

*“opinionway* pour **CESIN**

# Etude sur la rémunération et le positionnement organisationnel des responsables cybersécurité

Rapport d'étude – Juin 2024



**ESOMAR**<sup>24</sup>  
Corporate



# “ Contexte et objectifs

- Le CESIN a mené en 2017 et 2021 (avec OpinionWay) une étude centrée sur la **rémunération des RSSI** auprès de ses adhérents.
- Il souhaite renouveler cette étude en intégrant un volet sur le positionnement organisationnel et les activités des responsables cyber.



OpinionWay présente ci-après la méthodologie afin d'accompagner le CESIN pour cette étude 2024.



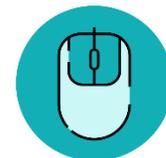
# La méthodologie



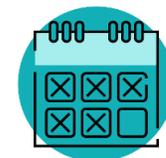
# “ La méthodologie



Étude réalisée auprès d'un échantillon de **390 responsables cybersécurité ou équivalent parmi les entreprises membres du CESIN**, sur la base d'un fichier de 838 contacts fourni par le CESIN.



L'échantillon a été interrogé par **questionnaire auto-administré en ligne sur système CAWI** (Computer Assisted Web Interview), avec un questionnaire d'une durée moyenne de 15 minutes.



Les interviews ont été réalisées **du 20 mai au 17 juin 2024**.



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 : 5,0 points au plus pour un échantillon de 390 répondants.



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

**« Sondage OpinionWay pour CESIN »**

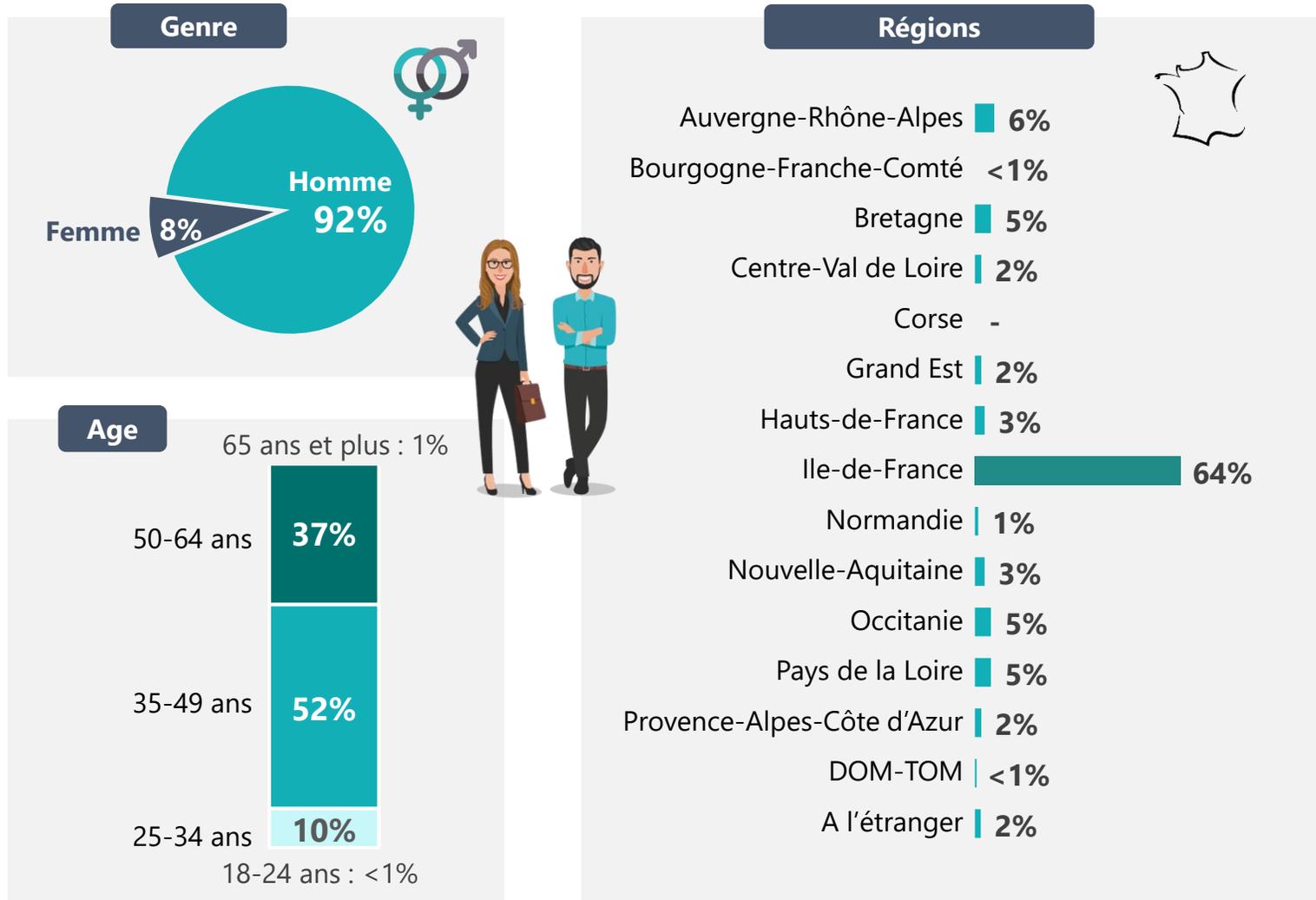
***et aucune reprise de l'enquête ne pourra être dissociée de cet intitulé.***



# **Le profil des responsables cybersécurité**



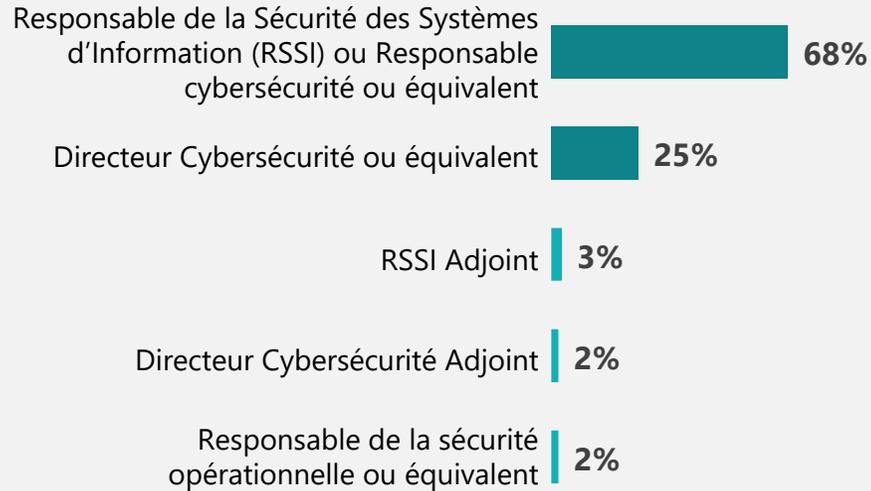
# “ Profil des responsables cybersécurité



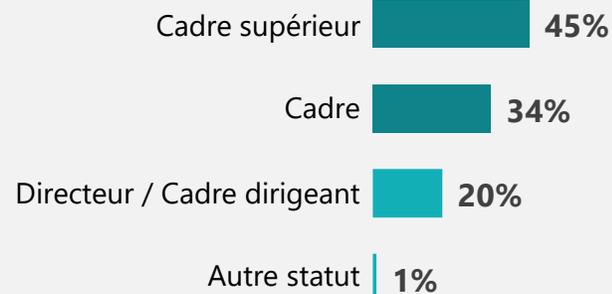


# Profil des responsables cybersécurité

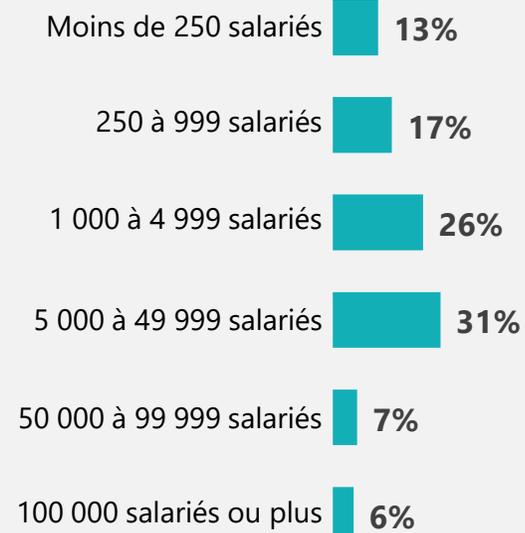
## Fonction



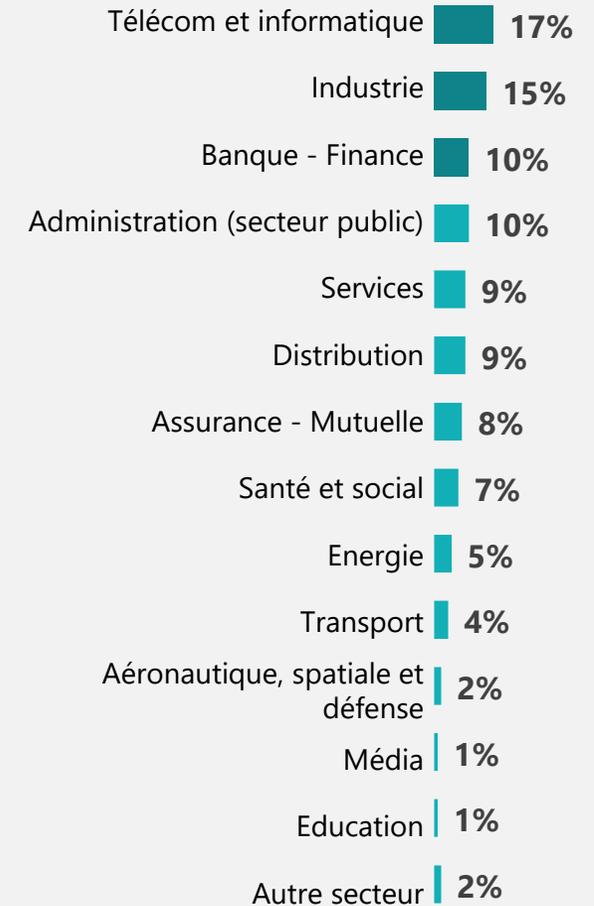
## Statut



## Nombre de salariés dans leur périmètre d'action



## Secteur d'activité





# L'analyse



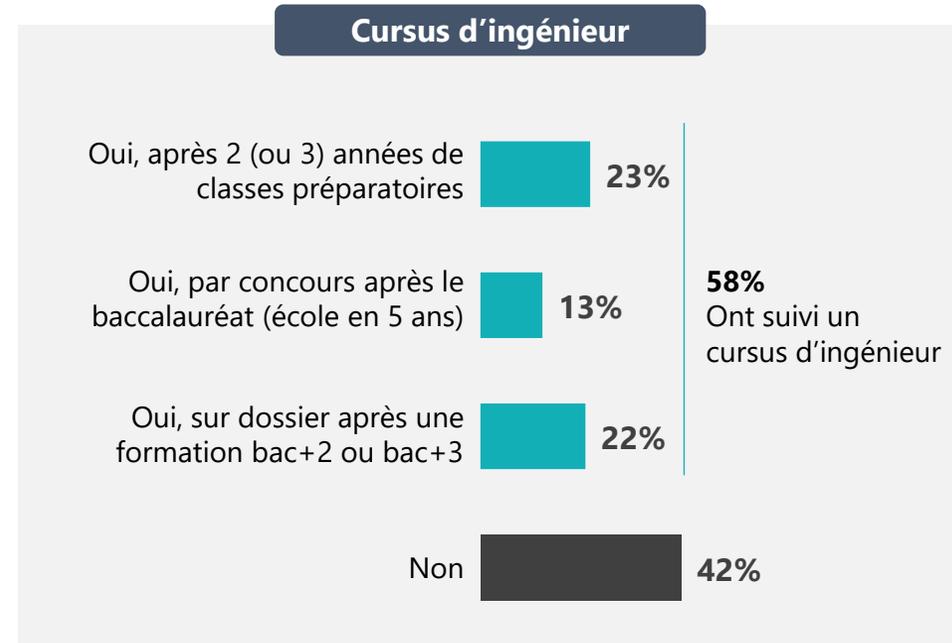
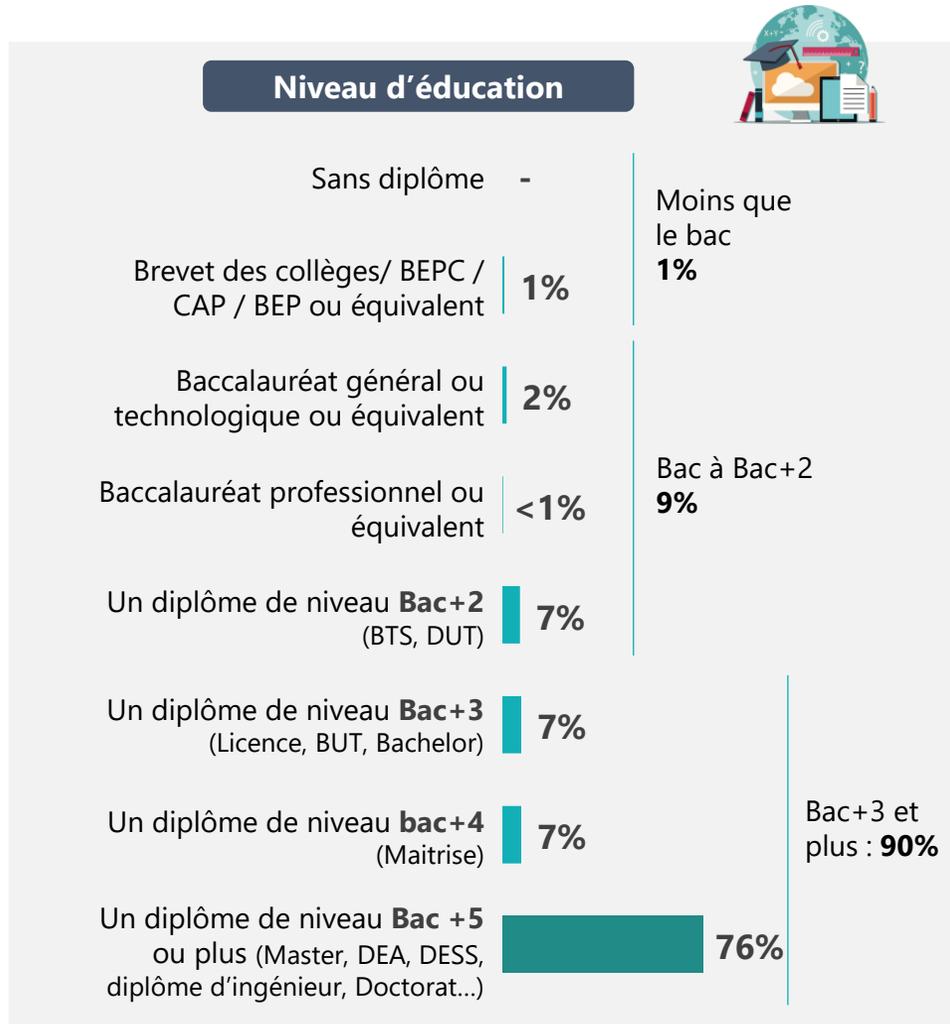


# 01

Quelle est la position des responsables cybersécurité dans les entreprises ?



# “ Les responsables cybersécurité membres du CESIN sont une population diplômée, la majorité ayant suivi un cursus d'ingénieur ”

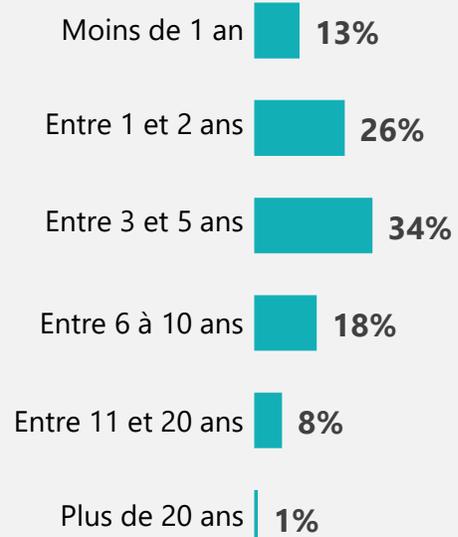


**81%** Ont fait leurs études **dans le domaine de l'informatique**

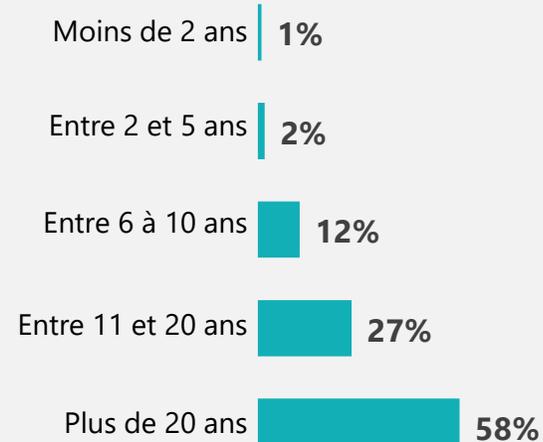
**30%** Ont fait tout ou partie de leurs études **dans le domaine de la cybersécurité**

# “ Ils sont expérimentés dans le domaine, la moitié d’entre eux travaillent dans la cybersécurité depuis plus de 10 ans

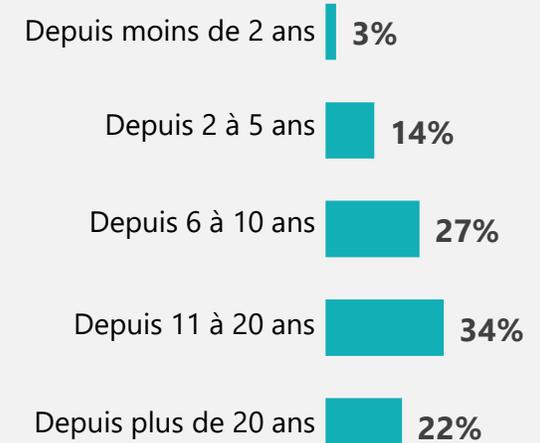
## Ancienneté de la fonction actuelle



## Nombre d’années d’expérience professionnelle



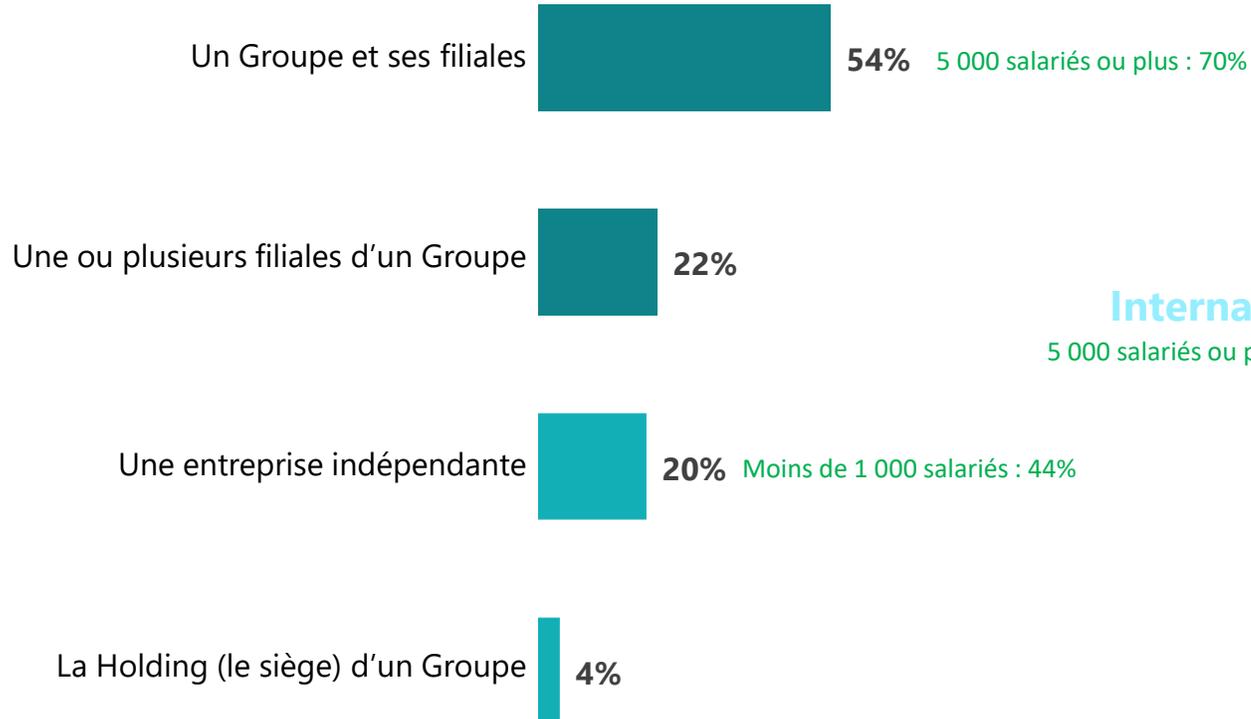
## Ancienneté métier dans la cybersécurité



# Leur activité s'exerce sur divers périmètres organisationnels et géographiques

Q3 : Sur quel périmètre s'exerce votre fonction ?

