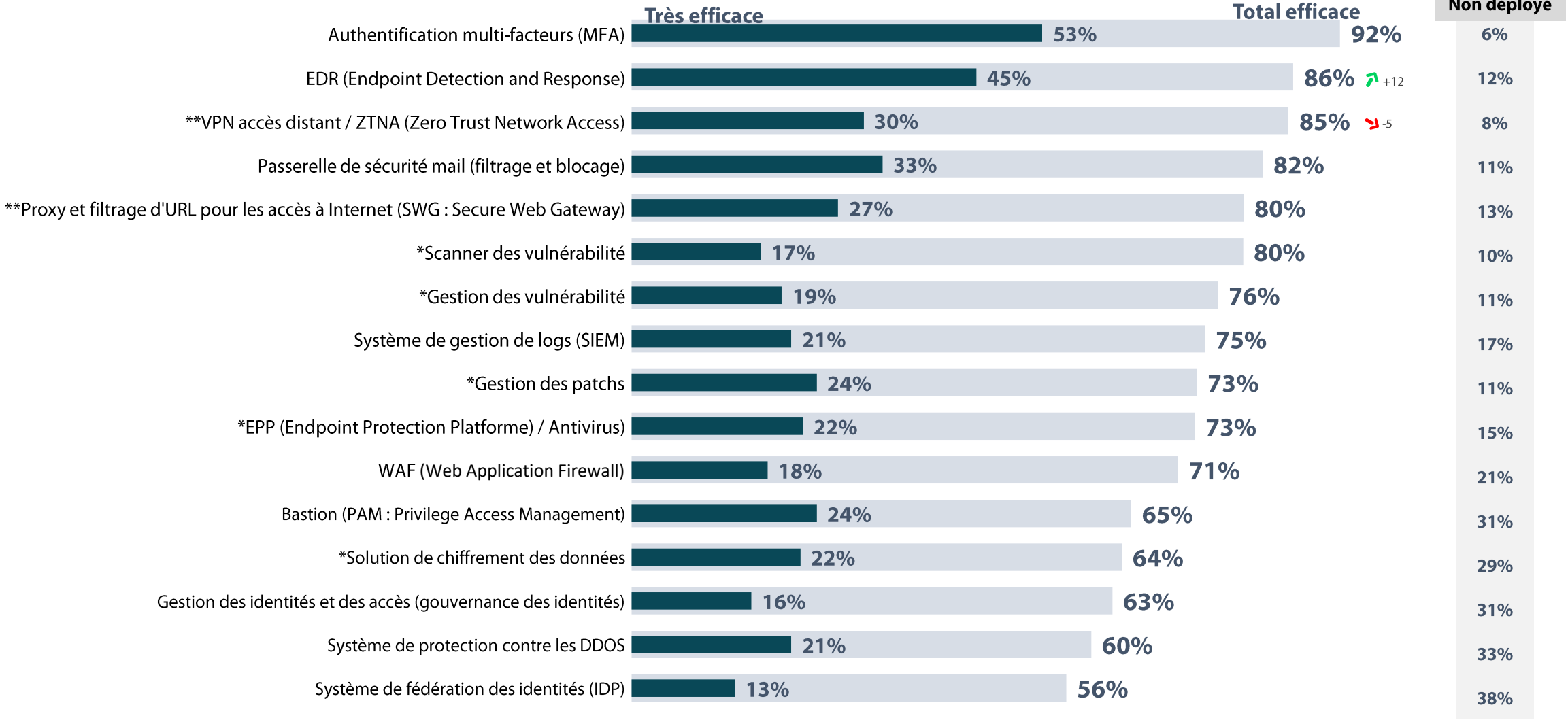
Capacité de reconstruction après l'attaque

On notera un plébiscite du couple MFA/EDR qui sont les deux solutions jugées les plus efficaces dans le contexte actuel, et la confiance de l'EDR a encore augmenté en 2022

328 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

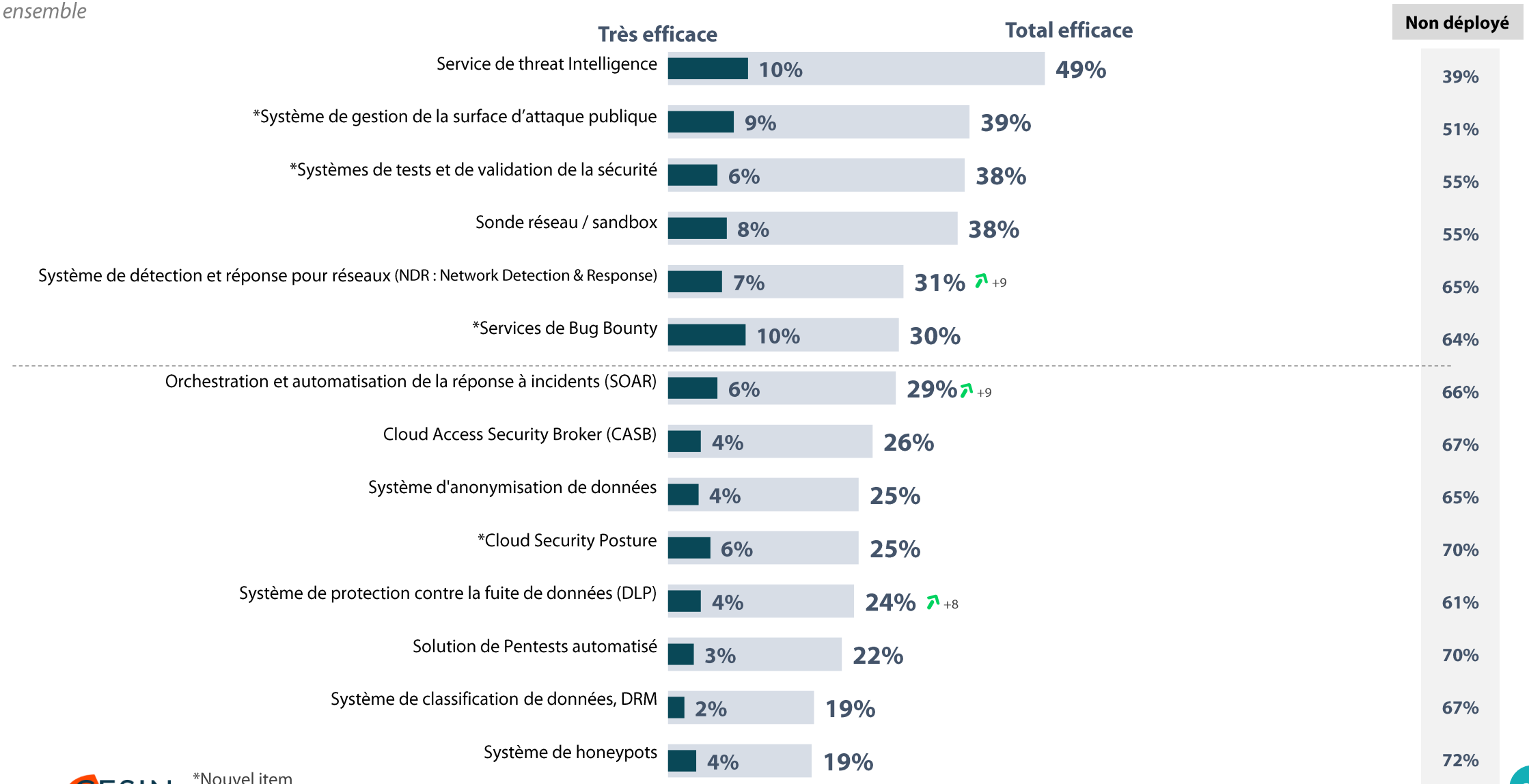


L'efficacité des autres solutions est un peu plus en retrait, un constat qui peut s'expliquer par le déploiement plus faible de ces solutions

328 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



*Nouvel item
** item modifié

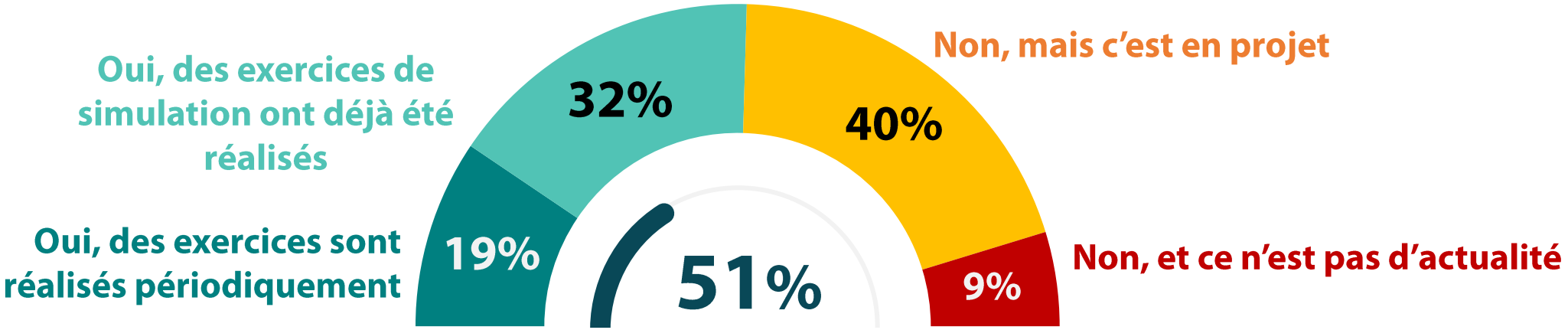
Évolution statistiquement significative par rapport à la vague précédente

