Club des Experts de la Sécurité de l'Information et du Numérique

Baromètre de la cyber-sécurité des entreprises

Vague 4 - Janvier 2019

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

OpinionWay, 15 place de la République, 75003 Paris

Sommaire

CESIN

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.

MÉTHODOLOGIE

Méthodologie

Méthodologie

Étude quantitative réalisée par OpinionWay auprès de **174 membres du CESIN**, à partir du fichier membre du CESIN (498 contacts).

Mode d'interrogation

L'échantillon a été interrogé par Internet sous système **CAWI** (*Computer Assisted Web Interview*).

Dates de terrain

Du **23 novembre** au **26 décembre 2018**.

Certification

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

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

« **Sondage OpinionWay pour le CESIN** »

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

MESSAGES CLÉS

Messages clés (1/2)

Les enseignements à retenir

1. Un impact de plus en plus décisif des cyber-attaques

Si le nombre de cyber-attaques constatées tend à se stabiliser, huit entreprises sur dix continuent d'être touchées chaque année.

- L'**impact de ces cyber-attaques sur le business** est remonté par 59% des répondants, soit **10 points de plus** que l'année dernière.
- Le **phising** est le mode d'attaque le plus fréquent (73% en ont été victimes), tandis que **l'arnaque au président** touche cette année une entreprise sur deux, soit plus que ce que l'on pourrait croire.
- Le **shadow IT** est le **cyber-risque le plus répandu**, cité par 64% des répondants comme étant un cyber-risque à traiter.

2. Cloud et IoT : des risques accrus avec la transformation numérique

Toutes les entreprises (98%) estiment que la transformation numérique a un impact sur la sécurité des systèmes d'information et les données. En tête des enjeux : le **recours massif au Cloud**, utilisé par 87% des entreprises dont 52% dans des Clouds publics. Un mode de stockage qui pose des **problèmes de non-maîtrise**, que ce soit par rapport **à l'accès aux données** de l'entreprise par les hébergeurs (via les administrateurs ou autres) ou par rapport à **la chaîne de sous-traitance** pratiquée par le fournisseur. En ce qui concerne l'IoT, la caractéristique la plus marquante reste les **failles de sécurité** présentes dans ces objets.

Ces enjeux qui impliquent pour les RSSI de **ne pas se contenter des solutions de sécurité proposées par les prestataires de service** Cloud et de disposer d'**outils de sécurisation supplémentaires** par rapport à ceux proposés par le prestataire, d'après 89% d'entre eux.

Messages clés (2/2)

Les enseignements à retenir

3. Face aux cyber-risques, une cyber-résilience à développer

Pour contrer ces cyber-risques, les RSSI déploient une panoplie de **solutions techniques**, globalement jugées **adaptées à leurs besoins** (75%), même si des progrès restent à faire dans leur adaptation à la transformation numérique. À noter **l'enjeu de l'IA** : 56% des répondants ont mis en place des solutions basées sur l'IA ou envisagent de le faire ; cependant, 55% estiment que **l'IA ne se substituera pas à l'expertise humaine** en matière de sécurité.

Pour autant, les RSSI sont moins confiants que l'année dernière quant à la capacité de leur entreprise à faire face aux cyber-risques (51% sont confiants, -12 points) ; et **moins d'un sur deux considère en particulier que son entreprise est préparée à gérer une cyber-attaque de grande ampleur**. Dans ce cadre, les souscriptions de cyber-assurance sont en hausse (+10 points), mais **seule une entreprise sur dix a mis en place un véritable programme de cyber-résilience**.

4. Trois enjeux pour l'avenir, avant tout humains

D'après les RSSI, l'enjeu principal pour l'avenir de la cyber-sécurité est celui de **la formation et de la sensibilisation des utilisateurs** (61%). Les usages des salariés apportent en effet leur lot de risques, notamment via le shadow IT. Et si les salariés sont sensibilisés, ils restent peu impliqués en ne suivant pas forcément les recommandations. Un important travail de pédagogie reste à faire.

La **gouvernance de la cyber-sécurité** doit également être placée au bon niveau pour 60% des RSSI. Malgré un impact positif de la mise en conformité RGPD sur la gouvernance (59% des entreprises), la confiance en la capacité des COMEX à prendre en compte les enjeux de la cyber-sécurité est très inégale en fonction des secteurs d'activité.

Les **ressources humaines** risquent de poser problème, avec une **pénurie de profils** constatée par 91% des RSSI… À l'heure où 50% des répondants prévoient d'augmenter les effectifs alloués à la protection contre les cyber-risques.

CESIN

RÉSULTATS

1. UN IMPACT DE PLUS EN PLUS DÉCISIF DES CYBER-ATTAQUES

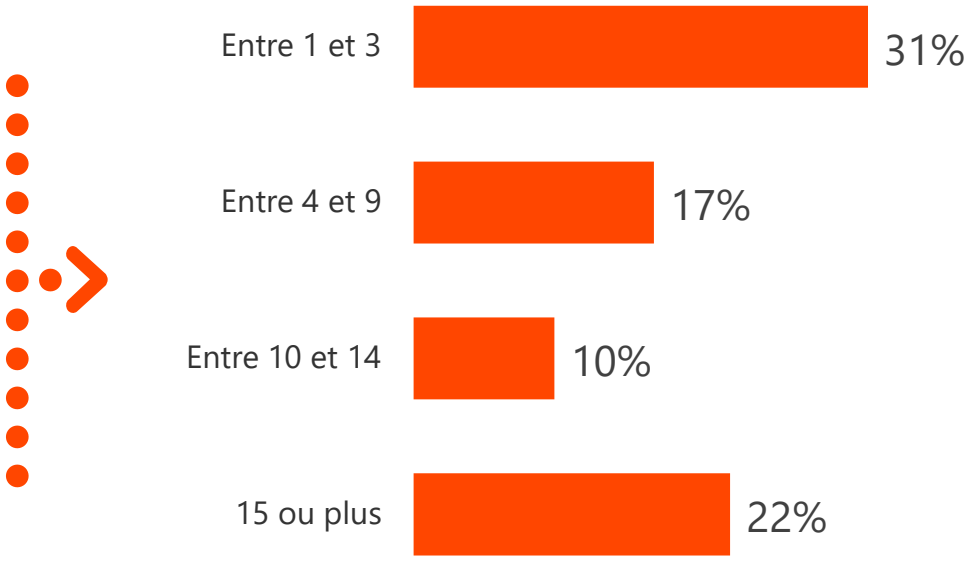
CESIN

Le taux d'entreprises touchées par une cyber-attaque reste très élevé

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (174 répondants)

80%

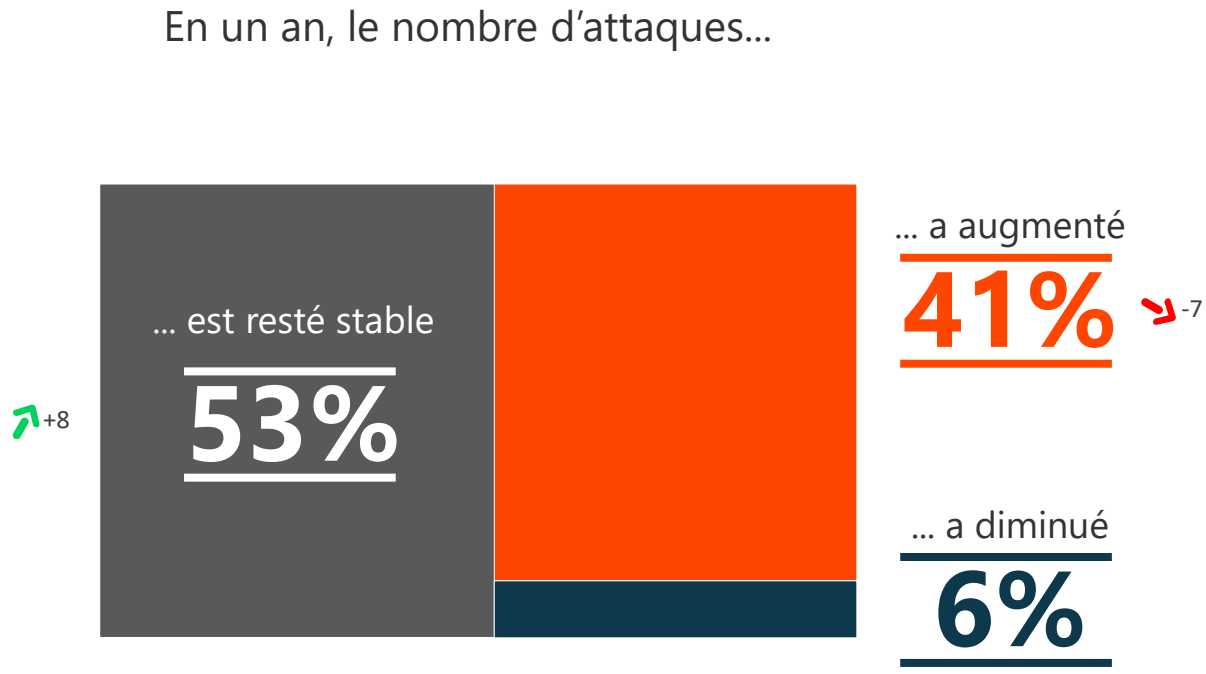
des entreprises ont constaté au moins une cyber-attaque



Pas d'évolution statistiquement significative vs. 01/2018

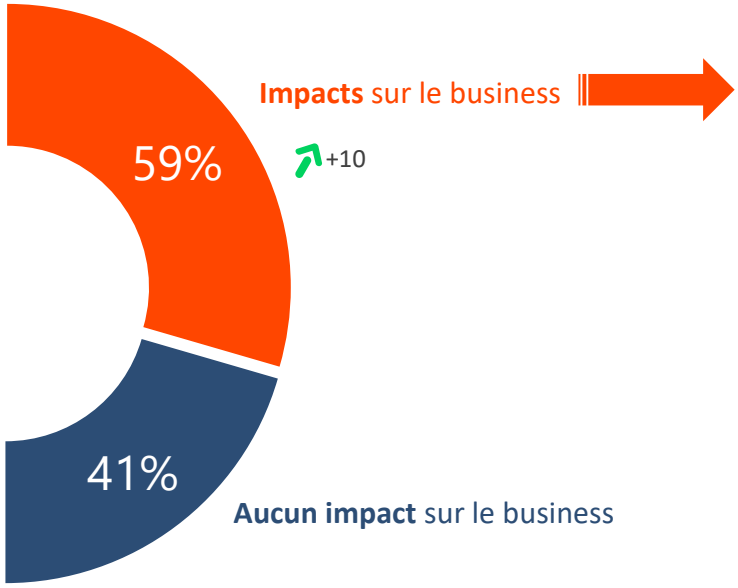
Pour autant, le nombre de cyber-attaques constatées par entreprise tend à se stabiliser