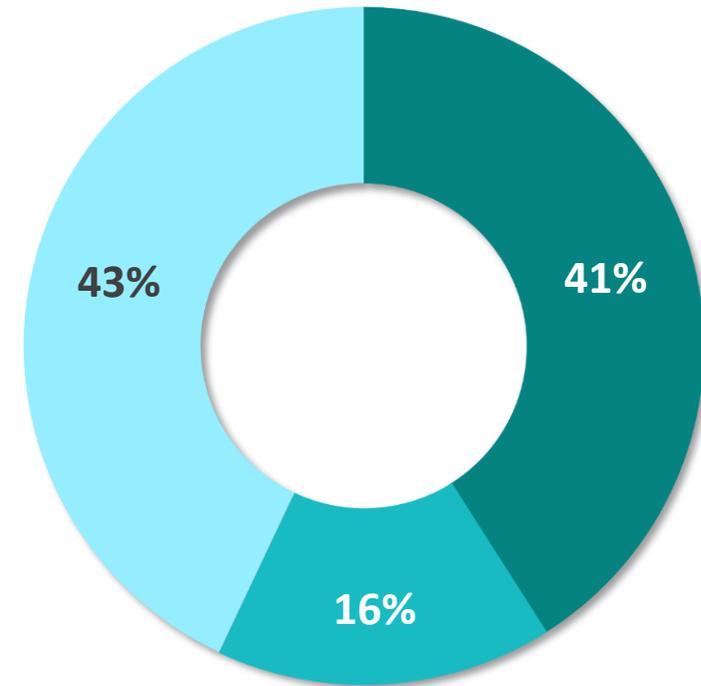
Base : ensemble (390)



Q7 : Votre activité s'exerce au plan...

Base : ensemble (390)

**International**  
5 000 salariés ou plus : 54%



**National**

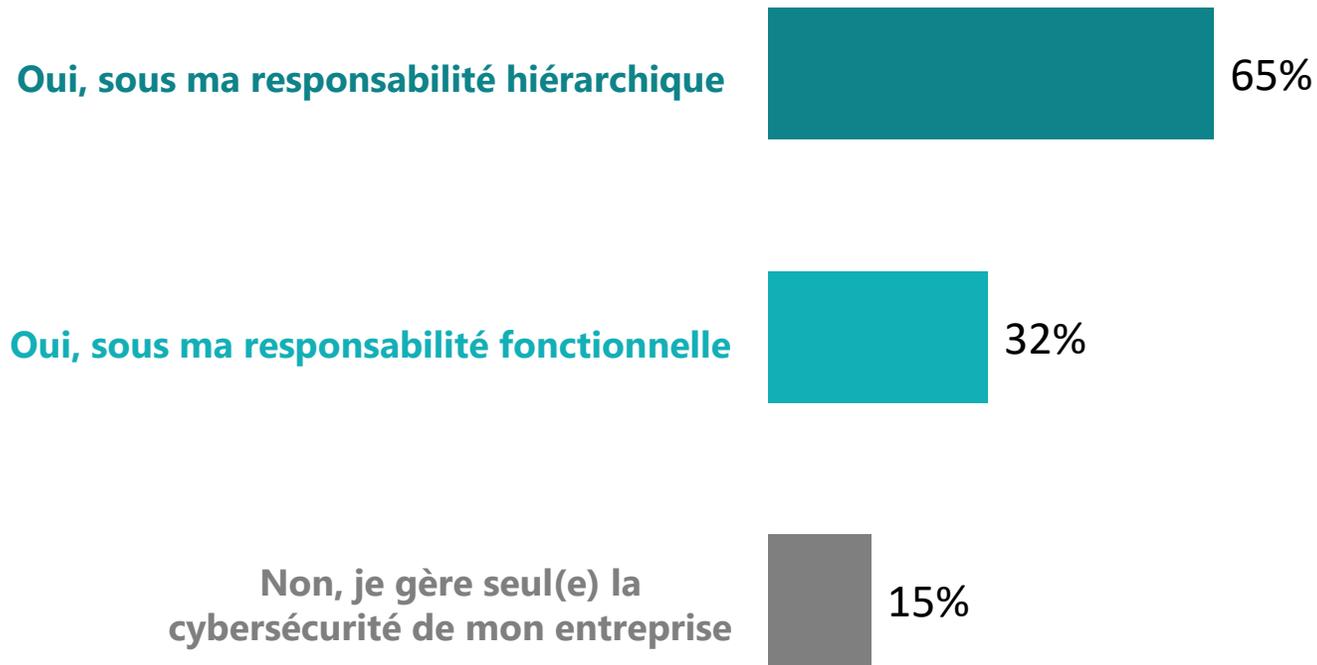
Moins de 1 000 salariés : 53%



# La majorité d'entre eux ont une équipe interne sous leur responsabilité

Q11 : Avez-vous une équipe interne à l'entreprise ?

Base : ensemble (390)



## 85%

### Ont une responsabilité hiérarchique ou fonctionnelle

De combien de personnes êtes-vous le responsable **hiérarchique** ?

13

personnes en moyenne

De combien de personnes internes êtes-vous le responsable **fonctionnel** ?

20

personnes en moyenne



# Assez logiquement, le niveau de responsabilité managériale est plus élevé au sein des grandes structures

Q11 : Avez-vous une équipe interne à l'entreprise ?

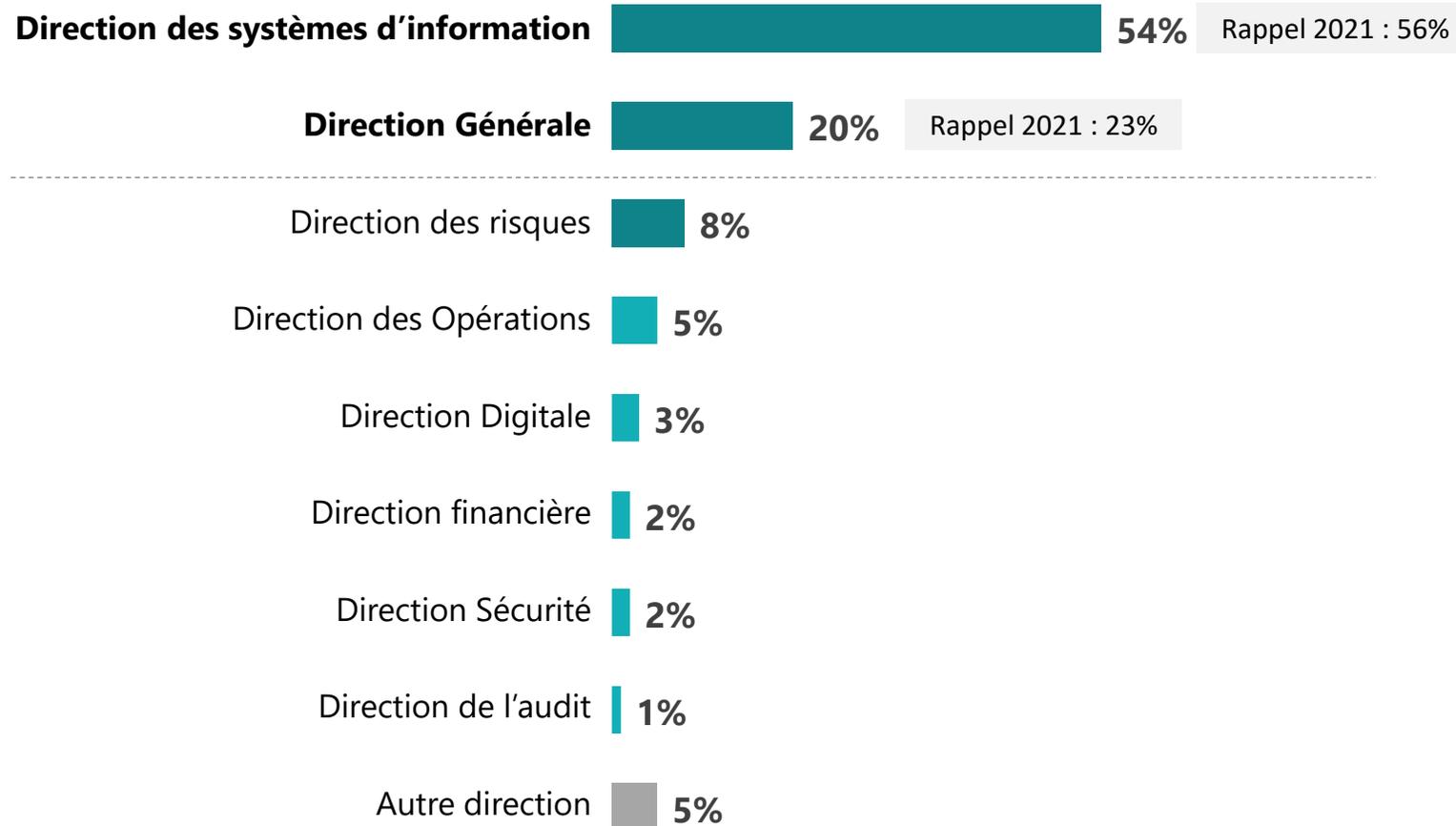
Base : ensemble (390)

|   | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble   |
|---|-------------------------|-------------------------------|------------------------|------------|
| <i>Base</i>   | 117                     | 101                           | 172                    | 390        |
| <b>Total Responsabilité</b>                             | <b>76%</b>              | <b>75%</b>                    | <b>97%</b>             | <b>85%</b> |
| Oui, sous ma responsabilité hiérarchique                | 50%                     | 53%                           | 81%                    | 65%        |
| Oui, sous ma responsabilité fonctionnelle               | 32%                     | 30%                           | 32%                    | 32%        |
| Non, je gère seul(e) la cybersécurité de mon entreprise | 24%                     | 25%                           | 3%                     | 15%        |

# Les responsables cyber sont majoritairement rattachés à la DSI, 1 responsable sur 5 reporte directement à la Direction Générale

Q15 : A quelle **Direction** êtes-vous rattaché(e) ?

Base : ensemble (390)





# Les responsables cyber des entreprises de moins de 1 000 salariés sont davantage rattachés à la direction générale plutôt qu'à la DSI, par rapport à leurs homologues dans des structures plus grandes

Q15 : A quelle **Direction** êtes-vous rattaché(e) ?

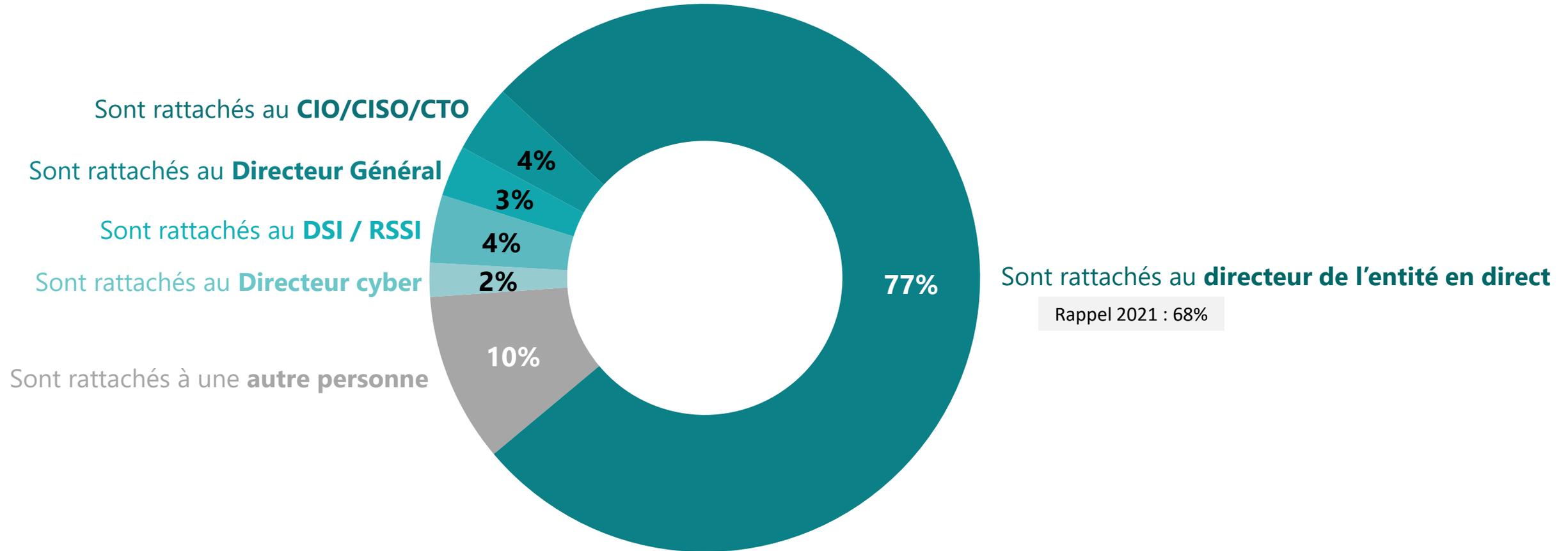
Base : ensemble (390)

|                                      | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble |
|--------------------------------------|-------------------------|-------------------------------|------------------------|----------|
| Base                                 | 117                     | 101                           | 172                    | 390      |
| Direction des systèmes d'information | 43%                     | 59%                           | 59%                    | 54%      |
| Direction générale                   | 31%                     | 12%                           | 16%                    | 20%      |
| Direction des risques                | 7%                      | 11%                           | 8%                     | 8%       |
| Direction des Opérations             | 7%                      | 6%                            | 3%                     | 5%       |
| Direction Digitale                   | 2%                      | 2%                            | 5%                     | 3%       |
| Direction financière                 | 2%                      | 2%                            | 2%                     | 2%       |
| Direction Sécurité                   | 1%                      | 2%                            | 3%                     | 2%       |
| Direction de l'audit                 | 1%                      | -                             | 1%                     | 1%       |
| Autre                                | 6%                      | 6%                            | 3%                     | 5%       |

# “ Lorsqu’un responsable cyber est rattaché à une Direction, il est, dans une large majorité des cas, un « direct report » du Directeur.

Q15bis : Et à qui êtes-vous rattaché dans cette direction ?

Base : ensemble (390)

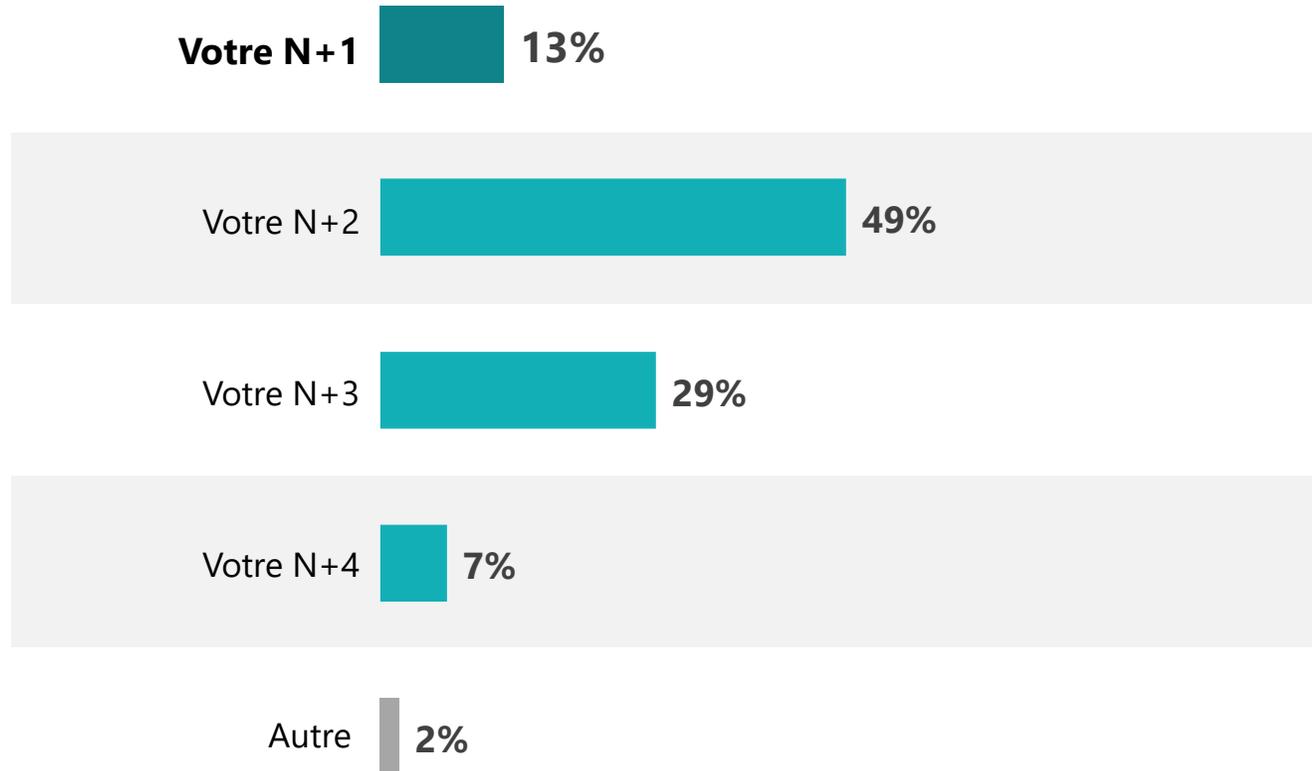




# ...Cela place en majorité les Responsables cyber à 2 ou 3 niveaux de la Direction Générale

Q16 : Le **Directeur Général de votre entreprise** est ?

Base : ensemble (390)





# Détail, par taille d'entreprise, de la relation à la Direction Générale.

Q16 : Le Directeur Général de votre entreprise est ?

Base : ensemble (390)

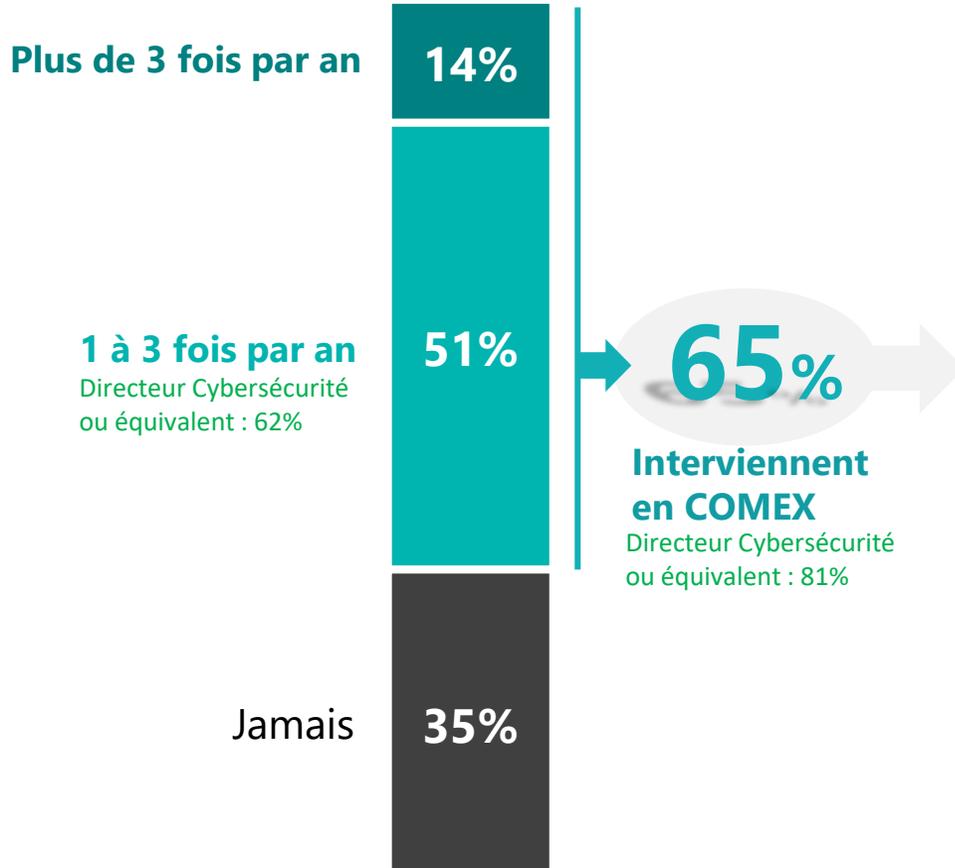
|           | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble |
|-----------|-------------------------|-------------------------------|------------------------|----------|
| Base      | 117                     | 101                           | 172                    | 390      |
| Votre N+1 | 26%                     | 10%                           | 6%                     | 13%      |
| Votre N+2 | 47%                     | 51%                           | 49%                    | 49%      |
| Votre N+3 | 21%                     | 31%                           | 35%                    | 29%      |
| Votre N+4 | 4%                      | 8%                            | 8%                     | 7%       |
| Autre     | 2%                      | -                             | 2%                     | 2%       |



# Deux tiers des responsables cyber sont amenés à intervenir en COMEX, principalement pour montrer leur feuille de route et l'avancement associé.