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

La moitié des entreprises a mis en place un programme d'entraînement à la crise cyber, un nombre qui ne cesse de croître d'année en année

328 personnes

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



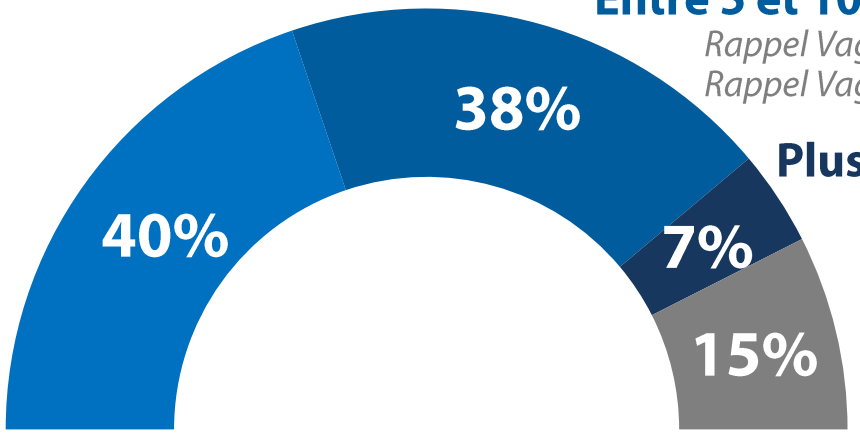
ONT MIS EN PLACE UN PROGRAMME D'ENTRAÎNEMENT À LA CYBER-CRISE

Rappel Vague 7 : 44%

Les budgets cyber se maintiennent voire augmentent légèrement et les budgets sont majoritairement au delà de 5% du budget IT

328 personnes

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



Moins de 5%
Rappel Vague 7 : 40%

Entre 5 et 10%
Rappel Vague 7 : 36%
Rappel Vague 6 : 26%

Plus de 10%
Rappel Vague 7 : 8%

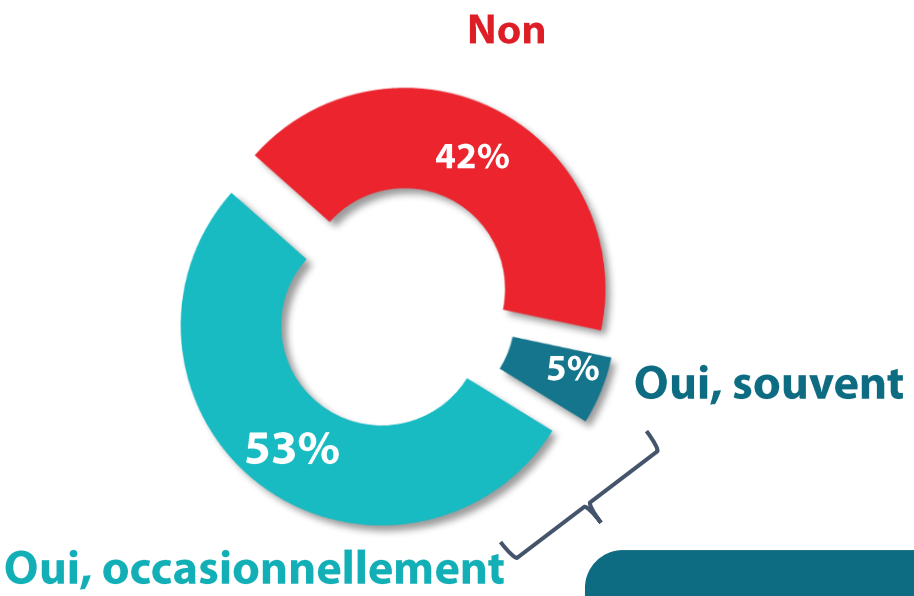
5% ou plus : 45%
Rappel Vague 7 : 44%

Ne sait pas
Rappel Vague 7 : 16%

Un recours à des solutions de start-up pour près de 6 entreprises sur 10

328 personnes

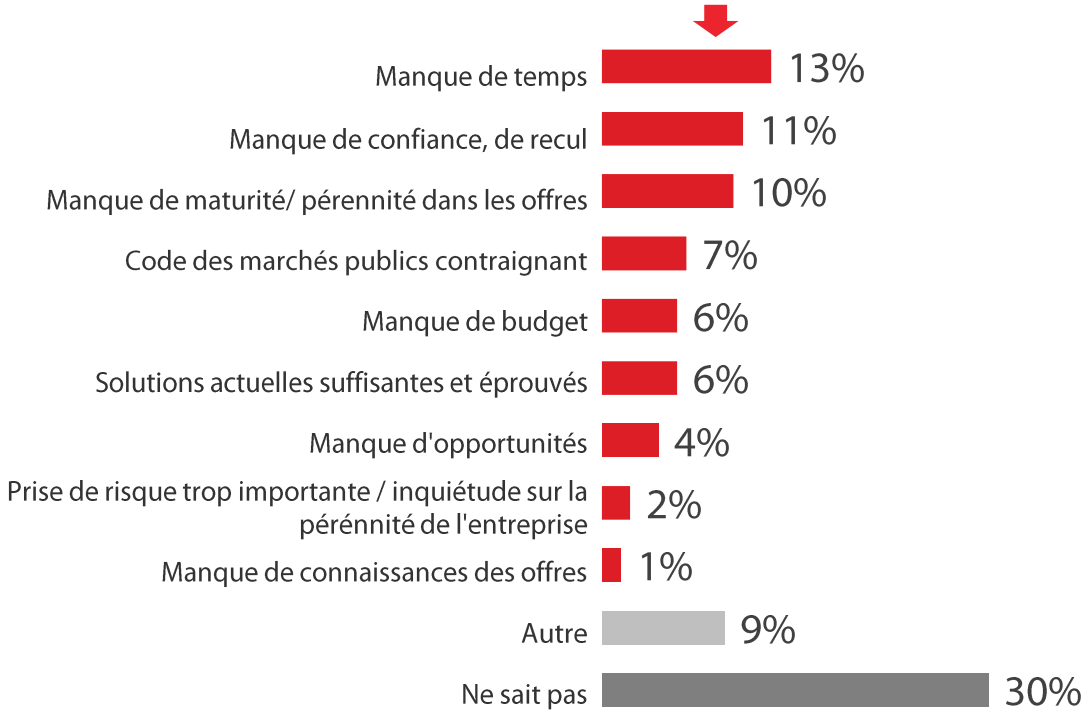
Q26. En matière de cybersécurité, recourrez-vous à des offres innovantes issues de start-up ? *Base ensemble*
Q26bis. Pour quelle(s) raison(s) ne le faites-vous pas ? *Base : ne fais pas appel à des offres issues de start-up (137)*