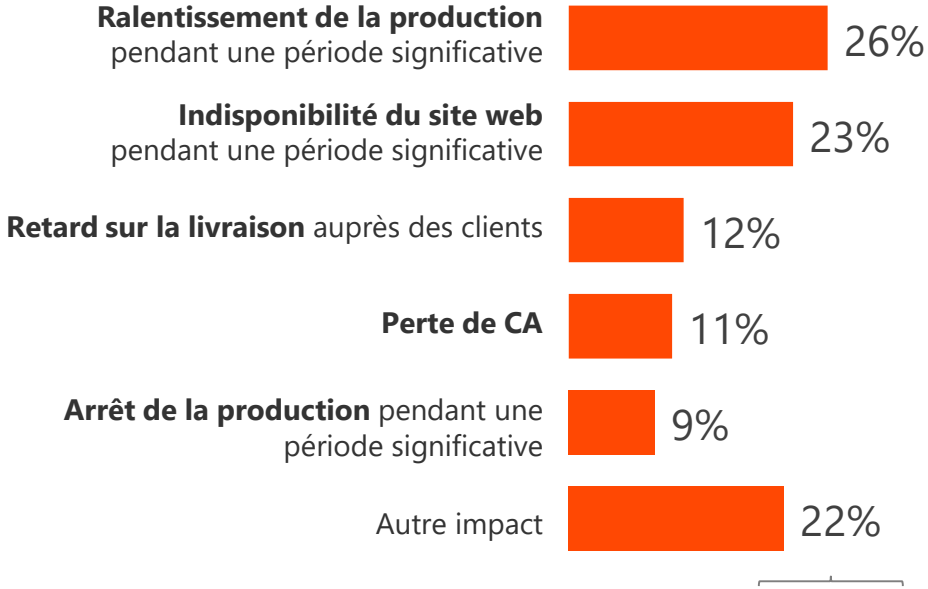
Q5BIS. Et par rapport à l'année dernière, ce nombre d'attaques constatées dans votre entreprise… ?
Base : ensemble (174 répondants)



En revanche, les cyber-attaques ont un impact plus important sur le business des entreprises visées

Q30. Quel a été l'impact des cyber-attaques sur votre business ?
Base : ensemble (174 répondants) / Plusieurs réponses possibles





Impacts spontanément cités par les répondants : augmentation de la charge de travail, baisse de productivité des collaborateurs, mauvaise réputation de l'entreprise

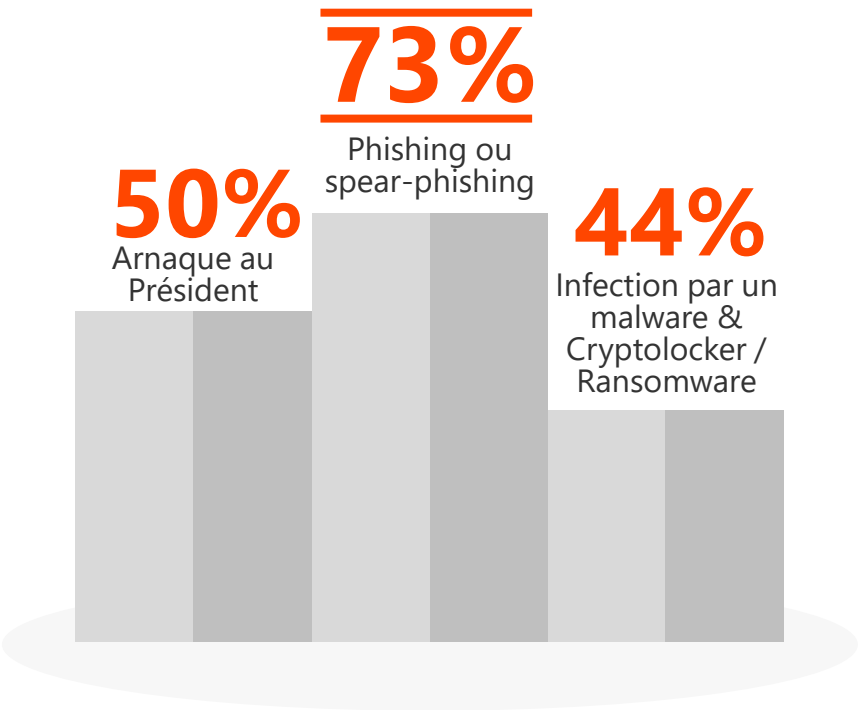
Évolution statistiquement significative vs. 01/2018

En 2018, le phishing prend la tête des attaques constatées et contrairement à ce que l'on pourrait penser, l'arnaque au président touche une entreprise sur deux

Q6. Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?
Base : ont constaté une attaque (139 répondants) / Plusieurs réponses possibles

Les attaques subies

TOP3



Question reformulée par rapport à la vague précédente du baromètre

En moyenne, les entreprises font face à cinq types d'attaques différents chaque année

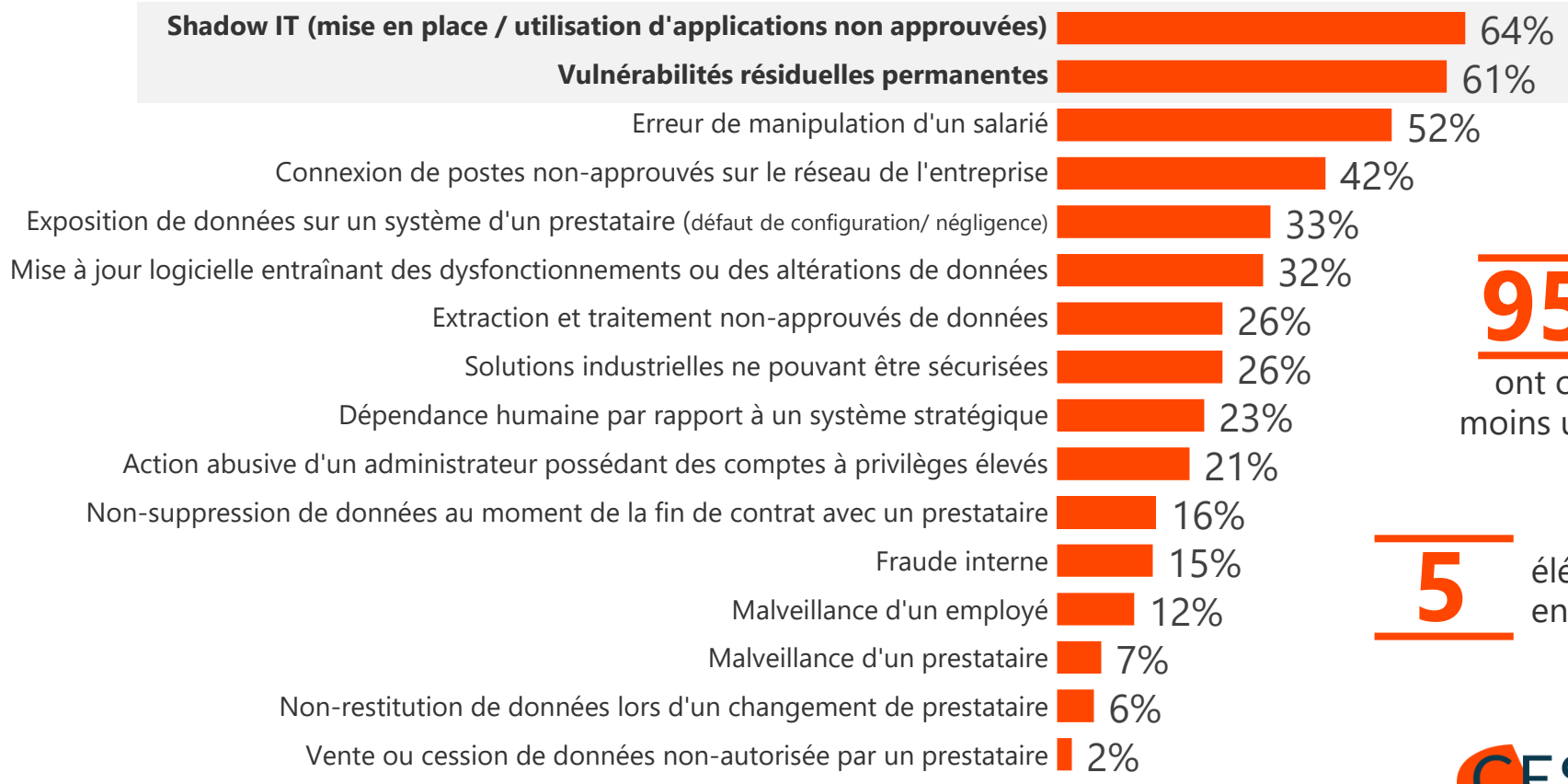
Q6. Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?
Base : ont constaté une attaque (139 répondants) / Plusieurs réponses possibles

Question reformulée par rapport à la vague précédente du baromètre

Le shadow IT est en tête des cyber-risques les plus fréquemment rencontrés

Q6BIS. Parmi les éléments suivants liés à la cyber-sécurité, quels sont ceux auxquels votre entreprise a été concrètement confrontée au cours des 12 derniers mois ? *Base : ensemble (174 répondants) / Plusieurs réponses possibles*

Les cyber-risques rencontrés



95%
ont connu au moins un élément

5 éléments en moyenne

Question reformulée par rapport à la vague précédente du baromètre

2. CLOUD ET IOT : DES RISQUES ACCRUS AVEC LA TRANSFORMATION NUMÉRIQUE

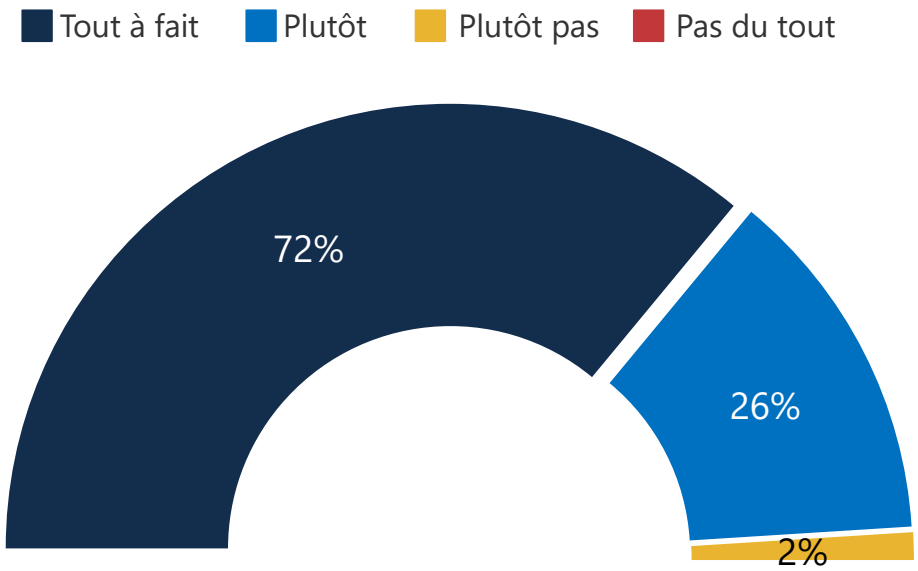
CESIN

La transformation numérique a un impact sur la sécurité des systèmes d'information de toutes les entreprises

Q2BIS. Dans votre entreprise, la transformation numérique a-t-elle un impact sur la sécurité des systèmes d'information et des données ? *Base : ensemble (174 répondants)*