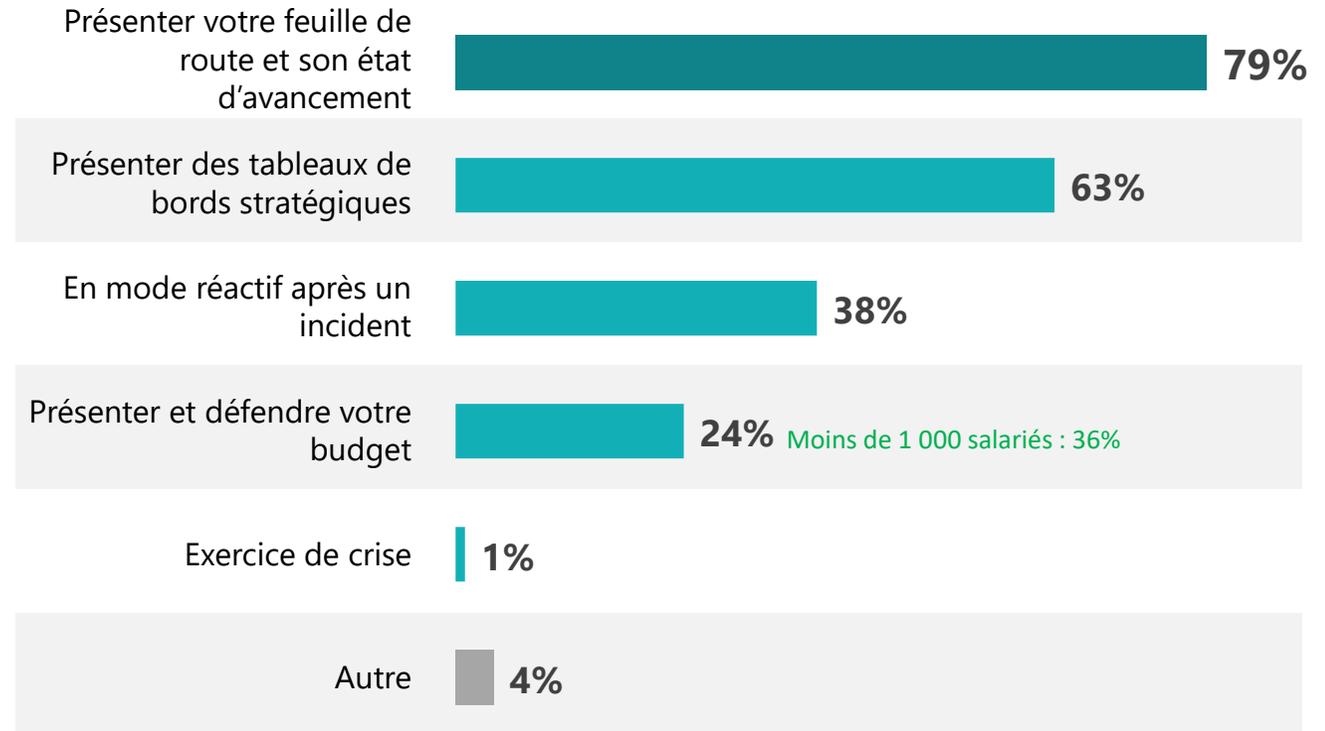
Q17 : Intervenez-vous en COMEX ?

Base : ensemble (390)



Q18 : Pour quelles raisons ?

Base : interviennent en COMEX (255) – Plusieurs réponses possibles

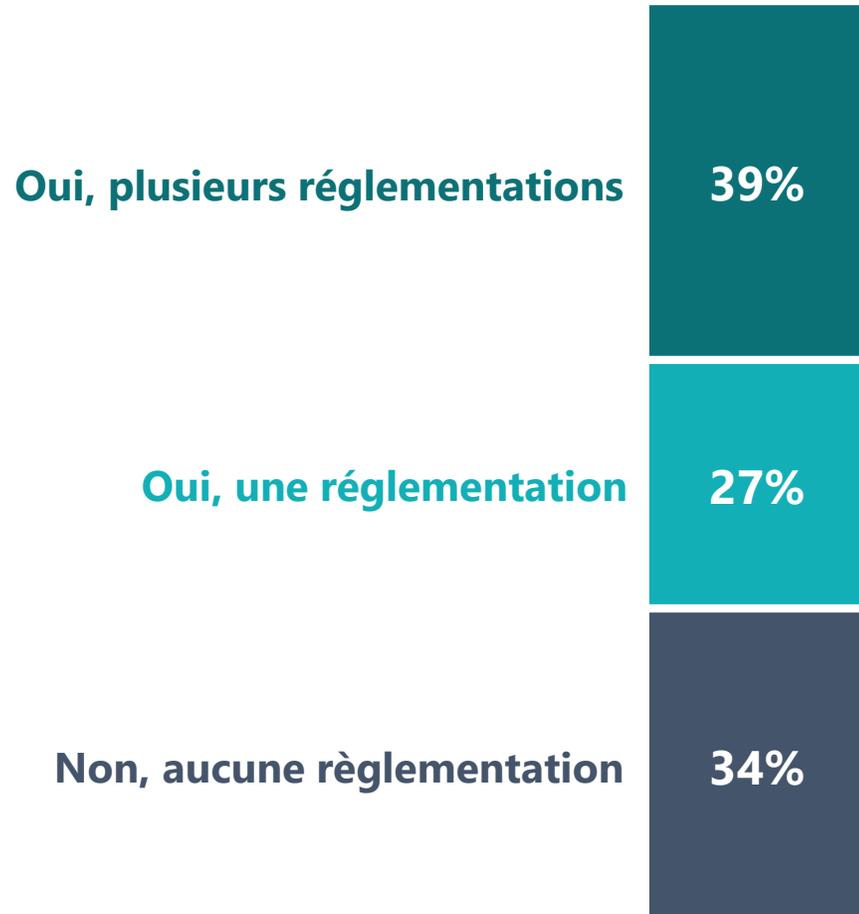




# Deux tiers d'entre eux sont assujettis à au moins une réglementation en lien avec la cybersécurité, en sus du GDPR...

Q6 : En dehors du GDPR, êtes-vous assujetti à au moins une réglementation du domaine cyber (OIV, NIS, RGS, ...)

Base : ensemble (390)



**66%**

Sont assujettis à au moins une réglementation du domaine cyber



## ...le poids des exigences réglementaires est indépendant de la taille de l'entreprise ...

Q6 : En dehors du GDPR, êtes-vous assujéti à au moins une réglementation du domaine cyber (OIV, NIS, RGS, ...)

Base : ensemble (390)

|                                | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble   |
|--------------------------------|-------------------------|-------------------------------|------------------------|------------|
| <i>Base</i>                    | 117                     | 101                           | 172                    | 390        |
| <b>Total Oui</b>               | <b>65%</b>              | <b>60%</b>                    | <b>70%</b>             | <b>66%</b> |
| Oui, une réglementation        | 27%                     | 27%                           | 27%                    | 27%        |
| Oui, plusieurs réglementations | 38%                     | 33%                           | 43%                    | 39%        |
| Non, aucune réglementation     | 35%                     | 40%                           | 30%                    | 34%        |



# ...mais il varie en revanche très nettement en fonction du secteur d'activité, les secteurs banques, assurances et secteur public restant les plus réglementés.

Q6 : En dehors du GDPR, êtes-vous assujetti à au moins une réglementation du domaine cyber (OIV, NIS, RGS, ...)

Base : ensemble (390)

|                                | Administration (secteur public) | Assurance-Mutuelle | Banque-Finance | Distribution | Industrie  | Services   | Télécom et Informatique | Ensemble   |
|--------------------------------|---------------------------------|--------------------|----------------|--------------|------------|------------|-------------------------|------------|
| Base                           | 38                              | 31                 | 39             | 35           | 57         | 36         | 66                      | 390        |
| <b>Total Oui</b>               | <b>92%</b>                      | <b>87%</b>         | <b>84%</b>     | <b>28%</b>   | <b>58%</b> | <b>31%</b> | <b>62%</b>              | <b>66%</b> |
| Oui, une réglementation        | 39%                             | 35%                | 33%            | 14%          | 25%        | 14%        | 23%                     | 27%        |
| Oui, plusieurs réglementations | 53%                             | 52%                | 51%            | 14%          | 33%        | 17%        | 39%                     | 39%        |
| Non, aucune réglementation     | 8%                              | 13%                | 16%            | 72%          | 42%        | 69%        | 38%                     | 34%        |



# 02

Comment les responsables cybersécurité travaillent-ils aujourd'hui ?





**A**

Une gestion des ressources  
maîtrisée mais des difficultés  
pour attirer de nouveaux talents

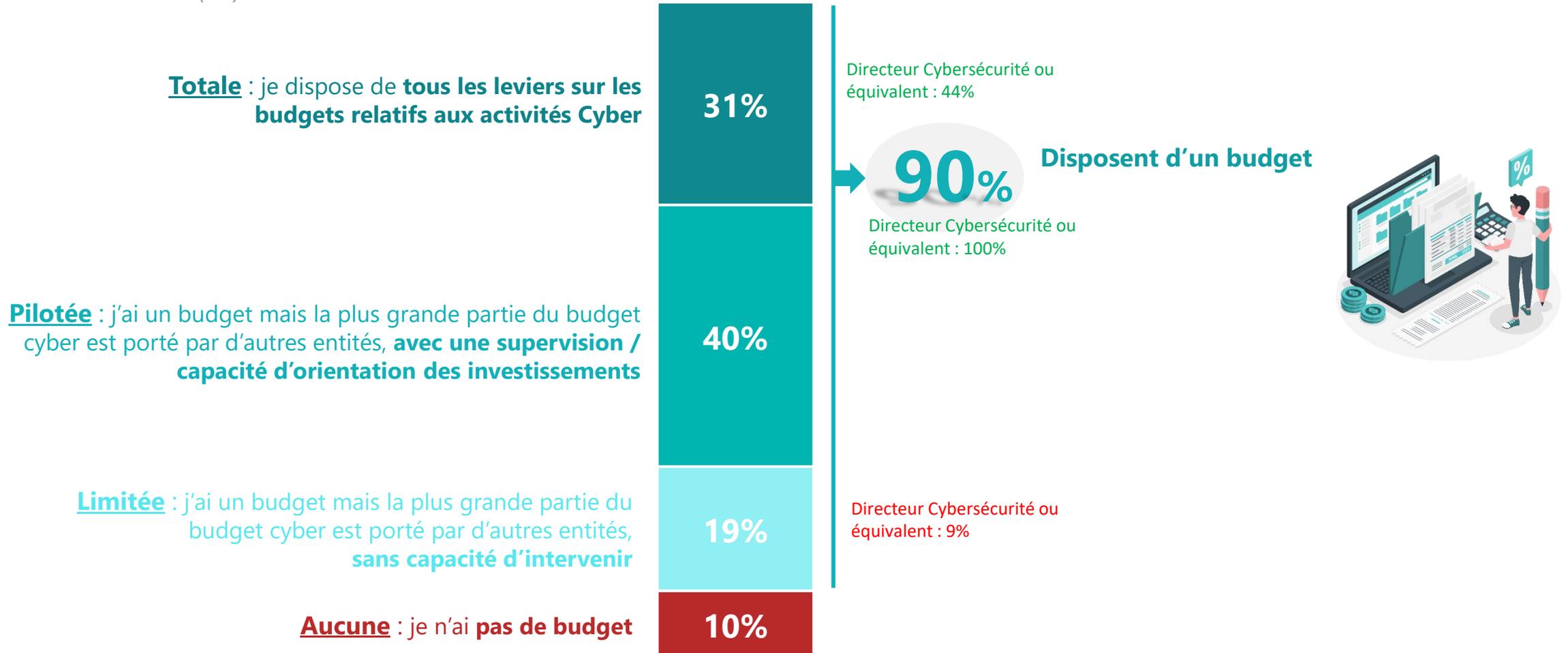




# Si la quasi-totalité des responsables cyber disposent d'un budget, et peuvent largement l'orienter, un responsable sur trois a tous pouvoirs de décision sur la dépense cyber

Q14 : De quelle **autonomie budgétaire** disposez-vous ?

Base : ensemble (390)



# “**Détail par taille d'entreprise. Les leviers sur les budgets sont peu corrélés à la taille de l'entreprise.**

Q14 : De quelle **autonomie budgétaire** disposez-vous ?

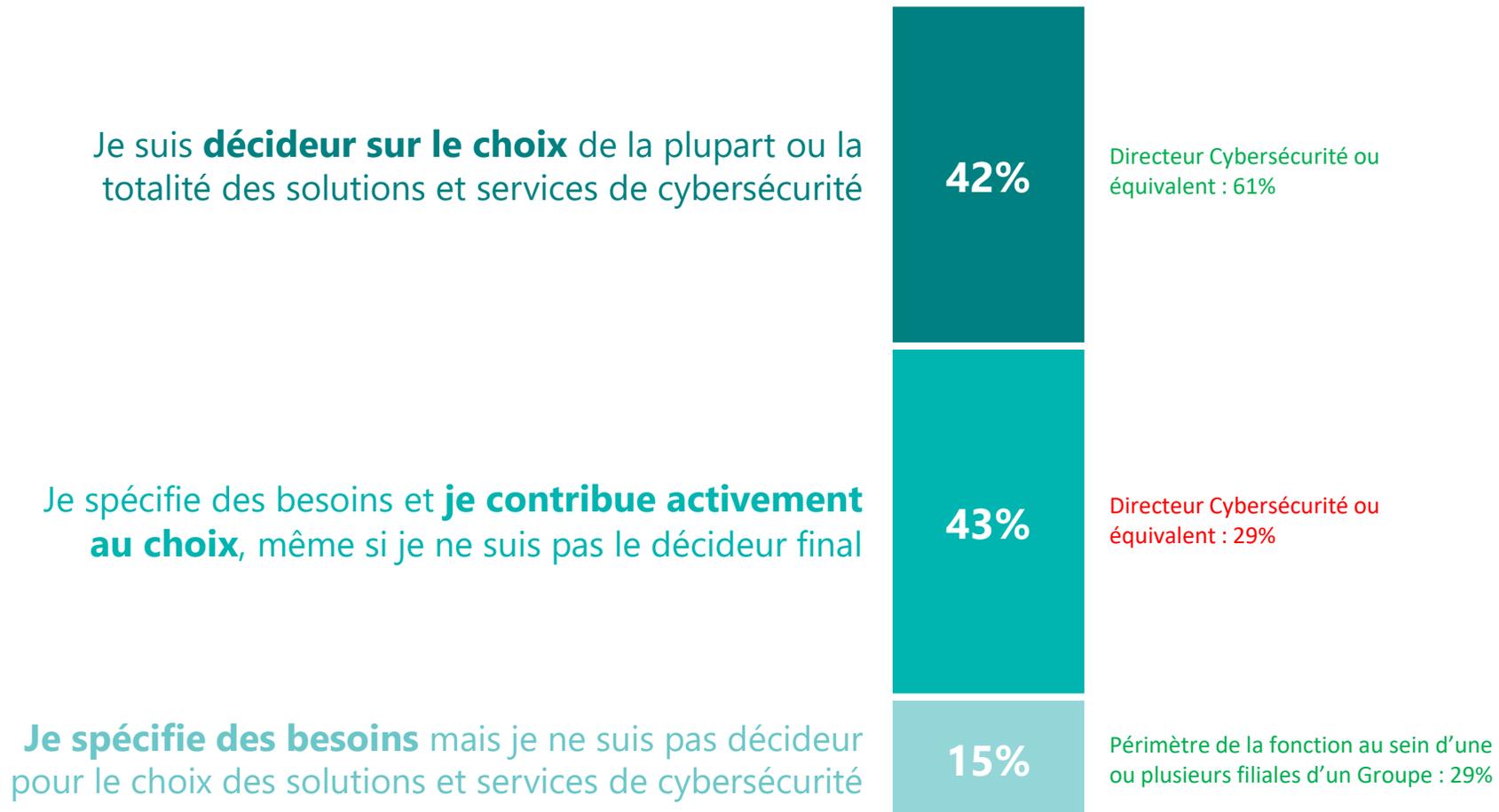
Base : ensemble (390)

|   | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble   |
|---|-------------------------|-------------------------------|------------------------|------------|
| <i>Base</i>   | 117                     | 101                           | 172                    | 390        |
| <b>Total Dispose d'un budget</b>  | <b>85%</b>              | <b>87%</b>                    | <b>96%</b>             | <b>90%</b> |
| Totale – Je dispose de tous les leviers sur les budgets relatifs aux activités Cyber  | 30%                     | 25%                           | 35%                    | 31%        |
| Pilotée – J'ai un budget mais la plus grande partie du budget cyber est porté par d'autres entités, avec une supervision/capacité d'orientation des investissements | 32%                     | 42%                           | 45%                    | 40%        |
| Limitée – J'ai un budget mais la plus grande partie du budget cyber est porté par d'autres entités, sans capacité d'intervenir                                      | 23%                     | 20%                           | 16%                    | 19%        |
| Aucune- Je n'ai pas de budget   | 15%                     | 13%                           | 4%                     | 10%        |

# Les responsables cyber sont autonomes ou au moins largement influents sur le choix des solutions et services de cybersécurité

Q14bis. De quelle autonomie disposez-vous dans le choix des solutions et services de cybersécurité ?

Base : ensemble (302)

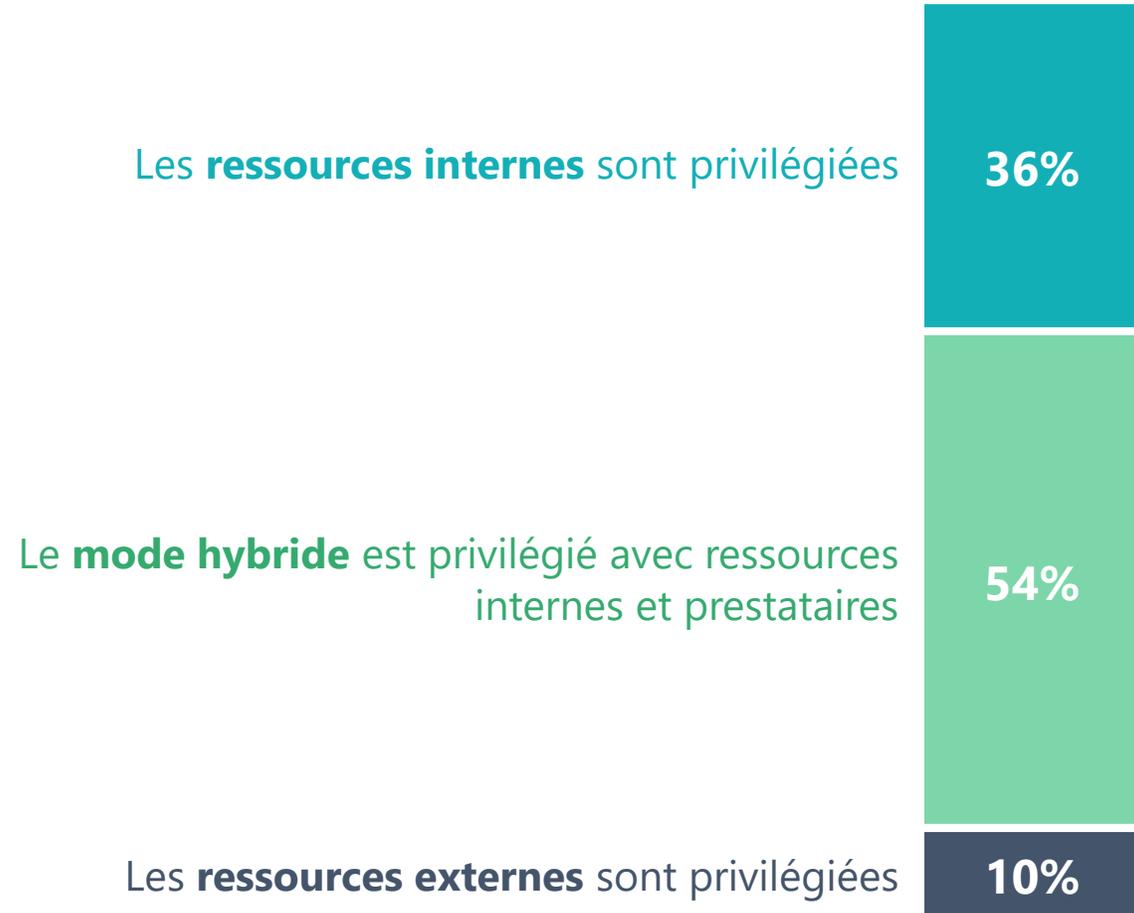




# La moitié des entreprises privilégient un mode hybride pour les ressources cyber, un tiers privilégie uniquement les ressources internes...

Q13 : Quelle évolution observez-vous dans votre entreprise, concernant le **développement des ressources cyber** ?

Base : ensemble (390)



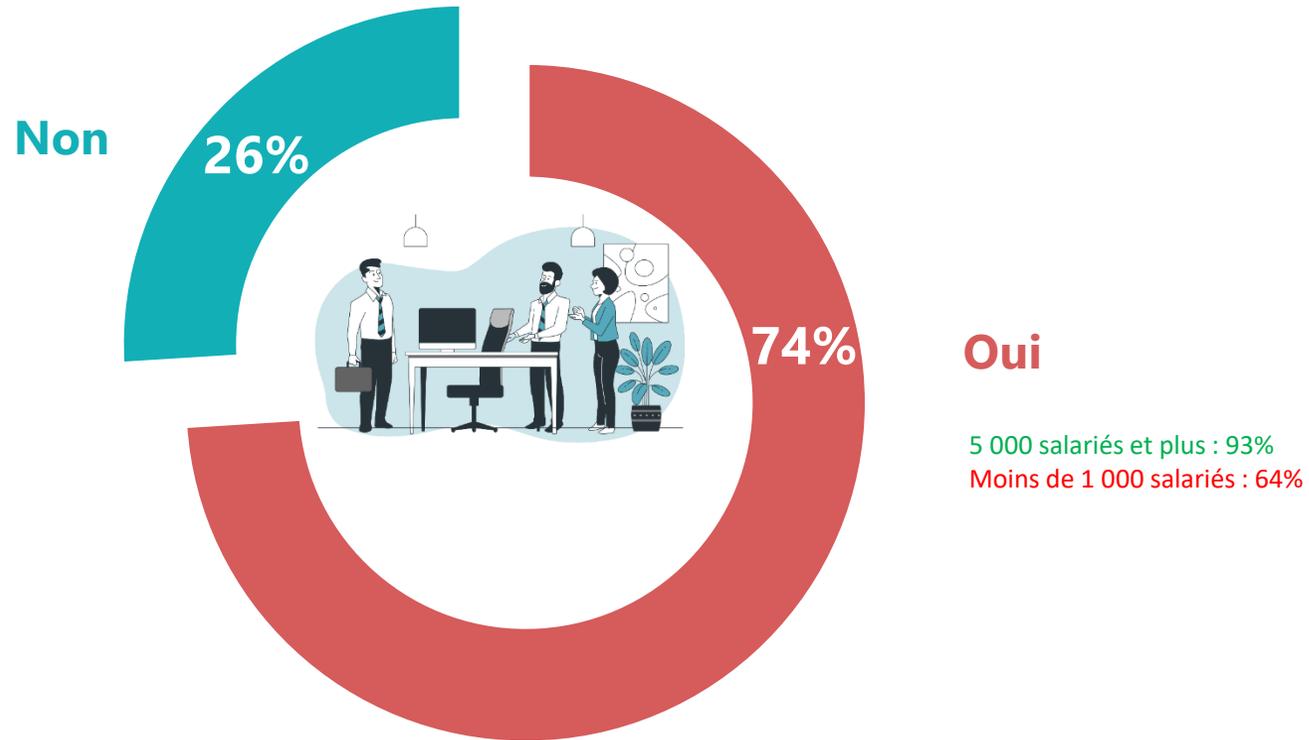
Périmètre de l'activité sur une entreprise indépendante : 51%



# “ ...bien que trois quarts des entreprises rencontrent des difficultés de recrutement des talents cyber

Q28 : Du fait de la pénurie de talents en cybersécurité, **rencontrez-vous des difficultés de recrutement de talents cyber ?**

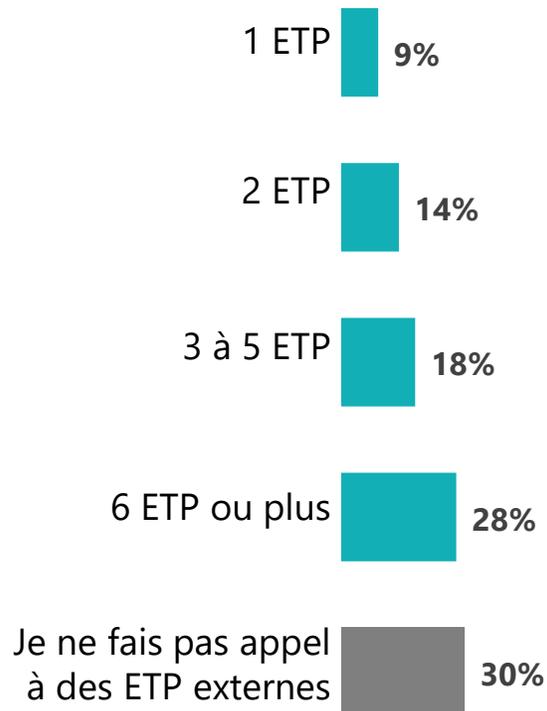
Base : ensemble (390)



# “ La grande majorité des entreprises fait appel à des ETP externes, que ce soit en mode hybride ou complètement externalisé

Q12 : A combien d'ETP externes à l'entreprise (prestataires sur sites et services managés de cybersécurité) faites-vous appel en moyenne ?