58% ont recours à des offres innovantes issues de start-up

Rappel Vague 7 : 62%

42% n'ont pas recours à ces offres



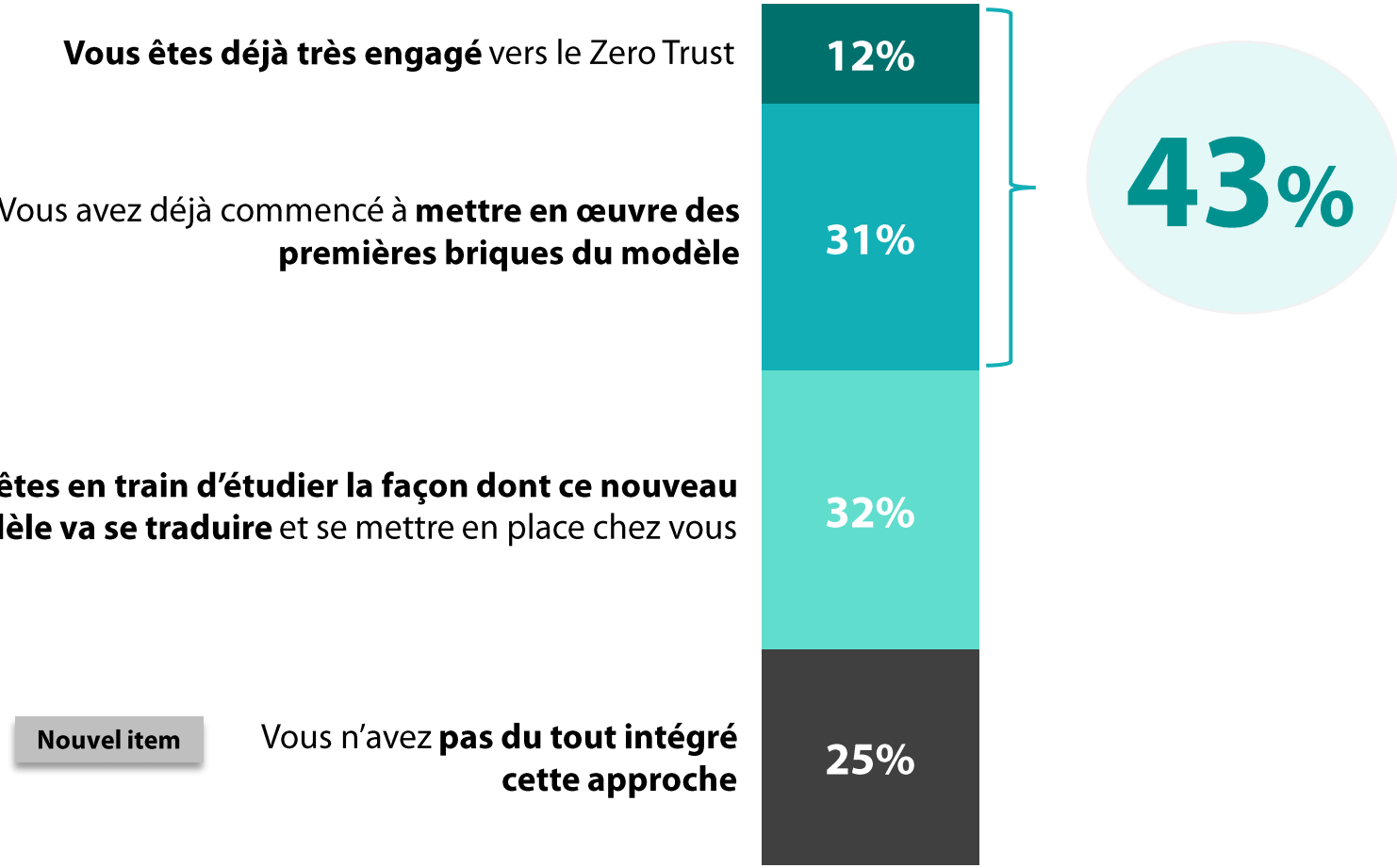
L'approche Zero Trust commence à être mise en place dans les entreprises, même si un quart se montre encore en retrait par rapport à cette approche

328 personnes

Question modifiée

Q28. Quelle est votre vision du concept Zero Trust ?

Base ensemble



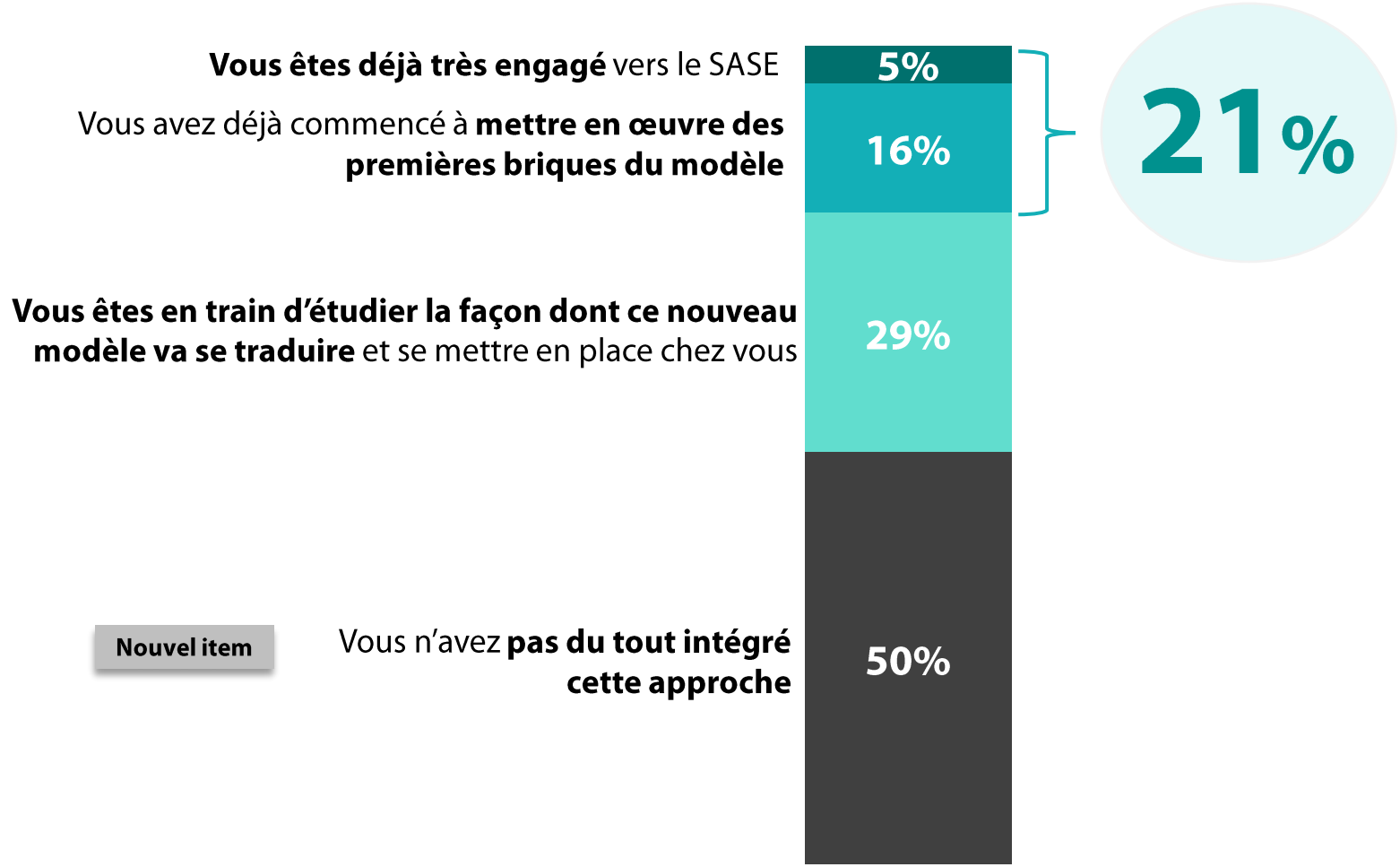
Le concept SASE ne semble pas encore avoir été intégré dans les entreprises

328 personnes

Question modifiée

Q34. Quelle est votre vision du concept SASE ?

Base ensemble



Focus sur…

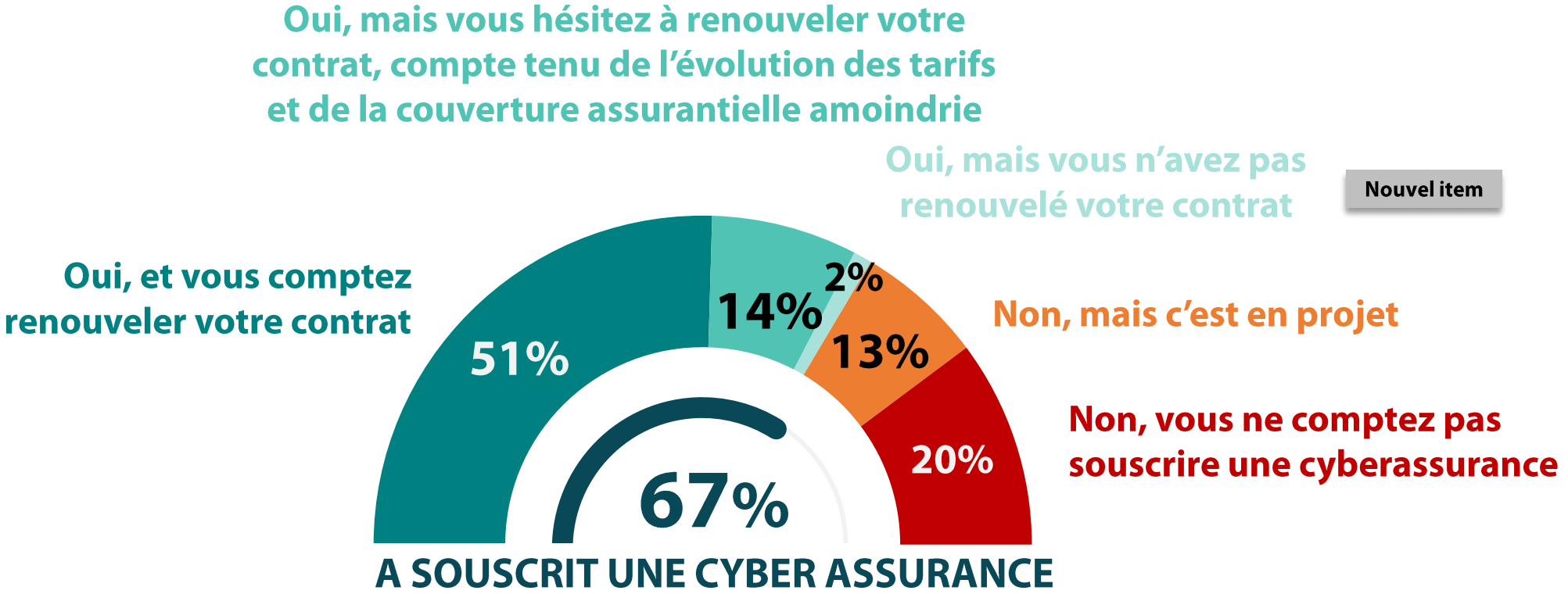
La cyberassurance

Deux tiers des entreprises ont souscrit une cyberassurance, avec toutefois plus d'1 entreprise sur 10 hésitant à renouveler son contrat, notons que 2% des entreprises y ont déjà renoncé

328 personnes

Q31. Avez-vous souscrit une cyberassurance ?