98%

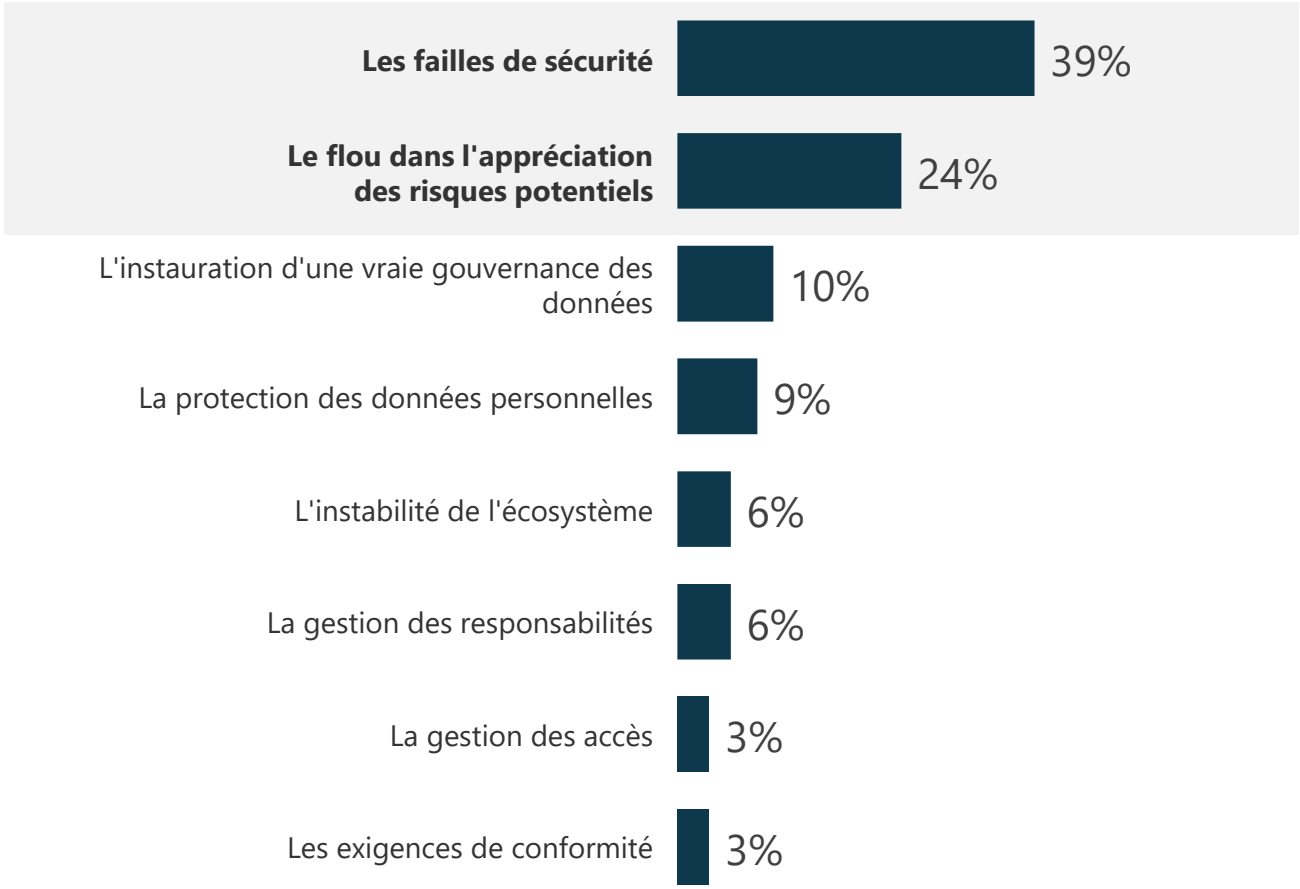
estiment que la transformation numérique a **un impact sur la sécurité** des systèmes d'information et des données



Pas d'évolution statistiquement significative vs. 01/2018

Les failles de sécurité restent la caractéristique la plus marquante des IOT

Q36. D'après vous, quel est le principal défi à relever pour le RSSI en ce qui concerne l'IoT (*Internet of Things*) en entreprise ?
Base : ensemble (174)

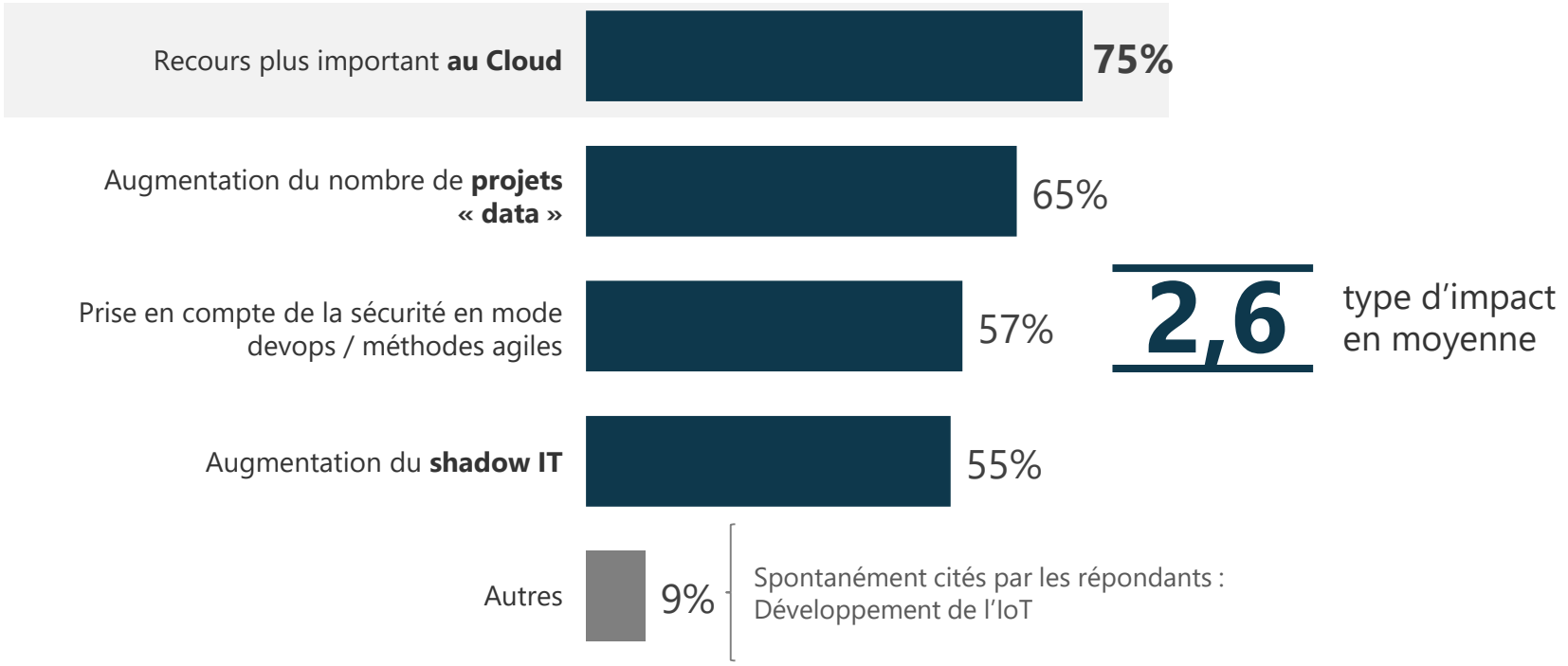


Pas d'évolution statistiquement significative vs. 01/2018

… mais l'impact le plus fréquent de la transformation numérique des entreprises est le recours au Cloud

Q2BISV4. En quoi la transformation numérique a-t-elle un impact sur la sécurité des systèmes d'information et des données de votre entreprise ?

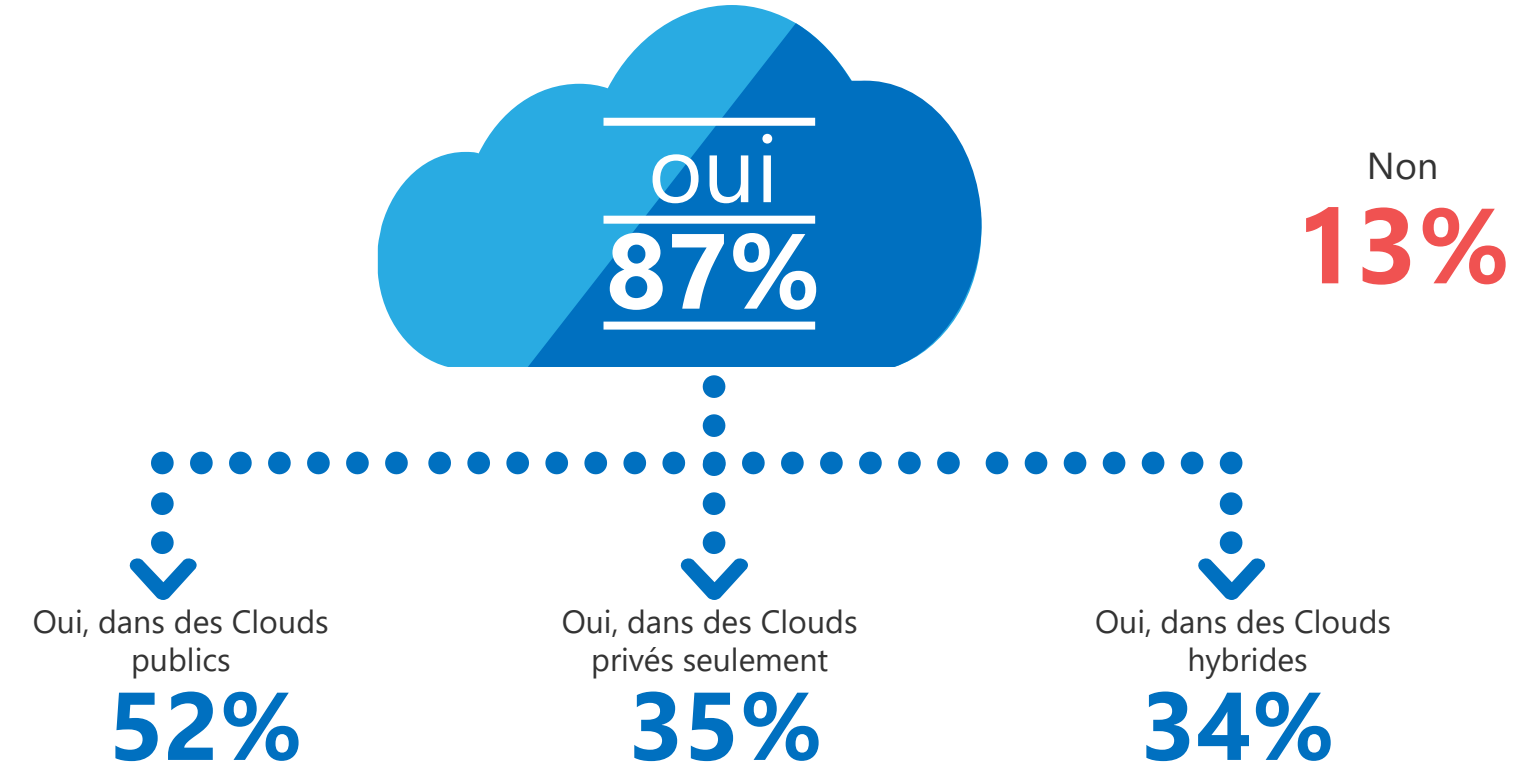
Base : estiment que la transformation numérique a un impact sur la sécurité des systèmes d'information et des données (170)



Nouvelle question

En effet, la plupart des entreprises stockent au moins une partie de leurs données dans un Cloud… … dont la majorité dans des Clouds publics

