Rapport automatique d’analyse des résultats

Généré automatiquement depuis la plateforme Selvitys.

Titre de l’étude :

cybersécurité 2024 V3

L’administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Informations générales

Titre de l’étude :

cybersécurité 2024 V3

Nom de l’auteur :

Raphael JASMIN

Adresse URL du sondage :

survey URL

Date de début de la diffusion :

25 septembre 2024

Date de fin de la diffusion :

19 octobre 2024

Durée moyenne du questionnaire :

36 minutes, 49 secondes

L’administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Méthodologie et échantillonnage

Nombre total de participants :

758

Nombre total de réponses complètes :

387

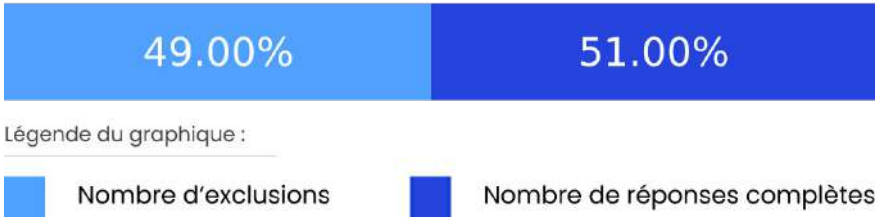
Nombre d’exclusions :

371

Taux de complétion du questionnaire :

51.06

Répartition des répondants interrogés :



Méthodologie de l’enquête :

La collecte des réponses a été effectuée à l'aide d'un sondage en ligne mené sur la plateforme de Selvitys, du undefined au 19 octobre 2024, auprès d'un échantillon de 758 participants. Parmi ces 758 participants, seuls undefined ont été conservés, répondant aux critères de ciblage et ayant réussi le contrôle qualité.

L’administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Liste des questions

1. Avant de commencer, vous répondez à ce questionnaire :
2. Dans le cadre de votre travail, à quelle fréquence travaillez-vous sur un ordinateur ?
3. Comment évaluez-vous votre niveau d'expertise en sécurité informatique /cybersécurité ?
4. Comment évaluez-vous votre degré de curiosité intellectuelle lors de la recherche d'une problématique spécifique sur Google ?
5. Dans quelle mesure faites-vous preuve de créativité dans les domaines suivants de la cybersécurité ?
6. Vous retrouvez-vous dans ces différents comportements ?
7. Avez-vous réussi à établir aisément votre propre politique de sécurité domestique (plan d'actions défini pour maintenir un certain niveau de sécurité) en vous basant sur votre compréhension de la politique de sensibilisation de votre entreprise ?
8. Quelle est votre opinion sur les idées couramment répandues que nous allons énumérer ci-dessous ?
9. Pensez-vous que les attitudes suivantes constituent des freins à l'implémentation d'une politique efficace de sécurité informatique et de cybersécurité ?
10. Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS D'ESCROQUERIES ?
11. Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS DE CYBERATTAQUES ?
12. Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS DE PHISHING (vol de comptes, mots de passe, données bancaires...) ?
13. Chez vous, comment pourriez-vous développer au quotidien des mesures de prévention en matière de sécurité/cybersécurité ?
14. Pour le BYOD (Bring Your Own Device), quelles sont les questions essentielles à poser pour assurer une mise en œuvre efficace et sécurisée ?
15. En tant que particulier, êtes-vous sensible aux recommandations des sites internet de sécurité comme l'ANSSI (séparation des usages pro-perso) ?
16. Selon vous, se former à la sécurité informatique pour développer ses compétences, c'est :
17. En entreprise, comment percevez-vous les idées couramment admises énumérées ci-dessous ?
18. En entreprise, pensez-vous que les attitudes suivantes constituent des freins à l'implémentation d'une politique efficace de sécurité informatique et de cybersécurité :
19. En entreprise, quelles peuvent être les conséquences d'une cyberattaque ?
20. Quelles seraient les meilleures stratégies pour développer quotidiennement la prévention en matière de sécurité et de cybersécurité au sein d'une entreprise ?

L’administration du questionnaire a été effectuée entre le et 19 octobre 2024.

Liste des questions

21. Vous sentez-vous concerné(e) par les recommandations de sécurité formulées par votre entreprise ?
22. Selon vous, se former à la sécurité/cybersécurité pour développer ses compétences en entreprise, c'est :
23. Selon vous, quelles stratégies pourraient être mises en œuvre pour stimuler l'intelligence collective en matière de cybersécurité au sein d'une équipe, qu'elle soit dédiée à la sécurité, constituée de salariés ou d'un service spécifique ?
24. Toujours pour stimuler l'intelligence collective, quelles autres stratégies pourraient être mises en œuvre ?
25. Comment évaluez-vous l'importance des propositions ci-dessous ?
26. Reprenons les mêmes propositions. Comment évaluez-vous leur facilité technique ?
27. Encore une fois sur les mêmes propositions, comment évaluez-vous votre niveau de maîtrise ?
28. Si vous lisez correctement cette question, veuillez sélectionner la proposition 2 :
29. Avez-vous actuellement un rôle de manager ou occupez-vous un poste d'encadrement dans votre entreprise ?
30. Dans votre entreprise, à quel service ou département appartenez-vous ?
31. Quelles sont les actions à privilégier pour renforcer la culture de la cybersécurité au sein de votre entreprise ?
32. Dans le cadre de sa politique de sensibilisation, diriez-vous que votre entreprise met en place une culture de la cybersécurité ?
33. Est-ce important pour vous d'être immédiatement informé par SMS en cas d'attaque informatique visant votre entreprise, incluant des instructions à suivre ?
34. En cas d'attaque informatique, de fraude, de vol, de phishing et autres incidents similaires, diriez-vous que :
35. En fonction de vos expériences personnelles et/ou professionnelles passées, quel serait votre niveau de stress ?
36. Selon vous, est-il nécessaire que le service informatique ou la DSI mette en place des simulations de cyberattaques pour sensibiliser efficacement les employés, évaluer les mesures de sécurité et tester leurs réflexes numériques ?
37. Considérez-vous comme nécessaire de signaler à votre service informatique ou à votre DSI en cas de piratage d'un ordinateur, d'une tablette ou d'un smartphone dans votre environnement familial ?
38. Disposez-vous des outils adéquats tels qu'un cahier de notes, des fichiers informatiques, des services en ligne, etc., pour organiser et planifier efficacement votre politique de sécurité (y compris une liste de plans d'action basés sur un processus) dans votre environnement domestique ?
39. Pour qu'une approche de sensibilisation à la sécurité informatique /cybersécurité soit pertinente et efficace, quelle serait la bonne répartition à adopter entre :
40. Dans votre entreprise, quels sont les freins à la sensibilisation à la sécurité informatique /cybersécurité ?

Liste des questions

41. Si vous deviez signaler un incident de sécurité ou une activité suspecte :
42. Dans votre entreprise, l'information pertinente concernant la sensibilisation à la sécurité informatique /cybersécurité est-elle diffusée ?
43. Dans quelle mesure vous sentez-vous engagé(e) envers votre politique de sécurité entreprise ?
44. La politique de sécurité de votre entreprise/organisation est-elle efficace pour prévenir les incidents de cybersécurité ?
45. Pour améliorer la sécurité et la conformité des données dans votre entreprise dans le cadre du RGPD (Règlement Général sur la Protection des Données), quelles sont les actions les plus importantes ?
46. Dans votre travail quotidien, quel pourcentage de votre temps consacrez-vous à l'application du RGPD ?
47. Avez-vous participé à une formation à la cybersécurité au cours de l'année écoulée ?
48. Si vous deviez suivre une formation à la cybersécurité dans les 6 prochains mois, que préféreriez-vous ?
49. Quelle serait pour vous la durée idéale d'une formation à la cybersécurité ?
50. Pour vous former à la cybersécurité, êtes-vous favorable à :
51. Diriez-vous que votre environnement de travail favorise le développement de l'innovation ouverte ?
52. Vous arrive-t-il de prendre l'initiative de partager des connaissances, des conseils sur la cybersécurité et d'encourager des pratiques sécuritaires dans votre entreprise ?
53. Avec l'évolution des cyberattaques, il est important d'établir des points de contact au sein des entreprises pour sensibiliser à la sécurité informatique /cybersécurité. Seriez-vous prêt(e) à participer à cette initiative en tant qu'ambassadeur de la sécurité ?
54. Comment évaluez-vous l'efficacité de vos managers et de la direction en tant qu'ambassadeurs de la cybersécurité dans votre entreprise ?
55. Quelles sont les stratégies à privilégier pour stimuler l'intelligence collective en matière de cybersécurité ?
56. Les neurosciences cognitives sont le domaine de recherche dans lequel sont étudiés les mécanismes neurobiologiques qui sous-tendent la cognition (perception, motricité, langage, mémoire, raisonnement, émotions). Qu'en savez-vous ?
57. Comment évaluez-vous l'efficacité des stratégies suivantes basées sur les neurosciences cognitives en matière de cybersécurité ?
58. Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant l'impact des neurosciences sur les programmes de formation en cybersécurité ?
59. Dans quelle mesure êtes-vous satisfait du contenu des formations cybersécurité proposé par les RH/DSI ?
60. Dans votre quotidien, estimez-vous que vous mettez en œuvre efficacement les bonnes postures de cybersécurité

pour vous protéger (contre les virus, le piratage, l
arnaques en ligne, etc.) ?

Liste des questions

61. Comment évaluez-vous l'efficacité de vos managers en tant qu'ambassadeurs de la cybersécurité dans votre service ?
62. Si vous travaillez dans le domaine de la cybersécurité, vous considérez-vous comme un expert légitime dans ce domaine ?
63. Quel est votre niveau d'anglais ?
64. Quel est le plus haut niveau de diplôme que vous avez obtenu ?
65. Quelle est votre tranche d'âge ?
66. Etes-vous ?
67. Dans quelle région travaillez vous ?
68. Quelle est votre ancienneté dans votre entreprise ?
69. Avez-vous des solutions ou suggestions pour booster la culture de la cybersécurité de votre entreprise ? C'est le moment de donner votre avis :
70. Qu'avez-vous pensé du fonctionnement de ce questionnaire ?

Résultats

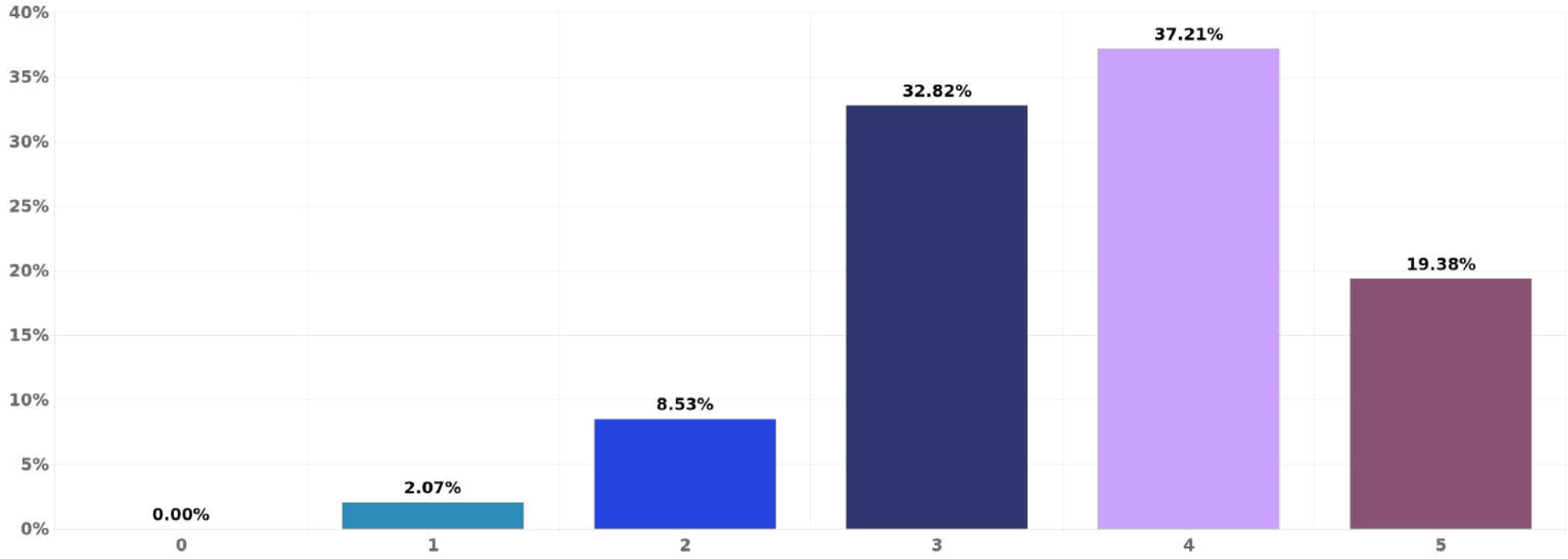
1.Avant de commencer, vous répondez à ce questionnaire :

Proposition des réponses	Effectif	Pourcentage
En tant que salarié en entreprise (privé/public)	387	100.00%
En tant qu'artisan, commerçant, profession libérale, indépendant	0	0.00%
En tant que chef d'entreprise de 10 salariés ou plus	0	0.00%
Dans le cadre de vos études (école, université)	0	0.00%
En tant que retraité	0	0.00%
En tant que demandeur d'emploi	0	0.00%
Autre	0	0.00%
Total	387	100.00%

Type de question : Choix unique Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

3.Comment évaluez-vous votre niveau d'expertise en sécurité informatique /cybersécurité ?