Base ensemble



Trois quarts des entreprises assurées n'ont jamais fait appel à leur cyberassurance

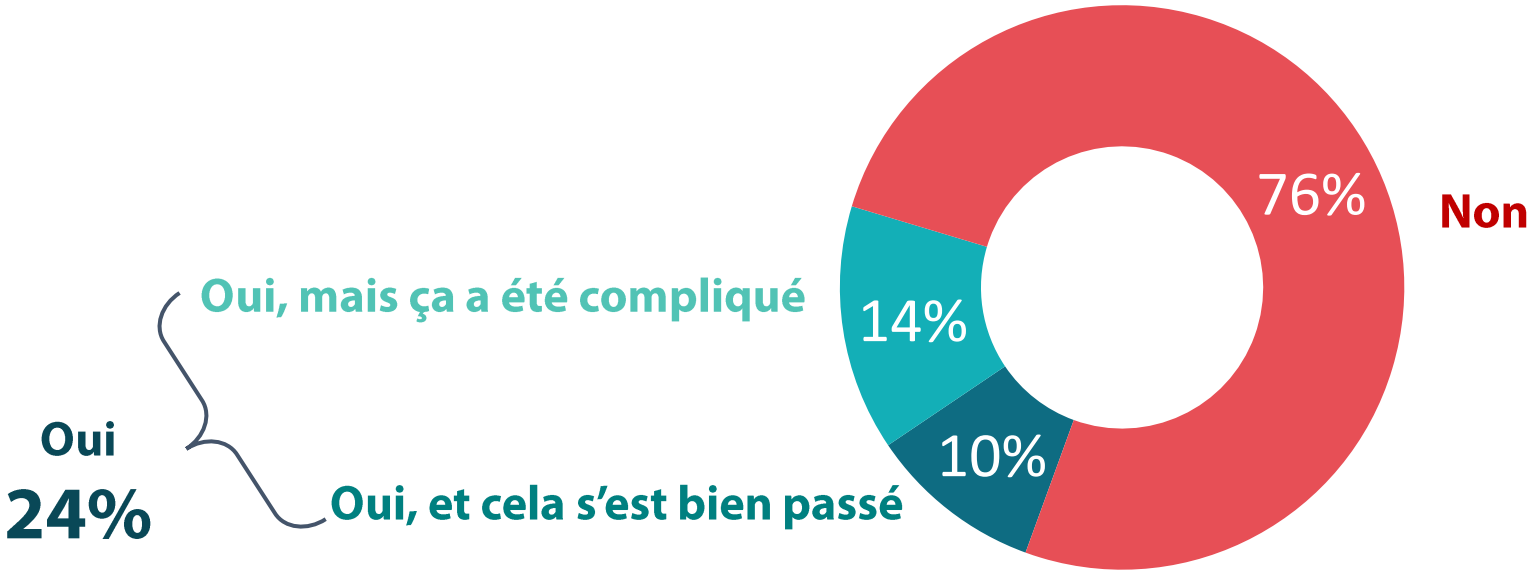
220 personnes

Filtre modifié

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

Base possède une cyber-assurance ou projette d'en posséder une

Utilisation de la cyberassurance



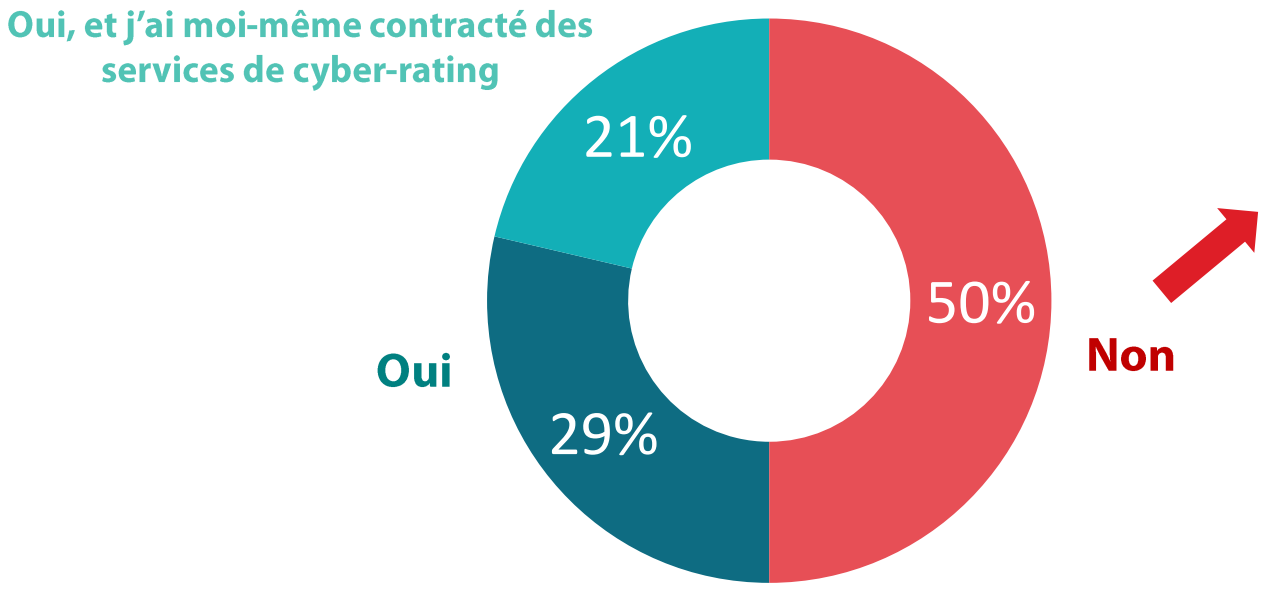
Le recours des cyberassureurs aux services d'agences de notation ne convainc que la moitié des entreprises. Les autres mettent en avant la qualité discutable des analyses

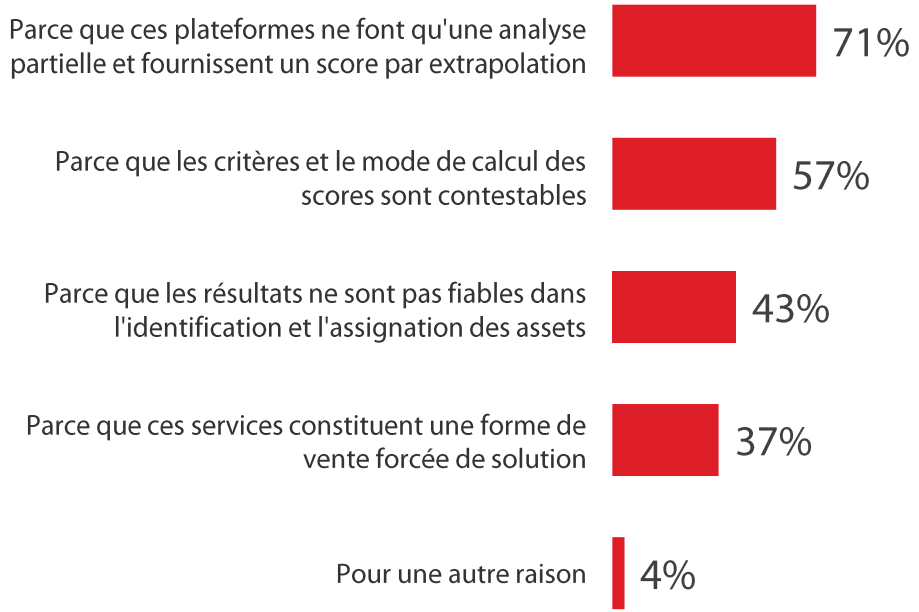
328 personnes

Question modifiée

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 (164)*

Le recours au service d'agence de notation



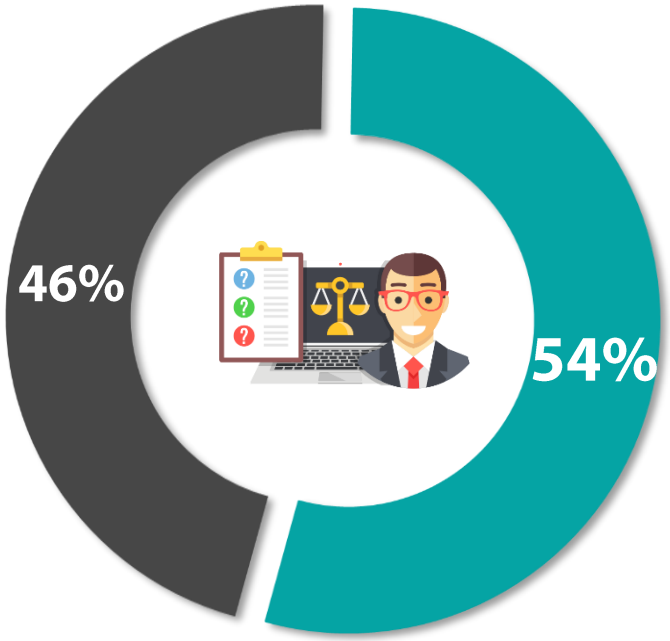


Comme pour 2021, près de la moitié des entreprises ayant subi une attaque ont déjà porté plainte…