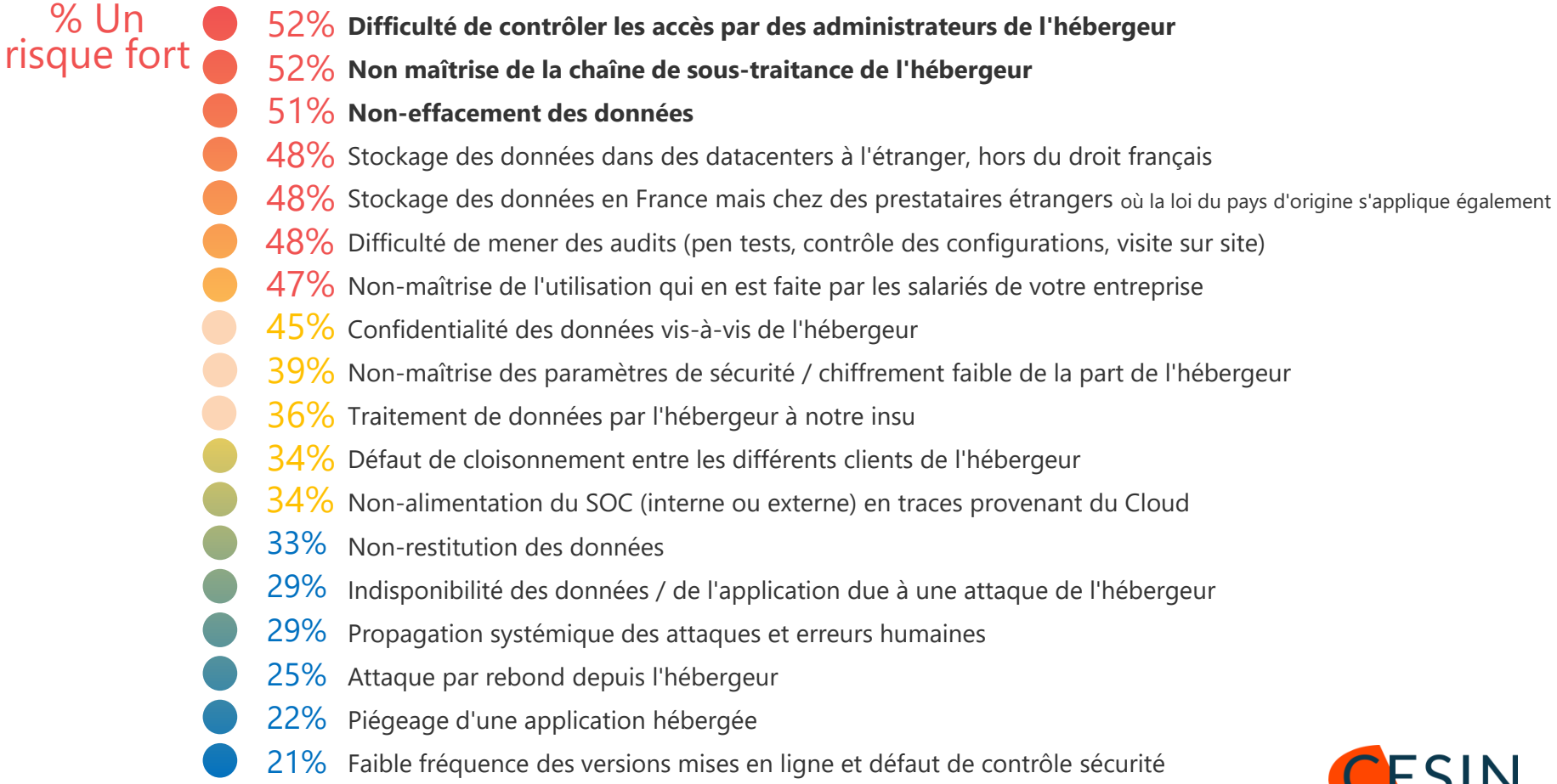
Q20. Certaines des données de votre entreprise sont-elles stockées dans un Cloud ?
Base : ensemble (174 répondants), plusieurs réponses possibles



Pas d'évolution statistiquement significative vs. 01/2018

De plus, le Cloud expose les entreprises à différents risques, notamment en raison d'un manque de maîtrise

Q22. Selon vous, les facteurs suivants représentent-ils un risque faible, modéré ou fort en ce qui concerne l'utilisation du Cloud ? *Base : ensemble (174 répondants)*

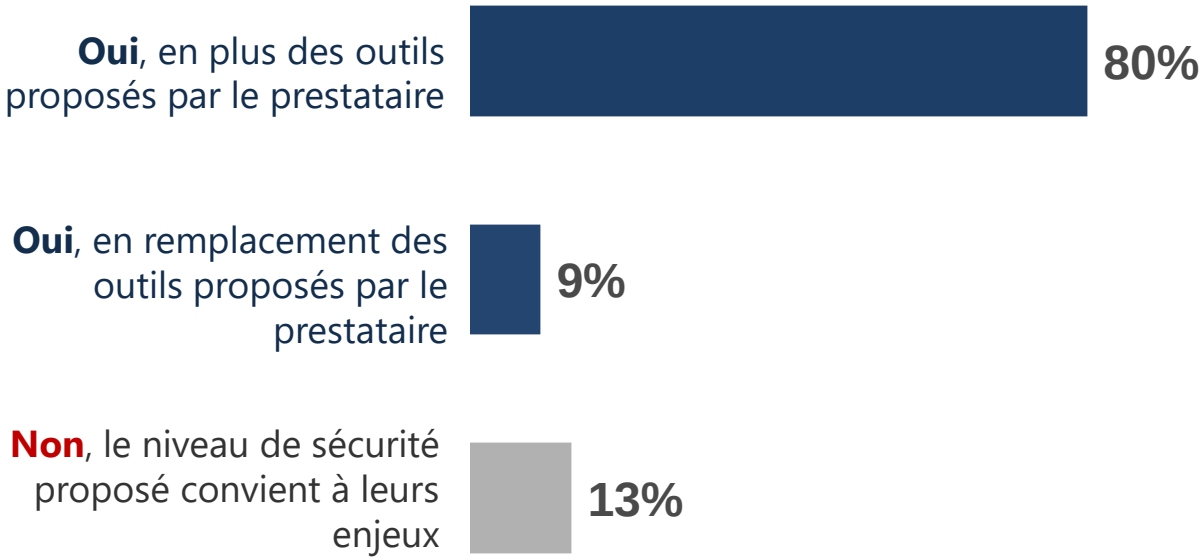


Question reformulée par rapport à la vague précédente du baromètre

Pour sécuriser les données stockées dans un Cloud public, le RSSI ne se contente pas des outils proposés par le prestataire…

Q23. D'après vous, la sécurisation des données stockées dans le Cloud requiert-elle des outils ou dispositifs spécifiques ?
Base : ensemble (174 répondants)

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

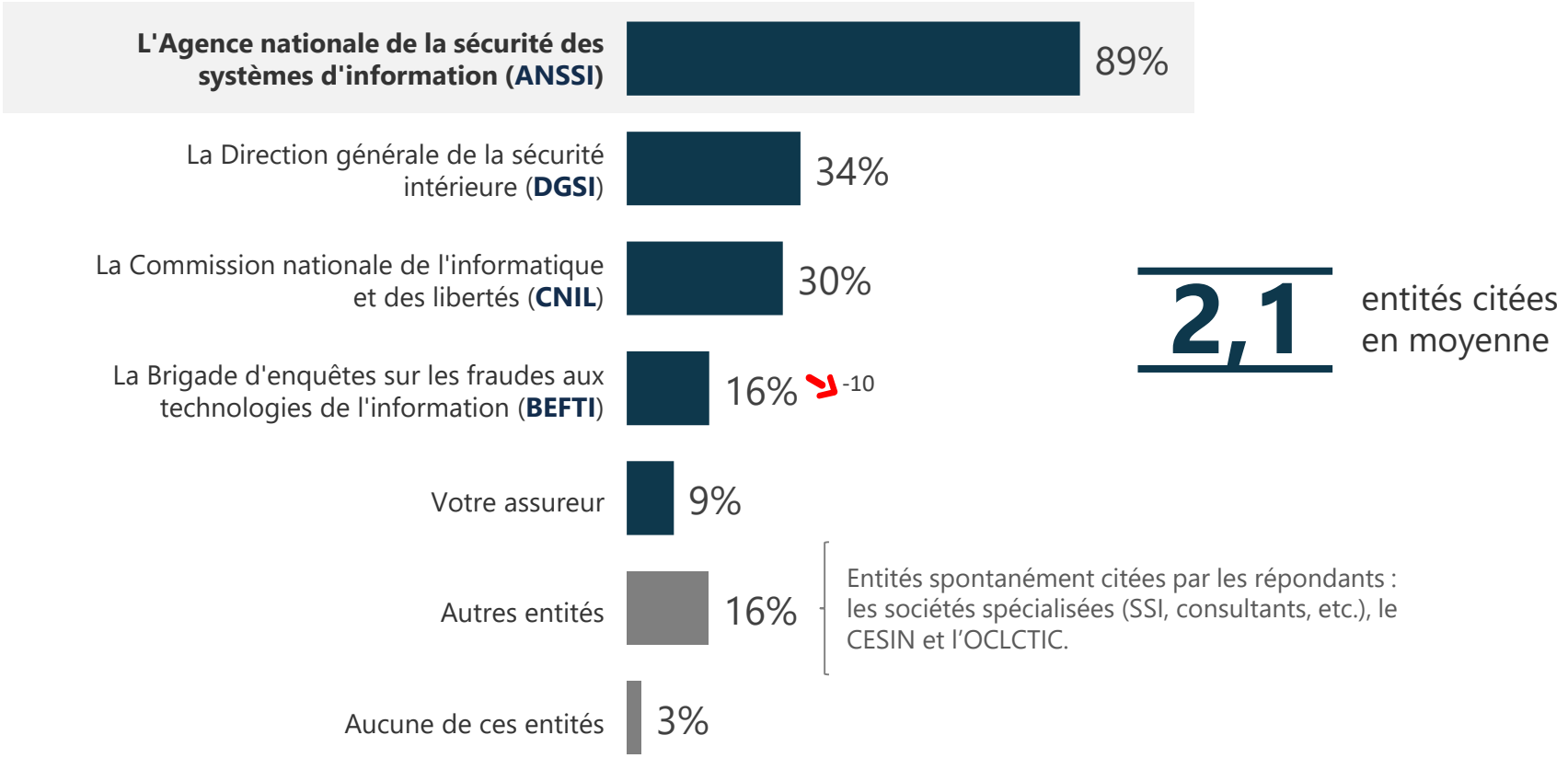


Question reformulée par rapport à la vague précédente du baromètre

3. FACE AUX CYBER-RISQUES, UNE CYBER-RÉSILIENCE À DÉVELOPPER

L'ANSSI reste l'entité référence en termes de conseil sur la gestion des cyber-risques