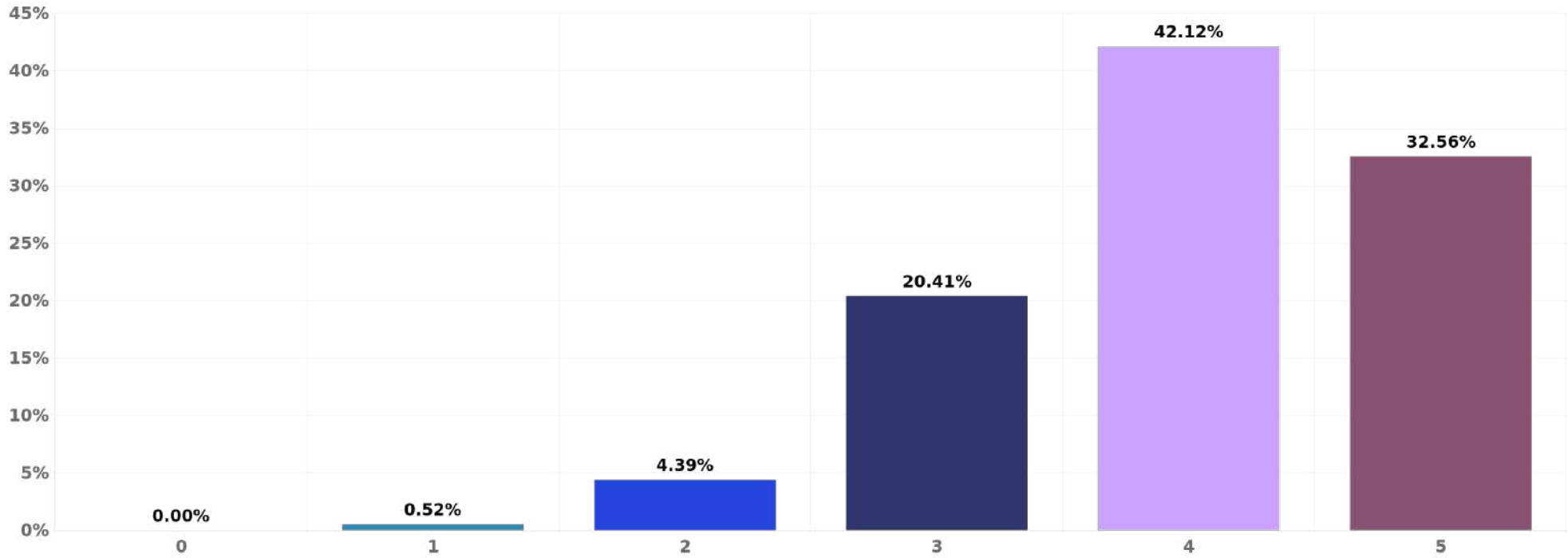
Type de question : Échelle

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

4.Comment évaluez-vous votre degré de curiosité intellectuelle lors de la recherche d'une problématique spécifique sur Google ?



Type de question : Échelle

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

5.Dans quelle mesure faites-vous preuve de créativité dans les domaines suivants de la cybersécurité ?

Question 5	1 - Pas du tout créatif	2 - Plutôt pas créatif	3 - Neutre	4 - Plutôt créatif	5 - Très créatif
dans la création de nouvelles idées cyber	11.63%	12.14%	28.94%	35.14%	12.14%
dans la résolution de problème informatique cyber	6.98%	13.70%	26.10%	41.60%	11.63%

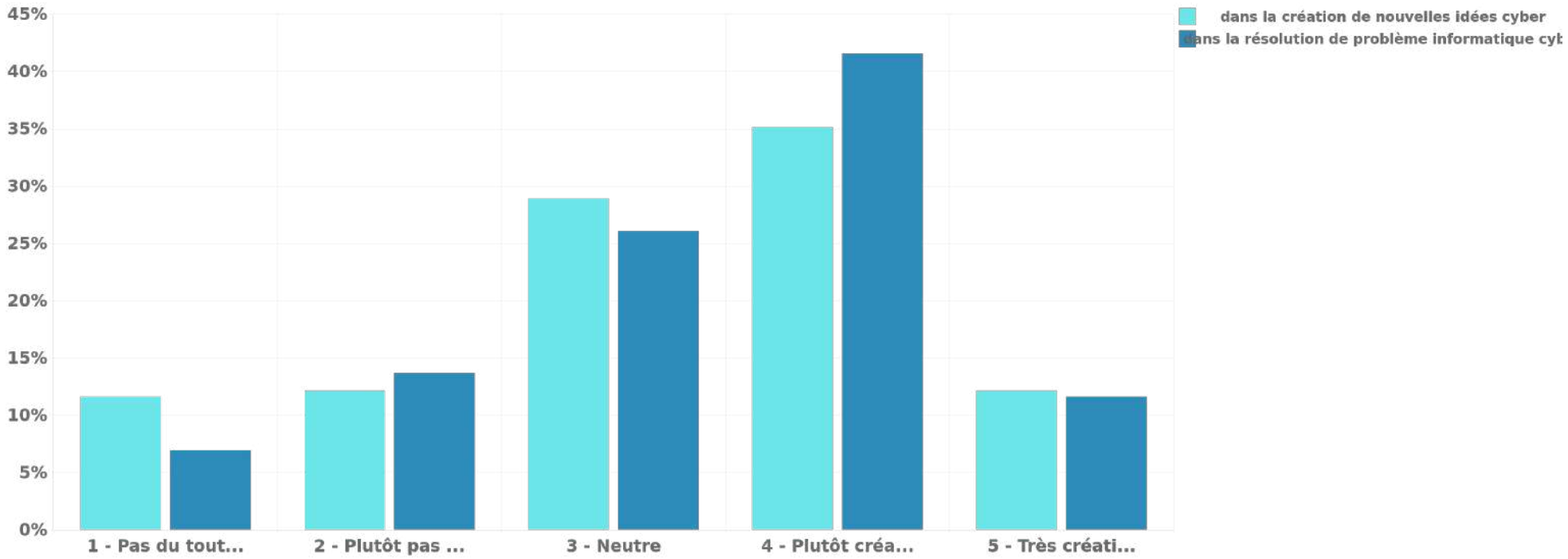
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

5.Dans quelle mesure faites-vous preuve de créativité dans les domaines suivants de la cybersécurité ?



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

6.Vous retrouvez-vous dans ces différents comportements ?

Question 6	1 - Tout à fait moi	2 - Moi	3 - Indifférent	4 - Peu moi	5 - Pas du tout moi
Formaliser sa politique de sécurité informatique	23.26%	33.59%	19.12%	14.73%	9.30%
Lister le matériel de son parc informatique	21.19%	32.82%	18.86%	13.95%	13.18%
Calculer son budget informatique à l'année	19.12%	31.78%	15.76%	13.95%	19.38%
Sensibiliser les utilisateurs du parc informatique	22.74%	38.76%	18.35%	12.14%	8.01%
Mettre à jour ses connaissances liées à la sécurité	27.91%	43.41%	12.14%	11.63%	4.91%
Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...)	43.41%	32.56%	11.63%	10.08%	2.33%
Mettre à jour les logiciels, navigateurs, plugins, Java, etc.	41.34%	32.30%	11.11%	12.14%	3.10%
Changer régulièrement de mots de passe	30.49%	36.95%	11.63%	14.47%	6.46%
Faire des sauvegardes ordinateurs/ smartphones régulières	36.69%	35.14%	9.30%	13.95%	4.91%
Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes	16.54%	33.59%	13.18%	17.31%	19.38%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

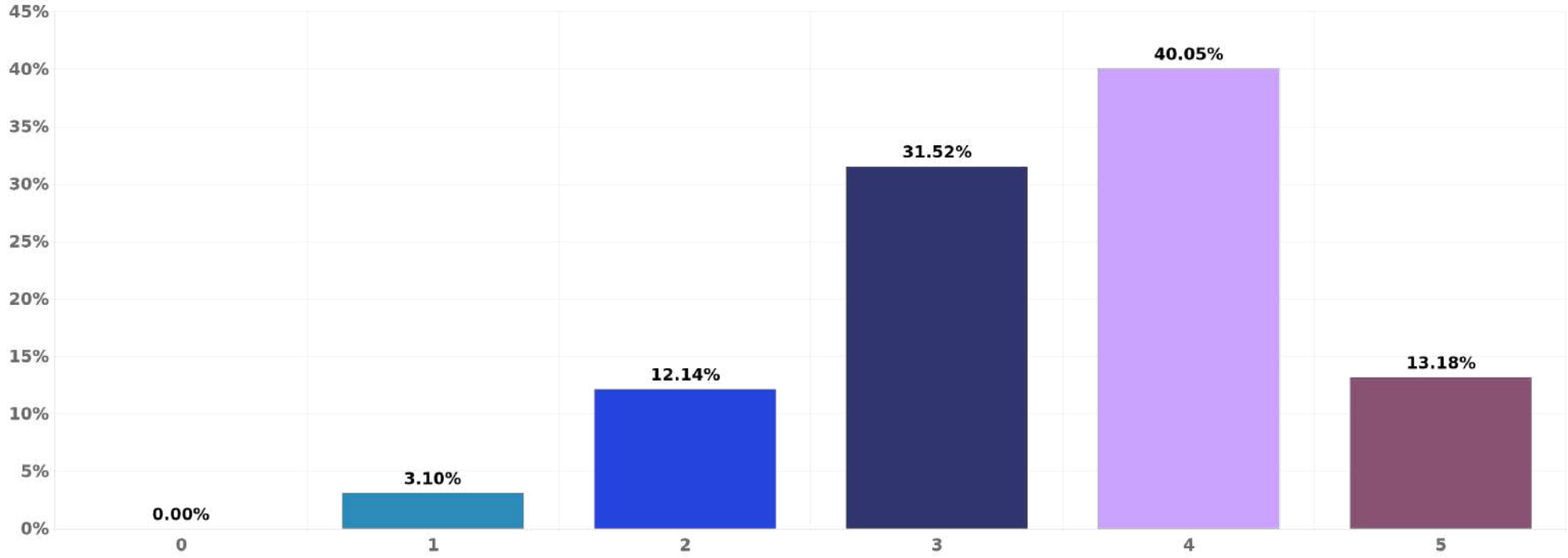
6.Vous retrouvez-vous dans ces différents comportements ?

Question 6	1 - Tout à fait moi	2 - Moi	3 - Indifférent	4 - Peu moi	5 - Pas du tout moi
Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique	18.86%	27.91%	18.09%	17.31%	17.83%
Respecter les règles relatives aux réseaux sociaux	40.57%	42.12%	8.79%	6.46%	2.07%
Respecter les règles de mot de passe WIFI	45.22%	39.79%	8.53%	4.13%	2.33%
Respecter les règles de paiement en ligne	48.84%	39.28%	6.46%	2.84%	2.58%
Respecter les chartes Internet utilisateurs	35.66%	39.79%	15.25%	6.72%	2.58%
Faire attention en ouvrant les e-mails (phishing, virus)	55.30%	32.30%	5.94%	4.39%	2.07%
Utiliser un firewall et/ou un VPN	29.46%	33.07%	17.31%	11.37%	8.79%
Protéger vos données en déplacement (nomadisme)	30.75%	36.43%	13.95%	13.44%	5.43%
Protéger son identité numérique en ligne	35.92%	39.28%	11.63%	11.37%	1.81%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

7.Avez-vous réussi à établir aisément votre propre politique de sécurité domestique (plan d'actions défini pour maintenir un certain niveau de sécurité) en vous basant sur votre compréhension de la politique de sensibilisation de votre entreprise ?



Type de question : Échelle

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

8.Quelle est votre opinion sur les idées couramment répandues que nous allons énumérer ci-dessous ?

Question 8	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord	6 - Ne sait pas
Naviguer uniquement sur des sites réputés écarte tout risque de sécurité.	9.82%	26.10%	19.12%	23.51%	20.41%	1.03%
La navigation en 'https' assure une protection complète en ligne.	9.30%	34.11%	23.77%	18.35%	11.63%	2.84%
Il n'y a aucun danger tant que je m'abstiens de télécharger des fichiers.	5.17%	16.80%	15.76%	28.17%	32.82%	1.29%
Sans l'installation de nouvelles applications, mon appareil est hors de danger.	7.24%	18.09%	16.54%	23.51%	33.33%	1.29%
Les attaques DDoS (attaques par déni de service distribué) visent uniquement à interrompre les services, sans intentions malicieuses supplémentaires.	6.46%	19.38%	20.16%	17.83%	25.32%	10.85%
Les virus informatiques affectent exclusivement les systèmes d'exploitation Windows.	7.75%	17.57%	12.14%	20.93%	39.28%	2.33%
Le risque de sécurité survient uniquement lors de l'installation d'applications sur mon ordinateur.	5.68%	19.38%	12.40%	23.26%	37.73%	1.55%
Les données personnelles ne constituent pas une catégorie de données sensibles.	6.72%	17.05%	10.85%	12.92%	50.65%	1.81%
L'adoption de protocoles Zero Trust offre une sécurité infaillible.	5.94%	19.38%	31.52%	18.35%	11.63%	13.18%
Seuls les acteurs étatiques sont à l'origine des attaques de type APT (Advanced Persistent Threat).	7.24%	13.95%	21.45%	16.80%	27.13%	13.44%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

9.Pensez-vous que les attitudes suivantes constituent des freins à l'implémentation d'une politique efficace de sécurité informatique et de cybersécurité ?

Question 9	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Considérer la sécurité informatique, la cybersécurité comme non essentielle	21.19%	21.71%	14.21%	21.71%	21.19%
Percevoir les budgets informatiques comme un obstacle à la sécurité informatique	16.80%	31.52%	26.36%	17.83%	7.49%
Croire que les attaques ne concernent que les autres	21.96%	22.74%	13.70%	19.64%	21.96%
Manquer de temps pour se consacrer à la sécurité informatique /cybersécurité	16.28%	39.79%	23.26%	14.73%	5.94%
Trouver la sécurité informatique trop complexe et technique	18.60%	38.76%	18.60%	15.76%	8.27%
Ressentir une difficulté à mettre en pratique les recommandations de sécurité	14.73%	39.02%	21.19%	18.09%	6.98%
Prévoir de déléguer la sécurité informatique à un proche plutôt d'agir immédiatement	13.95%	28.94%	25.84%	22.22%	9.04%
Faire confiance en la protection totale offerte par un antivirus	15.50%	32.82%	19.12%	25.06%	7.49%
Voir dans l'interopérabilité des systèmes sécurisés une source d'inefficacité opérationnelle	10.85%	28.94%	40.31%	14.21%	5.68%
L'évolution constante des menaces rend obsolètes les solutions mises en place en un temps record	15.76%	44.19%	25.58%	12.14%	2.33%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

10.Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS D'ESCROQUERIES ?