147 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

45% des entreprises ont subit au moins une cyberattaque en 2022



pour **toutes les attaques** : **27%**

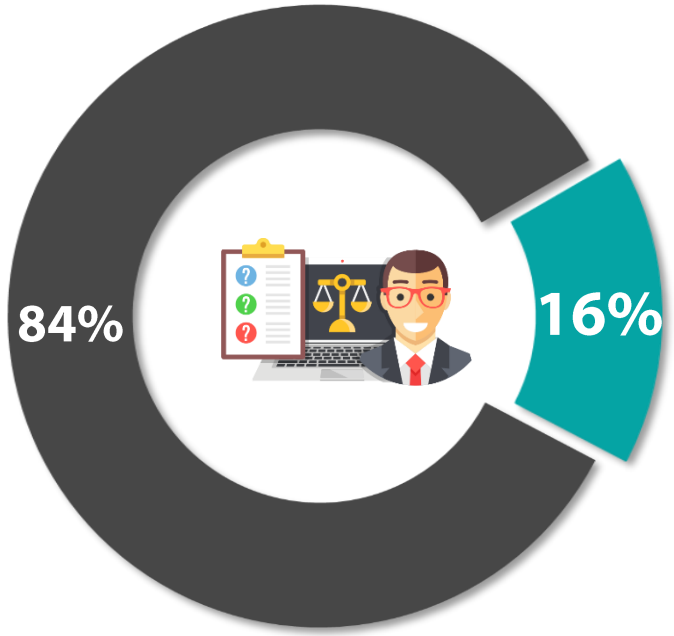
pour **certaines attaques** : **27%**

…mais l'identification/l'interpellation des attaquants se produit rarement

80 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

54% des entreprises ont porté plainte



Oui, l'enquête a permis une identification
Rappel Vague 7 : 16%

pour **toutes les plaintes: 4%**

pour **certaines plaintes : 12%**

03

Des salariés sensibilisés, mais qui doivent désormais appliquer les recommandations, notamment celles en lien avec le Cloud

Si les actions de sensibilisation aux cyber-risques sont entreprises pour un grand nombre d'utilisateurs, 2/3 seulement suivent les recommandations

328 personnes

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

85%

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

Rappel Vague 7 : 82%

66%

Les utilisateurs **respectent les recommandations**

Rappel Vague 7 : 70%

17%

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

Rappel Vague 7 : 18%

Si les administrateurs, architectes et développeurs semblent avoir bien été sensibilisés, ils manquent néanmoins d'expertise sur le plan de la sécurité

328 personnes

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

70%

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

Rappel Vague 7 : 68%

47%

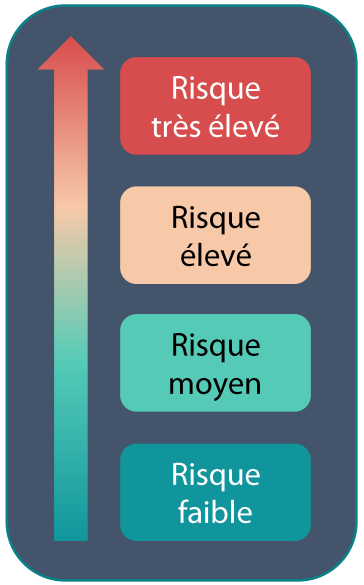
Les administrateurs, architectes et développeurs sont suffisamment formés et ont acquis l'expertise nécessaire, notamment sur les nouvelles technologies

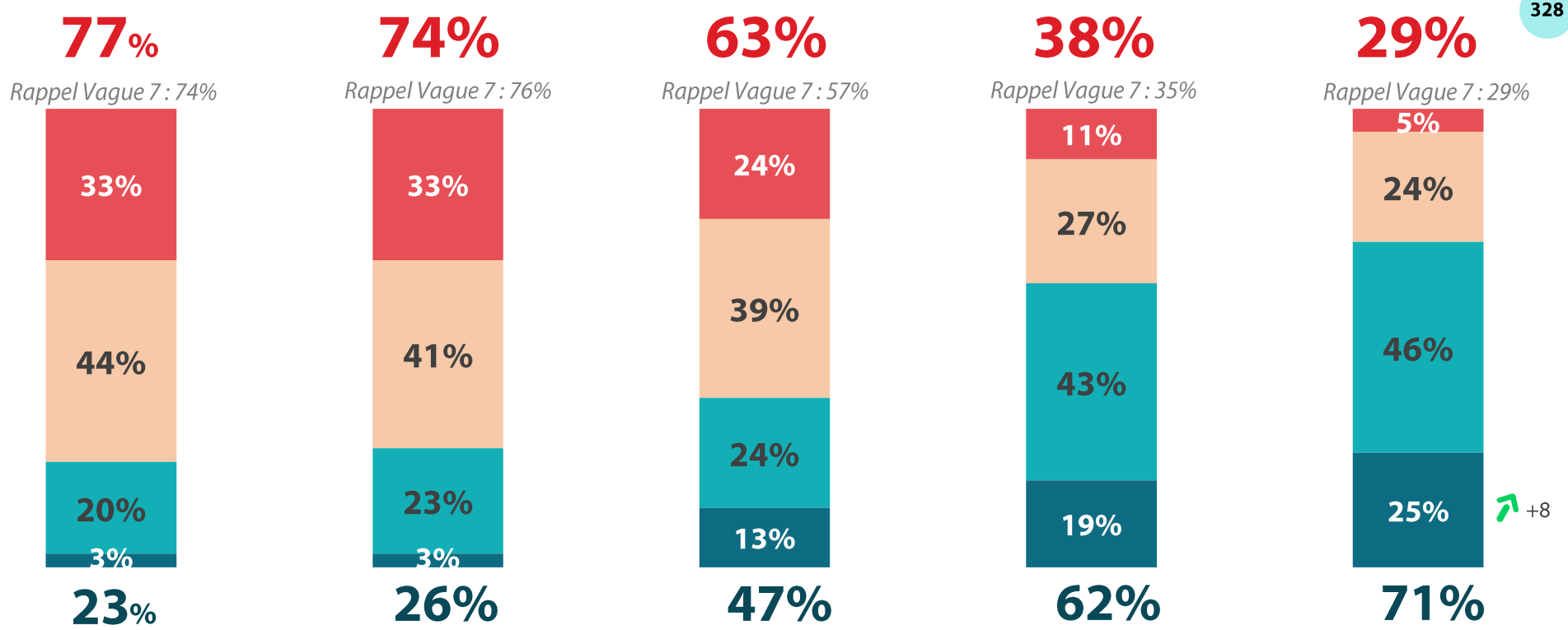
Item modifié

Similairement à 2021, les usages numériques perçus comme les plus risqués cette année résident autour du Cloud au travers du Shadow IT et l'exposition des données par les utilisateurs. Les risques relatifs au télétravail et aux usages personnels des équipements professionnels semblent désormais mieux maîtrisés

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

328 personnes





Les facteurs de risques de l'usage du Cloud résident tout d'abord sur la non-maîtrise de la chaîne de sous-traitance de l'hébergeur et la difficulté de contrôler les accès par des administrateurs de l'hébergeur

328 personnes

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 2021	% Un risque fort	
1	51%	**Non maîtrise de la chaîne de sous-traitance de l'hébergeur**
2	49%	**Difficulté de contrôler les accès par des administrateurs de l'hébergeur**
3	43%	Expertise encore trop rare, attendue de la part des architectes et des administrateurs
	42%	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
	40%	Difficulté de mener des audits (test d'intrusion, contrôle des configurations, visite sur site)
4	40%	Mauvaise visibilité de l'inventaire des ressources qu'il y a dans le cloud
	37%	Stockage des données dans des datacenters à l'étranger, hors du droit français
	36%	Non-effacement des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
	35%	Non-maîtrise des paramètres de sécurité / chiffrement faible de la part de l'hébergeur
	35%	Maîtrise difficile de l'utilisation qui en est faite par les salariés de votre entreprise
	32%	Difficulté ou impossibilité d'alimenter le SIEM par des logs provenant du Cloud
	32%	Indisponibilité des données / de l'application due à une attaque de l'hébergeur
	32%	Forte fréquence des nouvelles versions mises en ligne avec des potentielles évolutions non contrôlées des principes ou paramètres de sécurité
5	31%	Confidentialité des données vis-à-vis de l'hébergeur
	31%	Non-effacement des données au cours de l'usage, les suppressions et purges opérées par le client n'étant pas réellement effectives
	29%	Attaque par rebond depuis l'hébergeur
	27%	Défaut de cloisonnement entre les différents clients de l'hébergeur
	27%	Traitement et exploitation des données par l'hébergeur à l'insu de ses clients
	26%	Propagation systémique des attaques et erreurs humaines qui surviendraient au niveau de l'hébergeur
	23%	Non-restitution des données par l'hébergeur en fin de contrat (normal ou anticipé) alors que c'est prévu contractuellement
	16%	Piégeage d'une application hébergée