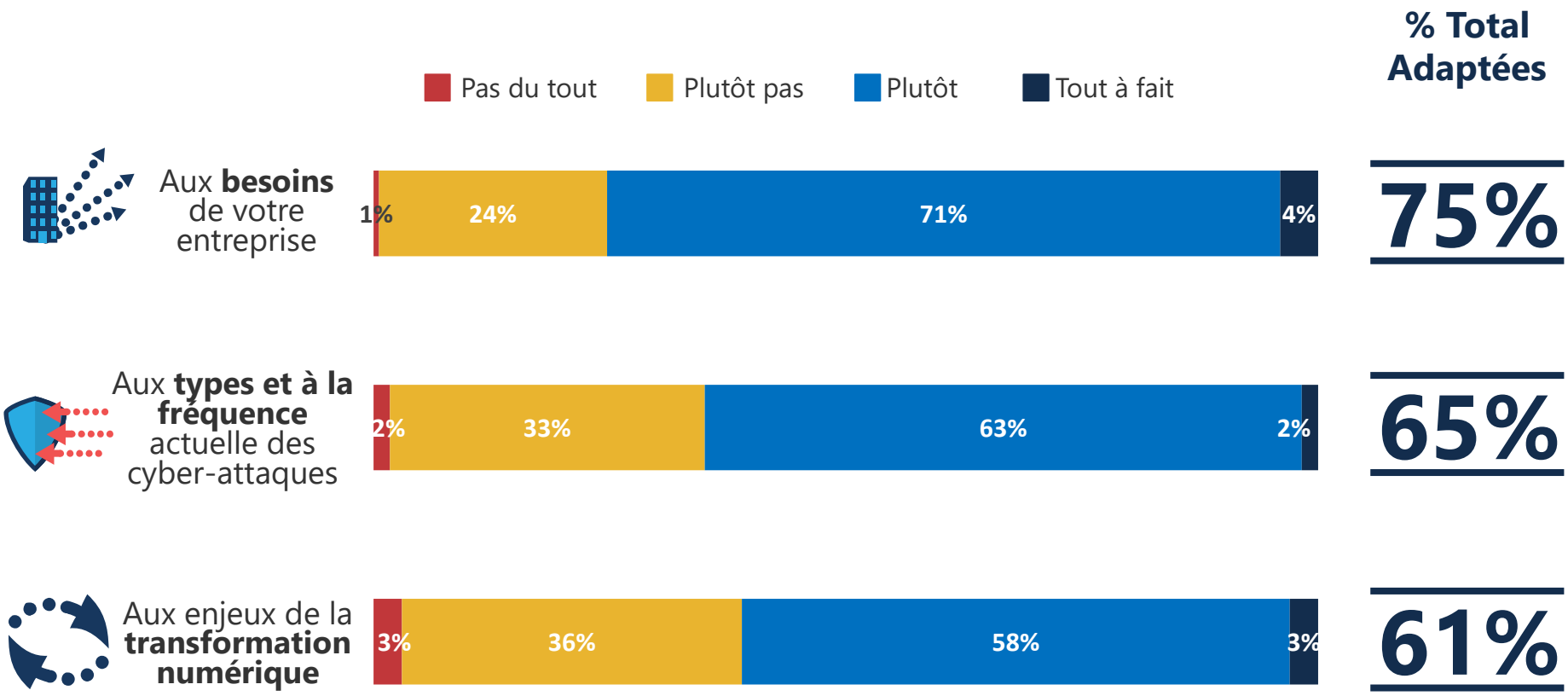
Q31. Quelles entités vous semblent les plus légitimes pour vous conseiller sur la gestion des cyber-risques ?
Base : ensemble (174 répondants) / Plusieurs réponses possibles



Évolution statistiquement significative vs. 01/2018

Sur un plan technique, les solutions proposées semblent en phase avec les attentes des entreprises mais restent challengées par la transformation numérique

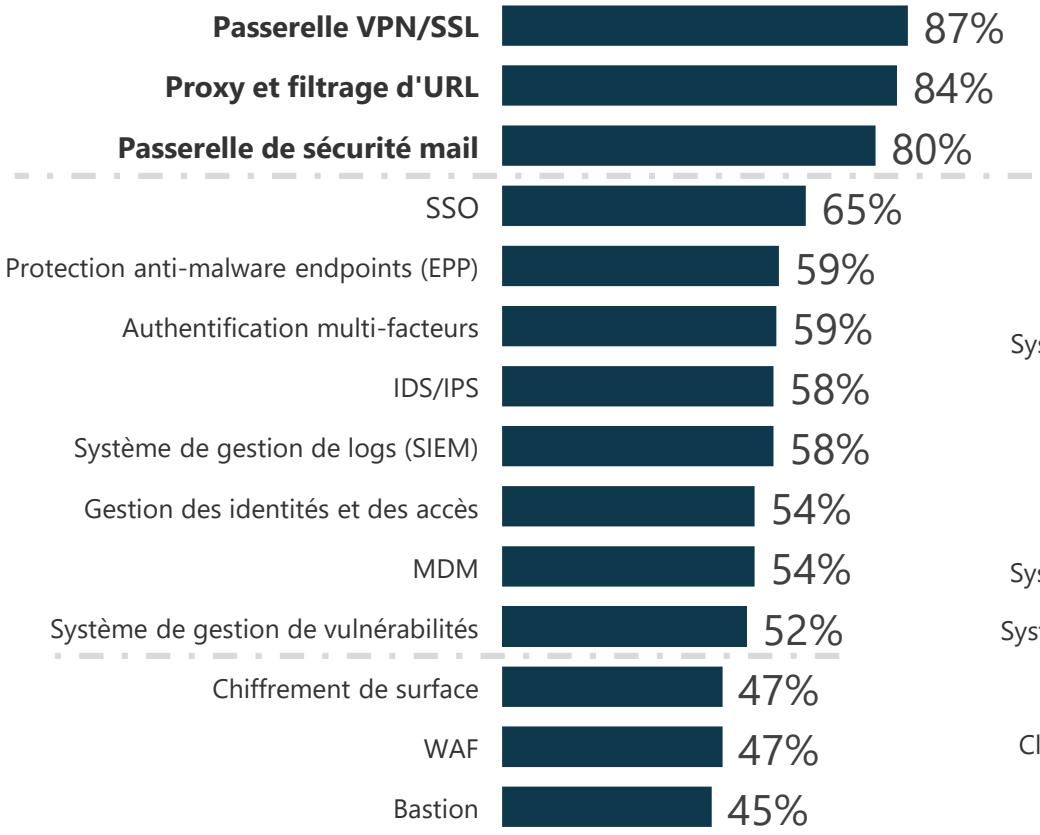
Q29. Pensez-vous que les solutions de protection disponibles sur le marché sont tout à fait, plutôt, plutôt pas ou pas du tout adaptées… ? *Base : ensemble (174 répondants)*



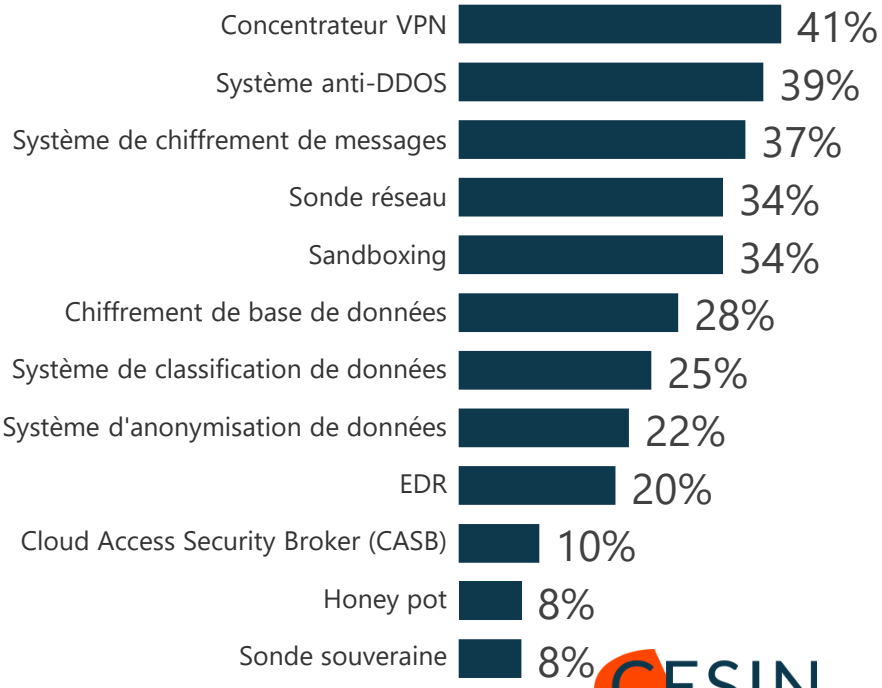
Pas d'évolution statistiquement significative vs. 01/2018

Concrètement, les entreprises déploient un peu plus d'une dizaine de solutions en moyenne…

Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ? *Base : ensemble (174 répondants) / Plusieurs réponses possibles*

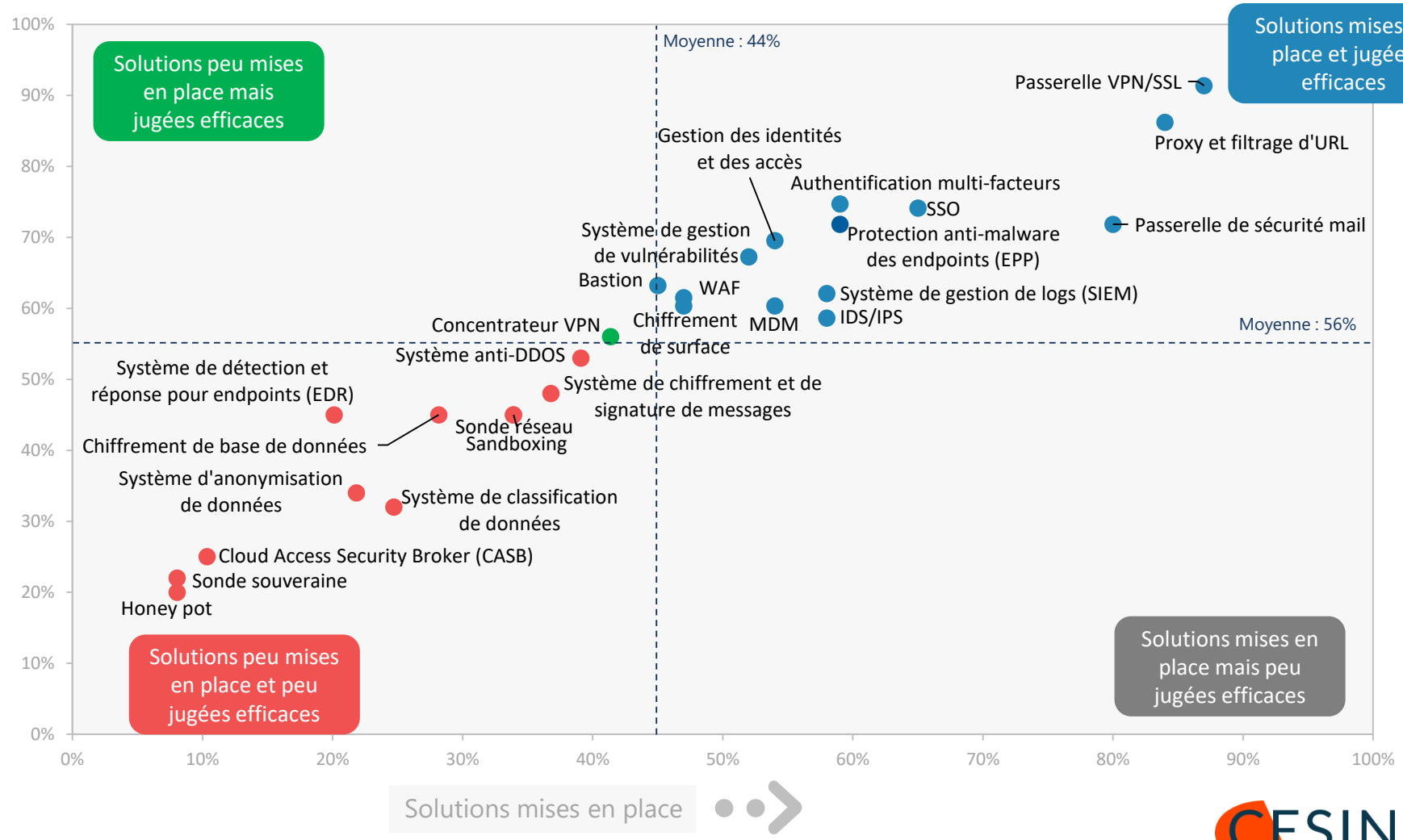


11,6 solutions en moyenne



Question reformulée par rapport à la vague précédente du baromètre

… et ces solutions mises en place sont jugées efficaces



Les solutions de protection contre les cyber-risques fondées sur l'IA sont de plus en plus adoptées…