Question 10	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Traçage des transactions financières suspectes.	41.34%	39.79%	14.47%	3.36%	1.03%
Identification des contacts suspects.	36.69%	45.48%	14.99%	2.07%	0.78%
Localisation des détails complets des cartes bancaires utilisées.	30.49%	44.70%	16.28%	6.72%	1.81%
Utilisation de l'adresse IP pour identifier les fraudeurs.	35.40%	42.89%	15.50%	4.13%	2.07%

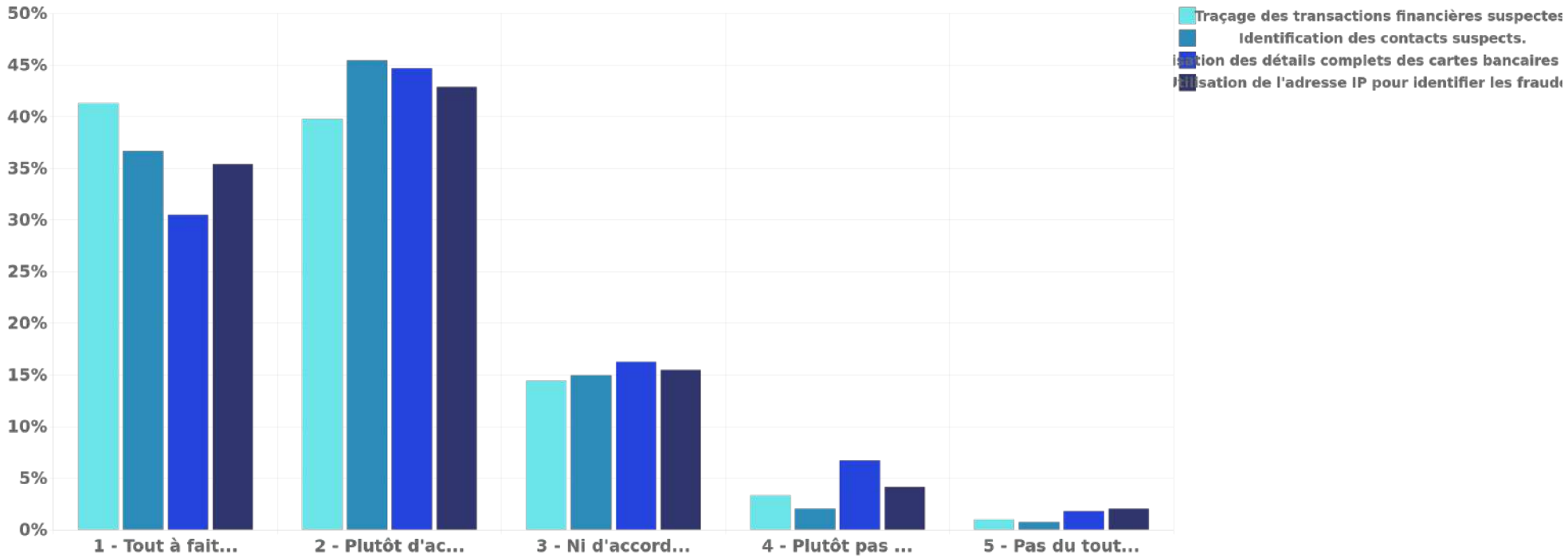
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

10.Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS D'ESCROQUERIES ?



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

11.Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS DE CYBERATTAQUES ?

Question 11	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Tentative de localisation des cybercriminels.	21.45%	35.66%	23.51%	12.92%	6.46%
Déconnexion immédiate d'internet en cas de menace.	44.96%	29.20%	16.02%	5.68%	4.13%
Nettoyage du système avec des outils antivirus / antimalware.	45.48%	32.56%	17.83%	3.36%	0.78%
Consultation d'un spécialiste si le système est compromis.	41.34%	39.28%	16.02%	2.84%	0.52%
Se faire justice soi-même.	6.46%	8.53%	15.50%	27.91%	41.60%
Paiement d'une rançon pour récupérer des données.	6.72%	11.37%	14.47%	19.64%	47.80%
Changement systématique des mots de passe après une attaque.	63.05%	23.26%	9.56%	2.84%	1.29%
Ne prévenir que la police dans un premier temps.	15.25%	24.81%	30.75%	19.12%	10.08%
Déposer une plainte officielle auprès des autorités compétentes.	53.75%	31.52%	11.63%	1.81%	1.29%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

12.Quels sont les bons renseignements à fournir et les bonnes actions à faire en premier lieu LORS DE PHISHING (vol de comptes, mots de passe, données bancaires...) ?

Question 12	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Méfiance face aux messages, appels ou SMS non sollicités.	64.86%	20.41%	10.34%	3.36%	1.03%
Non-divulgation d'informations sensibles.	60.21%	26.61%	9.82%	2.84%	0.52%
Vérification de la fiabilité des sites web visités.	52.20%	34.11%	10.59%	2.58%	0.52%
Prudence avec les e-mails d'expéditeurs inconnus.	67.96%	19.64%	8.79%	3.10%	0.52%
Faire confiance aux pièces jointes de vos proches et des sites marchands.	12.66%	15.50%	16.80%	27.91%	27.13%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

13.Chez vous, comment pourriez-vous développer au quotidien des mesures de prévention en matière de sécurité/cybersécurité ?

Question 13	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Anticiper les menaces en fonction de son utilisation d'internet.	39.28%	43.41%	14.73%	1.81%	0.78%
Se former seul(e) ou en entreprise sur les meilleures pratiques de sécurité.	28.17%	39.79%	20.67%	7.24%	4.13%
Lister les risques informatiques au niveau du foyer.	37.73%	41.86%	14.99%	4.13%	1.29%
Mettre en place des mesures de protection robustes pour les ordinateurs, les smartphones et les tablettes.	42.12%	43.41%	12.14%	1.29%	1.03%
Identifier des mesures préventives, comme le VPN et les sauvegardes.	40.05%	41.86%	14.21%	2.33%	1.55%
Élaborer une stratégie de sécurité adaptée au budget.	33.07%	43.15%	18.35%	3.88%	1.55%
Mettre en place des solutions préventives, avec ou sans assistance.	35.92%	43.41%	15.76%	3.36%	1.55%
Procéder à des évaluations régulières de votre politique de sécurité pour en vérifier l'efficacité sur le long terme.	33.59%	44.70%	18.09%	2.58%	1.03%
Utiliser des solutions de chiffrage avancé pour les données sensibles stockées sur les appareils domestiques.	34.88%	40.83%	17.57%	5.43%	1.29%
Utiliser des solutions avancées de protection de l'endpoint, allant au-delà des antivirus traditionnels.	34.11%	38.76%	22.22%	3.62%	1.29%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

14.Pour le BYOD (Bring Your Own Device), quelles sont les questions essentielles à poser pour assurer une mise en œuvre efficace et sécurisée ?

Question 14	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Vérification des bonnes pratiques et fourniture de guides de sécurité au format PDF.	34.63%	43.67%	16.80%	3.88%	1.03%
Recommandation de logiciels de sécurité spécifiques et établissement d'une charte informatique.	35.40%	43.15%	16.80%	3.36%	1.29%
Contrôle de l'accès et de la protection des données de l'entreprise sur les appareils personnels.	38.50%	40.31%	16.54%	3.36%	1.29%
Implémentation d'une application de gestion du parc mobile (MDM - Mobile Device Management).	26.87%	41.86%	25.58%	4.39%	1.29%
Anticipation des procédures en cas de panne ou de perte de dispositif spécifique.	35.40%	42.89%	16.80%	4.13%	0.78%
Conseils pour éduquer les enfants à une utilisation sécurisée d'Internet	49.61%	31.27%	14.99%	3.36%	0.78%

Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

15.En tant que particulier, êtes-vous sensible aux recommandations des sites internet de sécurité comme l'ANSSI (séparation des usages pro-perso) ?

Question 15	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Séparer clairement les mots de passe professionnels des mots de passe personnels.	51.68%	30.49%	13.18%	3.62%	1.03%
Réunir messagerie professionnelle et personnelle.	16.28%	18.35%	14.99%	17.83%	32.56%
Naviguer sur internet de manière responsable au travail.	51.42%	31.78%	11.89%	3.36%	1.55%
Se servir des réseaux Wi-Fi publics occasionnellement pour le travail.	16.54%	24.29%	18.09%	17.57%	23.51%
Éviter les solutions de chiffrement trop complexes.	16.80%	29.20%	26.61%	14.73%	12.66%
Gérer prudemment sa présence sur les réseaux sociaux.	48.58%	35.14%	13.44%	2.07%	0.78%

Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

16.Selon vous, se former à la sécurité informatique pour développer ses compétences, c'est :

Question 16	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Suivre les bonnes pratiques lors des déplacements.	47.03%	38.50%	11.37%	2.58%	0.52%
Connaître de façon approfondie les menaces, risques et types d'attaques.	37.47%	43.93%	13.18%	4.39%	1.03%
Connaître les différentes solutions à mettre en œuvre.	43.67%	41.34%	11.11%	3.62%	0.26%
Établir une politique de sécurité robuste.	44.19%	40.05%	12.66%	2.33%	0.78%
Prendre des mesures pour sécuriser son poste de travail.	49.35%	35.66%	11.11%	3.36%	0.52%
Gérer les méthodes d'authentification.	44.44%	40.31%	12.14%	2.33%	0.78%
Maitriser les bonnes pratiques pour les achats en ligne.	46.77%	35.92%	13.95%	2.58%	0.78%
Réagir appropriément en cas d'alerte de sécurité.	49.10%	37.21%	9.56%	3.36%	0.78%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

17.En entreprise, comment percevez-vous les idées couramment admises énumérées ci-dessous ?

Question 17	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord	6 - Ne sait pas
Les pertes de données proviennent principalement du matériel informatique.	11.11%	21.19%	27.39%	22.48%	15.25%	2.58%
A ce jour, les techniques de phishing sont considérées comme obsolètes.	5.43%	17.05%	20.41%	24.03%	28.17%	4.91%
L'espionnage via le cyberespace connaît une croissance significative.	31.27%	40.57%	15.50%	4.65%	1.29%	6.72%
Les attaques de type 'man-in-the-middle' sont restreintes aux réseaux locaux uniquement.	6.20%	17.05%	25.06%	18.86%	18.09%	14.73%
Payer la rançon demandée lors d'un ransomware garantit la restitution des données.	4.13%	14.21%	10.85%	12.14%	54.52%	4.13%
La prise en charge du paiement de la rançon par les cyberassureurs dispense de se préparer à une attaque de ransomware.	5.94%	13.70%	13.95%	10.85%	46.51%	9.04%
Les backups sont la protection la plus fiable face aux logiciels de rançon.	12.40%	34.11%	24.55%	9.82%	6.98%	12.14%
L'augmentation du télétravail entraîne une hausse des cyberattaques.	18.86%	37.21%	18.86%	8.53%	5.68%	10.85%
Les solutions EDR sont supérieures et peuvent remplacer tous les autres antivirus existants.	8.27%	20.41%	29.20%	10.85%	6.72%	24.55%
Les protocoles BGP sont pleinement sécurisés et immunisés contre les risques de détournement et d'interception.	6.98%	19.64%	29.20%	14.99%	5.17%	24.03%

18.En entreprise, pensez-vous que les attitudes suivantes constituent des freins à l'implémentation d'une politique efficace de sécurité informatique et de cybersécurité :

Question 18	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Lors des conséquences d'un sous-investissement face aux risques.	26.36%	46.47%	20.38%	5.16%	1.63%
Lors des dangers de sous estimer les cyberattaques.	31.35%	44.05%	19.19%	3.51%	1.89%
Lorsqu'on rencontre des obstacles à l'adoption des mesures de sécurité recommandées parmi les salariés.	24.26%	43.94%	25.07%	5.93%	0.81%
Lorsqu'une diversité de solutions de sécurité peut mener à une cohérence opérationnelle fragmentée.	17.84%	45.68%	29.19%	5.95%	1.35%
Lors de l'identification et la hiérarchisation des ressources.	15.99%	41.73%	30.62%	9.49%	2.17%
Lors de l'évaluation des risques d'incidents de sécurité.	19.46%	42.70%	26.76%	7.84%	3.24%
Lors de la compréhension du paysage de risque de l'entreprise.	18.06%	41.24%	29.92%	7.55%	3.23%
Lors de la mise en œuvre du télétravail sécurisé.	20.81%	38.92%	26.22%	9.73%	4.32%
Lorsque la stratégie de sécurité n'est pas alignée avec les objectifs métier de l'entreprise.	28.38%	45.41%	21.08%	4.32%	0.81%
Lorsqu'il y a des préoccupations sur la souveraineté des données et la dépendance envers les fournisseurs étrangers.	20.70%	43.28%	28.23%	5.91%	1.88%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

19.En entreprise, quelles peuvent être les conséquences d'une cyberattaque ?

Question 19	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Risques liés à la perte de données sensibles.	55.56%	29.20%	12.14%	2.58%	0.52%
Interruption prolongée des services.	52.20%	28.94%	15.25%	2.58%	1.03%
Menaces liées aux ransomwares et autres formes de chantage.	46.77%	29.46%	17.83%	5.43%	0.52%
Réduction des délais de livraison promis aux clients.	30.75%	31.27%	19.90%	10.85%	7.24%
Dommages à la réputation de l'entreprise et création d'une image négative dans les médias.	43.41%	34.63%	15.76%	4.91%	1.29%
Exposition à des sanctions pécuniaires imposées par les autorités régulatrices ou judiciaires.	26.61%	37.21%	26.61%	6.72%	2.84%
Indisponibilité du site internet de l’entreprise pour ses clients.	50.39%	27.91%	15.50%	4.13%	2.07%
Risques d'une paralysie totale des systèmes d'information.	53.49%	29.72%	13.18%	3.36%	0.26%
Des coûts accrus liés à la remédiation et à l'investigation.	43.15%	34.88%	17.05%	3.62%	1.29%
L’obligation de notifier l’incident.	41.34%	35.66%	16.80%	5.17%	1.03%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

20.Quelles seraient les meilleures stratégies pour développer quotidiennement la prévention en matière de sécurité et de cybersécurité au sein d'une entreprise ?