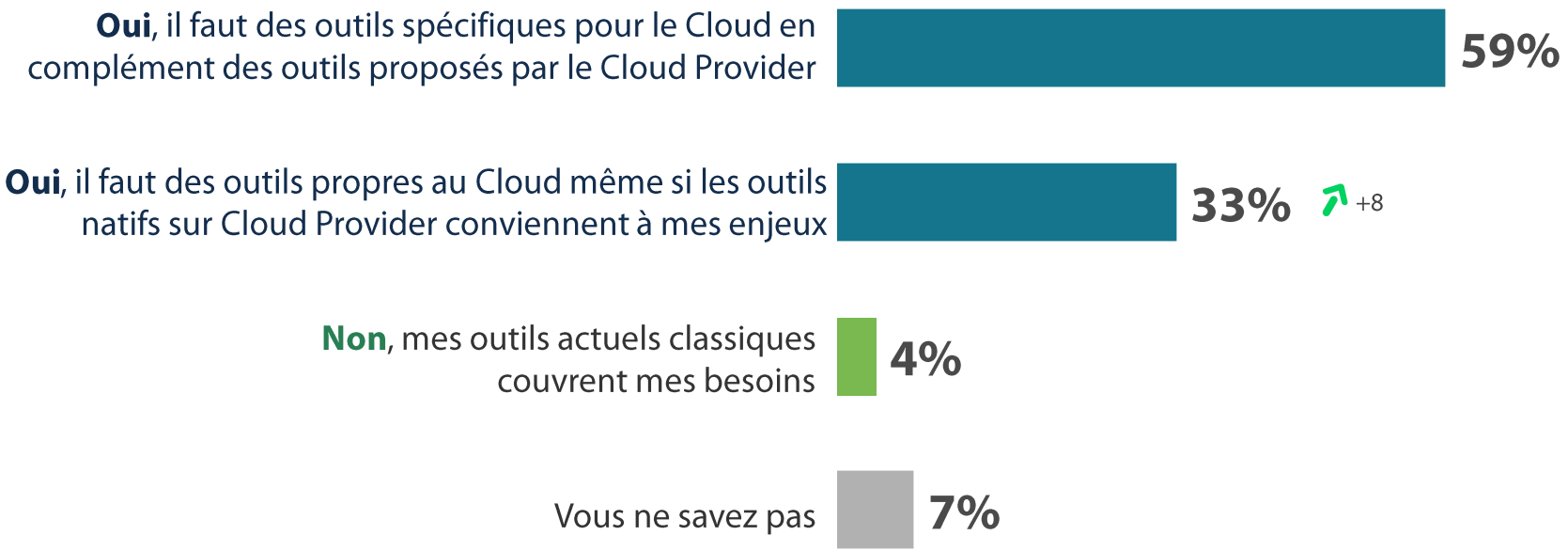
Les RSSI considèrent qu'il faut des outils spécifiques pour surveiller le Cloud, pas nécessairement ceux proposés nativement par les Cloud Providers

328 personnes

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

… 89% estiment que la sécurisation des données stockées dans le Cloud requiert des outils spécifiques

Rappel Vague 7 : 86%



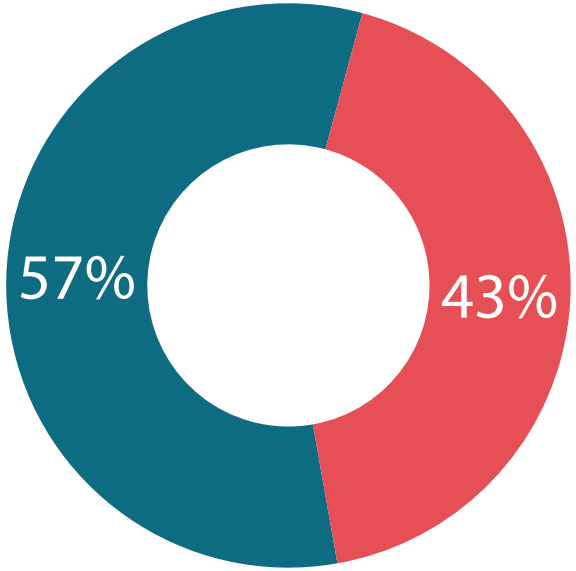
Les sujets de souveraineté et de Cloud de Confiance préoccupent près de 6 entreprises sur 10

328 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

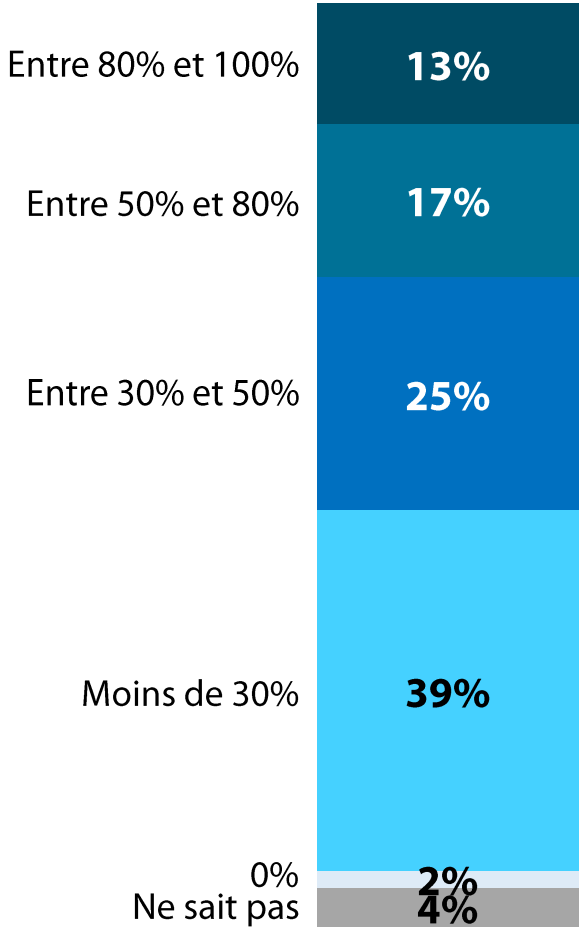
Le cloud représente moins de 50% du SI dans encore beaucoup d'entreprises

328 personnes

Question modifiée

Q20. Quelle est la part du Cloud dans votre SI, que ce soit en mode Iaas, Paas ou Saas ?

Base ensemble



04

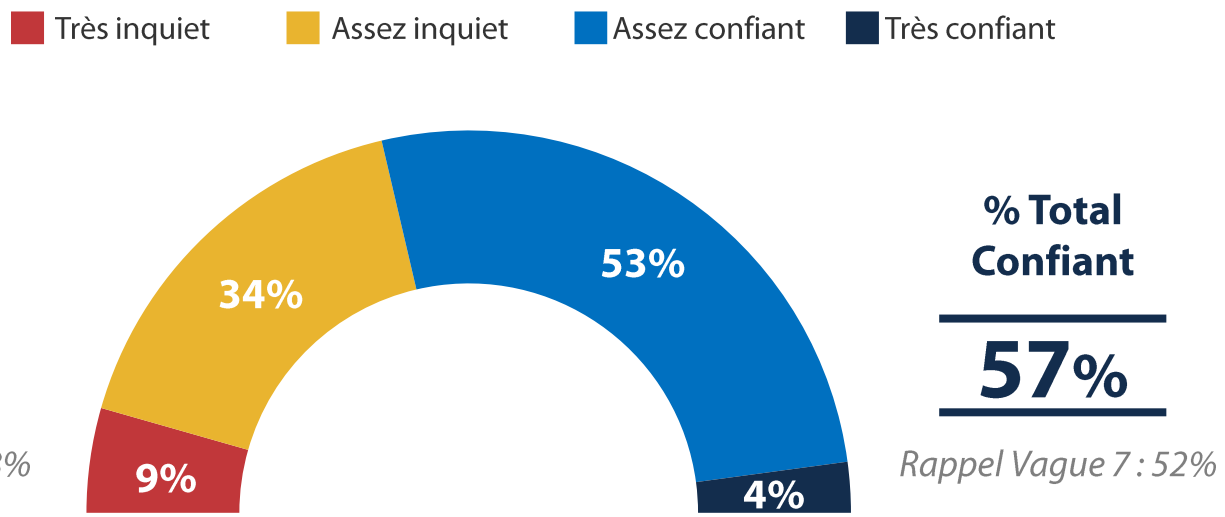
La cybersécurité reste un enjeu primordial pour les entreprises