Q40. Parlons maintenant du rôle potentiel de l'IA dans la sécurité informatique. Dans votre entreprise, avez-vous mis en place des solutions de protection ou de détection fondées sur l'IA ? *Base : ensemble (174 répondants)*

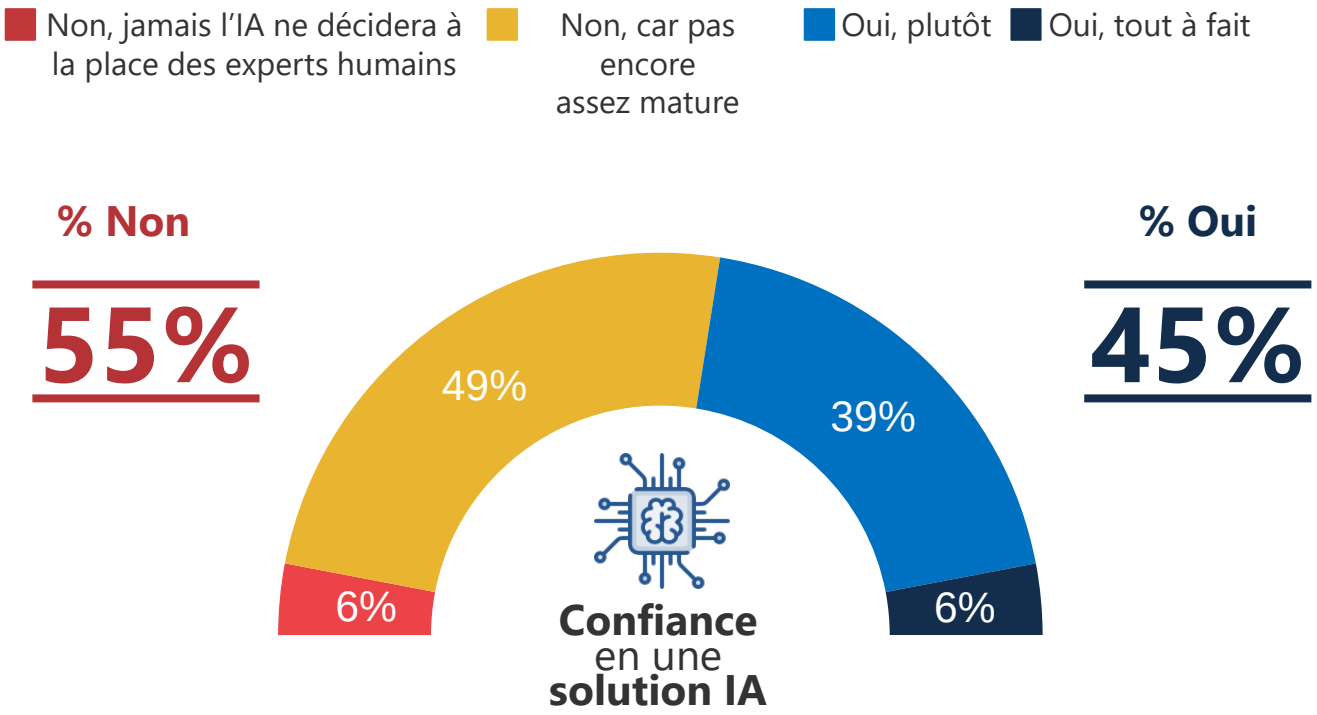
56% **ont mis en place des solutions fondées sur l'IA ou envisagent de le faire**

Pour 44%, ce n'est pas en projet.

Nouvelle question

… même si l'intervention humaine reste nécessaire aux yeux des RSSI

Q41. Seriez-vous prêt(e) à laisser une solution IA prendre des décisions en matière de sécurité pour ce qui concerne la détection et/ou la remédiation ? *Base : ensemble (174 répondants)*



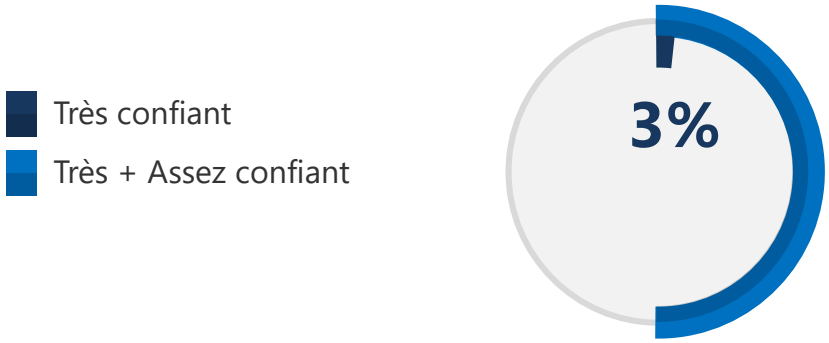
Nouvelle question

Malgré toutes ces solutions, la confiance dans la capacité à faire face aux cyber-risques est en baisse

Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (174 répondants)

51% ↘ -12

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

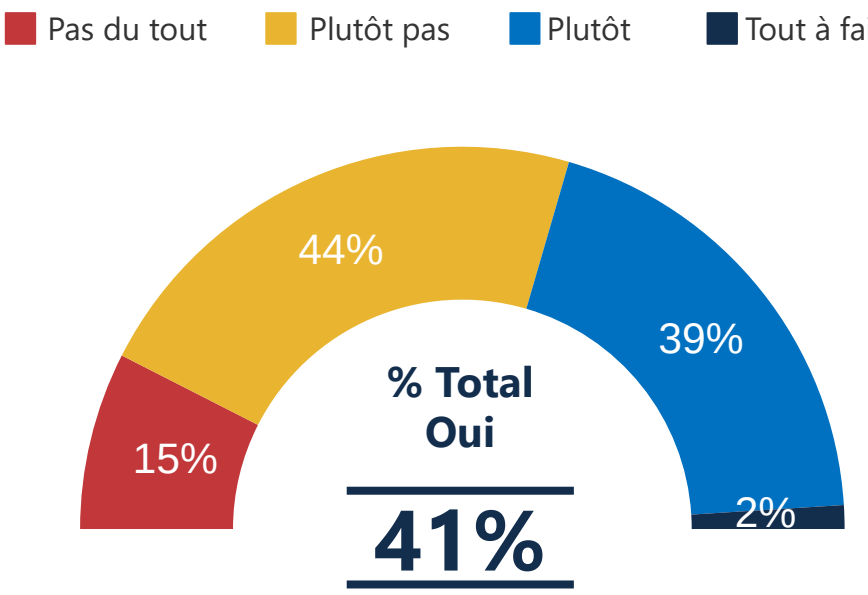


↗↘ Évolution statistiquement significative vs. 01/2018

Et moins d'une entreprise sur deux se sent capable de gérer une cyber-attaque de grande ampleur

Q38. Selon vous, votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur ?
Base : ensemble (174)

« Votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur »



Nouvelle question

Dans ce contexte, de plus en plus d'entreprises souscrivent une cyber-assurance

Q9. Par ailleurs, votre entreprise a-t-elle souscrit une cyber-assurance ?
Base : ensemble (174 répondants)

50% ↗ +10

10%

18%

↗ ↘ Évolution statistiquement significative vs. 01/2018

CESIN

La cyber-résilience devient un enjeu pour deux tiers des entreprises, qui mettent en place un programme

Q39. Votre entreprise a-t-elle mis en place un programme de cyber-résilience ?
Base : ensemble (174 répondants)

79% **ont mis en place un programme de cyber-résilience ou envisagent de le faire**

12%

33%

34%

Pour 21%, ce n'est pas en projet.