Question 20	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord	6 - Ne sait pas
Parier sur une formation personnalisée pour les employés.	32.56%	38.50%	18.60%	5.68%	1.81%	2.84%
Se préparer à la création d'une équipe d'intervention d'urgence.	34.11%	38.76%	18.35%	3.36%	1.55%	3.88%
Vérifier l'existence d'un Plan de Reprise d'Activité (PRA).	34.88%	31.01%	18.60%	4.39%	0.78%	10.34%
Appliquer des mises à jour et correctifs aux logiciels et aux systèmes d'exploitation (OS).	43.41%	34.63%	13.70%	2.58%	1.55%	4.13%
Gérer les droits d'accès des administrateurs.	44.70%	34.63%	11.63%	4.91%	2.33%	1.81%
Réaliser des sauvegardes régulières afin de restaurer les données et logiciels.	52.71%	29.72%	12.66%	2.33%	1.29%	1.29%
Utiliser un VPN uniquement pour les salariés cadres.	18.60%	21.71%	17.57%	15.76%	20.16%	6.20%
Défendre, surveiller les passerelles Internet, isoler les applications Web.	36.43%	40.83%	12.66%	3.36%	2.84%	3.88%
Assurer une veille constante sur les Threat Intelligence pour être informé des menaces actuelles et émergentes spécifiques à l'industrie.	31.27%	40.83%	16.80%	3.36%	1.55%	6.20%
Intégrer un framework de gestion des risques cybersécuritaires, comme le NIST, pour structurer et orienter les efforts.	27.13%	36.43%	18.60%	3.88%	1.81%	12.14%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

21.Vous sentez-vous concerné(e) par les recommandations de sécurité formulées par votre entreprise ?

Question 21	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Suivre les recommandations de l'ANSSI.	34.11%	39.02%	21.71%	3.88%	1.29%
Protéger et identifier les données sensibles.	48.06%	34.88%	14.99%	2.07%	0.00%
Vérifier la vigilance lors de l'ouverture d'e-mails et la vérification des destinataires.	52.45%	31.78%	12.66%	2.07%	1.03%
Sensibiliser les collaborateurs aux risques en ligne.	48.06%	33.07%	13.95%	2.84%	2.07%
Adopter une 'hygiène informatique' quotidienne rigoureuse.	43.41%	38.24%	14.47%	2.84%	1.03%
Télécharger les applications sur les sites ou magasins officiels ou non.	17.57%	28.17%	24.29%	14.73%	15.25%
Utiliser un gestionnaire de mots de passe recommandé.	33.85%	36.69%	18.60%	7.49%	3.36%
Autoriser l'accès de votre PC professionnel à vos enfants.	10.85%	20.41%	13.95%	14.73%	40.05%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

22.Selon vous, se former à la sécurité/cybersécurité pour développer ses compétences en entreprise, c'est :

Question 22	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord	6 - Ne sait pas
Mener régulièrement des audits de sécurité pour identifier les failles.	36.69%	38.50%	15.76%	2.33%	3.10%	3.62%
Maîtriser des outils pointus pour repérer les intrusions.	32.04%	39.02%	15.76%	6.46%	1.55%	5.17%
Organiser des simulations d’attaque pour tester les défenses (Red Teaming).	34.63%	36.18%	15.25%	5.43%	1.03%	7.49%
Élaborer des stratégies de sécurité informatique.	41.60%	33.85%	15.25%	3.62%	1.81%	3.88%
Utiliser des techniques de cryptographie sophistiquées.	29.20%	31.78%	20.93%	4.65%	3.36%	10.08%
Préparer un plan de continuité des opérations (type PRA).	33.07%	33.59%	18.60%	4.13%	1.29%	9.30%
Acquérir des ressources spécialisées du darknet.	15.25%	26.87%	21.45%	8.27%	16.02%	12.14%
Adopter la norme ISO 27001 dans la gestion de la sécurité.	27.13%	30.75%	20.67%	3.36%	1.55%	16.54%
Gérer les identités et les accès efficacement (IAM).	36.95%	32.82%	17.57%	3.36%	1.29%	8.01%
Prévenir les fuites de données (DLP).	37.73%	38.76%	14.99%	2.33%	2.58%	3.62%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

22.Selon vous, se former à la sécurité/cybersécurité pour développer ses compétences en entreprise, c'est :

Question 22	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord	6 - Ne sait pas
Opérer des systèmes de gestion de la sécurité de l'information (ISMS).	27.91%	35.66%	20.93%	3.10%	0.78%	11.63%
Configurer des outils de cryptographie comme DSA et RSA.	21.96%	30.23%	22.22%	5.94%	2.84%	16.80%
Naviguer entre les rôles de Gray Hat Hacker.	16.80%	24.03%	25.06%	5.43%	6.20%	22.48%
Isoler les applications avec sandboxing et conteneurisation.	23.77%	31.52%	20.93%	6.20%	2.07%	15.50%
Comprendre la réalisation d’une Analyse d’Impact relative à la Protection des Données (AIPD).	26.10%	40.05%	17.57%	4.39%	0.78%	11.11%
Chasser proactivement les menaces numériques (Threat Hunting).	31.78%	35.92%	15.76%	4.91%	2.07%	9.56%

Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

23.Selon vous, quelles stratégies pourraient être mises en œuvre pour stimuler l'intelligence collective en matière de cybersécurité au sein d'une équipe, qu'elle soit dédiée à la sécurité, constituée de salariés ou d'un service spécifique ?

Question 23	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Instaurer une culture d'entreprise qui valorise la sécurité et la cybersécurité.	38.76%	40.31%	18.09%	2.07%	0.78%
Développer des programmes de formation en cybersécurité adaptés au profil de chaque employé.	34.88%	43.15%	15.76%	5.43%	0.78%
Sensibiliser spécifiquement chaque service de l'entreprise à la cybersécurité.	44.44%	36.95%	14.47%	3.36%	0.78%
Tisser des liens solides entre les équipes dédiées à la sécurité et tous les salariés.	36.18%	39.28%	17.31%	5.68%	1.55%
Assurer une veille technologique et réglementaire constante pour l'équipe de sécurité.	39.28%	40.05%	18.60%	1.03%	1.03%
Mettre en place une cellule de crise inter-départementale et interfiliale.	32.30%	37.47%	25.32%	3.62%	1.29%
Promouvoir le partage de savoir-faire en matière de sécurité avec les fournisseurs et partenaires.	33.07%	41.60%	20.67%	3.88%	0.78%
S'engager en faveur de la formation continue des équipes de sécurité et des prestataires externes.	40.57%	36.18%	18.09%	3.10%	2.07%
Encourager une ouverture d'esprit via des visioconférences dédiées à la sécurité.	34.11%	41.60%	19.64%	3.62%	1.03%
Stimuler la curiosité intellectuelle pour les meilleures pratiques en informatique.	32.56%	44.19%	18.60%	3.88%	0.78%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

24.Toujours pour stimuler l'intelligence collective, quelles autres stratégies pourraient être mises en œuvre ?

Question 24	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Inculquer une vigilance permanente lors de l'utilisation de réseaux connectés.	44.19%	34.88%	17.83%	2.84%	0.26%
Clarifier les risques et conséquences liés aux différents usages informatiques.	40.31%	39.79%	16.80%	2.33%	0.78%
Établir des mesures de sécurité de base à mettre en place au domicile des employés.	36.95%	40.05%	18.09%	4.13%	0.78%
Concevoir des formations en cybersécurité qui intègrent les aspects de l'intelligence artificielle.	34.37%	41.34%	17.83%	4.91%	1.55%
Former les équipes en fonction des applications utilisées et de leur environnement numérique.	37.21%	40.57%	17.57%	4.13%	0.52%
Organiser des simulations d'attaques de phishing pour tester la réactivité des employés.	35.66%	38.24%	19.64%	3.88%	2.58%
Instituer une heure annuelle de 'blackout' par service pour sensibiliser au risque de dépendance au numérique.	26.87%	34.63%	25.06%	10.85%	2.58%
Prévoir des journées dédiées à la sensibilisation à la sécurité et à la cybersécurité.	39.28%	37.21%	18.09%	4.65%	0.78%
Proposer des sessions informelles de formation à la sécurité pendant le déjeuner en télétravail (choix libre).	27.65%	36.95%	21.71%	9.56%	4.13%
Diffuser un podcast sur la sécurité et les cyberattaques, accessible lors des trajets quotidiens (choix libre).	24.29%	35.92%	28.42%	9.30%	2.07%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

25.Comment évaluez-vous l'importance des propositions ci-dessous ?

Question 25	Très important	Moins important
Formaliser sa politique de sécurité informatique	86.05%	13.95%
Sensibiliser les utilisateurs du parc informatique	89.66%	10.34%
Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...)	88.63%	11.37%
Mettre à jour les logiciels, navigateurs, plugins, Java, etc...	89.15%	10.85%
Changer régulièrement de mots de passe	87.86%	12.14%
Faire des sauvegardes ordinateurs/ smartphones régulières	91.73%	8.27%
Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes	71.58%	28.42%
Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique	81.65%	18.35%
Respecter les règles relatives aux réseaux sociaux	83.98%	16.02%
Respecter les règles de mot de passe WIFI	88.11%	11.89%

Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

25.Comment évaluez-vous l'importance des propositions ci-dessous ?

Question 25	Très important	Moins important
Respecter les règles de paiement en ligne	91.73%	8.27%
Respecter les chartes Internet utilisateurs	81.91%	18.09%
Faire attention en ouvrant les e-mails (phishing, virus)	93.02%	6.98%
Utiliser un firewall et/ou VPN	78.81%	21.19%
Protéger vos données en déplacement	90.96%	9.04%
Protéger son identité numérique en ligne	91.99%	8.01%

Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

26.Reprenons les mêmes propositions. Comment évaluez-vous leur facilité technique ?

Question 26	Facile techniquement	Difficile techniquement
Formaliser sa politique de sécurité informatique	68.99%	31.01%
Sensibiliser les utilisateurs du parc informatique	76.23%	23.77%
Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...)	80.36%	19.64%
Mettre à jour les logiciels, navigateurs, plugins, Java, etc...	80.10%	19.90%
Changer régulièrement de mots de passe	87.60%	12.40%
Faire des sauvegardes ordinateurs/ smartphones régulières	82.95%	17.05%
Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes	40.83%	59.17%
Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique	54.52%	45.48%
Respecter les règles relatives aux réseaux sociaux	85.01%	14.99%
Respecter les règles de mot de passe WIFI	87.86%	12.14%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

26.Reprenons les mêmes propositions. Comment évaluez-vous leur facilité technique ?

Question 26	Facile techniquement	Difficile techniquement
Respecter les règles de paiement en ligne	85.53%	14.47%
Respecter les chartes Internet utilisateurs	84.75%	15.25%
Faire attention en ouvrant les e-mails (phishing, virus)	86.56%	13.44%
Utiliser un firewall et un VPN	72.87%	27.13%
Protéger vos données en déplacementProposition 15	60.21%	39.79%
Protéger son identité numérique en ligne	68.73%	31.27%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

27.Encore une fois sur les mêmes propositions, comment évaluez-vous votre niveau de maîtrise ?

Question 27	Maîtrisé	A approfondir
Formaliser sa politique de sécurité informatique	56.85%	43.15%
Sensibiliser les utilisateurs du parc informatique	55.30%	44.70%
Mettre à jour les systèmes d'exploitation (OS) sur tous les matériels (ordinateurs, tablettes, smartphones...)	72.87%	27.13%
Mettre à jour les logiciels, navigateurs, plugins, Java, etc...	75.19%	24.81%
Changer régulièrement de mots de passe	76.23%	23.77%
Faire des sauvegardes ordinateurs/ smartphones régulières	75.97%	24.03%
Surveiller la présence éventuelle de ses données personnelles sur le darknet et autres plateformes	35.92%	64.08%
Réaliser des audits de sécurité pour vérifier l'intégrité de son écosystème informatique	41.09%	58.91%
Respecter les règles relatives aux réseaux sociaux	72.35%	27.65%
Respecter les règles de mot de passe WIFI	79.33%	20.67%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

27.Encore une fois sur les mêmes propositions, comment évaluez-vous votre niveau de maîtrise ?

Question 27	Maîtrisé	A approfondir
Respecter les règles de paiement en ligne	77.26%	22.74%
Respecter les chartes Internet utilisateurs	68.99%	31.01%
Faire attention en ouvrant les e-mails (phishing, virus)	76.74%	23.26%
Utiliser un firewall et un VPN	63.57%	36.43%
Protéger vos données en déplacement	57.88%	42.12%
Protéger son identité numérique en ligne	58.14%	41.86%

Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

29.Avez-vous actuellement un rôle de manager ou occupez-vous un poste d'encadrement dans votre entreprise ?

Proposition des réponses	Effectif	Pourcentage
Oui	227	58.66%
Non	160	41.34%
Total	387	100.00%

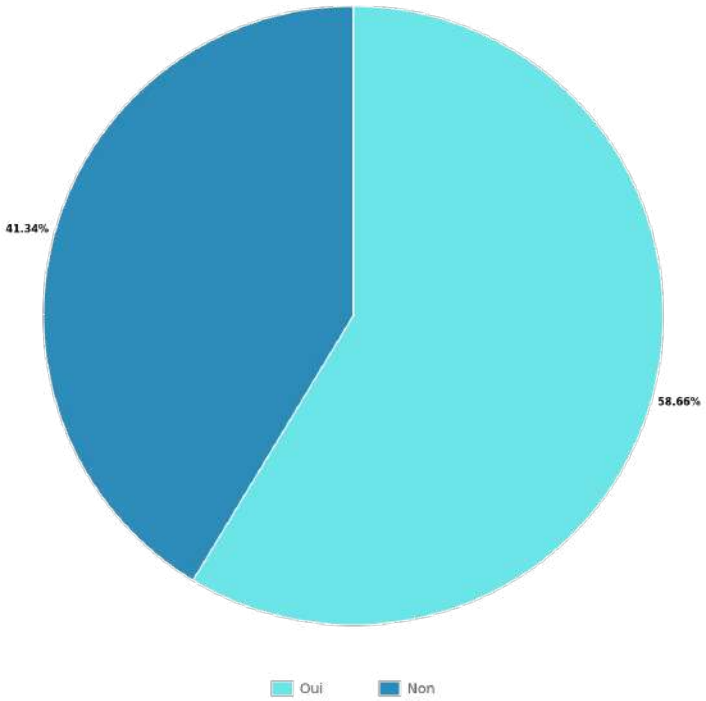
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

29.Avez-vous actuellement un rôle de manager ou occupez-vous un poste d'encadrement dans votre entreprise ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

30.Dans votre entreprise, à quel service ou département appartenez-vous ?