Base : ensemble (390)



**70%**  
font appel à des ETP  
externes

5 000 salariés et plus : 83%  
Moins de 1 000 salariés : 57%  
Secteur télécom et informatique : 52%

Nombre moyen d'ETP  
externes à l'entreprise

**10,8**





**B**

Un rôle central et multiple au sein des organisations

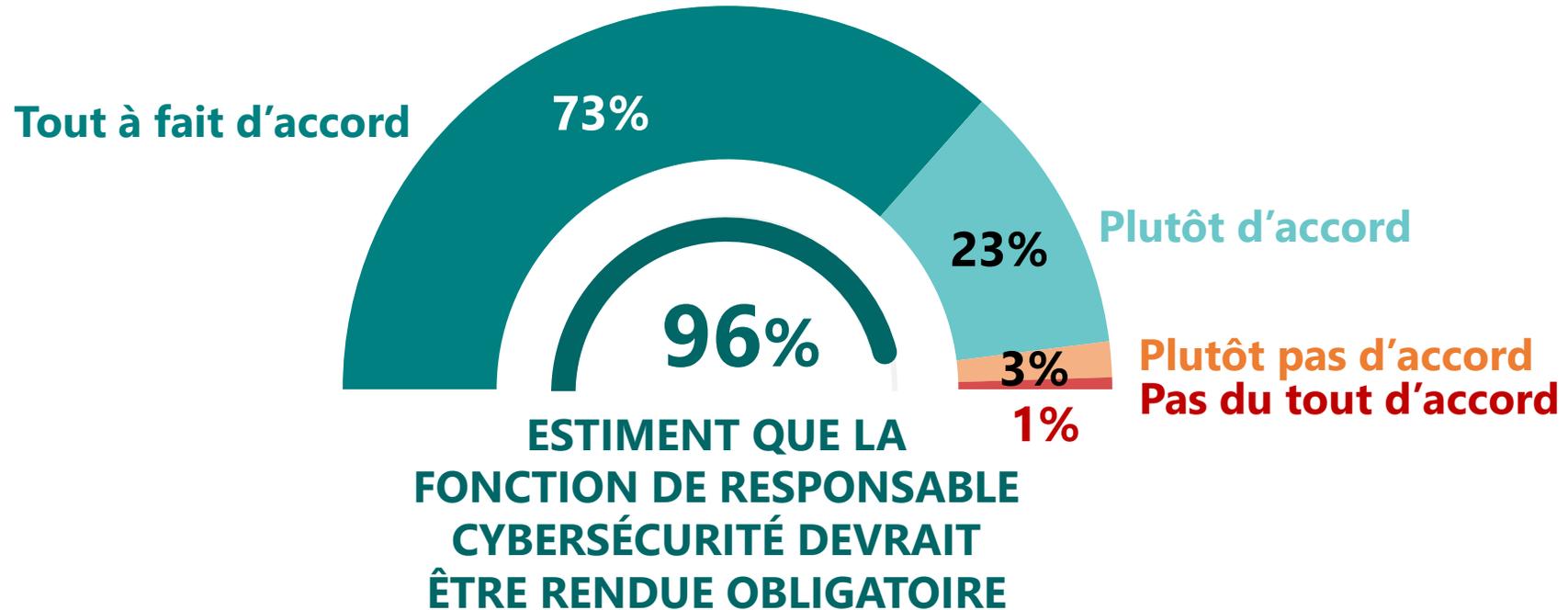




# La quasi-totalité des responsables cyber considèrent que leur fonction devrait être rendue obligatoire à partir d'une certaine taille d'entreprise

Q27 : Pensez-vous que la fonction de Responsable Cybersécurité devrait être rendue obligatoire, à partir d'un certain seuil pour les entreprises ?

Base : ensemble (390)

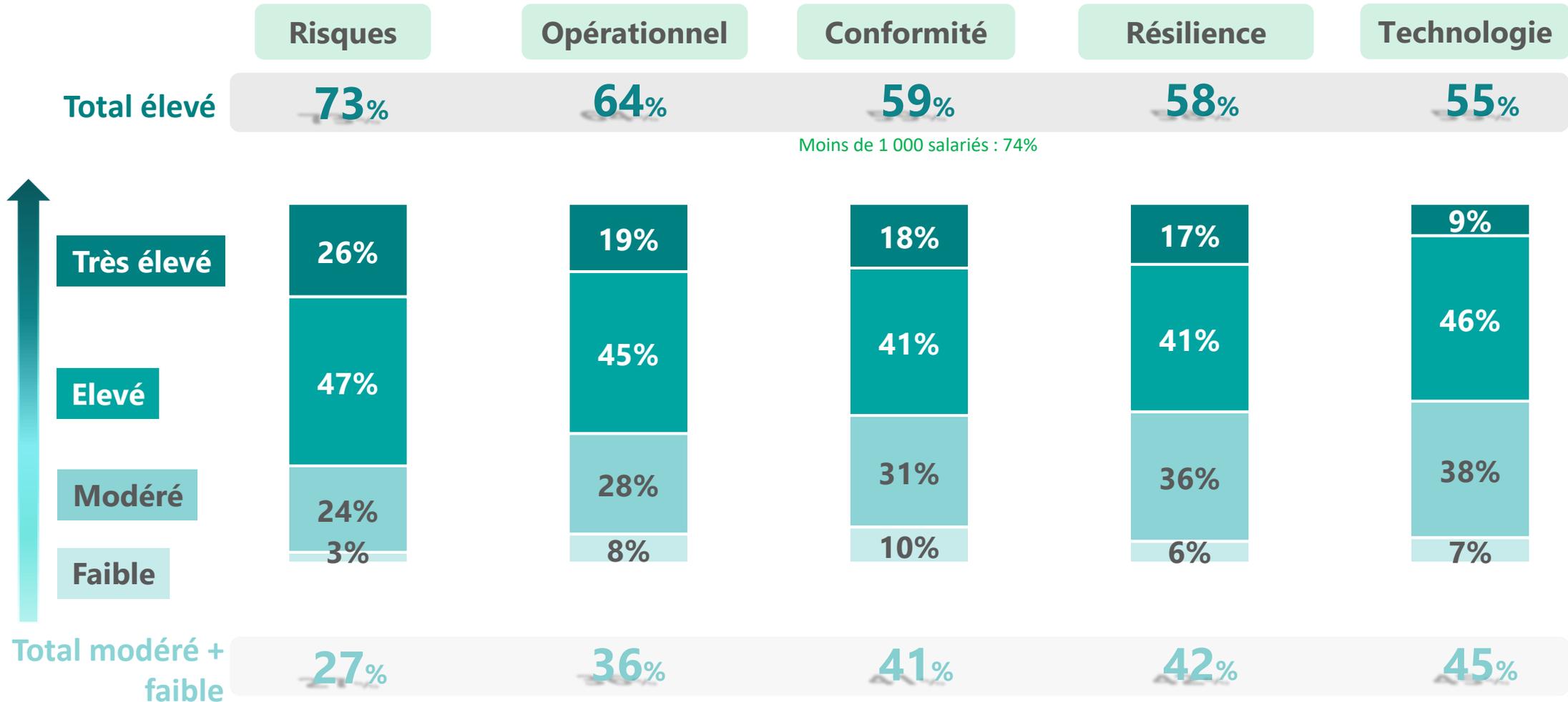




# La gestion des risques est le critère impactant le plus la fonction de responsable cybersécurité, mais l'opérationnel prend aussi une part importante dans l'activité...

Q19 : Pour chacun des critères que nous allons vous présenter, merci de nous indiquer, selon vous, le poids qu'ils exercent actuellement dans votre fonction ?

Base : ensemble (390)

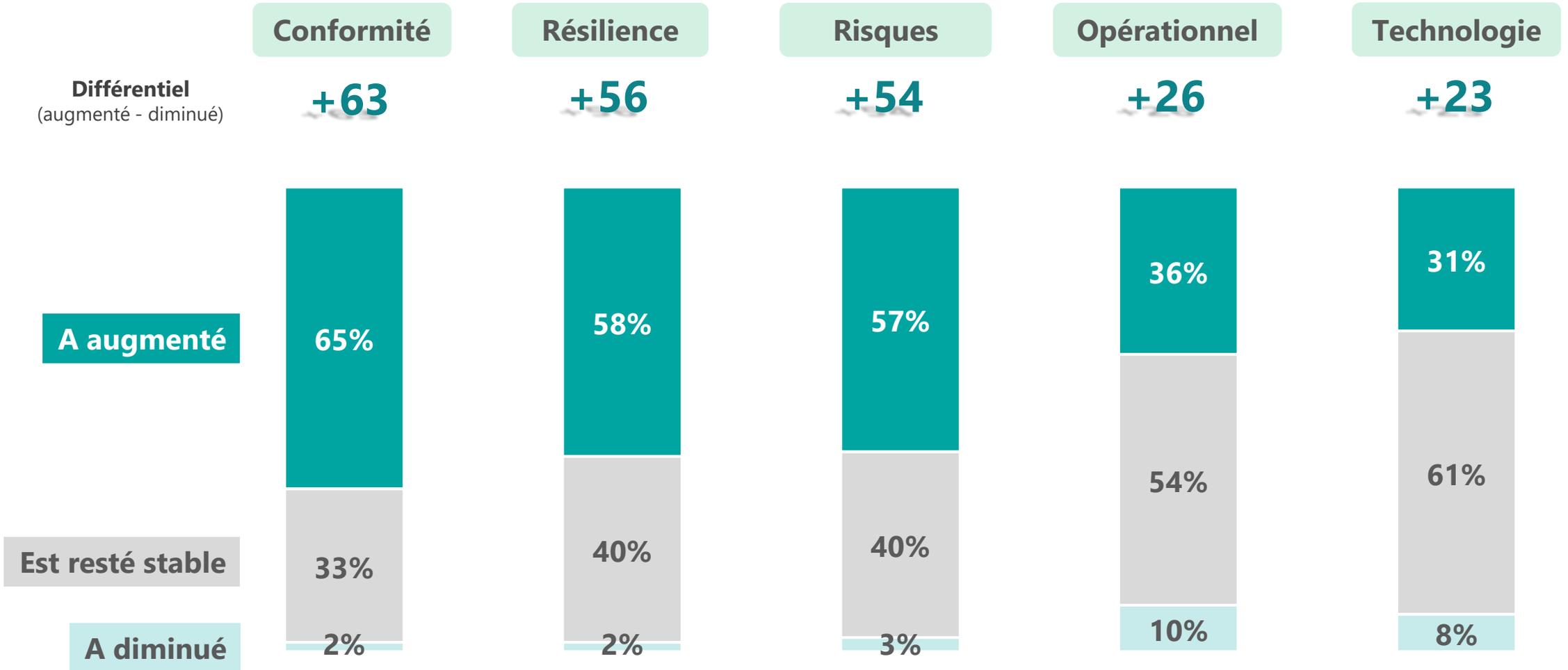




# ...bien que ce soit les sujets de conformité qui aient le plus progressé durant les 5 dernières années, avec le développement de nombreuses réglementations

Q19b : Et toujours pour ces mêmes critères, merci de nous indiquer si, selon vous, le poids qu'ils exercent dans votre fonction a évolué durant les 5 dernières années ?

Base : ensemble (390)





# Rôles et responsabilités des responsables cyber – L'analyse du CESIN

## Méthodologie

L'enquête a permis d'établir les rôles et responsabilités des Responsables cyber sur les différents sujets de cybersécurité ou connexes à la cybersécurité. L'objectif est de placer les activités du Responsable Cyber selon un RACI.

Il a été demandé aux répondants de se positionner sur une liste de 32 activités avec la question suivante : *Nous allons vous présenter un certain nombre d'activité pouvant être incluses dans votre champ d'action, merci de nous dire pour chacune d'entre elle si vous en êtes le Responsable (au sens 'Accountable'), le Réalisateur (R: celui qui réalise l'activité), les deux (A/R), un Contributeur à l'activité (C) ou une personne tenu informée (I) sur cette activité.*

# Rôles et responsabilités des responsables cyber – L'analyse du CESIN

**4 activités cœur, communes pour lesquelles les responsables cyber sont responsables et/ou réalisateurs à plus de 80%**

- Les analyses des risques cyber (92%)
- Les politique de sécurité (89%)
- La sensibilisation (86%)
- la sécurité offensive (audits, pen tests, red teams, bug bounties) : 80%

# “ Rôles et responsabilités des responsables cyber – L’analyse du CESIN

**La gestion des risques :** tous les responsables cyber contribuent à la gestion du risque IT, et 60% conduisent cette activité. Historiquement le risque IT était géré indépendamment du risque cyber.

## **Les activités de pilotage :**

- 3 responsables cyber sur 4 sont responsables ou en charge de la veille cyber, de la stratégie, de la roadmap cyber, du budget et du reporting stratégique.
- 2 responsables cyber sur 3 sont des décideurs pour le choix des solutions cyber et pilotent leur intégration, les autres étant a minima contributeurs sur l’acquisition et l’implémentation de ces solutions.

**L’ensemble des responsables cyber sont impliqués sur l’activité de sécurité dans les projets et dans la gestion des risques liés aux tiers** et 67% d’entre eux pilotent et réalisent ces activités. On peut noter toutefois qu’ils ne sont pas leaders (31%) sur la sécurité des architectures, qui reste sous pilotage IT, même s’ils y contribuent largement (84%).

**Un responsable cybersécurité sur trois est pleinement investi dans la sécurité des développements (DevSecOps, formation des développeurs, ...)**

**Tous les responsables cyber sont des parties prenantes dans le pilotage des crises cyber, 74% des Responsables cyber sont pleinement responsables de cette activité.**

## **Rôles et responsabilités des responsables cyber – L'analyse du CESIN**

**Environ 80% des Responsables Cyber assurent ou contribuent à la gestion opérationnelle de la cybersécurité (SOC, CERT, opérations de solutions de cybersécurité, tableaux de bord opérationnels associés), 60% des Responsables Cyber en sont même responsables. Ce mouvement général est observé depuis les 5 dernières années en lien avec la croissance des attaques... et celle des vulnérabilités.**

**On peut noter un cas particulier pour la gestion opérationnelle des firewalls et VPN, ainsi que le durcissement des systèmes, qui restent traditionnellement des tâches sous la responsabilité des opérations IT, car très imbriquées avec la gestion des réseaux et des systèmes.**

**Les responsables cyber sont largement (86%) impliqués dans la gestion des vulnérabilités (veille, scans, détections, alertes, priorisation), 2 responsables cyber sur 3 en sont même responsables ou en charge de réaliser cette activité, la gestion du patching restant dévolue aux équipes IT. 16% des Responsables cyber sont également responsables ou en charge de la gestion de l'obsolescence, qui est une activité en lien avec les vulnérabilités, et qui est historiquement assurée par les équipes opérationnelles IT. Ces profils-là s'inscrivent dans un profil cyber très orienté « opérationnel » et concernent à 80% des entreprises de moins de 5000 personnes.**

**Continuité d'activité :** les Responsables cyber sont très largement impliqués (84%) dans les Plans de continuité d'activité ou peut-être a minima leur sous-ensemble de cyber-résilience, c'est-à-dire les questions de continuité et de reprise d'activité liées à des incidents d'origine cyber. Un Responsable cyber sur 3 est même responsable de l'activité.

## **Rôles et responsabilités des responsables cyber – L’analyse du CESIN**

La fonction de DPO, créée depuis moins de 10 ans, est diversement rattachée dans les entreprises. **3 Responsables cyber sur 4 ont des niveaux de collaboration élevés ou très élevés avec le DPO** de leur entreprise. Et 18% des Responsables Cyber ont même la charge de la Privacy, soit parce que le DPO leur est rattaché, soit parce qu’ils portent la double fonction, selon la taille de l’organisation. A contrario, 11% des Responsables Cyber ne travaillent pas du tout et ne sont pas impliqués sur les sujets de Privacy.

**Conformité : tous les responsables cyber sont engagés dans la gestion de la conformité** mais seulement un responsable cyber sur deux (49%) est leader sur les questions de conformité.

**Gestion des Identités et des Accès** : 80% des Responsables Cyber conduisent ou sont impliqués dans la **gestion des identités**, et 38% en assument la responsabilité et la mise en œuvre.

Les activités **les plus en dehors du champ d’action du Responsable cyber ou pour lesquelles les Responsables Cyber sont simplement informés** sont les opérations de sauvegarde (63%), la sûreté (51%), et la lutte contre la fraude (44%).

A noter, pour ces activités, que :

- 14% des Responsables cyber ont également la responsabilité de la sûreté. Ces Responsables Cyber sont généralement (80%) dans des structures de moins de 5000 personnes
- 25% des Responsables cyber contribuent aux opérations de sauvegarde.
- 7% des Responsables cyber sont en charge de la lutte contre la fraude.

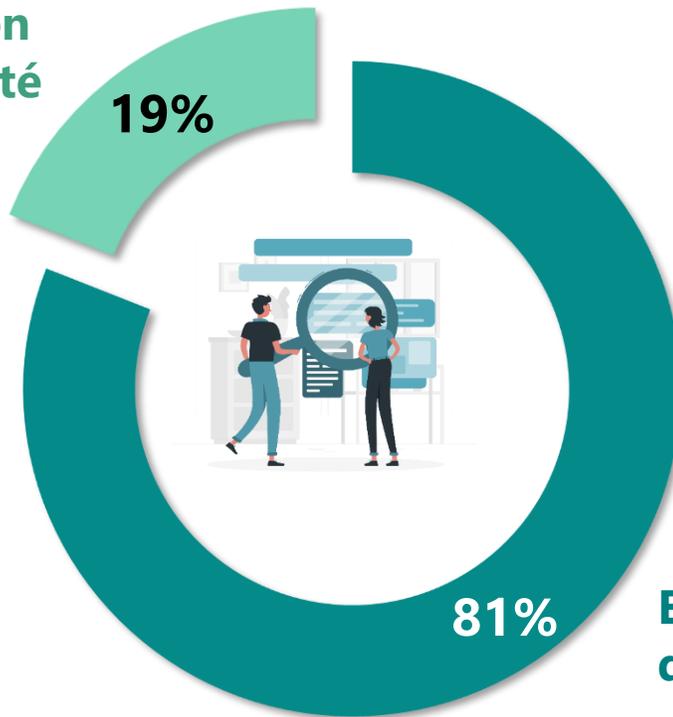


# Lorsque l'entreprise est concernée par un périmètre OT, l'activité est très majoritairement dans le périmètre du responsable cyber

Q21 : Comment est traitée la cybersécurité sur le volet industriel / OT dans votre entreprise ?

Base : ensemble (187) - en base hors concerné

La responsabilité du sujet est en dehors de l'équipe cybersécurité



Elle est dans mon périmètre de responsabilité



# Cette responsabilité sur la cybersécurité de l'OT se vérifie soit au sein des grandes entreprises, pour une cohérence de la gouvernance cyber, soit dans les petites entreprises qui ne peuvent pas multiplier les équipes.

Q21 : Comment est traitée la cybersécurité sur le volet industriel / OT dans votre entreprise ?

Base : ensemble (187) - en base hors concerné

|   | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble |
|---|-------------------------|-------------------------------|------------------------|----------|
| <i>Base</i>   | 25                      | 47                            | 115                    | 187      |
| Elle est dans mon périmètre de responsabilité                         | 92%                     | 68%                           | 83%                    | 81%      |
| La responsabilité du sujet est en dehors de l'équipe de cybersécurité | 8%                      | 32%                           | 17%                    | 19%      |



# 03

Quelle est la vision des responsables cybersécurité sur leur travail et leur rémunération ?