Nouvelle question

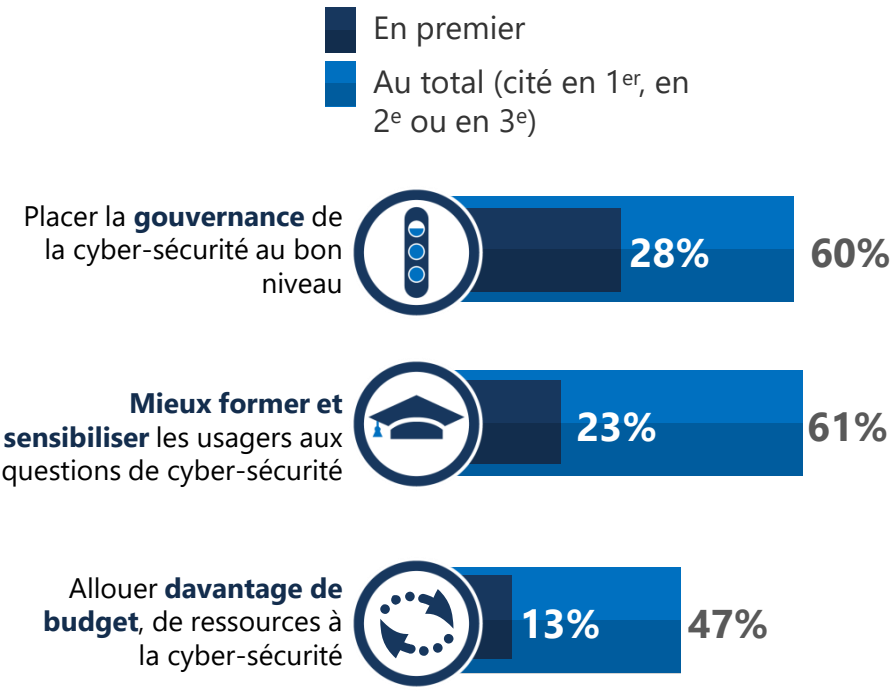
4. TROIS ENJEUX POUR L'AVENIR

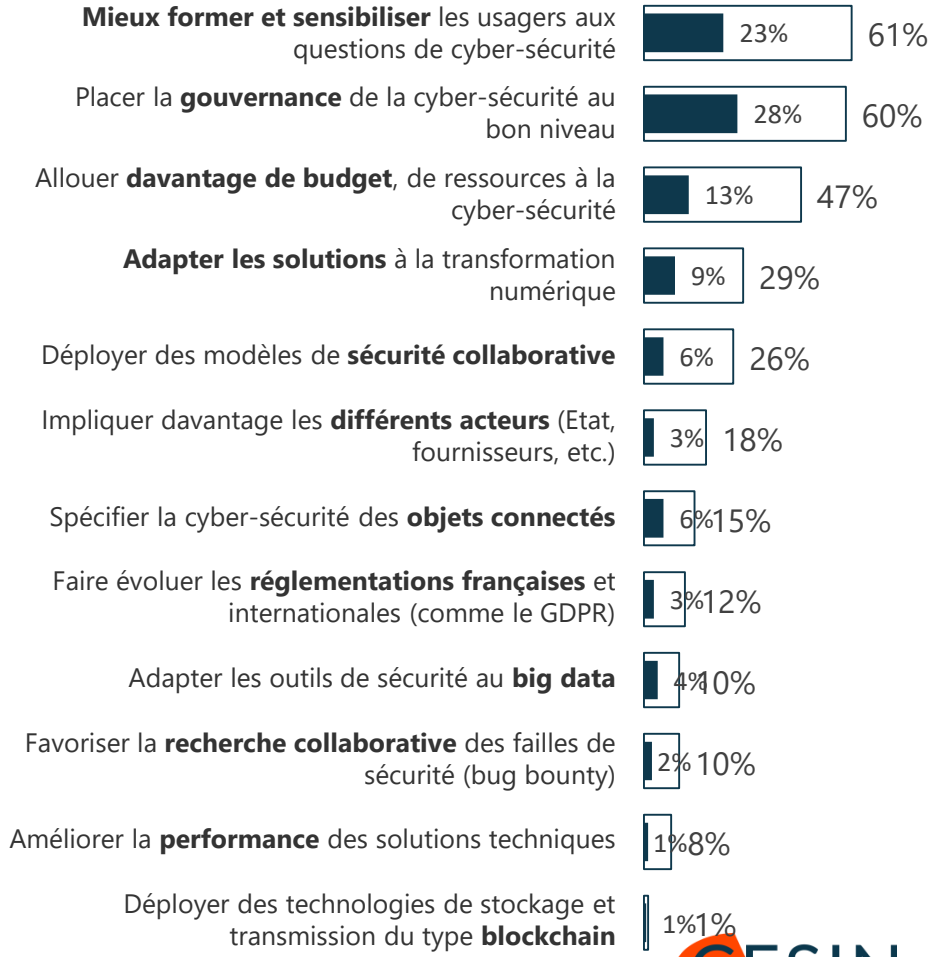
- LA SENSIBILISATION
- LA GOUVERNANCE
- LES RESSOURCES

L'enjeu pour l'avenir reste plus humain que technique

Q28. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cyber-sécurité des entreprises ? *Base : ensemble (174 répondants)*

TOP3 des enjeux





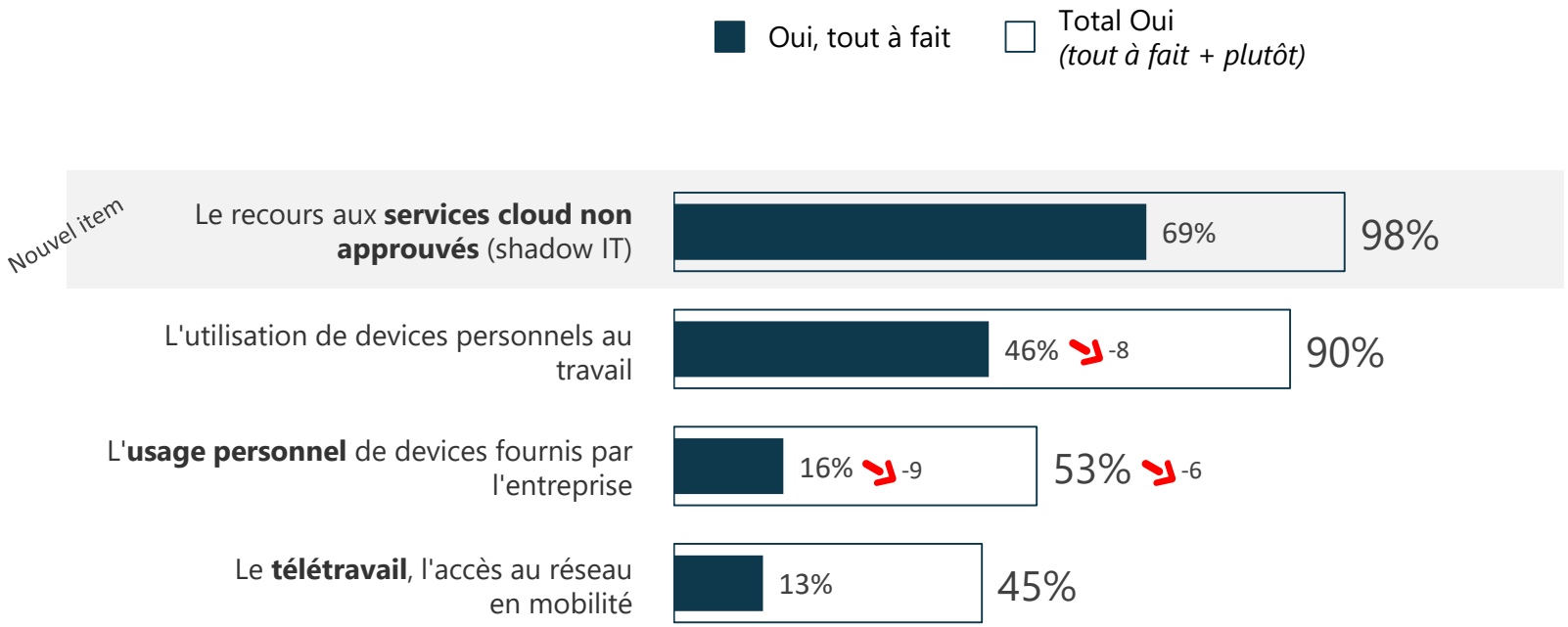
Pas d'évolution statistiquement significative vs. 01/2018

4. TROIS ENJEUX POUR L'AVENIR

- **LA SENSIBILISATION**
- **LA GOUVERNANCE**
- **LES RESSOURCES**

Les usages du numérique par les salariés représentent un risque réel, en particulier le shadow IT

Q24. À vos yeux, les usages suivants du numérique par les salariés représentent-ils un risque pour la cyber-sécurité des entreprises ? *Base : ensemble (174 répondants)*



Évolution statistiquement significative vs. 01/2018

Et même s'ils sont sensibilisés à la cyber-sécurité, les salariés se montrent peu impliqués d'après les RSSI

Q15. En ce qui concerne la cyber-sécurité, pensez-vous que les salariés de votre entreprise… ?
Base : ensemble (174 répondants)

71%
pensent que les salariés **sont sensibilisés** aux cyber-risques

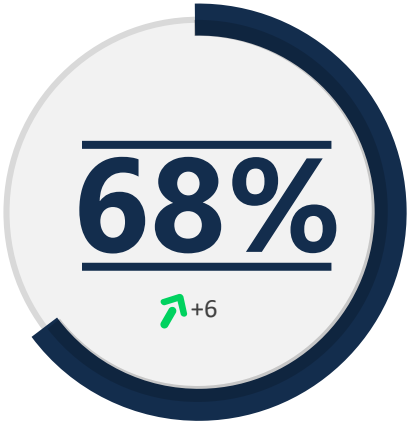
54%
pensent que les salariés **respectent les recommandations**

13%
pensent que les salariés **prennent des précautions au-delà des recommandations** données

Pas d'évolution statistiquement significative vs. 01/2018

Dans ce cadre, de plus en plus d'entreprises mettent en place des vérifications du respect des recommandations

Q15BIS. Avez-vous mis en place des procédures pour tester l'application des recommandations par les salariés dans des situations concrètes, comme des audits, campagnes de faux phishing, contrôles internes, etc. ?
Base : ensemble (174 répondants)



ont **mis en place des procédures pour tester** l'application des recommandations par les salariés

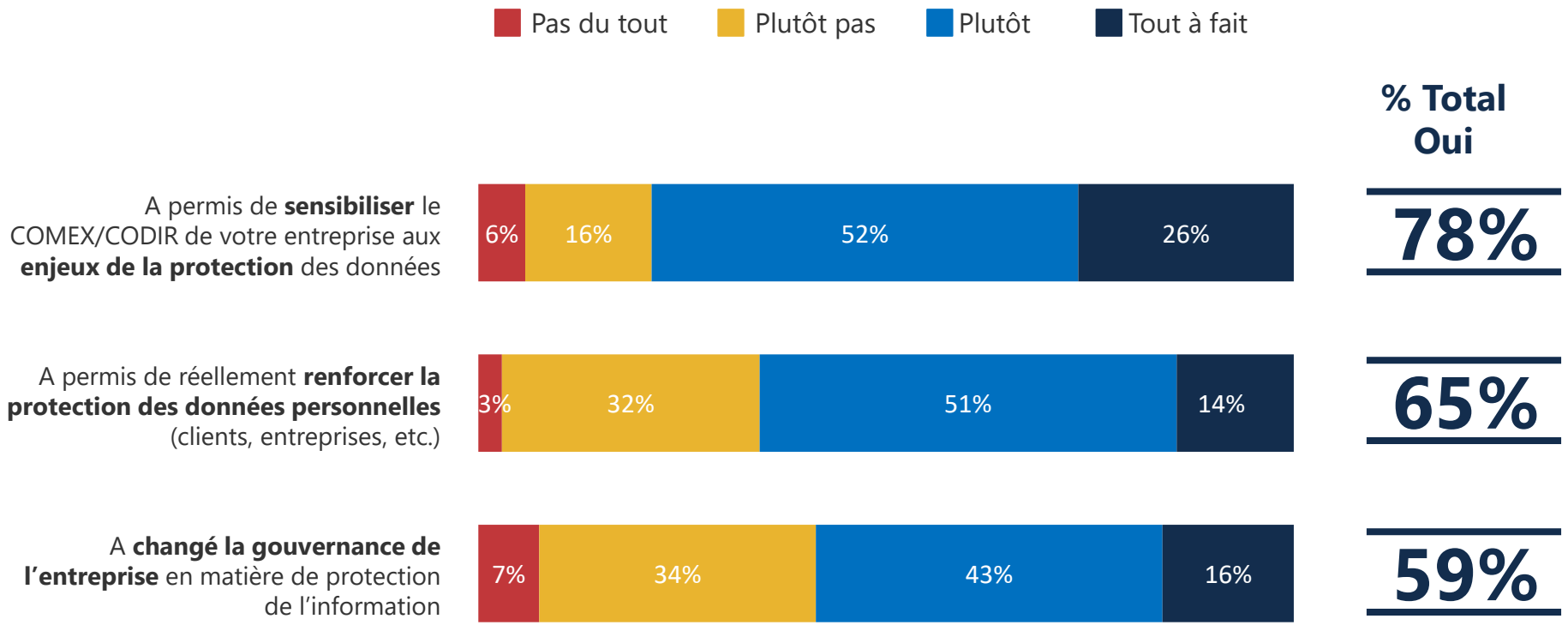
Évolution statistiquement significative vs. 01/2018

4. TROIS ENJEUX POUR L'AVENIR

- LA SENSIBILISATION
- **LA GOUVERNANCE**
- LES RESSOURCES

La mise en conformité RGPD a permis de sensibiliser les entreprises aux enjeux de la protection des données