Proposition des réponses	Effectif	Pourcentage
DIRECTION	32	8.27%
COMPTABILITE	27	6.98%
RESSOURCES HUMAINES	25	6.46%
VENTES	20	5.17%
FINANCE	17	4.39%
LOGISTIQUE	27	6.98%
PRODUCTION	8	2.07%
ACHATS	1	0.26%
INFORMATIQUE	125	32.30%
COMMUNICATION	6	1.55%

Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

30.Dans votre entreprise, à quel service ou département appartenez-vous ?

Proposition des réponses	Effectif	Pourcentage
SERVICE CLIENT	11	2.84%
SUPPORT DES VENTES	0	0.00%
MAINTENANCE	2	0.52%
SECRETARIAT	12	3.10%
QUALITE	5	1.29%
R&D	30	7.75%
SERVICES GENERAUX	1	0.26%
ASSURANCE	0	0.00%
FORMATION	6	1.55%
ORGANISATION	0	0.00%

Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

30.Dans votre entreprise, à quel service ou département appartenez-vous ?

Proposition des réponses	Effectif	Pourcentage
DOCUMENTATION	0	0.00%
JURIDIQUE	2	0.52%
BUREAU D ETUDES	7	1.81%
CONTRÔLE DE GESTION	0	0.00%
GESTION DE PROJETS	7	1.81%
E-COMMERCE	4	1.03%
INTERNATIONAL	2	0.52%
IMMOBILIER	0	0.00%
TRAVAUX	0	0.00%
SECURITE	4	1.03%

Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

30.Dans votre entreprise, à quel service ou département appartenez-vous ?

Proposition des réponses	Effectif	Pourcentage
RELATIONS PUBLIQUES	6	1.55%
PENVIRONNEMENT ET DURABILITÉ	0	0.00%
Total	387	100.00%

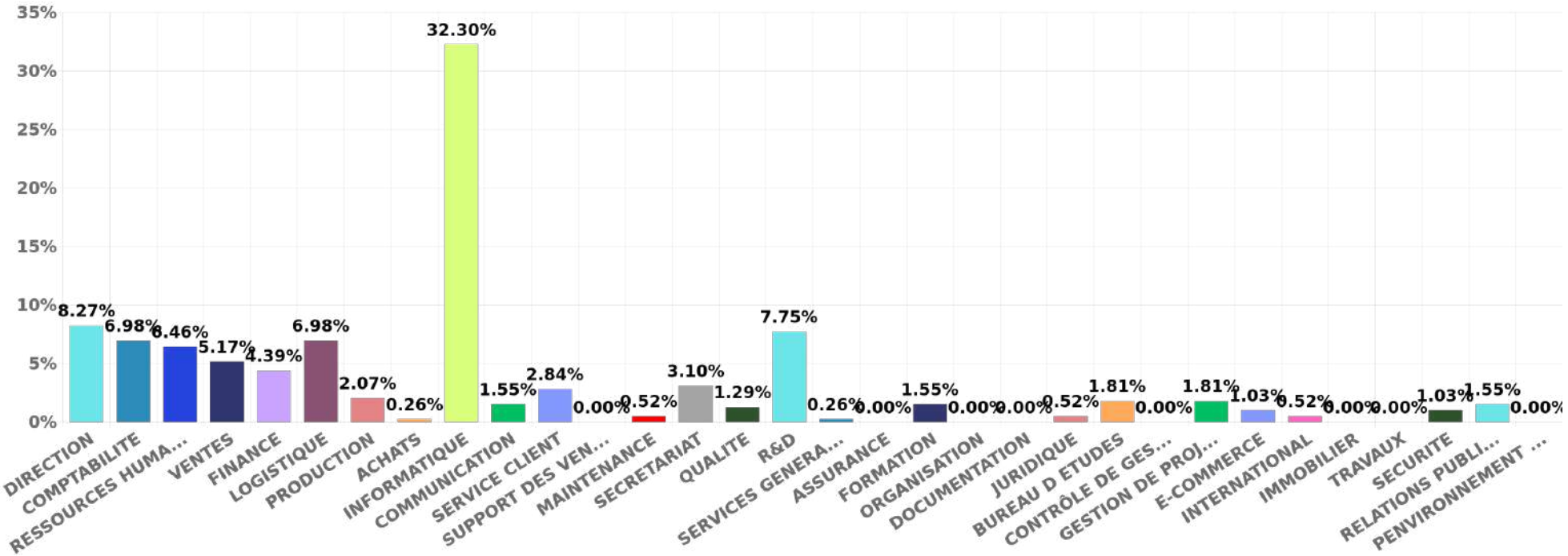
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

30.Dans votre entreprise, à quel service ou département appartenez-vous ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

31.Quelles sont les actions à privilégier pour renforcer la culture de la cybersécurité au sein de votre entreprise ?

Proposition des réponses	Effectif	Pourcentage
Partager avec pédagogie la vision cybersécurité de l'entreprise auprès de l'ensemble des salariés.	90	23.26%
Utiliser la prévention pour se protéger face aux menaces en tous genres.	134	34.63%
Alerter l'ensemble du personnel sur les risques potentiels informatiques et cybermenaces.	156	40.31%
Appliquer les recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) afin de sensibiliser les salariés.	100	25.84%
Améliorer les moyens mis en oeuvre pour l'éducation et la sensibilisation des salariés.	113	29.20%
Impliquer l'ensemble des salariés, l'équipe sécurité de l'entreprise et pas uniquement les actions du RSSI.	140	36.18%
Consacrer du temps par l'équipe de sécurité afin de s'assurer que le personnel est toujours idéalement informé.	113	29.20%
Engager l'écosystème de l'entreprise, aussi bien les collaborateurs que les prestataires, les fournisseurs et les partenaires.	61	15.76%
Informer le personnel lorsqu'une attaque intervient, pour tenter de l'amener à comprendre et à agir de manière appropriée.	128	33.07%
Total	387	100.00%

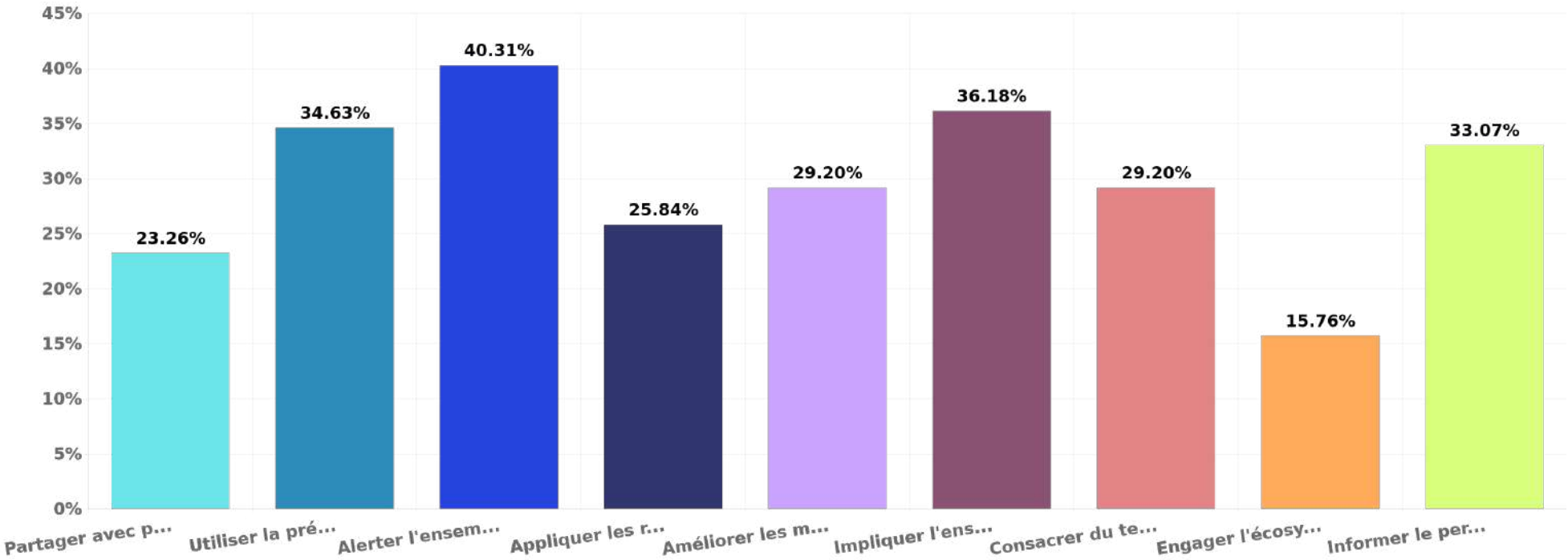
Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

31.Quelles sont les actions à privilégier pour renforcer la culture de la cybersécurité au sein de votre entreprise ?



Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

32.Dans le cadre de sa politique de sensibilisation, diriez-vous que votre entreprise met en place une culture de la cybersécurité ?

Minimun	Quartile 1	Moyenne	Médianne	Quartile 3	Maximum	Total
1	3	3.75	4	4	5	387

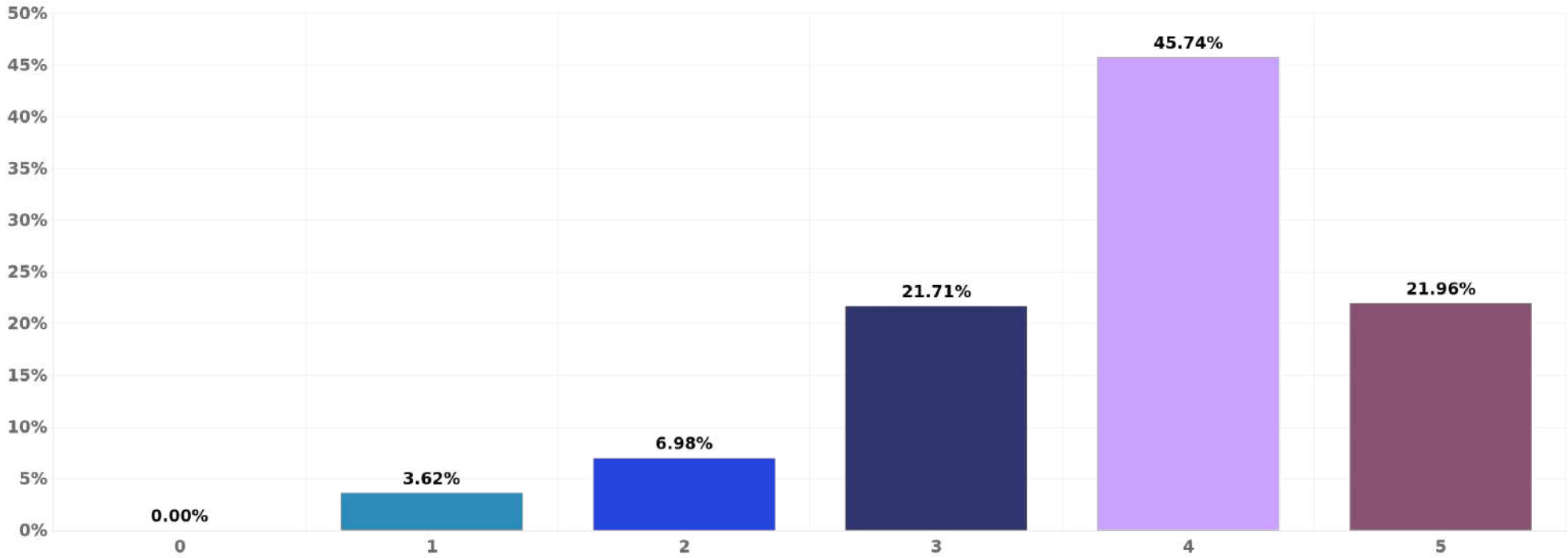
Type de question : Échelle

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

32.Dans le cadre de sa politique de sensibilisation, diriez-vous que votre entreprise met en place une culture de la cybersécurité ?



Type de question : Échelle

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

33.Est-ce important pour vous d'être immédiatement informé par SMS en cas d'attaque informatique visant votre entreprise, incluant des instructions à suivre ?