**A**

Des responsables cybersécurité  
satisfaits, soutenus par le Top  
Management





# La satisfaction au travail des responsables cybersécurité se maintient à un niveau élevé, les « très satisfaits » sont même plus nombreux qu'en 2021

Q22 : D'une manière générale, êtes-vous **satisfait de votre travail actuel** ?

Base : ensemble (390)

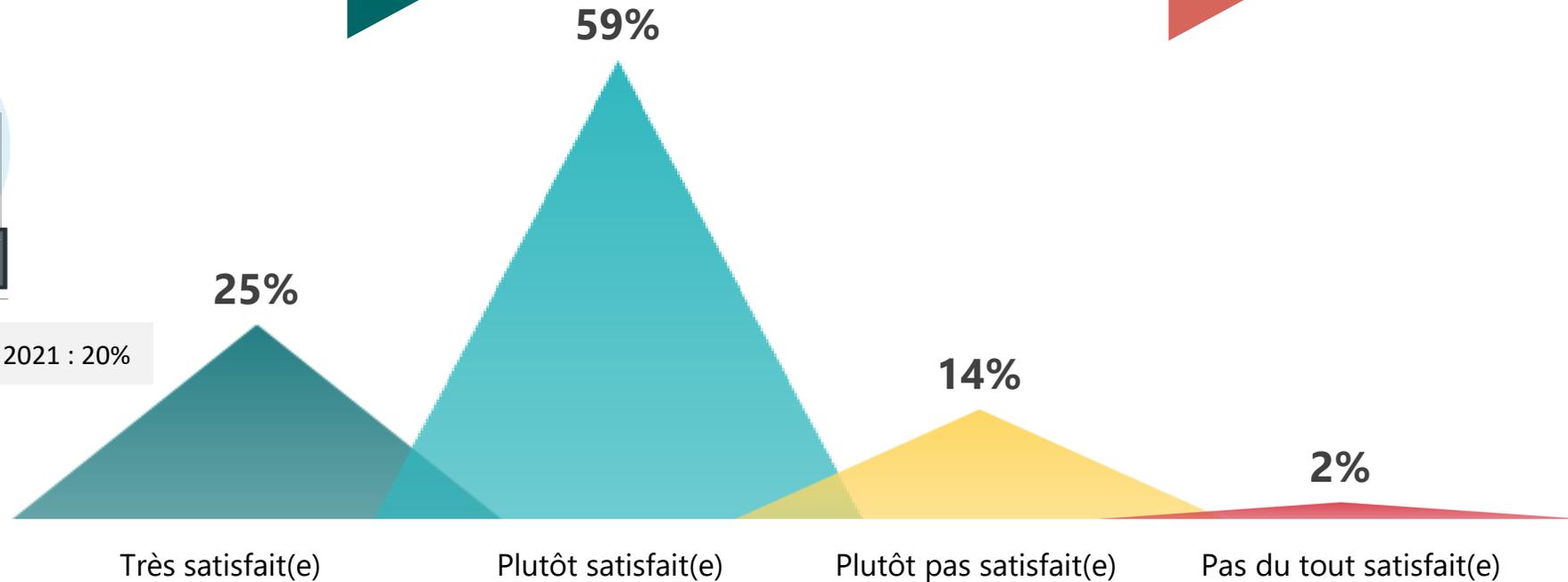
Rappel 2021 : 83%

**84%** Estiment être satisfait de leur travail actuel

Estiment ne pas être satisfait de leur travail actuel **16%**



Rappel 2021 : 20%

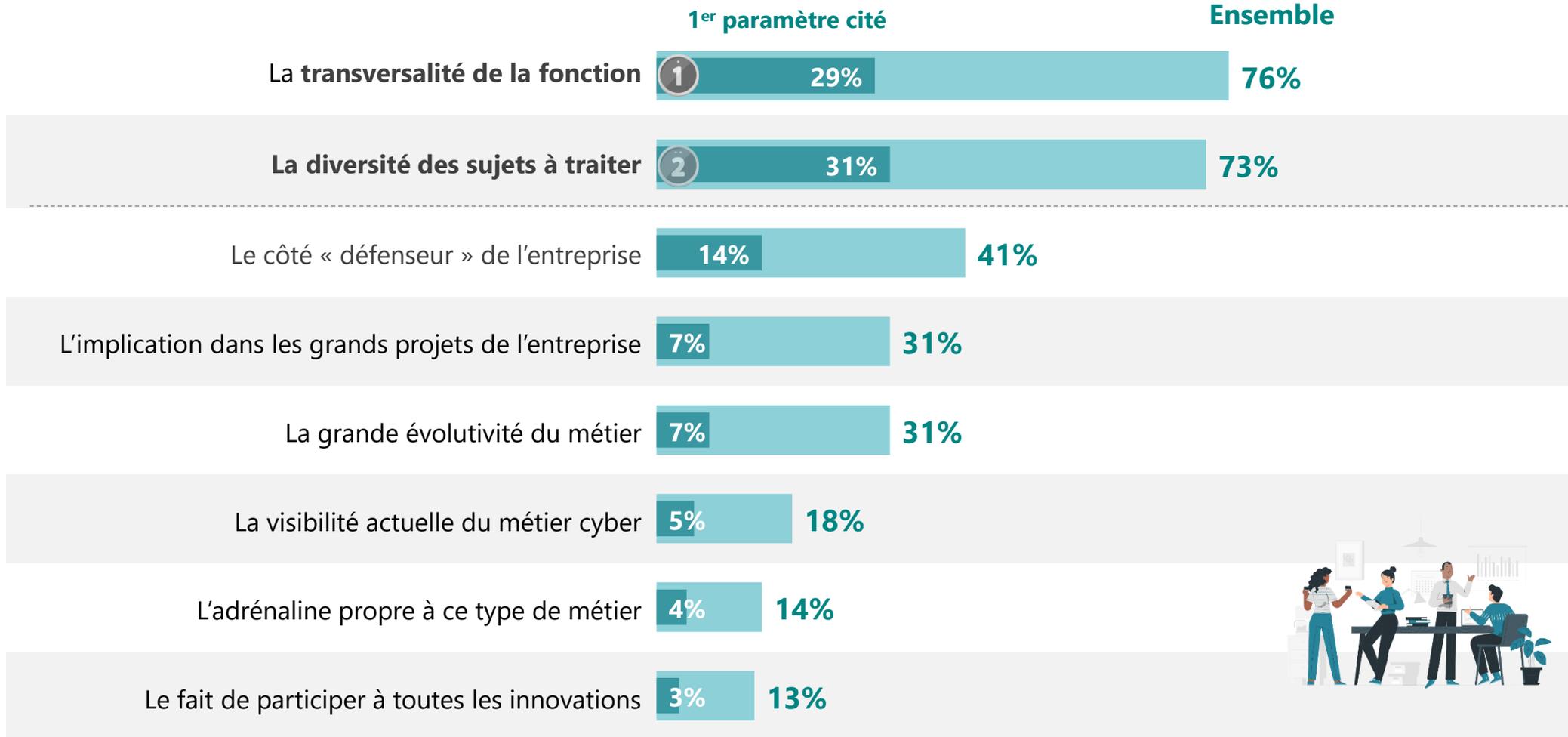


Directeur Cybersécurité ou équivalent : 39%

# “ La transversalité de la fonction et la diversité des sujets sont les deux paramètres ayant le plus d’influence sur leur motivation

Q26 : Pour vous, quels sont les 3 paramètres qui influencent le plus votre motivation professionnelle ?

Base : ensemble (390) – Trois réponses par ordre d’importance.



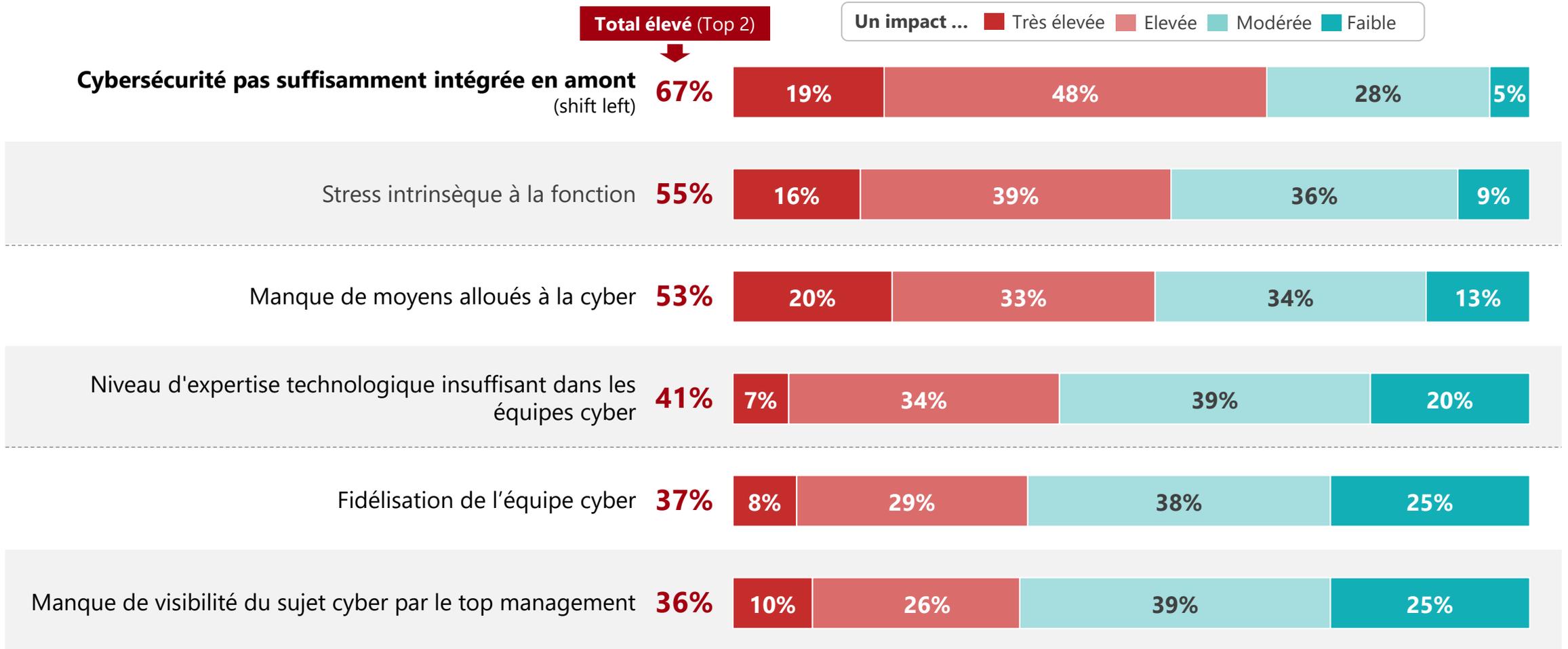


# Le manque d'intégration de la cybersécurité en amont dans les projets est la principale difficulté rencontrée par les responsables cyber, dont la moitié se déclare par ailleurs sous stress et en manque de moyens



Q23 : Parmi les **difficultés** suivantes, merci de nous indiquer **leur niveau d'impact sur l'exercice de votre fonction ?**

Base : ensemble (390)





# La collaboration reste particulièrement forte avec les opérations IT et le DPO

Q25 : Quelle **qualité de collaboration** avez-vous avec les métiers suivants ?

Base : ensemble (390)



Total élevé (Top 2)

Une collaboration ...

Très élevée

Elevée

Modérée

Faible

Ce métier n'est pas présent dans l'entreprise

Production / Opérations IT

77%

38%

39%

20%

3% <1%

DPO

71%

36%

35%

19%

8%

2%

Chefs de projets IT

57%

14%

43%

36%

5%

2%

Audit

50%

19%

31%

26%

7%

17%

Juridique

48%

14%

34%

35%

11%

6%

Contrôle interne

44%

14%

30%

27%

14%

15%

Métiers

42%

8%

34%

46%

12%

<1%

Ressources humaines

31%

8%

23%

45%

24%

Sûreté

30%

9%

21%

29%

24%

17%

Développeurs

30%

6%

24%

43%

21%

6%



# Les responsables cyber jugent recevoir suffisamment de soutien de la part du Top Management, pour un tiers, le soutien est même total

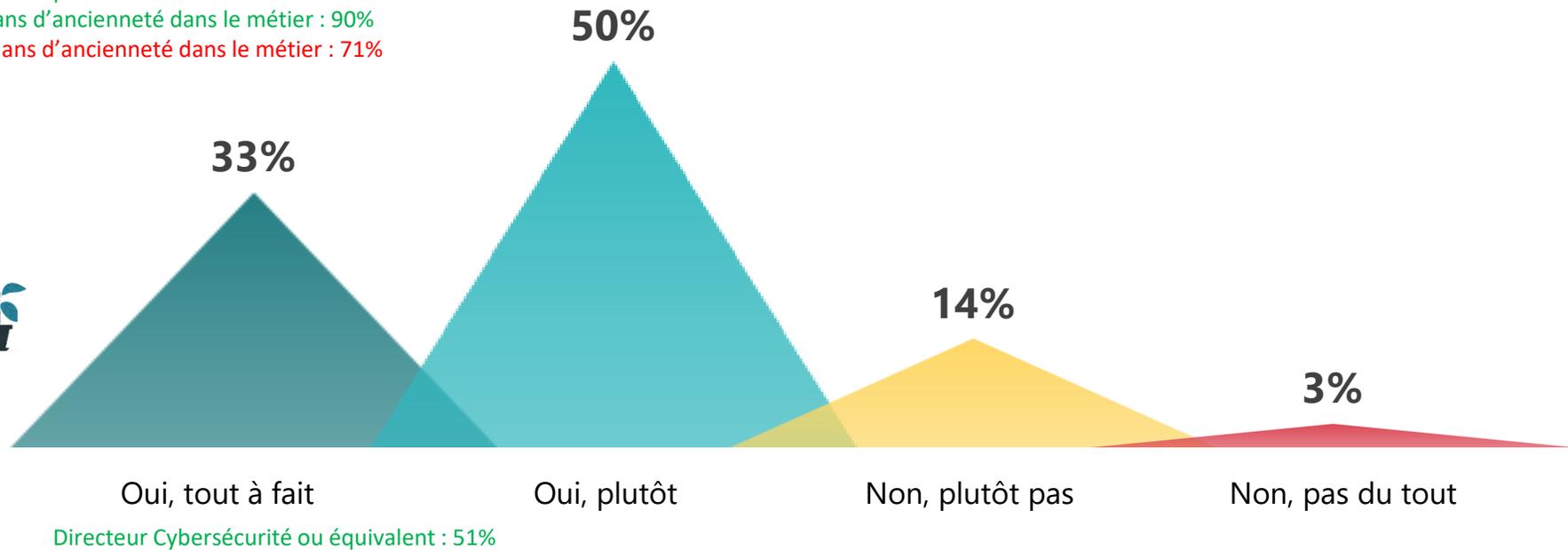
Q24 : Disposez-vous des appuis suffisants du top management pour l'exercice de votre fonction ?

Base : ensemble (390)

**83%** Estiment avoir des appuis suffisants du Top Management

Estiment ne pas avoir des appuis suffisants du Top Management **17%**

Directeur Cybersécurité ou équivalent : 94%  
5 000 salariés et plus : 90%  
Plus de 10 ans d'ancienneté dans le métier : 90%  
Moins de 5 ans d'ancienneté dans le métier : 71%

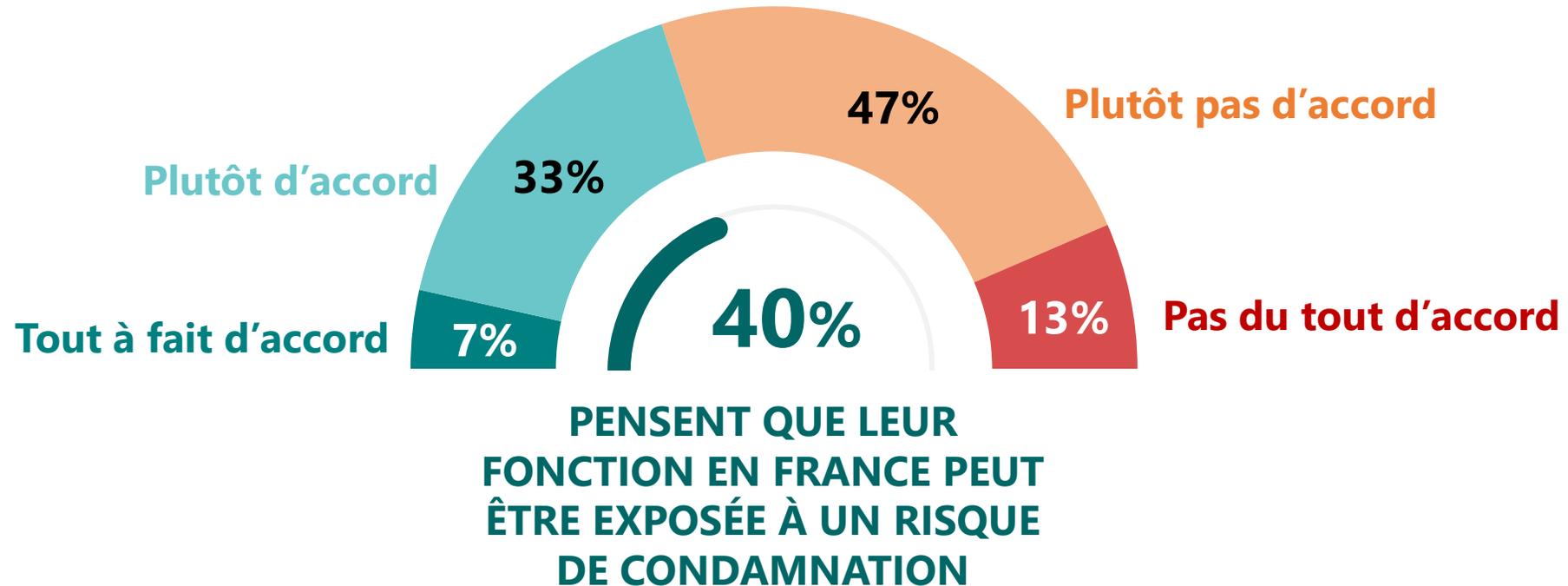




## 2 responsables cyber sur 5 estiment que leur fonction pourrait être exposée à un risque de condamnation

Q29 : Pensez-vous que  **votre fonction en France puisse être exposée à un risque de condamnation**, suite à un incident ?

Base : ensemble (390)





**B**

Une rémunération qui ne satisfait pas l'ensemble des responsables cyber

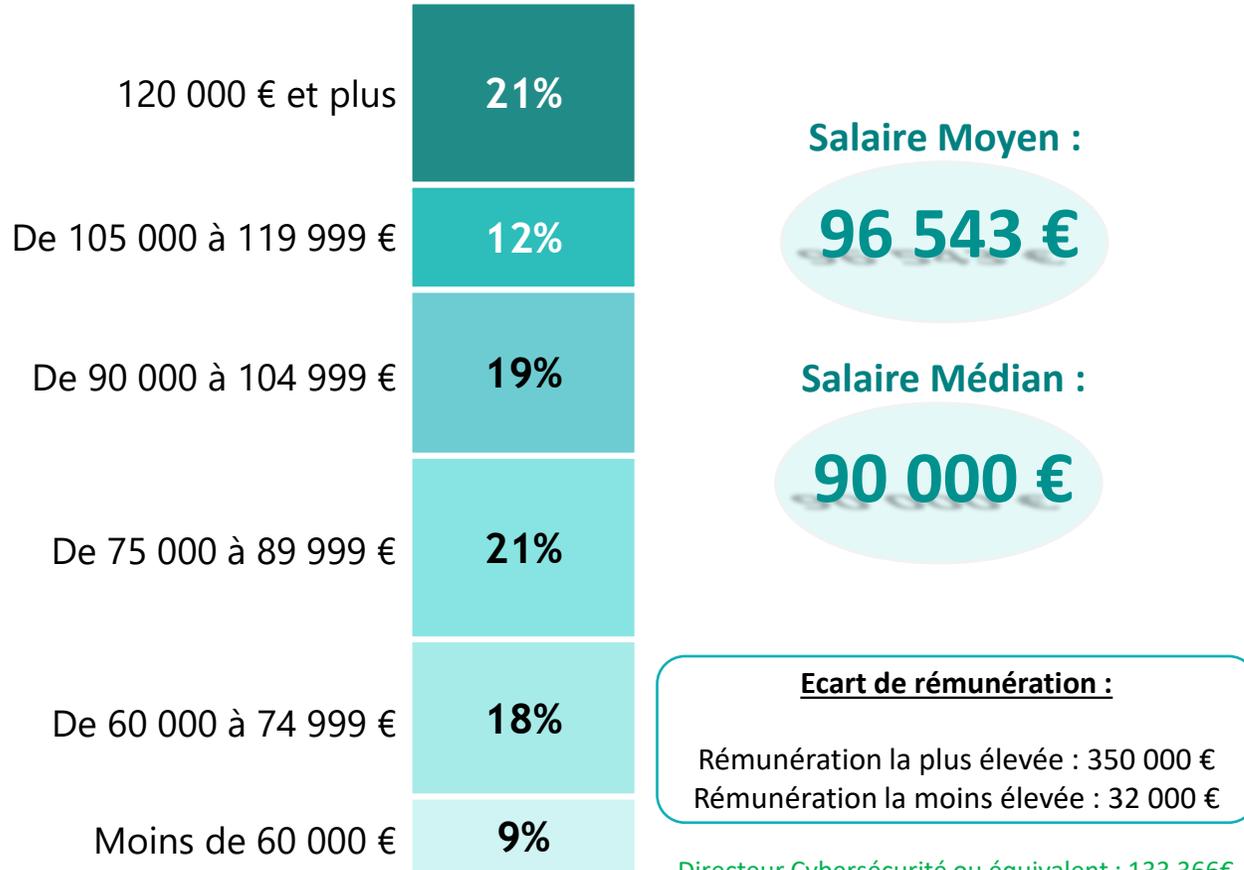




# La rémunération fixe moyenne d'un responsable cybersécurité en 2023 est de 96 543 €, à noter que ce salaire moyen est largement supérieur dans les grandes entreprises

Q30 : Quelle a été votre **rémunération annuelle fixe en 2023** (en brut avant impôts) ?