Les entreprises nourrissent encore une inquiétude à l'égard de leur capacité à faire face aux cyber-risques à l'avenir, même si la confiance est orientée à la hausse

328 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

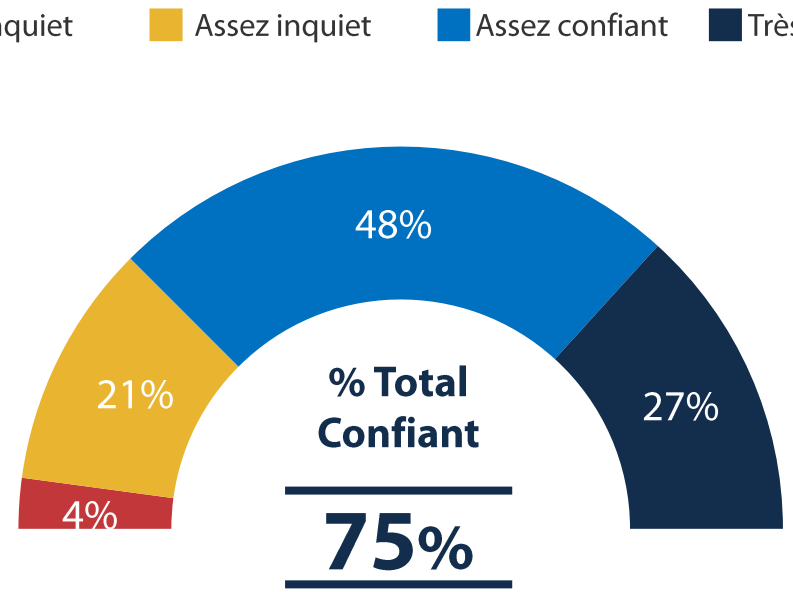


La cybersécurité est perçue comme un sujet important et pris en compte au sein du COMEX

328 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 7 : 79%

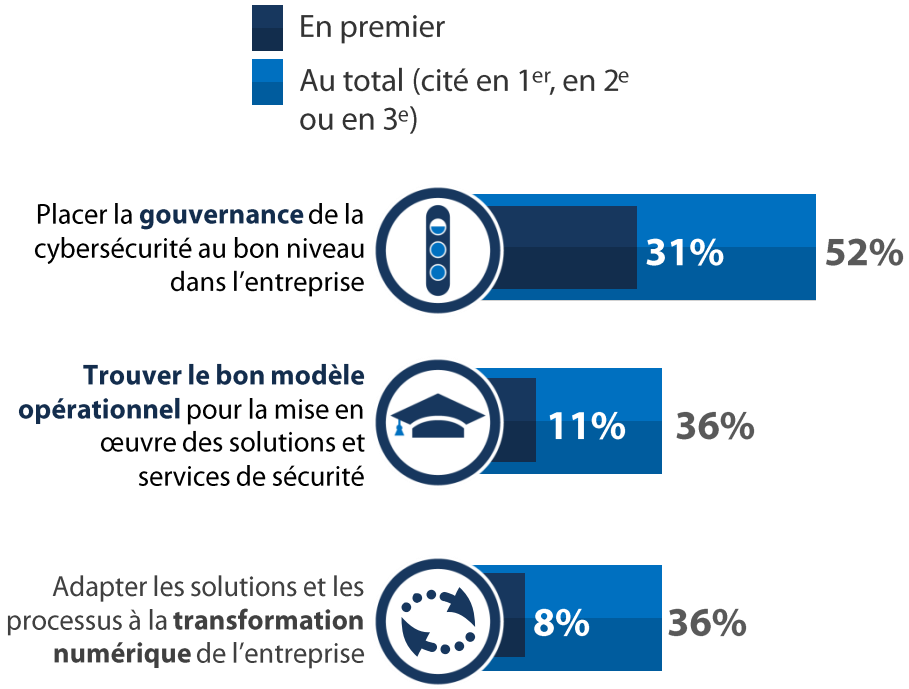
L' enjeu principal de demain autour de la cybersécurité réside dans la bonne structuration de gouvernance de la cybersécurité dans l'entreprise.

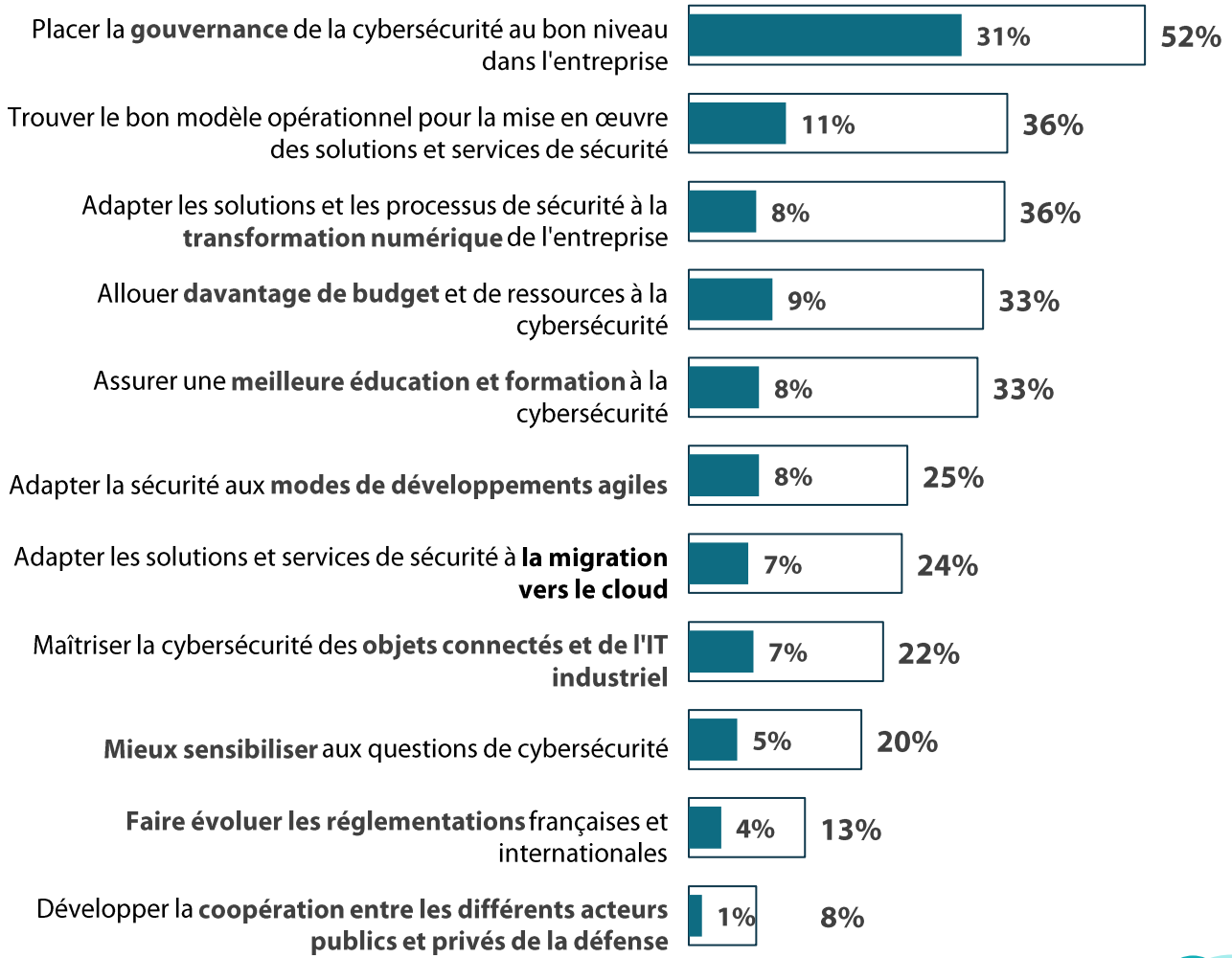
328 personnes

Items modifiés

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





Évolution statistiquement significative par rapport à la vague précédente

Dans ce contexte, près de 2/3 des entreprises prévoient une augmentation des budgets alloués à la protection contre les cyber-risques, une proportion moins élevée qu'en 2021

328 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 7 : 70%

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

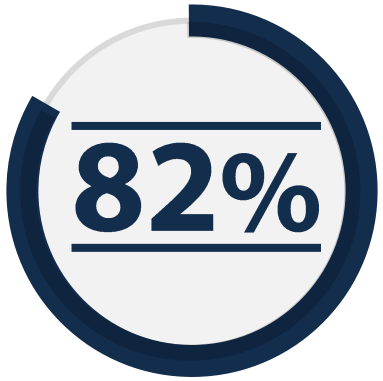
Rappel Vague 7 : 56%

Plus de 8 entreprises sur 10 ont prévu d'acquérir de nouvelles solutions de protection