Proposition des réponses	Effectif	Pourcentage
Oui, indispensable	165	42.86%
Oui, très important	154	40.00%
Oui, assez important	45	11.69%
Non	21	5.45%
Total	385	100.00%

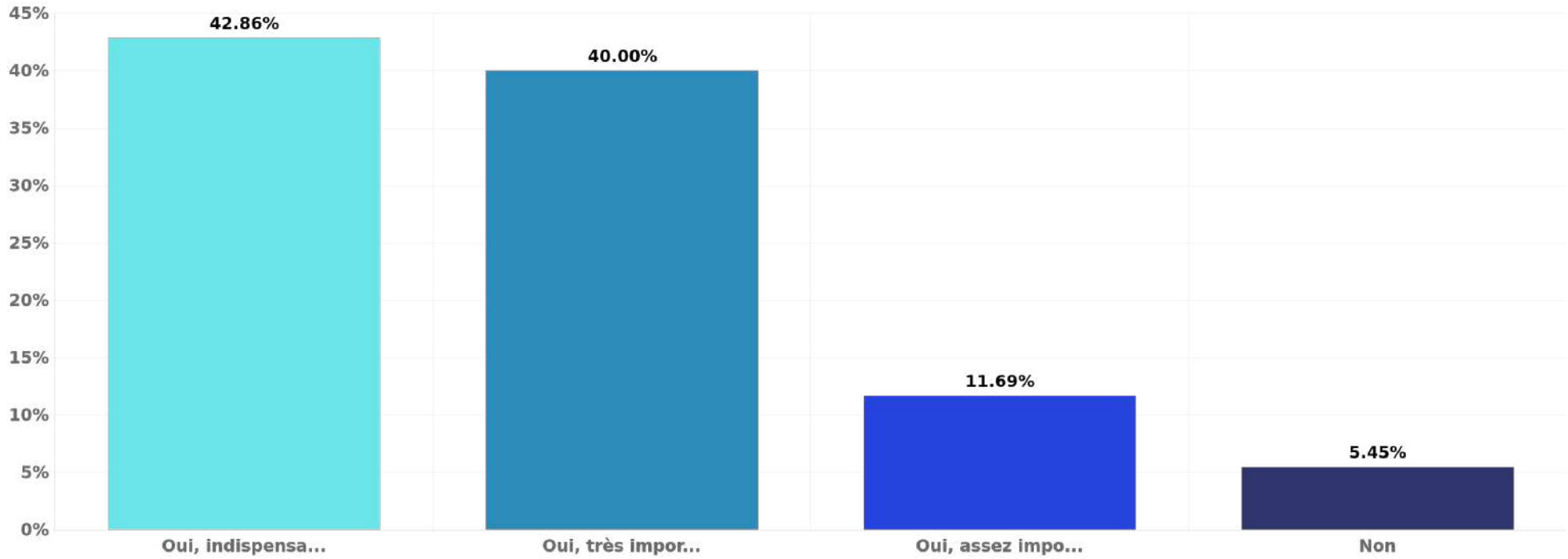
Type de question : Choix unique

Nombre de répondants à cette question : 385

Nombre de répondants à cette question : 2

Résultats

33.Est-ce important pour vous d'être immédiatement informé par SMS en cas d'attaque informatique visant votre entreprise, incluant des instructions à suivre ?



Type de question : Choix unique

Nombre de répondants à cette question : 385

Nombre de répondants à cette question : 2

Résultats

34.En cas d'attaque informatique, de fraude, de vol, de phishing et autres incidents similaires, diriez-vous que :

Question 34	1 - Oui, tout à fait	2 -Oui, en partie	3 - Non, pas vraiment	4 - Non, pas du tout	5 - Ne sait pas
Vous avez les informations nécessaires pour comprendre la situation et agir de manière appropriée.	25.32%	48.58%	18.09%	5.43%	2.58%
Vous êtes au courant des premières mesures à prendre.	36.95%	37.21%	17.83%	5.17%	2.84%
Vous avez confiance en la capacité de réaction de l'équipe en charge de la sécurité informatique.	45.74%	38.50%	10.59%	3.10%	2.07%

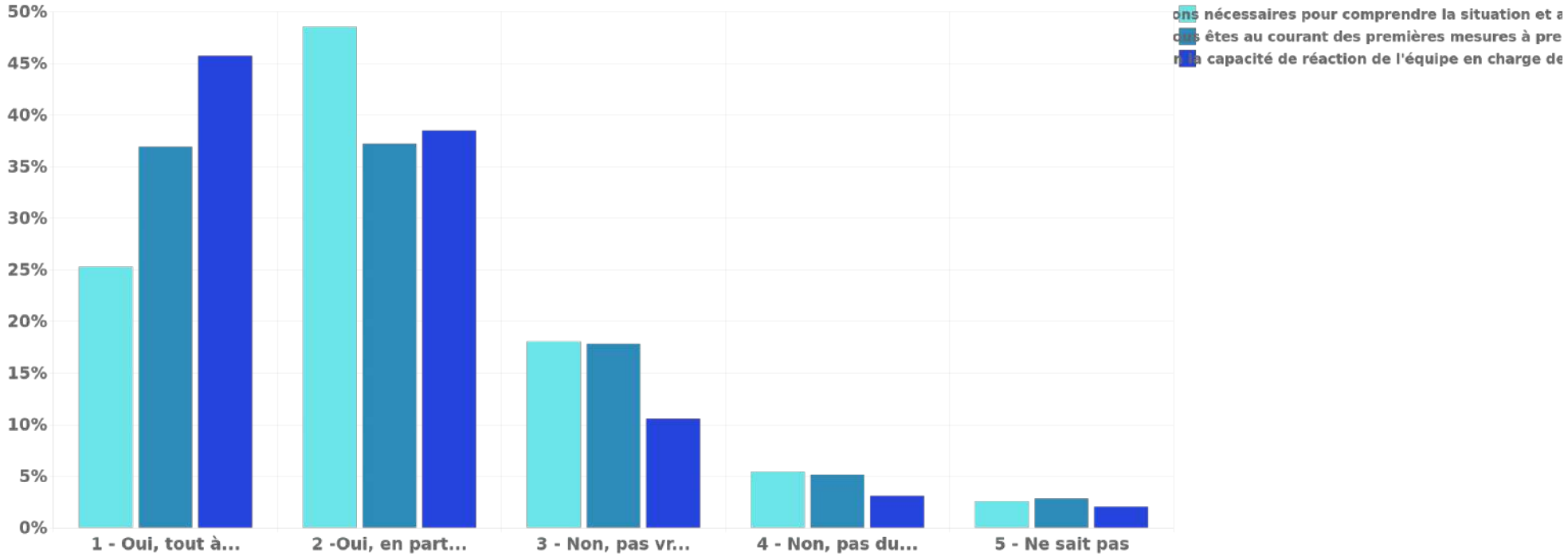
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

34.En cas d'attaque informatique, de fraude, de vol, de phishing et autres incidents similaires, diriez-vous que :



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

35.En fonction de vos expériences personnelles et/ou professionnelles passées, quel serait votre niveau de stress ?

Proposition des réponses	Effectif	Pourcentage
Pas du tout stressé	19	4.91%
Peu stressé	111	28.68%
Modérément stressé	181	46.77%
Très stressé	65	16.80%
Extrêmement stressé	11	2.84%
Total	387	100.00%

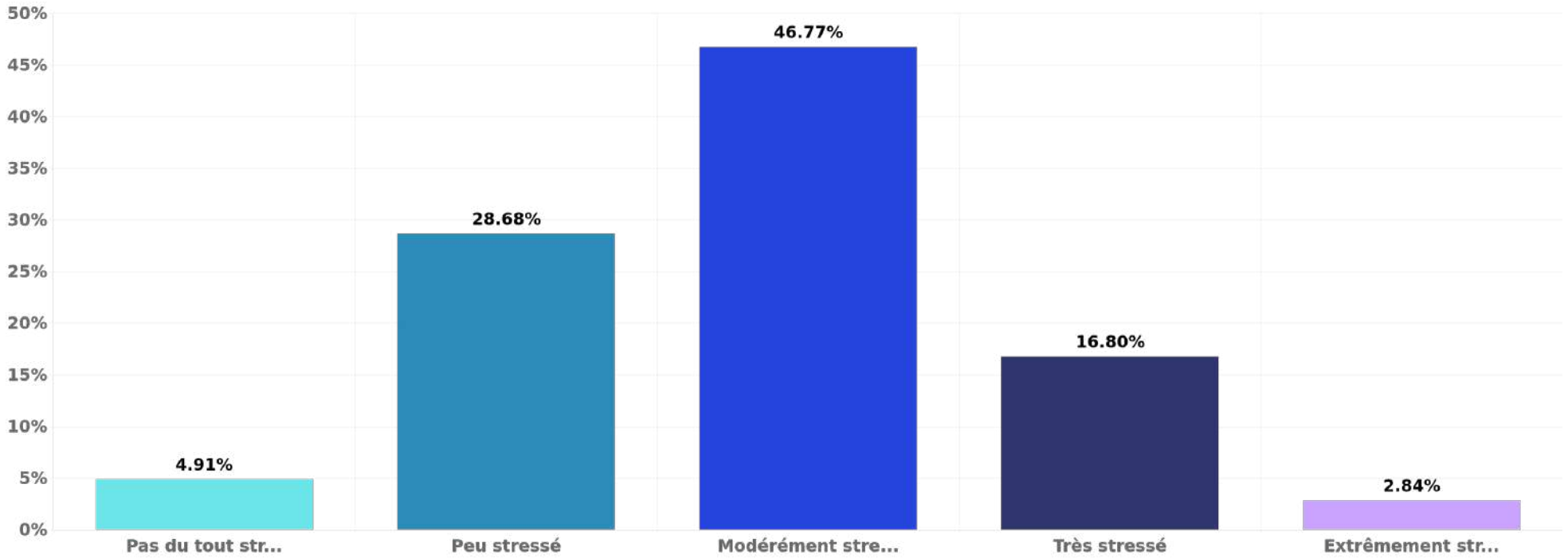
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

35.En fonction de vos expériences personnelles et/ou professionnelles passées, quel serait votre niveau de stress ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

36.Selon vous, est-il nécessaire que le service informatique ou la DSI mette en place des simulations de cyberattaques pour sensibiliser efficacement les employés, évaluer les mesures de sécurité et tester leurs réflexes numériques ?

Proposition des réponses	Effectif	Pourcentage
Oui, indispensable	152	39.28%
Oui, par précaution	194	50.13%
Non	27	6.98%
Ne sait pas	14	3.62%
Total	387	100.00%

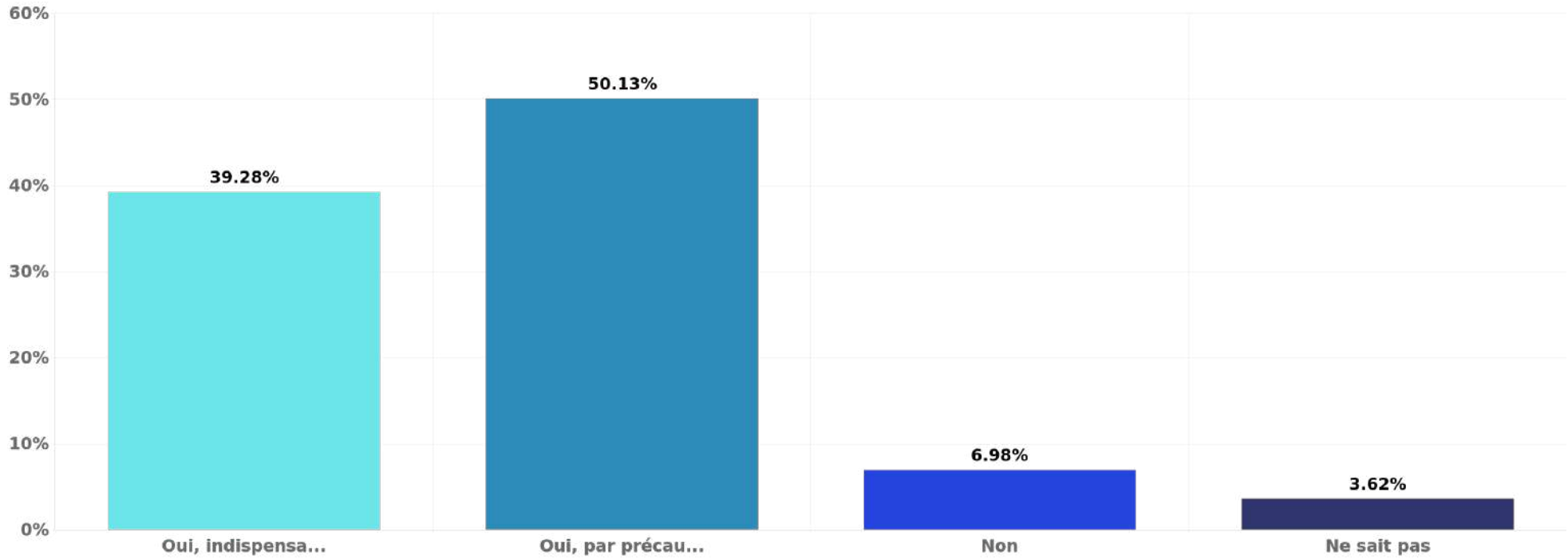
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

36.Selon vous, est-il nécessaire que le service informatique ou la DSI mette en place des simulations de cyberattaques pour sensibiliser efficacement les employés, évaluer les mesures de sécurité et tester leurs réflexes numériques ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

37.Considérez-vous comme nécessaire de signaler à votre service informatique ou à votre DSI en cas de piratage d'un ordinateur, d'une tablette ou d'un smartphone dans votre environnement familial ?

Proposition des réponses	Effectif	Pourcentage
Oui, indispensable	164	42.38%
Oui, par précaution	162	41.86%
Non	50	12.92%
Ne sait pas	11	2.84%
Total	387	100.00%

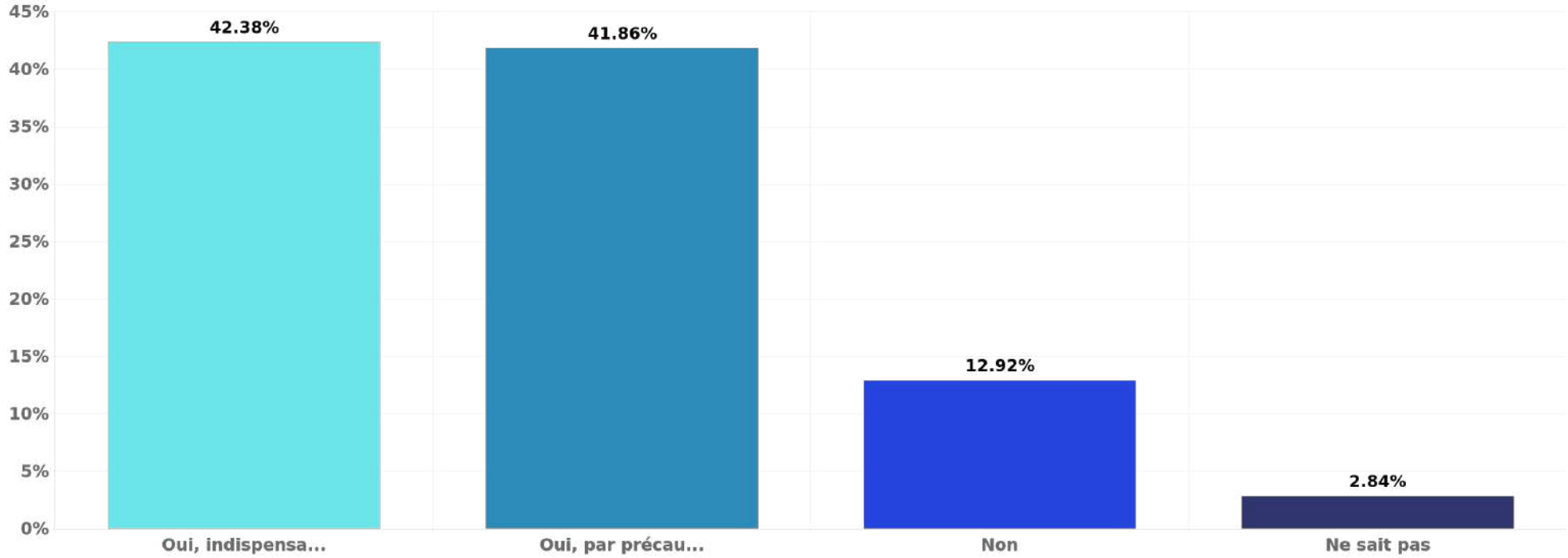
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

37.Considérez-vous comme nécessaire de signaler à votre service informatique ou à votre DSI en cas de piratage d'un ordinateur, d'une tablette ou d'un smartphone dans votre environnement familial ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

38.Disposez-vous des outils adéquats tels qu'un cahier de notes, des fichiers informatiques, des services en ligne, etc., pour organiser et planifier efficacement votre politique de sécurité (y compris une liste de plans d'action basés sur un processus) dans votre environnement domestique ?