Base : ensemble – hors valeurs aberrantes (377)

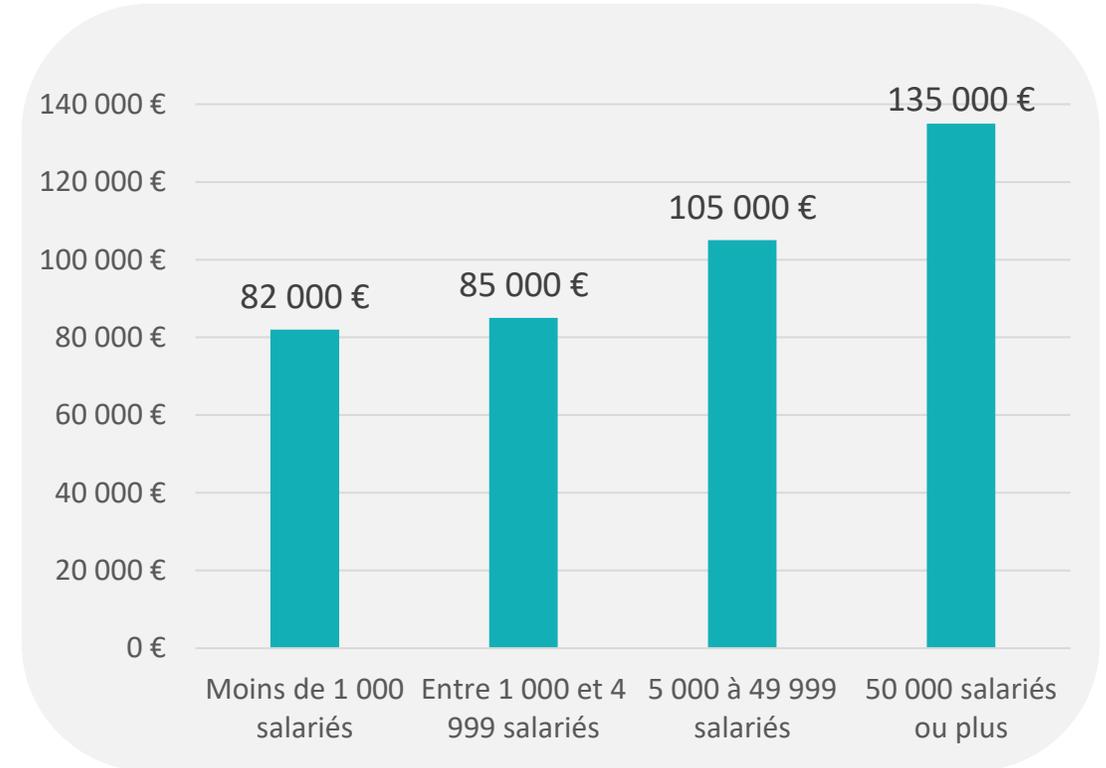


Directeur Cybersécurité ou équivalent : 133 366€

Responsable de la Sécurité des Systèmes

d'Information (RSSI) ou équivalent : 84 247€

## Rémunération fixe moyenne selon la taille d'entreprise



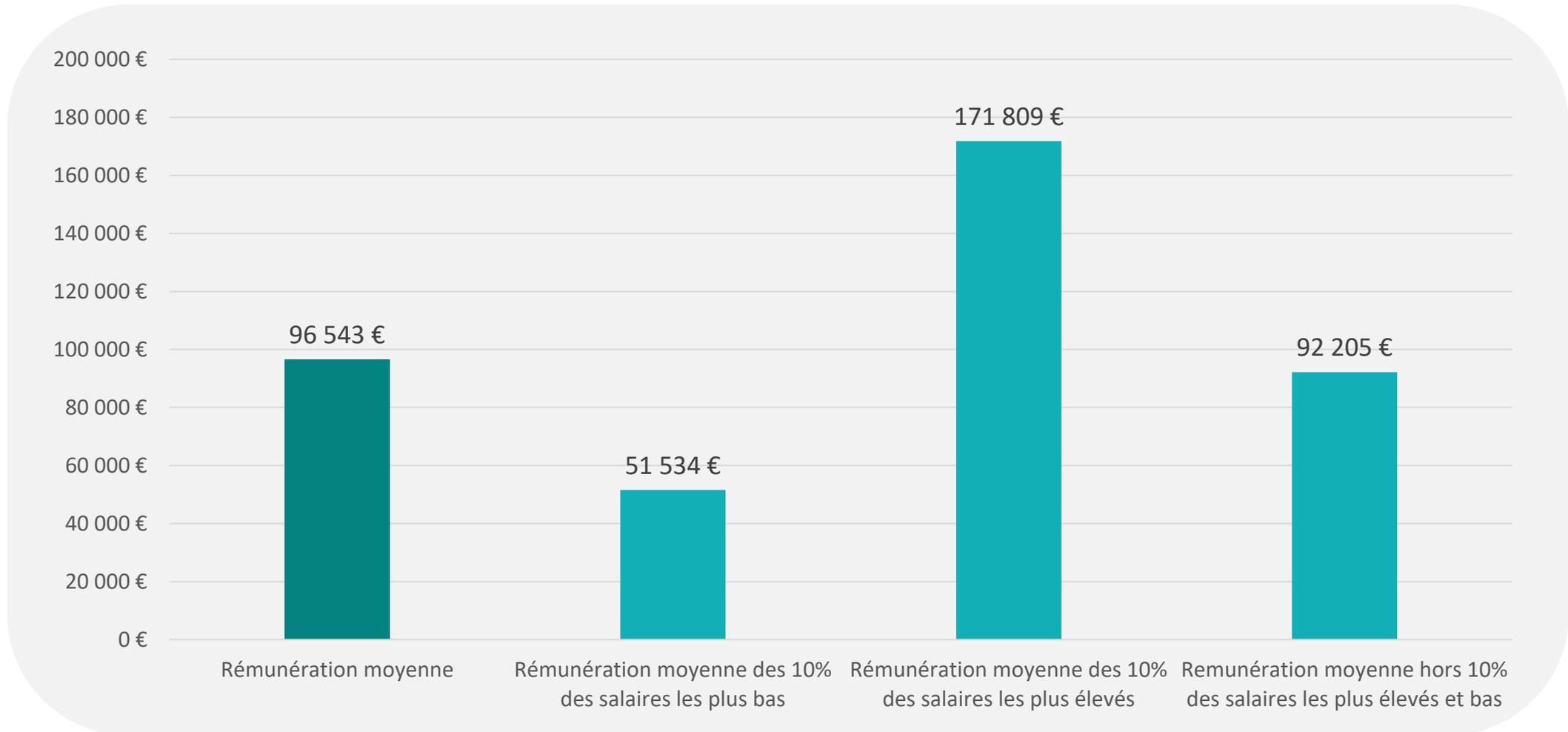
Les résultats ont été arrondies au millier



# Il est à noter l'écart très important mais logique de la rémunération moyenne des 10% des salaires les plus bas et des 10% des salaires les plus élevés

Q30 : Quelle a été votre **rémunération annuelle fixe en 2023** (en brut avant impôts) ?

Base : ensemble – hors valeurs aberrantes (377)

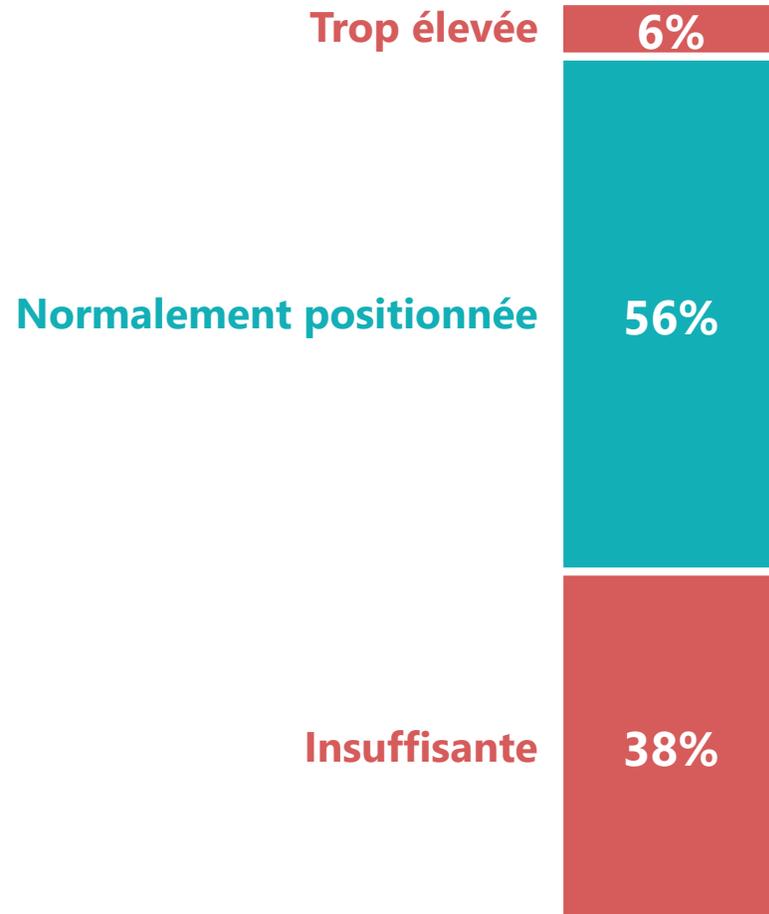




# Plus d'un tiers des responsables cyber estiment que la rémunération moyenne du métier cyber est insuffisante par rapport à d'autres fonctions dans l'entreprise

Q36 : Estimez-vous que la rémunération actuelle moyenne du métier cyber est, par rapport à d'autres fonctions de l'entreprise ?

Base : ensemble (390)



# “ Ce qui peut expliquer que plus d'un tiers d'entre eux n'est pas satisfait de leur niveau de rémunération...

Q35 : Estimez-vous que **votre rémunération actuelle est...** ?

Base : ensemble (390)

Rappel 2021 : 62%

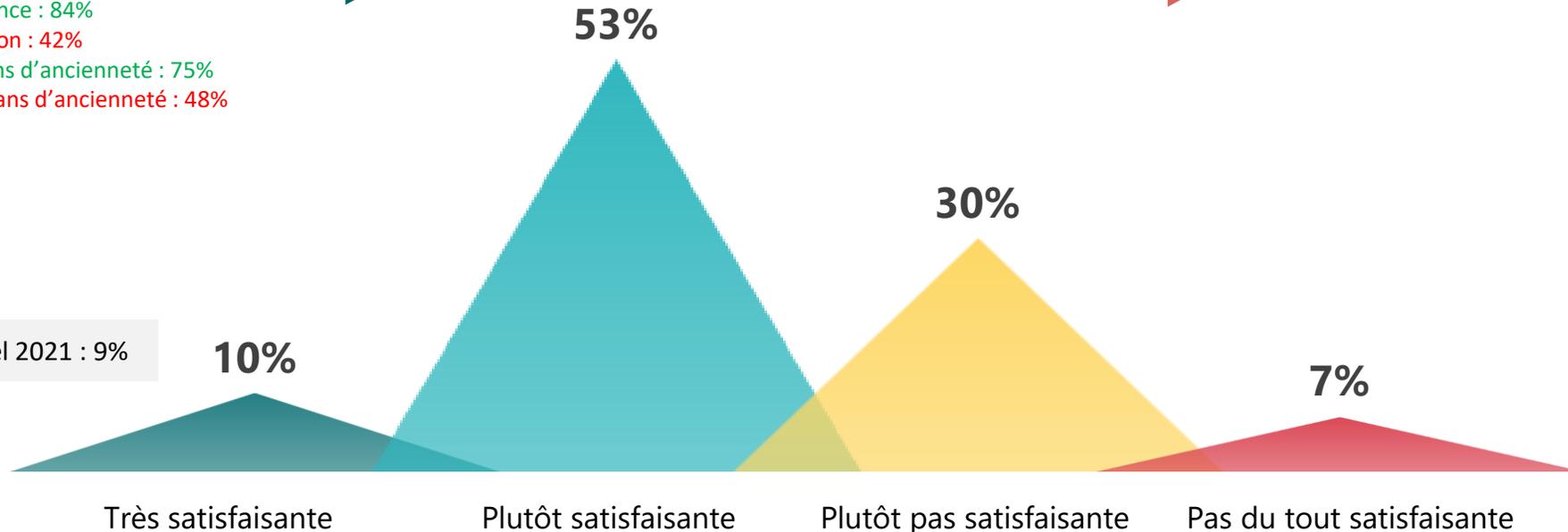
**63%** Estiment que leur rémunération actuelle est satisfaisante

Estiment que leur rémunération actuelle n'est pas satisfaisante **37%**

Directeur Cybersécurité ou équivalent : 80%  
Banque Finance : 84%  
Administration : 42%  
Plus de 20 ans d'ancienneté : 75%  
Entre 2 et 5 ans d'ancienneté : 48%



Rappel 2021 : 9%



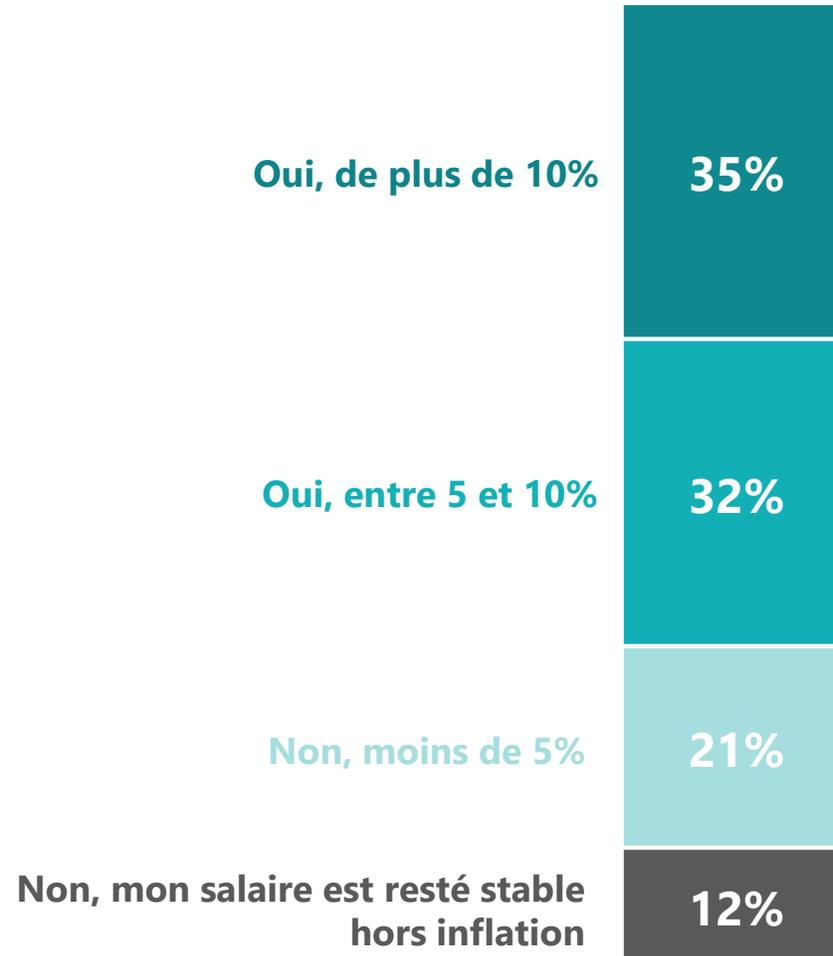
Directeur Cybersécurité ou équivalent : 22%  
Responsable de la Sécurité des Systèmes d'Information (RSSI) ou équivalent : 5%



# ...seulement un tiers des Responsables Cyber ont bénéficié d'une augmentation réellement significative (+ de 10%) au cours des trois dernières années en tenant compte de l'inflation

Q31 : Votre salaire a-t-il évolué significativement depuis trois ans ?

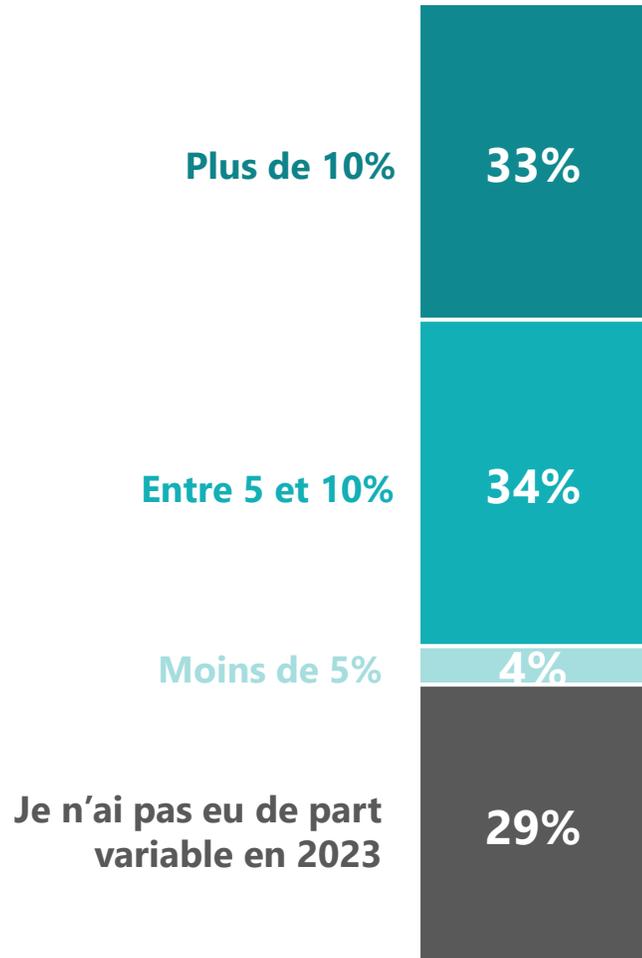
Base : ensemble (390)



# 7 responsables cyber sur 10 bénéficient d'une part variable, pour un tiers d'entre eux cette dernière dépasse les 10%

Q32 : Et quelle a été la part variable complémentaire de votre rémunération en 2023 ?

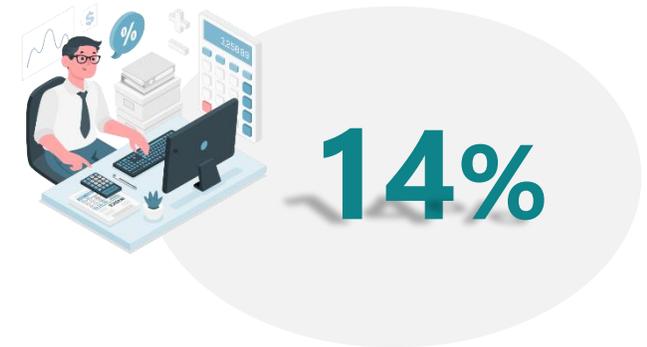
Base : ensemble (390)



**71%** A une part variable

Rappel 2021 : 75%

Directeur Cybersécurité ou équivalent : 89%  
Responsable de la Sécurité des Systèmes d'Information (RSSI) ou équivalent : 62%  
5 000 salariés et plus : 82%  
Moins de 1 000 salariés : 59%



Part variable complémentaire moyenne de leur rémunération en 2023

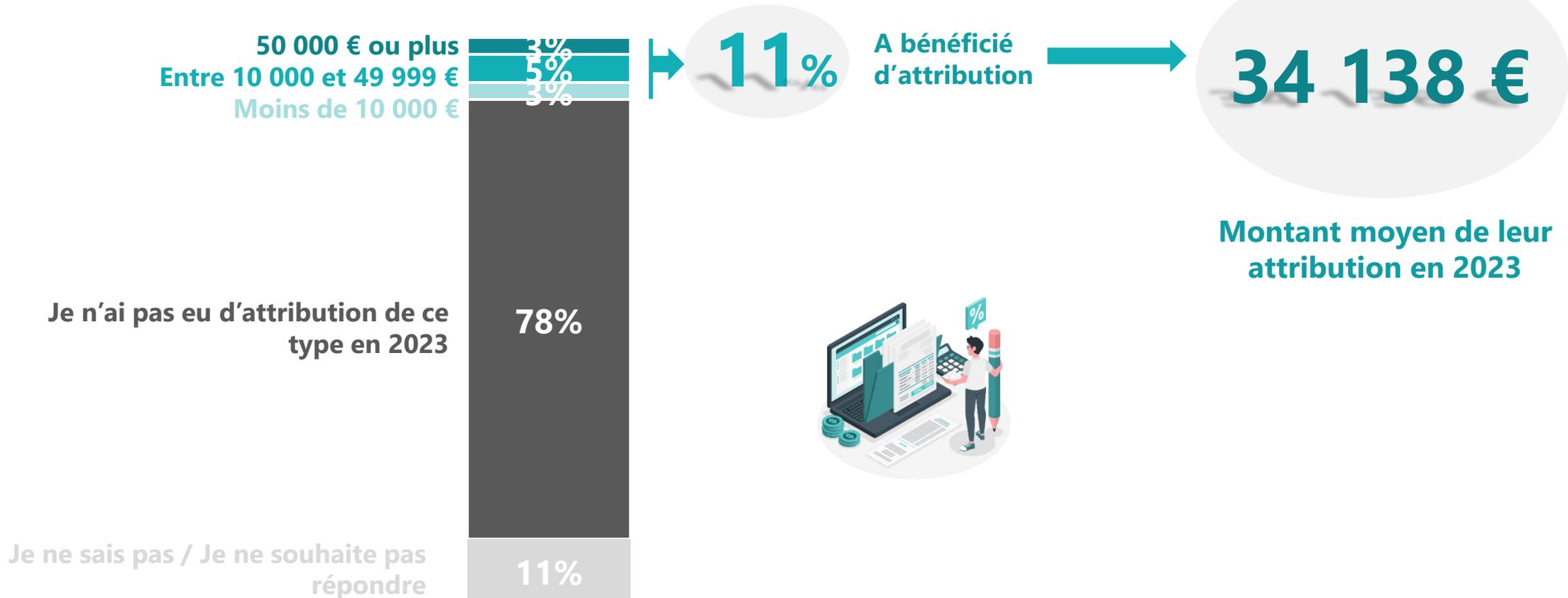
Directeur Cybersécurité ou équivalent : 18%  
Responsable de la Sécurité des Systèmes d'Information (RSSI) ou équivalent : 12%  
5 000 salariés et plus : 17%  
Entre 1 000 et 4 999 salariés : 11%