328 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 7 : 84%

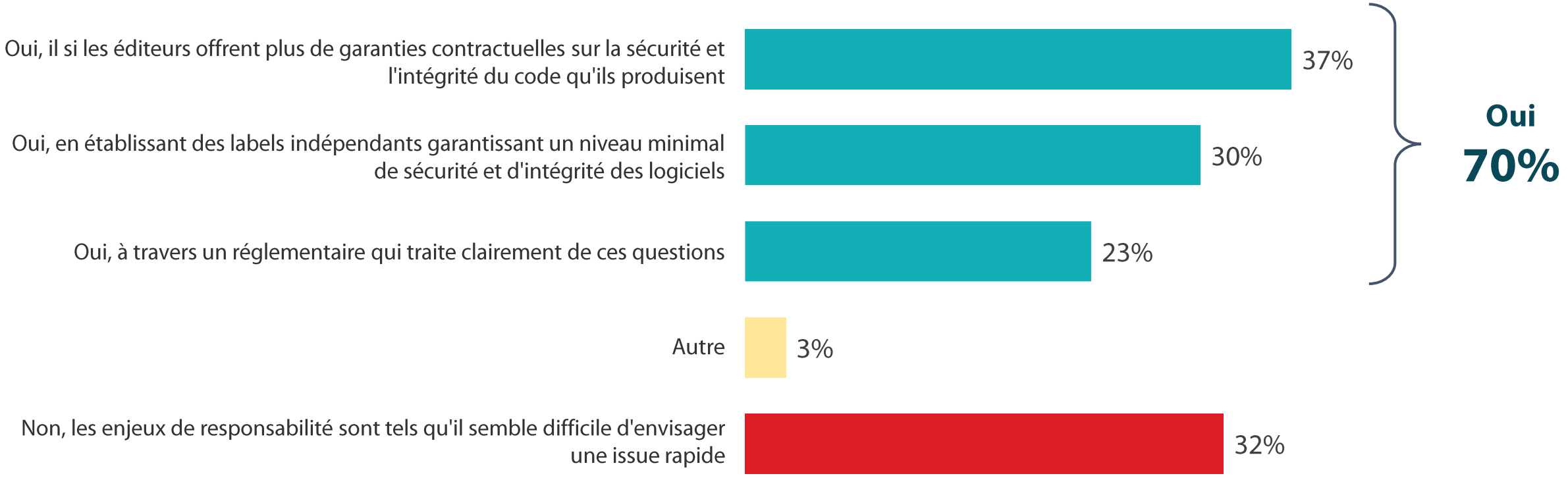
La majorité des entreprises estime que les questions de sécurité de la supply chain peuvent trouver une issue, à la condition d'une plus grande garantie du code et des labels

Items modifiés

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

Base ensemble / plusieurs réponses possibles

328 personnes



La synthèse

Une dynamique de baisse des cyberattaques

Une tendance baissière qui se confirme : 45% des entreprises déclarent avoir subi au moins une attaque en 2022

La part d'entreprises déclarant avoir subi au moins une cyberattaque impactante en 2022 ne cesse de baisser depuis quelques années (54% en 2021 et 57% en 2020 et 65% en 2019), toutefois il en demeure encore près d'1 sur 2.

Une baisse du nombre de cyberattaques réussies qui peut s'expliquer par les différentes mesures de prévention, de protection et de détection/réaction mises en place qui portent aujourd'hui leurs fruits.

Le phishing ou spear phishing reste très nettement le principal vecteur d'attaque. Des cyberattaques donnant surtout lieu à des vols de données et à des usurpations d'identité, et qui in fine, impactent assez fortement le business des entreprises (60%), au travers notamment de perturbations de la production.

La sensibilisation des utilisateurs au cœur de la lutte contre les cyberattaques

Pour plus de 8 entreprises sur 10, la 1ère étape pour réduire les risques de cyberattaque consiste à sensibiliser les utilisateurs.

Les actions de sensibilisation aux cyber-risques sont largement proposées aux utilisateurs, bien que deux tiers seulement d'entre eux suivent les recommandations.

Les administrateurs, architectes et développeurs semblent eux avoir bien été sensibilisés même s'ils manquent d'expertise sur ce sujet.

Par ailleurs, on notera que les programmes d'entraînement à la crise cyber rencontrent de plus en plus de succès (51% en 2022 et 44% en 2021 et 33% en 2020).

Une intensification des solutions mises en place pour lutter

Une mise en place de nombreuses solutions de cybersécurité, avec un déploiement plus marqué de l'EDR

Aujourd'hui, les entreprises détiennent de multiples solutions et services de lutte contre les cyberattaques. On note par ailleurs la place croissante des outils de détection et de réponse rapide, comme l'EDR (81%, +13 points) et le NDR (21%, +8 points).

Les RSSI renforcent les dispositifs jugés les plus efficaces comme l'EDR, les outils de gestion des vulnérabilités ou encore les services de SOC.

Une cyber-assurance aux profits limités

Près de 2/3 des entreprises ont souscrit une cyber-assurance. Toutefois, un peu moins d'1 sur 5 hésite à renouveler son contrat, un constat qui peut s'expliquer par le faible recours à leur cyber-assurance.

Par ailleurs, le recours aux services d'agences de notation ne semble pas donner plus de légitimité aux cyberassureurs.

Des données Cloud à sécuriser

Les usages numériques autour du Cloud constituent un risque important (77%) selon les RSSI.

La part du cloud dans le SI des entreprises reste encore minoritaire : moins de 50% pour près de 2/3 d'entre-elles. En effet, son utilisation peut être perçue comme risquée, notamment au regard des facteurs tels que la non-maîtrise de la chaîne de sous-traitance de l'hébergeur ou la difficulté de contrôler les accès par des administrateurs de l'hébergeur.

Dans ce contexte, la quasi-totalité des RSSI (89%) estime que l'utilisation du Cloud doit s'accompagner d'outils spécifiques pour sa surveillance, n'étant pas forcément proposés par les Cloud Providers.

Un enjeu toujours essentiel pour demain

La cybersécurité : un enjeu d'avenir pour les entreprises

Même si la part d'entreprises victimes de cyberattaques est en baisse, l'inquiétude subsiste :

- 50% estiment que les menaces relatives au cyberespionnage dans leur entreprise sont élevées
- 43% se disent inquiètes en ce qui concerne leur capacité à faire face aux cyber-risques, une part importante même si la confiance est orientée à la hausse (57% vs 52% en 2021).

De la même manière qu'en 2021, les entreprises sont assez confiantes concernant leur capacité de se prémunir d'une cyberattaque de grande ampleur, mais elles doutent de leur capacité de réponse ou de reconstruction post attaque.

Et c'est dans ce contexte que les entreprises envisagent pour la plupart la prise en compte des enjeux de la cybersécurité au sein de leur COMEX, car le principal objectif pour la cybersécurité de demain réside dans la bonne structuration de gouvernance de cette thématique dans l'entreprise.

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.

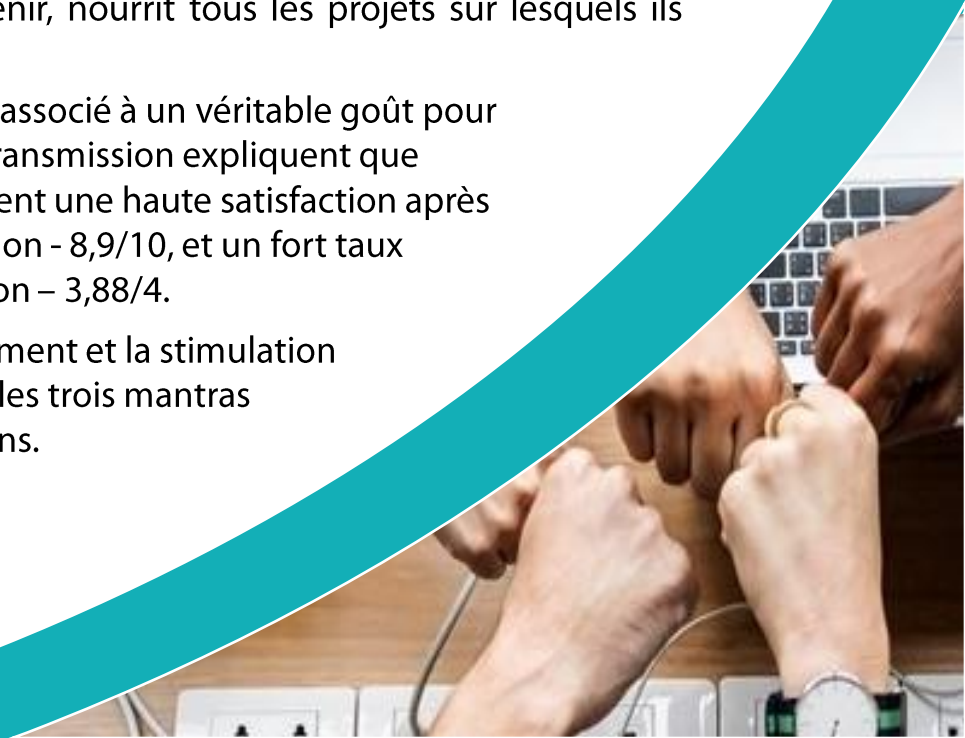
RENDRE LE MONDE INTELLIGIBLE POUR AGIR AUJOURD'HUI ET IMAGINER DEMAIN

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