Proposition des réponses	Effectif	Pourcentage
J'ai déjà les outils adéquats	125	32.30%
Je suis en phase de recherche de solution	136	35.14%
Je n'ai pas ce type d'outils	97	25.06%
Ne sait pas	29	7.49%
Total	387	100.00%

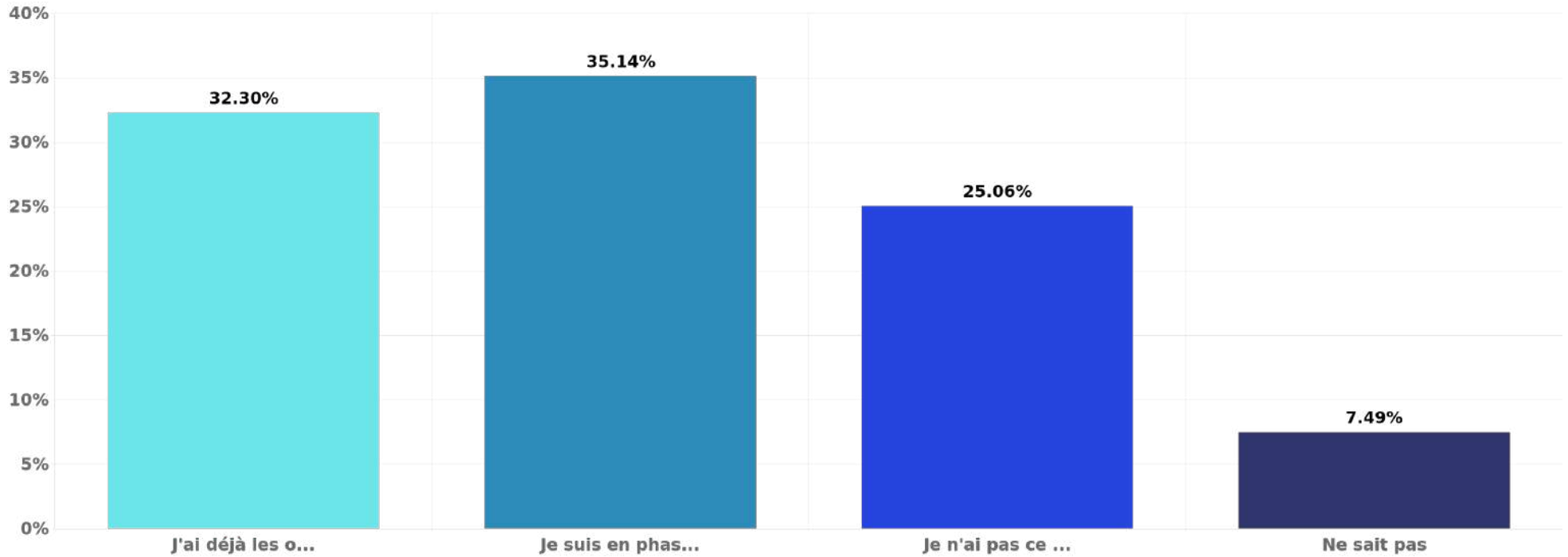
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

38.Disposez-vous des outils adéquats tels qu'un cahier de notes, des fichiers informatiques, des services en ligne, etc., pour organiser et planifier efficacement votre politique de sécurité (y compris une liste de plans d'action basés sur un processus) dans votre environnement domestique ?



Type de question : Choix unique Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

39.Pour qu'une approche de sensibilisation à la sécurité informatique /cybersécurité soit pertinente et efficace, quelle serait la bonne répartition à adopter entre :

Proposition des réponses	Moyenne	Minimun	Maximum
La sensibilisation liée à l'environnement personnel	40.6%	0%	100%
La sensibilisation liée à l'environnement professionnel	59.4%	0%	100%

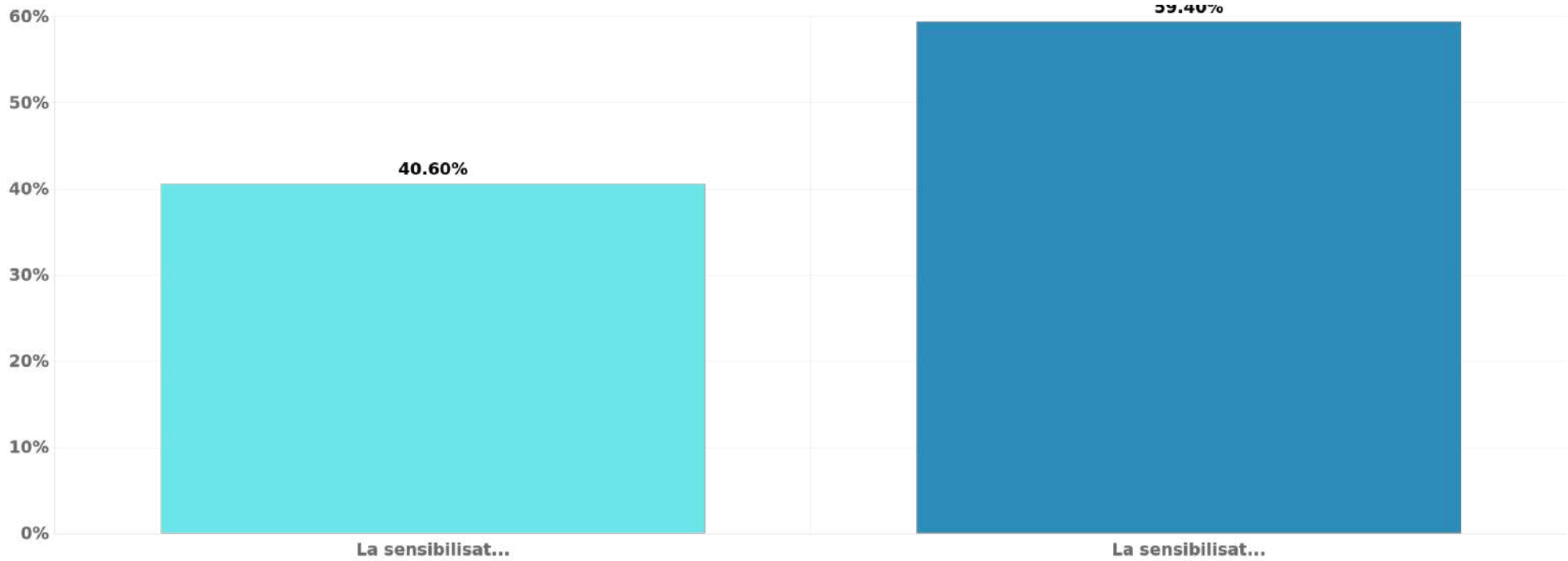
Type de question : Répartition

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

39.Pour qu'une approche de sensibilisation à la sécurité informatique /cybersécurité soit pertinente et efficace, quelle serait la bonne répartition à adopter entre :



Type de question : Répartition

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

40.Dans votre entreprise, quels sont les freins à la sensibilisation à la sécurité informatique /cybersécurité ?

Question 40	1- Pas du tout un frein	2 - Plutôt pas un frein	3 - Frein modéré	4 - Frein plutôt important	5 - Frein très important
La malveillance	14.47%	26.10%	29.72%	19.38%	10.34%
L'erreur humaine	7.75%	19.38%	38.24%	23.51%	11.11%
Le manque de temps en entreprise	9.56%	19.90%	30.23%	27.65%	12.66%
Le manque d'investissement dans la création et/ou l'achat de supports de formation	11.63%	24.81%	32.56%	22.22%	8.79%
Le manque d'implication des salariés	9.04%	18.09%	36.95%	26.36%	9.56%
Le manque de volonté d'apprendre dans le cadre de la formation continue	10.34%	20.41%	35.14%	26.10%	8.01%

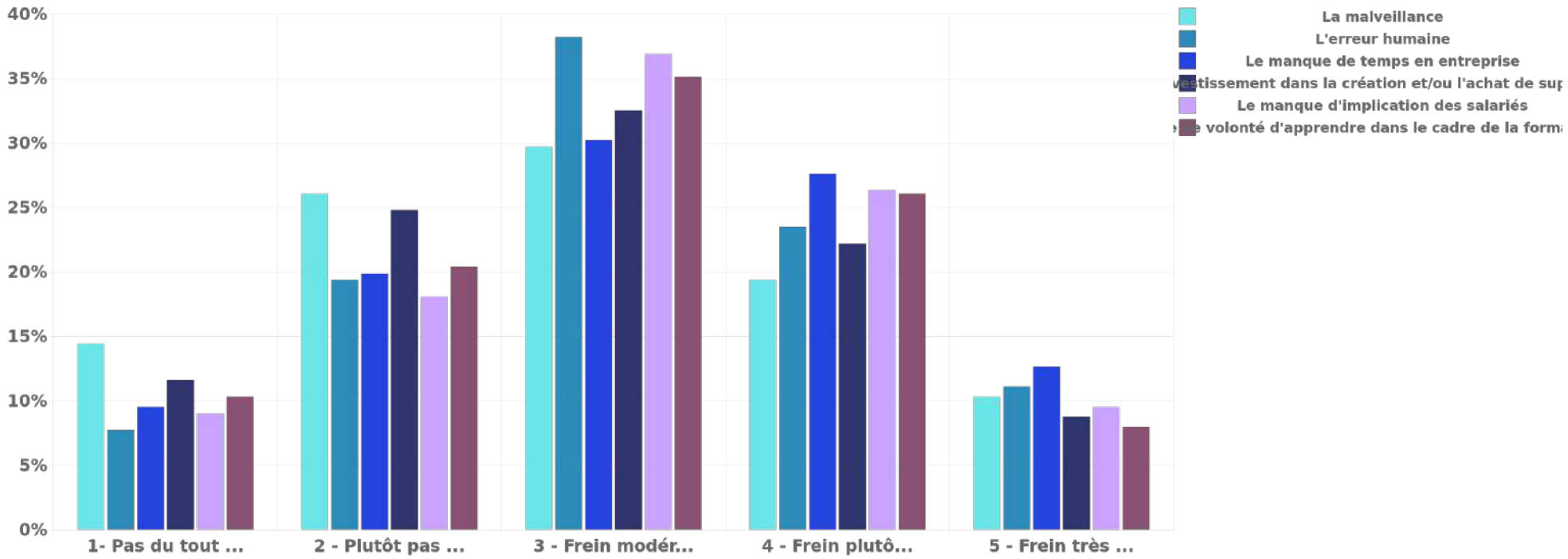
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

40.Dans votre entreprise, quels sont les freins à la sensibilisation à la sécurité informatique /cybersécurité ?



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

41.Si vous deviez signaler un incident de sécurité ou une activité suspecte :

Question 41	Oui	Non	Ne sait pas
Je serais à l'aise pour signaler un incident de sécurité.	79.59%	13.70%	6.72%
Je serais à l'aise pour signaler une activité suspecte.	77.52%	15.50%	6.98%
Je sais comment faire pour signaler un incident de sécurité.	76.74%	17.05%	6.20%
Je sais comment faire pour signaler une activité suspecte.	79.07%	13.44%	7.49%

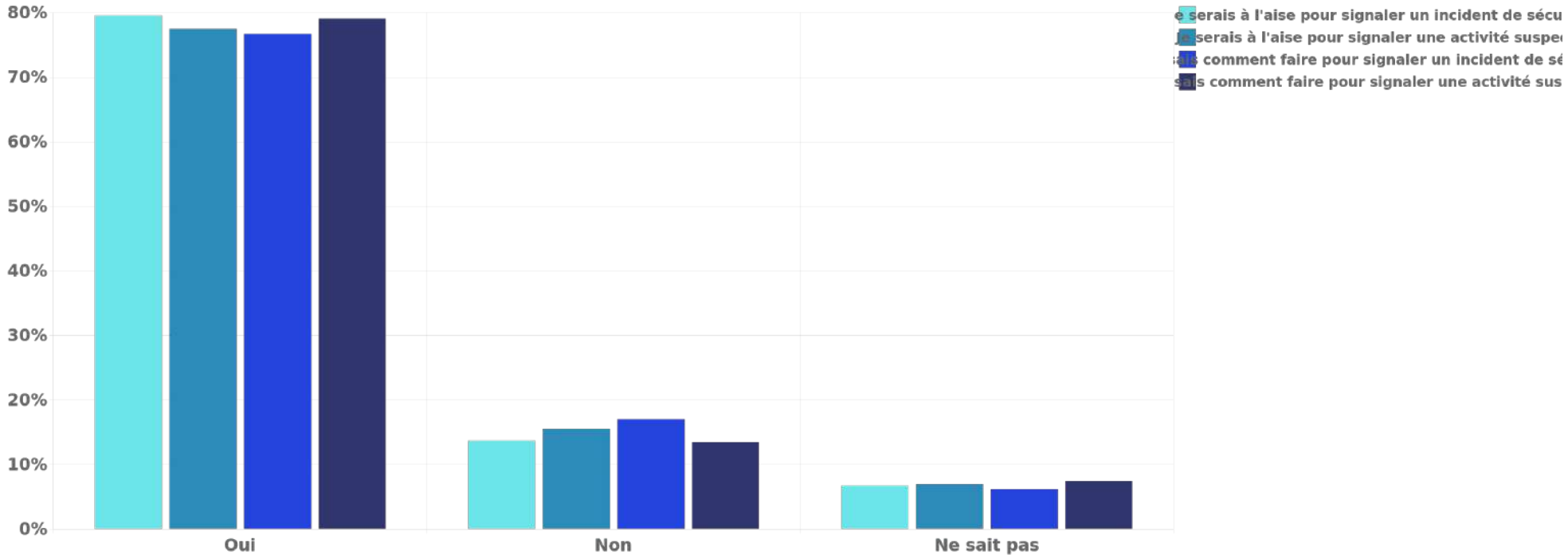
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

41.Si vous deviez signaler un incident de sécurité ou une activité suspecte :



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

42.Dans votre entreprise, l'information pertinente concernant la sensibilisation à la sécurité informatique /cybersécurité est-elle diffusée ?