# Les plans d'attribution « d'incitation à long terme » sont encore peu développés, 1 responsable cyber sur 10 en a bénéficié en 2023

Q34 : En plus de votre rémunération fixe et variable, vous bénéficiez peut-être d'un plan d'attribution « d'incitation à long terme » (Long Term Incentive), sous la forme d'actions gratuites et/ou stock-options (soumise ou non à des conditions de performance de l'entreprise) qui vous seront distribuées sous condition de présence dans l'entreprise au bout d'un certain nombre d'années. **Si vous avez bénéficié de ce type de plan, quel a été le montant de votre attribution en 2023 ?**

Base : ensemble (390)

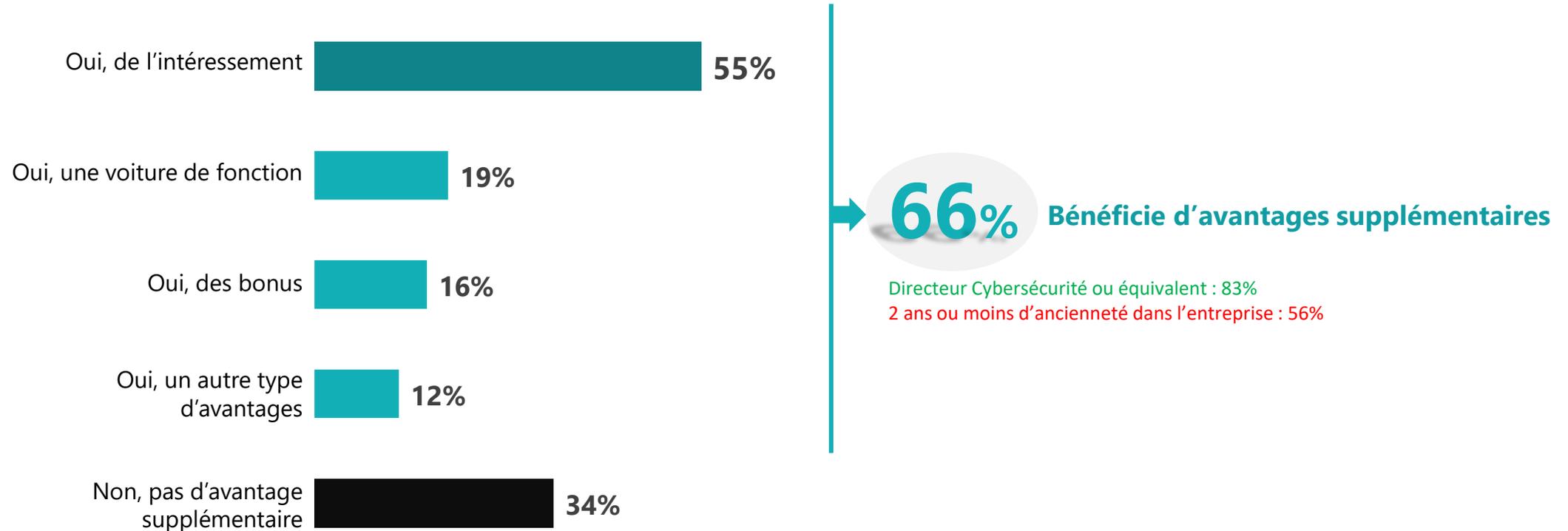




# En revanche, deux tiers ont perçu d'autres avantages notamment par le biais de l'intéressement

Q33 : Bénéficiez-vous d'avantages supplémentaires ?

Base : ensemble (390) – Plusieurs réponses possibles





## Détail par taille d'entreprise

### Q33 : Bénéficiez-vous d'avantages supplémentaires ?

Base : ensemble (390) – Plusieurs réponses possibles

|  | Moins de 1 000 salariés | Entre 1 000 et 4 999 salariés | 5 000 salariés et plus | Ensemble   |
|--|-------------------------|-------------------------------|------------------------|------------|
| <i>Base</i>                                  | 117                     | 101                           | 172                    | 390        |
| <b>Bénéficie d'avantages supplémentaires</b> | <b>54%</b>              | <b>60%</b>                    | <b>78%</b>             | <b>66%</b> |
| Oui, de l'intéressement                      | 44%                     | 55%                           | 62%                    | 55%        |
| Oui, une voiture de fonction                 | 9%                      | 3%                            | 35%                    | 19%        |
| Oui, des bonus                               | 12%                     | 11%                           | 22%                    | 16%        |
| Oui, un autre type d'avantages               | 10%                     | 11%                           | 13%                    | 12%        |
| Non, pas d'avantage supplémentaire           | 46%                     | 40%                           | 22%                    | 34%        |

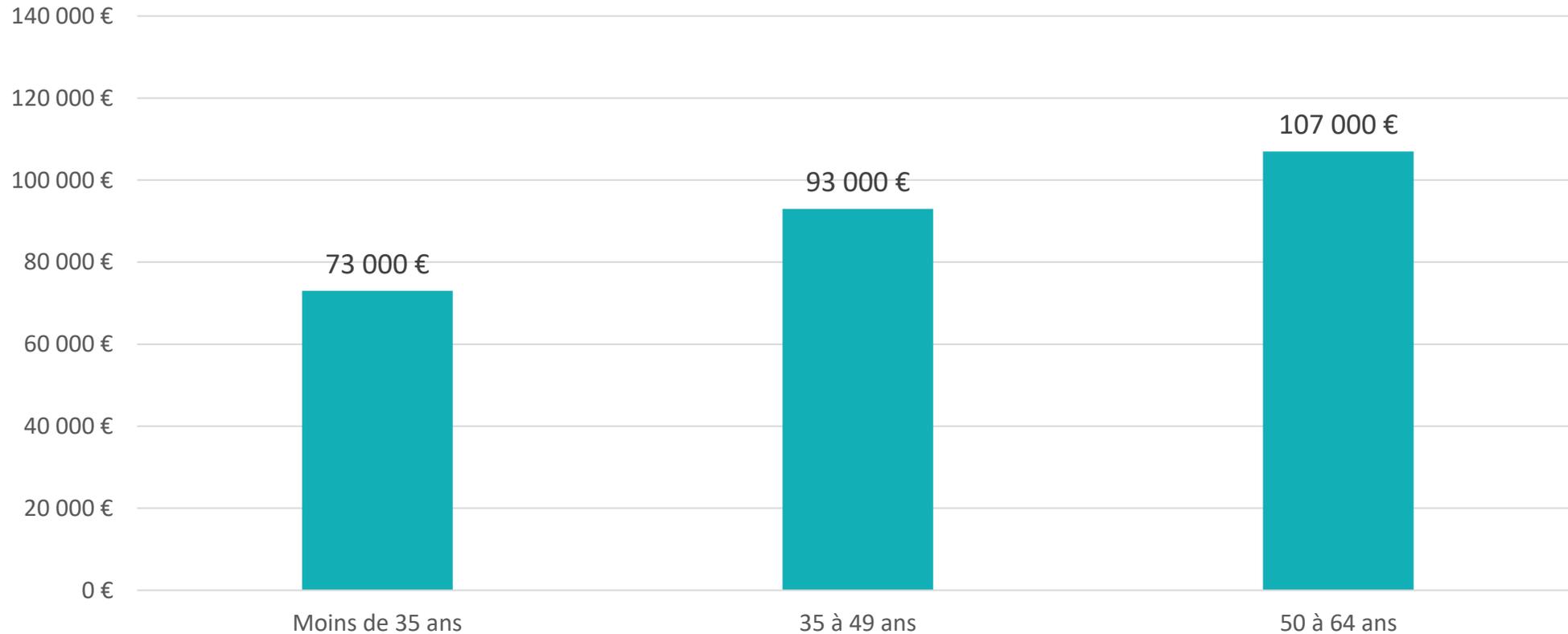


# Le niveau de rémunération fixe varie en fonction de certains critères comme l'âge...

Q30 : Quelle a été votre **rémunération annuelle fixe en 2023** (en brut avant impôts) ?

Base : ensemble – hors valeurs aberrantes (377)

## Rémunération fixe moyenne selon l'âge



Ecart de rémunération :

Rémunération la + élevée : 145 000 €  
Rémunération la - élevée : 38 000 €

Ecart de rémunération :

Rémunération la + élevée : 250 000 €  
Rémunération la - élevée : 32 000 €

Ecart de rémunération :

Rémunération la + élevée : 350 000 €  
Rémunération la - élevée : 36 000 €

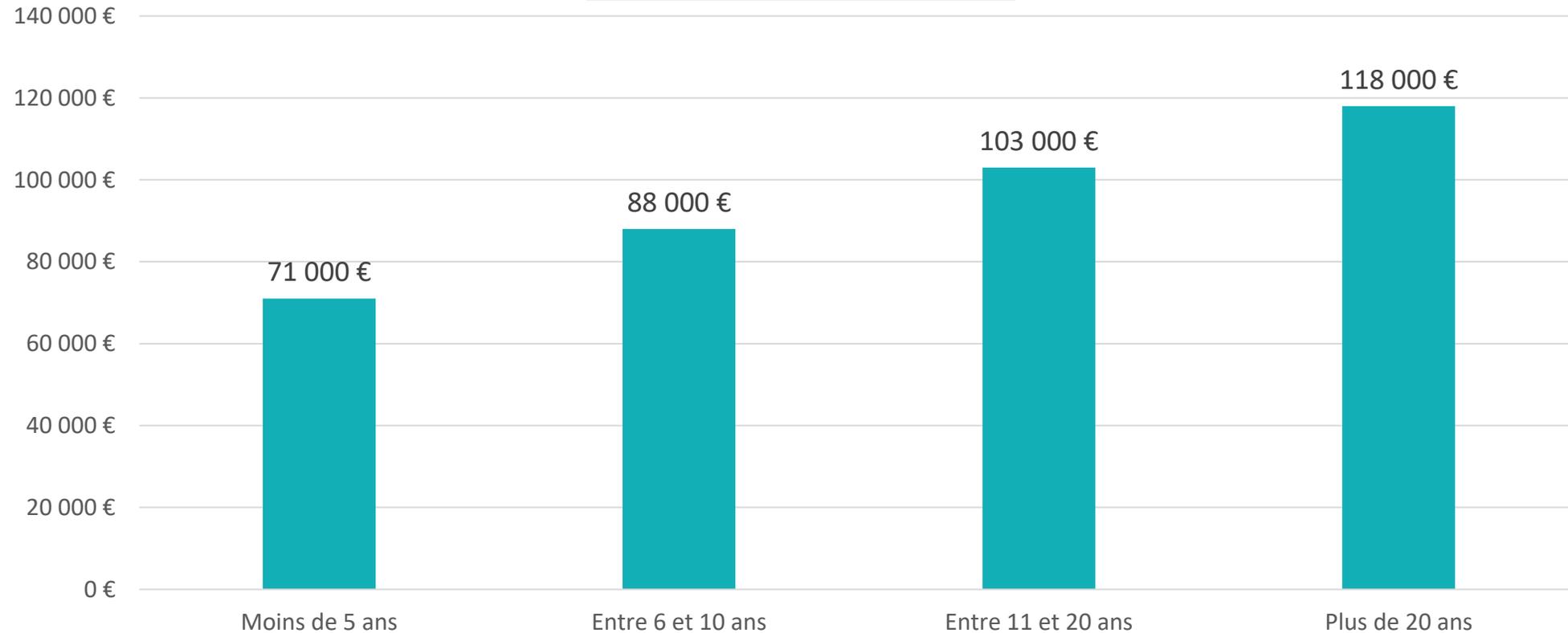


# ...ou l'ancienneté dans le métier

Q30 : Quelle a été votre **rémunération annuelle fixe en 2023** (en brut avant impôts) ?

Base : ensemble – hors valeurs aberrantes (377)

## Rémunération fixe moyenne selon l'ancienneté dans le métier



Ecart de rémunération :

Rémunération la + élevée : 140 000 €  
Rémunération la - élevée : 32 000 €

Ecart de rémunération :

Rémunération la + élevée : 200 000 €  
Rémunération la - élevée : 54 000 €

Ecart de rémunération :

Rémunération la + élevée : 350 000 €  
Rémunération la - élevée : 43 000 €

Ecart de rémunération :

Rémunération la + élevée : 250 000 €  
Rémunération la - élevée : 36 000 €

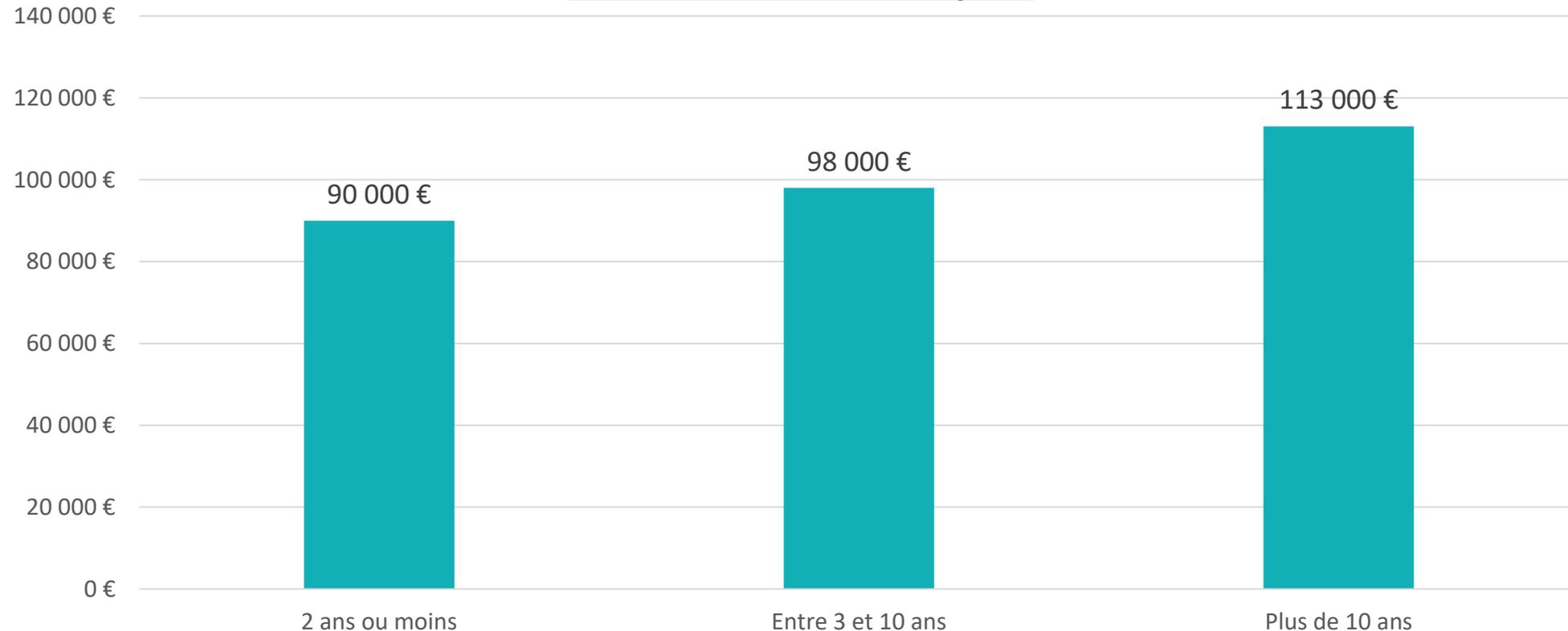


# La différence semble être moins visible en fonction de l'ancienneté dans l'entreprise

Q30 : Quelle a été votre **rémunération annuelle fixe en 2023** (en brut avant impôts) ?

Base : ensemble – hors valeurs aberrantes (377)

## Rémunération fixe moyenne selon l'ancienneté dans l'entreprise



Ecart de rémunération :

Rémunération la + élevée : 250 000 €  
Rémunération la - élevée : 35 000 €

Ecart de rémunération :

Rémunération la + élevée : 350 000 €  
Rémunération la - élevée : 40 000 €

Ecart de rémunération :

Rémunération la + élevée : 250 000 €  
Rémunération la - élevée : 32 000 €

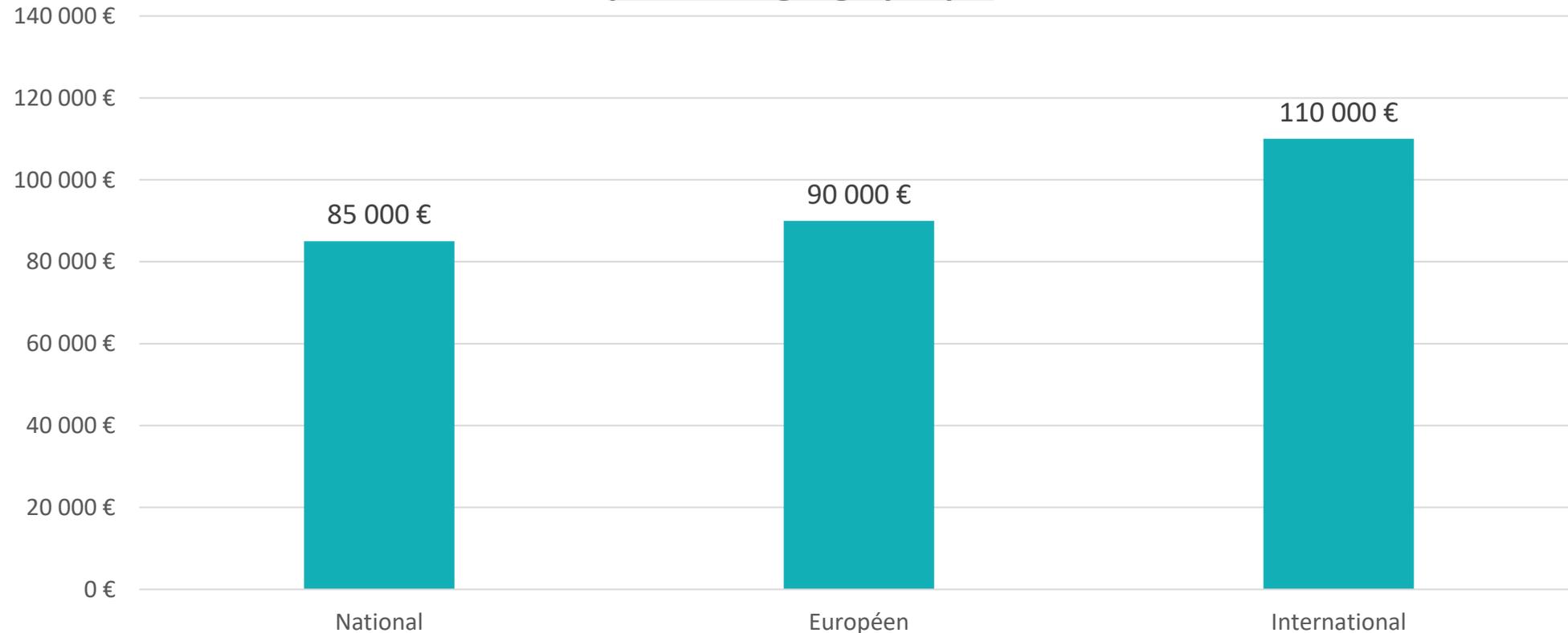


# Les entreprises internationales proposent une rémunération sensiblement plus élevée que les autres

Q30 : Quelle a été votre **rémunération annuelle fixe en 2023** (en brut avant impôts) ?