Q32. Concernant la mise en conformité RGPD, diriez-vous que… ? *Base : ensemble (174)*



Nouvelle question

Pour autant, les RSSI se montrent peu confiants en la capacité de leur COMEX a prendre en compte les enjeux de la cyber-sécurité

Q26. Pour l'avenir, diriez-vous que vous êtes très confiant, assez confiant, assez inquiet ou très inquiet en ce qui concerne… ?
Base : ensemble (174 répondants)

66% ↘ -5

La **prise en compte des enjeux** de la cyber-sécurité au sein du COMEX votre entreprise

Très confiant

Très + Assez confiant

↗ ↘ Évolution statistiquement significative vs. 01/2018

4. TROIS ENJEUX POUR L'AVENIR

- LA SENSIBILISATION
- LA GOUVERNANCE
- **LES RESSOURCES**

La plupart des entreprises envisagent d'investir davantage dans la cyber-sécurité, via des acquisitions de solutions et des augmentations de budget

Q11BIS. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ? *Base : ensemble (174 répondants)*

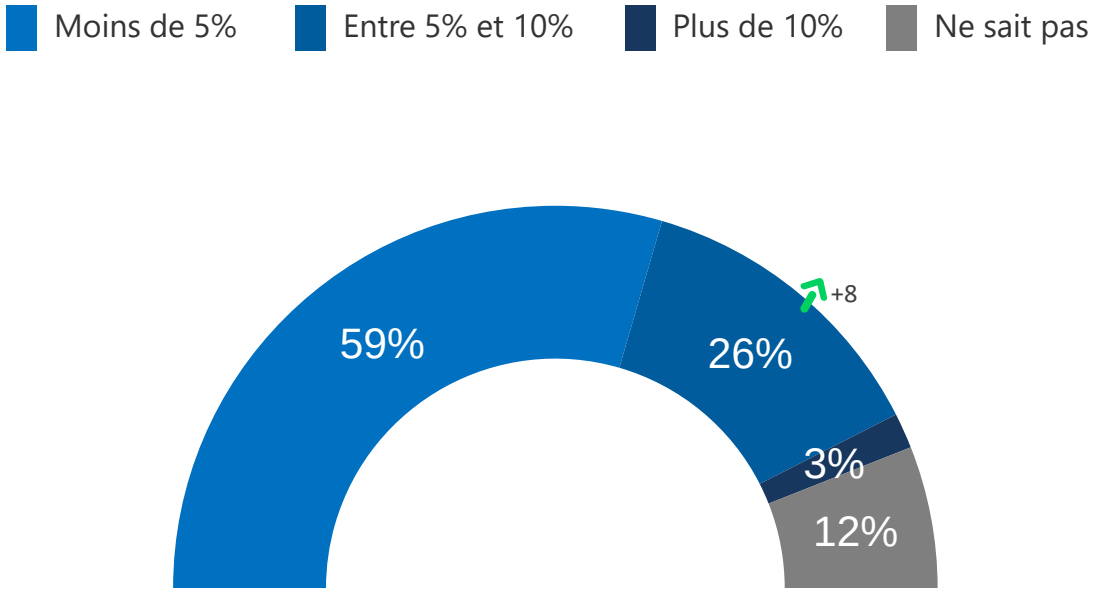
d'acquérir de **nouvelles solutions techniques** destinées à la protection contre les cyber-risques

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

Évolution statistiquement significative vs. 01/2018

Des investissements qui commencent à se sentir dans la part du budget IT consacrée à la sécurité, même si celle-ci reste faible

Q37. Dans votre entreprise, quelle part du budget IT est consacrée à la sécurité ? *Base : ensemble (174 répondants)*



Évolution statistiquement significative vs. 01/2018

En revanche, le taux d'entreprises envisageant d'augmenter les effectifs diminue

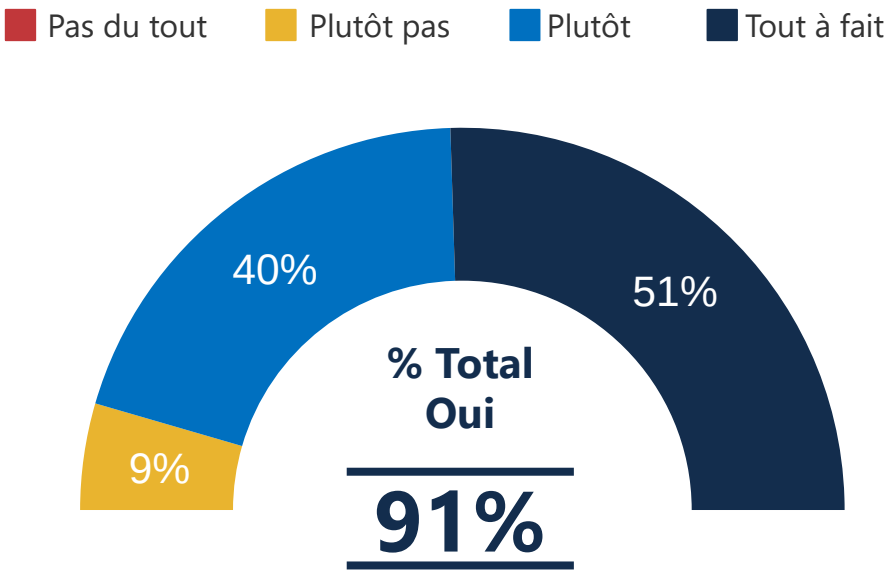
Q11BIS. Au cours des 12 prochains mois, votre entreprise envisage-t-elle… ? *Base : ensemble (174 répondants)*

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

Une situation qui fait écho à une pénurie de profils constatée par la plupart des RSSI

Q43. Pour finir, voici quelques questions sur le sujet du recrutement en SSI. Constatez-vous une pénurie de profils en SSI entraînant des difficultés de recrutement ? *Base : ensemble (174)*

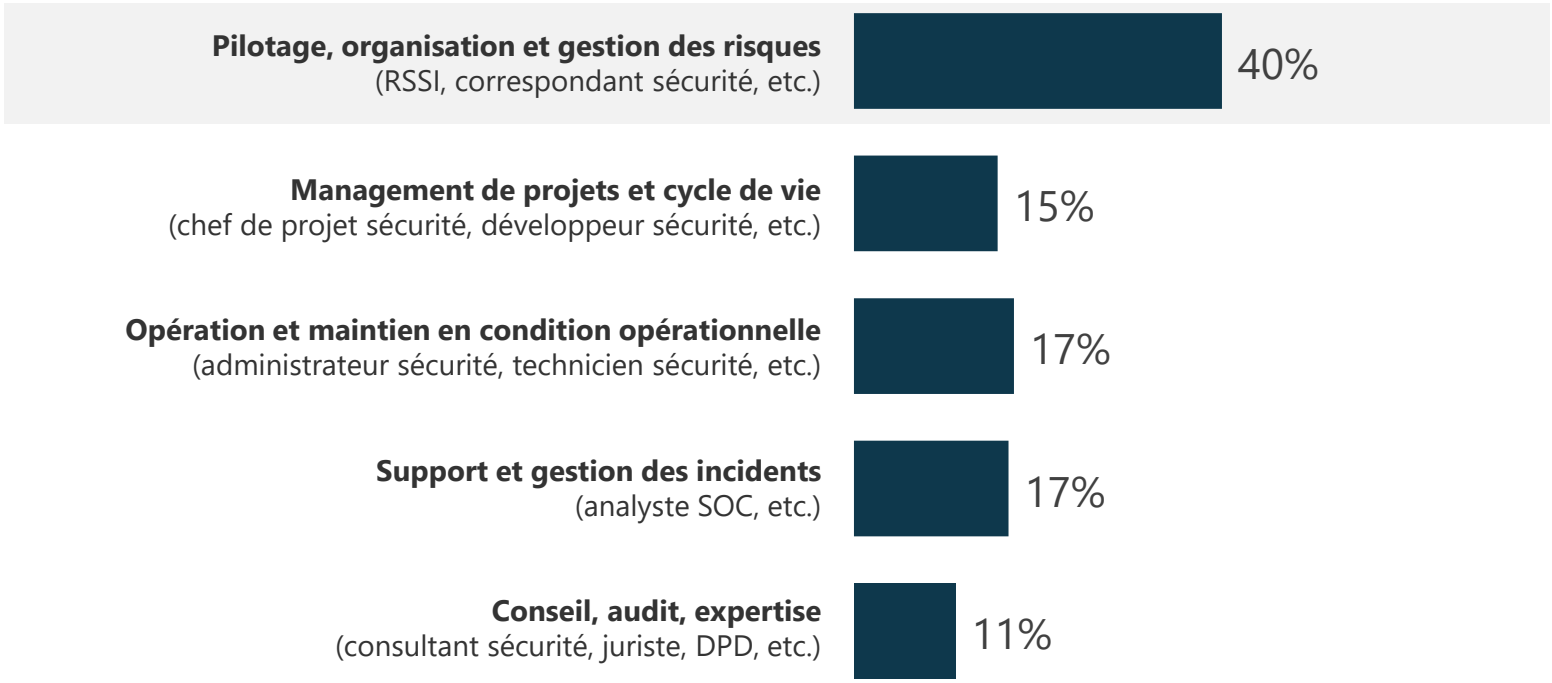
« Le constat d'une **pénurie de profils en SSI** entraînant des difficultés de recrutement »



Nouvelle question

Une pénurie qui touche avant tout les métiers du pilotage des risques

Q44. Quel est, d'après vous, le métier de la SSI le plus touché par une pénurie de profils ?
Base : ensemble (174)



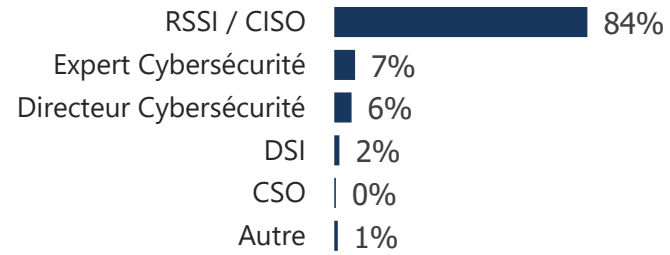
Nouvelle question

ANNEXES

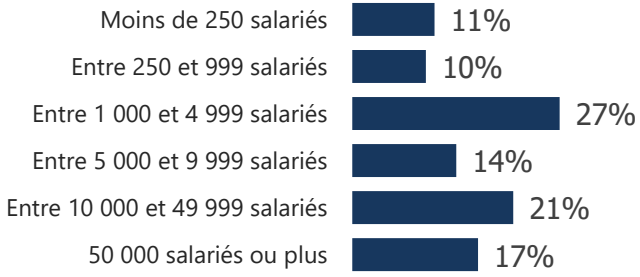
Profil des répondants

174 membres du CESIN ont participé à cette enquête

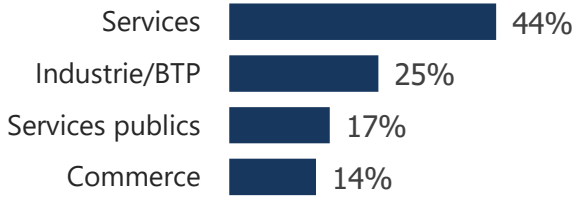
Fonction des répondants :



Nombre de salariés de l'entreprise :



Secteur d'activité de l'entreprise :



Évolution statistiquement significative vs. 01/2018