Base : ensemble – hors valeurs aberrantes (377)

## Rémunération fixe moyenne selon le périmètre géographique



Ecart de rémunération :

Rémunération la + élevée : 180 000 €  
Rémunération la - élevée : 38 000 €

Ecart de rémunération :

Rémunération la + élevée : 155 000 €  
Rémunération la - élevée : 32 000 €

Ecart de rémunération :

Rémunération la + élevée : 350 000 €  
Rémunération la - élevée : 36 000 €



C

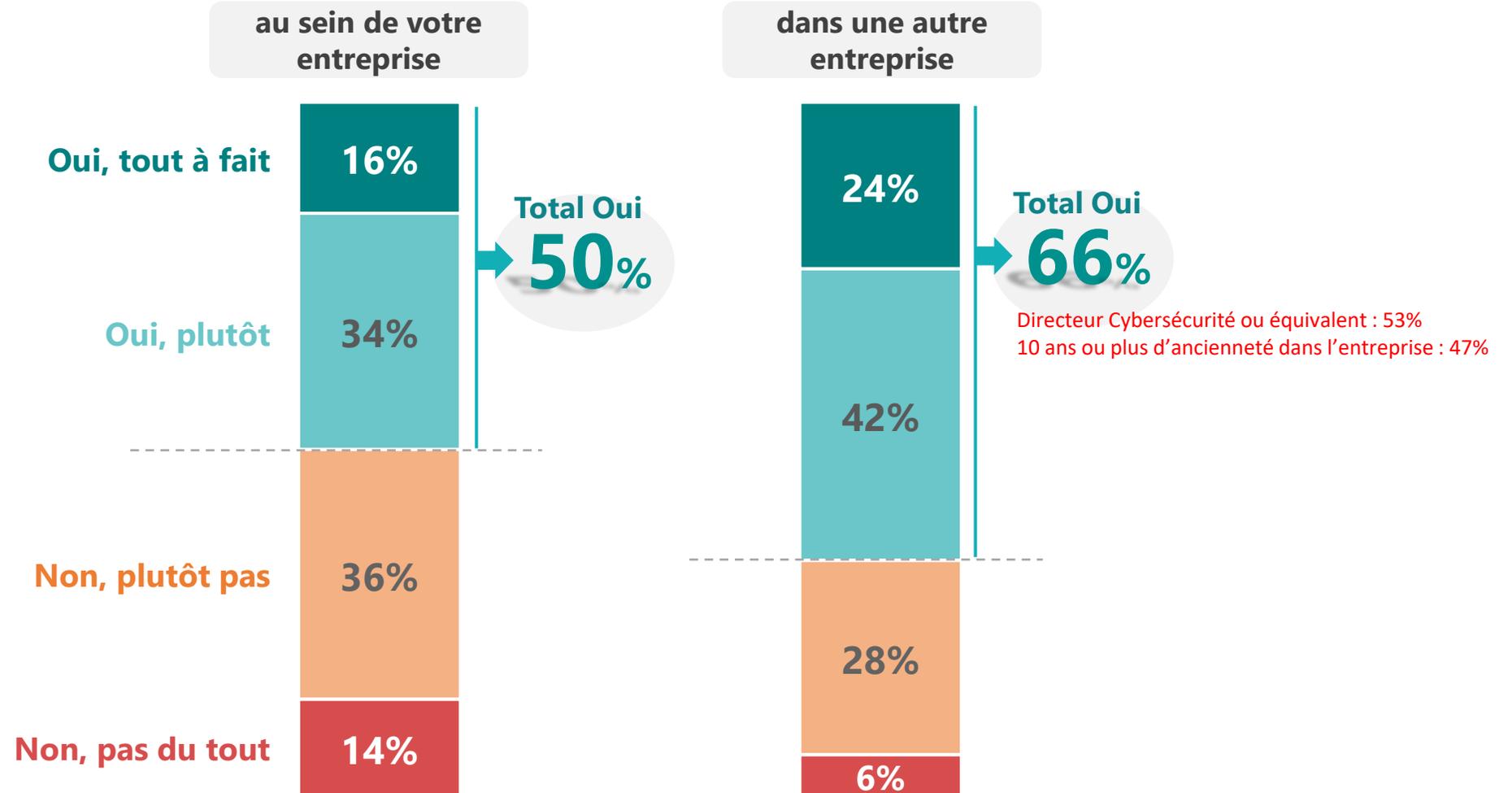
Une évolution dans les métiers  
cyber plus facile en dehors de  
l'entreprise



# Deux tiers des responsables cyber envisagent d'évoluer dans une autre entreprise, plutôt que dans leur propre structure

RS9 : Envisagez-vous d'évoluer...?

Base : ensemble (390)

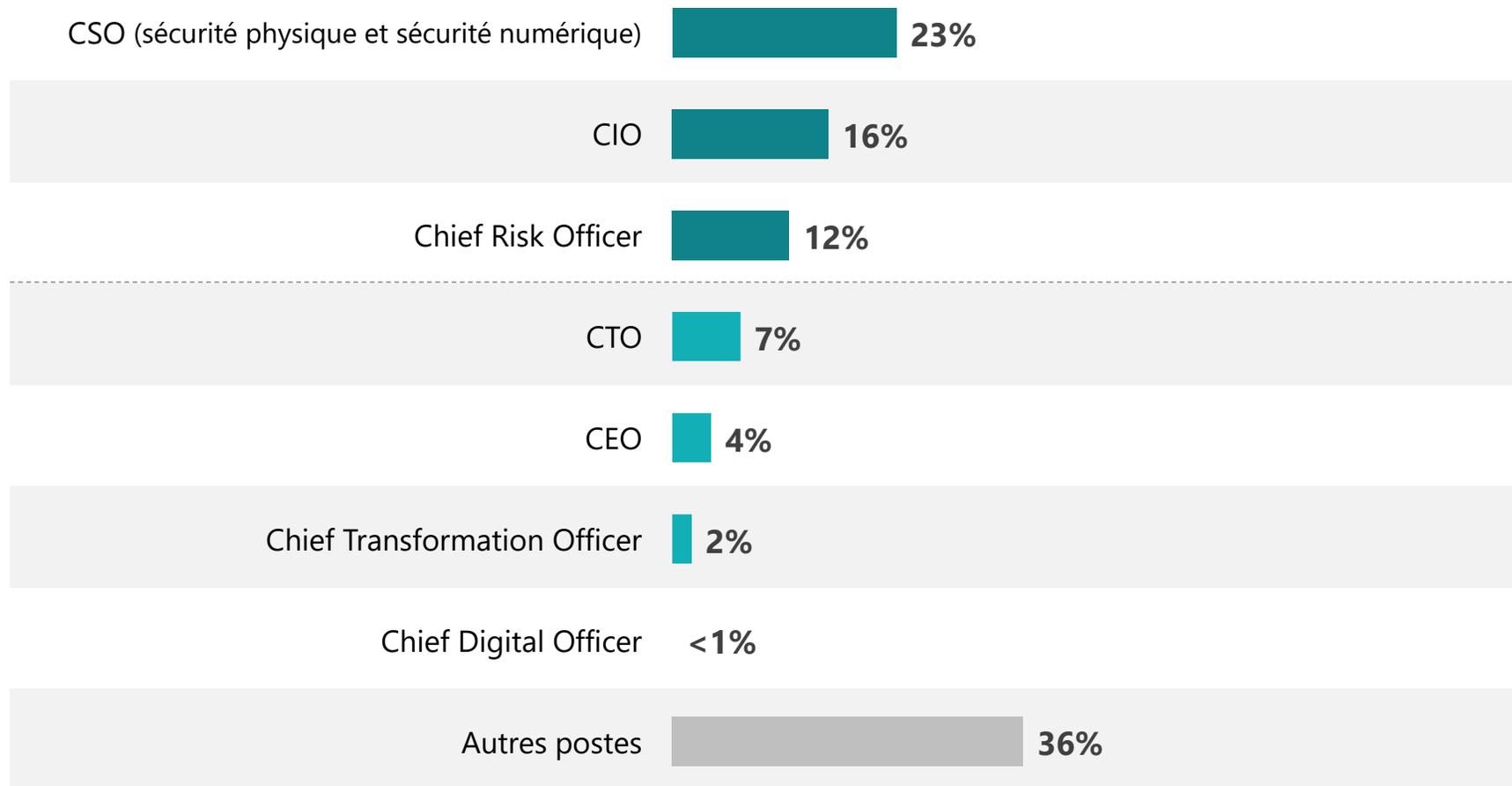




# Ceux qui envisagent d'évoluer dans leur structure espèrent occuper la position de leur N+1 actuel (CIO,CSO,CRO...)

RS10 : Et à quel poste envisagez-vous d'évoluer au sein de votre entreprise ?

Base : envisagent d'évoluer au sein de leur entreprise (192)

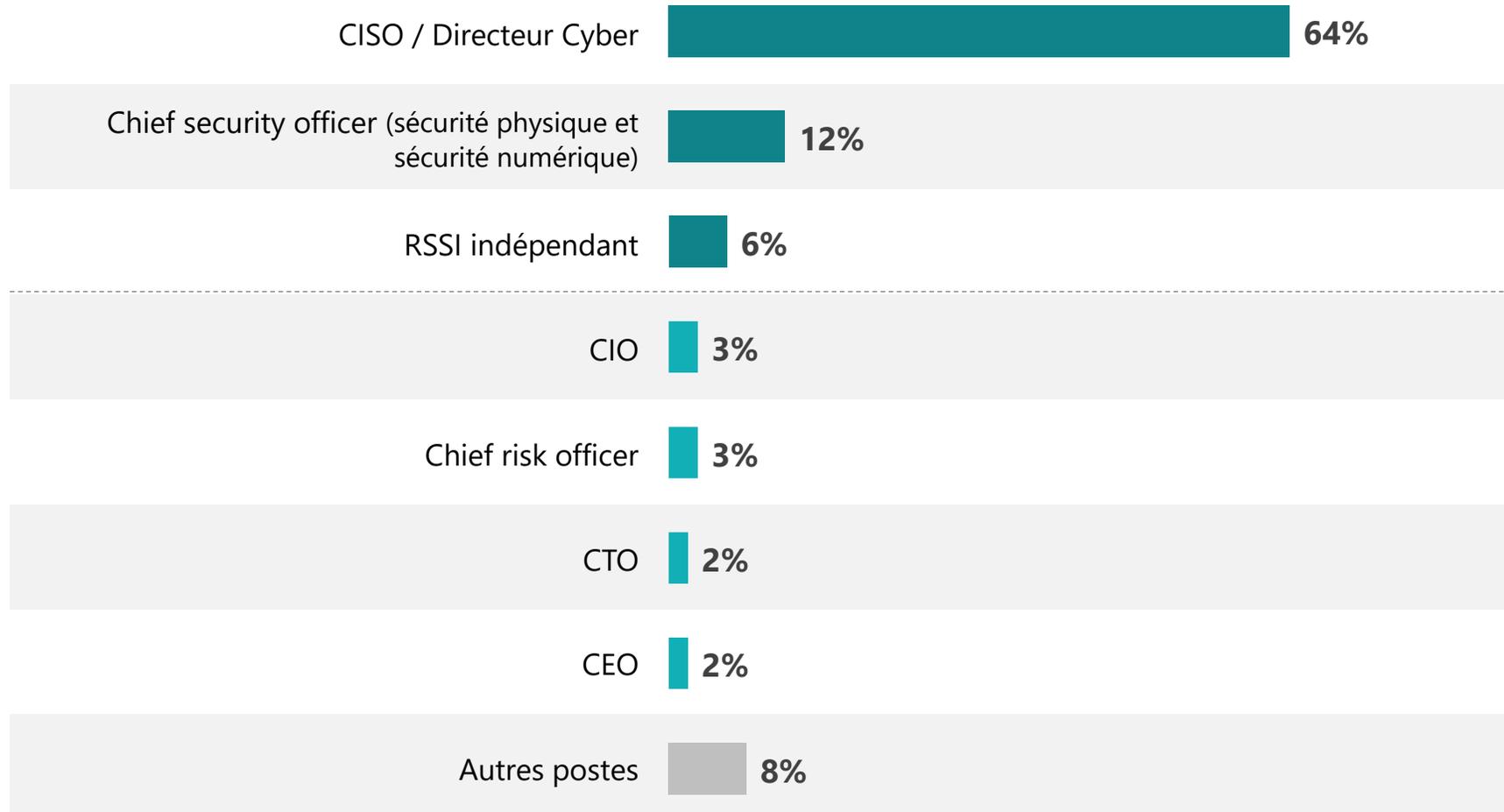




# Ceux qui envisagent d'évoluer dans une autre entreprise entendent conserver la même fonction

RS11 : Et à **quel poste envisagez-vous d'évoluer** au sein d'[une autre entreprise](#) ?

Base : envisagent d'évoluer au sein d'une autre entreprise (254)





# Près de 90% des entreprises ne sont pas préparées au départ de leur responsable cyber, trois quarts n'ont aucun plan de succession...

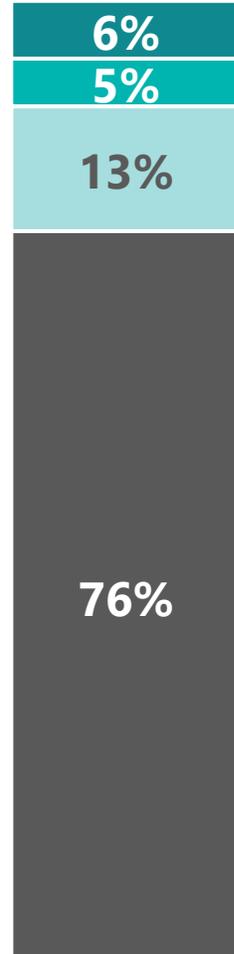
RS8 : Un **plan de succession** est-il prévu ?

Base : ensemble (390)

Nous avons un plan de succession avec un successeur en place  
Nous avons un plan de succession qui a identifié plusieurs candidats

Nous n'avons pas encore de plan de relève en place,  
mais nous sommes en train d'en élaborer un

Nous n'avons pas actuellement de  
plan de relève et n'en avons pas prévu



**11%** Un plan de succession est mis en place ou en cours d'élaboration

10 ans ou plus d'ancienneté dans l'entreprise : 28%  
Directeur Cybersécurité ou équivalent : 22%





## ...et cela quel que soit l'âge de leur responsable cyber

RS8 : Un **plan de succession** est-il prévu ?

Base : ensemble (390)

|  | Moins de 35 ans | 35 à 49 ans | 50 à 64 ans | Ensemble   |
|--|-----------------|-------------|-------------|------------|
| <i>Base</i>  | 40              | 202         | 146         | 390        |
| <b>Un plan de succession est mis en place ou en cours d'élaboration</b>                        | <b>7%</b>       | <b>10%</b>  | <b>13%</b>  | <b>11%</b> |
| Nous avons un plan de succession avec un successeur en place                                   | 7%              | 5%          | 5%          | 6%         |
| Nous avons un plan de succession qui a identifié plusieurs candidats                           | -               | 5%          | 8%          | 5%         |
| Nous n'avons pas encore de plan de relève en place, mais nous sommes en train d'en élaborer un | 15%             | 10%         | 16%         | 13%        |
| Nous n'avons pas actuellement de plan de relève et n'en avons pas prévu                        | 78%             | 80%         | 71%         | 76%        |



# La synthèse



## Quelle est la position des responsables cybersécurité dans les entreprises ?

Une population très majoritairement masculine, bien que la part des femmes soit en légère augmentation passant de 5% en 2021 à 8% cette année au sein de l'échantillon. **Les responsables cybersécurité sont une population mature et expérimentée**, 52% ont entre 35 et 49 ans et 37% entre 50 et 64 ans. Plus de la moitié (56%) ont plus de 10 ans d'expérience dans le métier de la cybersécurité.

**Les responsables cybersécurité ont un niveau d'études supérieures**, 90% d'entre eux ont un niveau de BAC+3 ou plus et les trois-quarts ont un Bac+5 ou plus. 58% ont suivi un cursus d'ingénieur avec, comme en 2021, une prédominance d'informaticiens : 81% ont fait leurs études dans ce domaine et 30% dans le domaine de la cybersécurité.

L'exercice de leur fonction peut cependant différer d'une entreprise à l'autre que ce soit **en termes de périmètre d'action, de responsabilité managériale ou de positionnement dans la hiérarchie**. 85% des responsables cyber assure des responsabilités managériales hiérarchiques ou fonctionnelles, et gèrent en moyenne entre 13 et 20 personnes, ce chiffre varie bien évidemment en fonction de la taille de l'entreprise.

La majorité d'entre eux (77%) sont directement rattachés au directeur de l'entité dans laquelle ils exercent, qui est principalement la DSI (54%) ou la Direction Générale (20%). **Ils sont pour la plupart à 2 ou 3 niveaux de la Direction Générale.**

## Comment les responsables cybersécurité travaillent-ils aujourd'hui ?

**Ils bénéficient aujourd'hui d'une grande autonomie ou de pouvoir d'influence en termes de budget ou dans le choix des solutions et services** de cybersécurité, pour cette dernière dimension 42% sont le décideur final.

**Une fonction dont l'exercice comprend plusieurs dimensions**, celle qui prend le plus de poids dans leur mission, est la dimension **Risques qui** (73%) puis la **dimension Opérationnelle** (64%). Il est cependant à noter que ce sont les activités de Conformité et de Résilience qui ont le plus progressé ces 5 dernières années.

# Synthèse

Parmi la multitude d'activités spécifiques aux métiers de la cybersécurité, celles dont les **Responsables cyber sont le plus souvent responsables et principaux réalisateurs** sont les missions en lien avec la politiques sécurité (56%), la sensibilisation et la formation (54%) et enfin dans l'analyse des risques cyber (51%).

Les activités qui sont les plus hors de leur champ d'action concernent la sécurité physique, la lutte contre la fraude, ou encore les opérations IT de sauvegarde dans le domaine de la cyber résilience.

## Quelle est la vision des responsables cybersécurité sur leur travail...

**Comme en 2021, les responsables cybersécurité se déclarent satisfaits de leur travail (84%)**, le ratio de « très satisfaits » s'améliore en tendance passant de 20% en 2021 à 25% aujourd'hui. Dans le détail, les éléments qui influencent le plus leur motivation et donc implicitement leur satisfaction, sont la transversalité de la fonction (76%) et la diversité des sujets à traiter (73%).

Les meilleurs alliés des Responsables cyber sont la production IT et les DPO, avec qui ils ont un niveau de collaboration particulièrement élevé. **Par ailleurs, les responsables cybersécurité se sentent suffisamment soutenus (83% dont 33% se disent « très soutenus ») par le top management.**

La moitié des responsables cybersécurité envisagent aujourd'hui d'évoluer au sein de leur entreprise et **66% l'envisagent au sein d'une autre structure, 24% en sont certains.** Dans le cadre d'une évolution interne, les postes les plus recherchés sont les postes de CSO et de CIO tandis qu'une évolution externe les inciterait plutôt à rester sur un poste de CISO/Directeur cyber.

**Ces intentions d'évolution au sein d'une autre organisation représentent un enjeu important pour les entreprises qui doivent s'efforcer de penser à leur futur**, en effet 11% seulement des structures ont aujourd'hui mis en place un plan de succession ou compte le mettre en place très prochainement.

## ...et sur leur rémunération ?

**Le salaire annuel fixe moyen (en brut avant impôts) en 2023 pour les responsables cybersécurité s'élève à 96 543 €**, à titre de comparaison il était de 88 342 € en 2020. Une rémunération moyenne légèrement en hausse. Il est à noter qu'un tiers du panel interrogé dispose d'une rémunération supérieure à 105 000 €

Près de 4 responsables cybersécurité sur 10 estiment que **leur niveau de rémunération est insuffisant par rapport à d'autres fonctions de l'entreprise**. Au final, 63% se disent satisfaits de leur rémunération (62% en 2021), une satisfaction moyenne bien que deux tiers (67%) aient bénéficié d'une augmentation.

Il est à noter qu'en plus de la rémunération fixe, **71% des responsables cybersécurité ont touché une part variable en 2023**, pour un tiers (33%) elle correspond à plus de 10% de leur rémunération. Deux tiers (66%) bénéficient enfin d'autres avantages supplémentaires comme de l'intéressement pour 55% d'entre eux, une voiture de fonction (19%) ou encore d'autres bonus (16%).

**Au final, le niveau de rémunération peut fortement varier en fonction de l'âge, de l'expérience, de la taille d'entreprise ou du secteur d'activité.**



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

# 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.

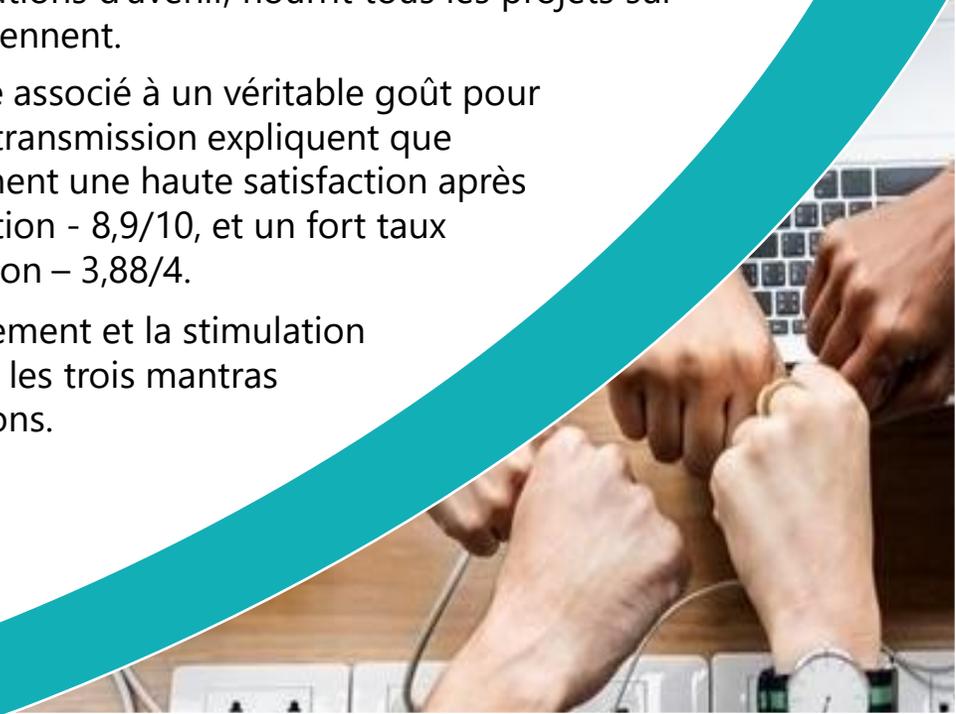
Aujourd'hui OpinionWay poursuit sa dynamique de croissance en s'implantant géographiquement sur des zones à fort potentiel que sont l'Europe de l'Est et l'Afrique.

**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](http://www.opinion-way.com)



### Envie d'aller plus loin ?

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

[newsletter !](#)

# “*opinion*way”

15 place de la République  
75003 Paris

PARIS  
CASABLANCA  
ALGER  
VARSOVIE  
ABIDJAN

vo  
tre  
con  
tact

**Stéphane Lefebvre-Mazurel**

Directeur du pôle B2B, SmartCity & Inside

Tel. +33 1 81 81 83 48 / +33 6 76 92 66 43  
[slefebvre@opinion-way.com](mailto:slefebvre@opinion-way.com)