Question 42	Toujours	Souvent	Parfois	Jamais
Aux bons destinataires	44.44%	33.59%	17.05%	4.91%
Dans le bon timing, au bon moment	28.17%	39.79%	24.55%	7.49%
De façon claire et compréhensible par tous	35.14%	37.73%	22.74%	4.39%
De façon utilisable par tous	34.11%	39.02%	20.41%	6.46%
Permettant l'apprentissage tout au long du contrat de travail	33.07%	35.40%	23.26%	8.27%
En alliant la théorie et la pratique	27.65%	38.76%	21.71%	11.89%

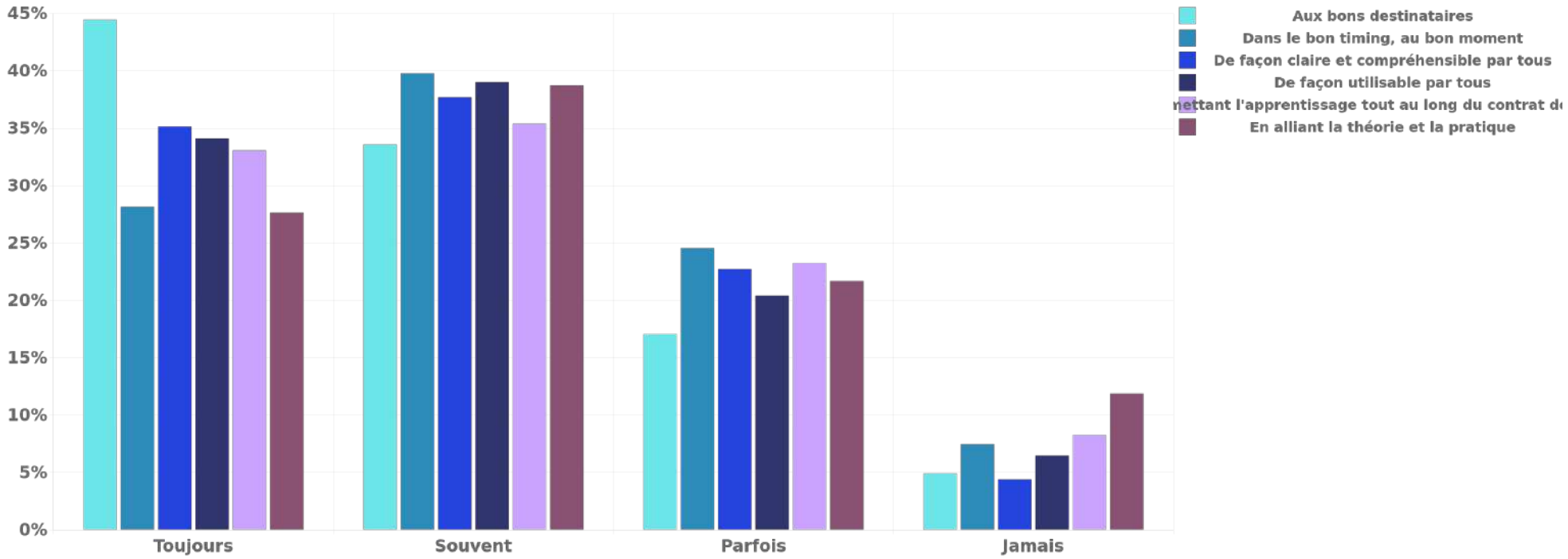
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

42.Dans votre entreprise, l'information pertinente concernant la sensibilisation à la sécurité informatique /cybersécurité est-elle diffusée ?



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

43.Dans quelle mesure vous sentez-vous engagé(e) envers votre politique de sécurité entreprise ?

Proposition des réponses	Effectif	Pourcentage
Pas du tout engagé(e) : Je ne suis pas du tout concerné par la politique de sécurité et je ne pense pas que ce soit important pour mon travail.	6	1.55%
Peu engagé(e) : Je suis conscient de la politique de sécurité, mais je ne la considère pas comme une priorité dans mon travail quotidien.	42	10.85%
Modérément engagé(e) : Je comprends l'importance de la politique de sécurité et je m'efforce de respecter ses règles autant que possible.	84	21.71%
Plutôt engagé(e) : Je prends la politique de sécurité au sérieux et je suis attentif à respecter toutes ses règles dans mon travail.	159	41.09%
Très engagé(e) : La politique de sécurité est une priorité pour moi. Je suis toujours à jour avec ses exigences et j'encourage également mes collègues à la respecter.	96	24.81%
Total	387	100.00%

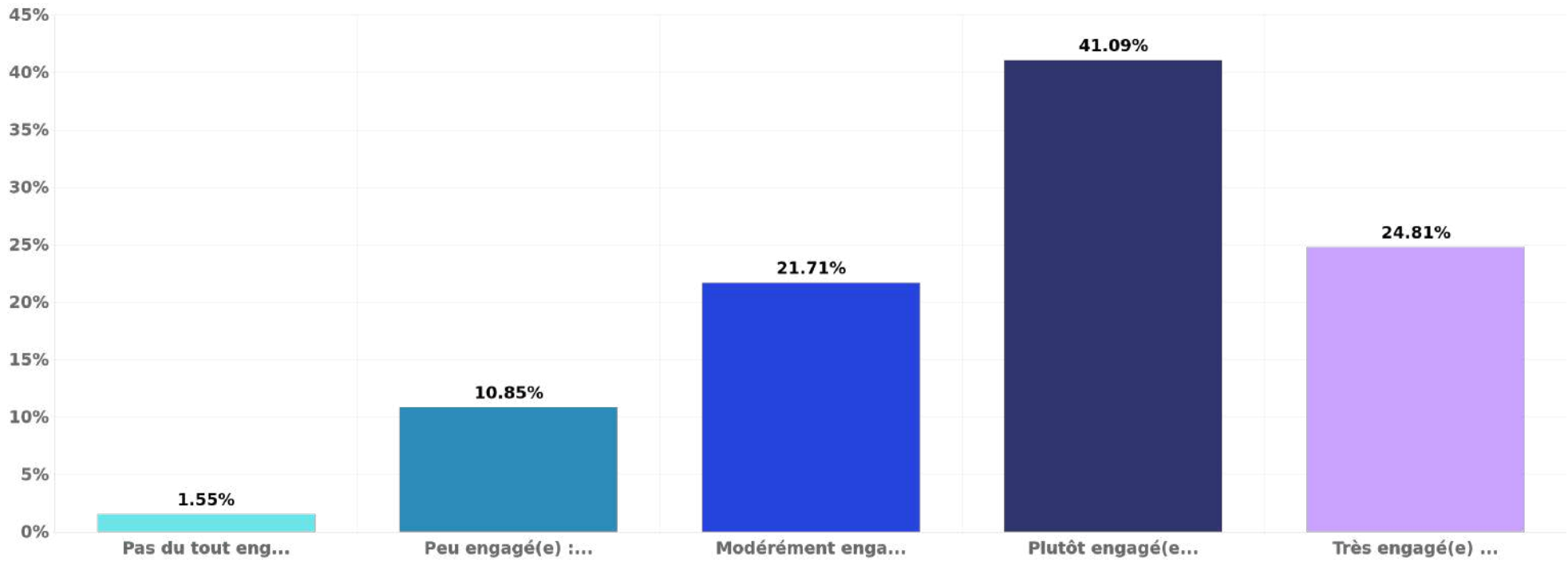
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

43.Dans quelle mesure vous sentez-vous engagé(e) envers votre politique de sécurité entreprise ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

44.La politique de sécurité de votre entreprise/organisation est-elle efficace pour prévenir les incidents de cybersécurité ?

Proposition des réponses	Effectif	Pourcentage
Pas du tout efficace : Je pense que notre politique de sécurité n'a aucun effet sur la prévention des incidents de cybersécurité.	6	1.55%
Peu efficace : Notre politique de sécurité pourrait avoir un effet mineur sur la prévention des incidents de cybersécurité, mais je pense qu'il y a beaucoup d'améliorations à faire.	33	8.53%
Modérément efficace : Notre politique de sécurité a un certain impact sur la prévention des incidents de cybersécurité, bien qu'il y ait encore des domaines à améliorer.	94	24.29%
Efficace : Je crois que notre politique de sécurité est en grande partie efficace pour prévenir les incidents de cybersécurité.	178	45.99%
Très efficace : Je suis convaincu que notre politique de sécurité est extrêmement efficace et joue un rôle crucial dans la prévention des incidents de cybersécurité.	76	19.64%
Total	387	100.00%

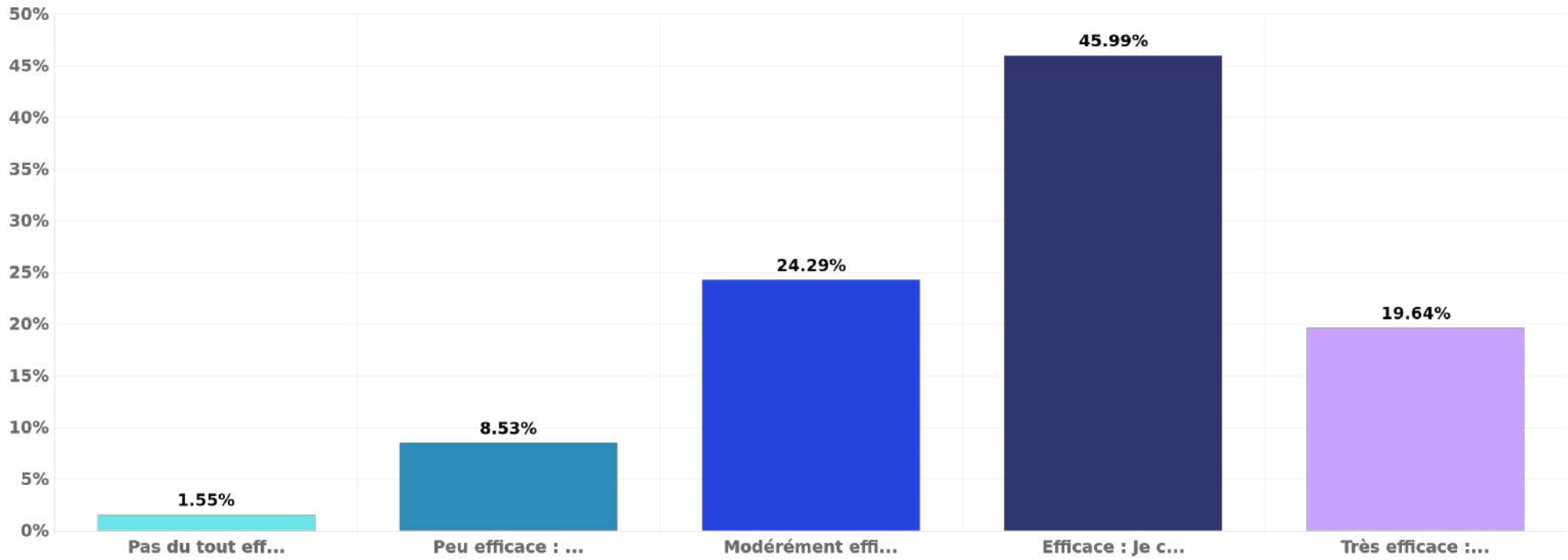
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

44.La politique de sécurité de votre entreprise/organisation est-elle efficace pour prévenir les incidents de cybersécurité ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

45.Pour améliorer la sécurité et la conformité des données dans votre entreprise dans le cadre du RGPD (Règlement Général sur la Protection des Données), quelles sont les actions les plus importantes ?

Proposition des réponses	Effectif	Place la plus basse	Place la plus haute	Place moyenne
Sensibiliser les salariés à la conformité RGPD (note d'information interne, réunion d'information par service, e-learning	387	1	6	3.13
Limiter l'accès aux données par : MFA, VPN, mail chiffré, cryptage des disques, gestionnaire de mot de passe	387	1	6	3.63
Identifier les données dites sensibles (données sensibles interdites en entreprise et les données sensibles obligatoires)	387	1	6	3.15
Planifier la politique de sécurité des données (Autorisation de contrôle d'accès, Accès aux réseaux, Responsabilités des utilisateurs)	387	1	6	3.63
Prévoir et faire face aux demandes d'accès aux données des intéressés (utilisateurs, clients, fournisseurs, etc.)	387	1	6	3.44
Vérifier l'application des mises à jour et sauvegarder régulièrement les données de votre entreprise	387	1	6	4.02

Type de question : Classement

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

46.Dans votre travail quotidien, quel pourcentage de votre temps consacrez-vous à l'application du RGPD ?

Proposition des réponses	Effectif	Pourcentage
100%	16	4.13%
75%	78	20.16%
50%	82	21.19%
25%	128	33.07%
Non concerné	83	21.45%
Total	387	100.00%

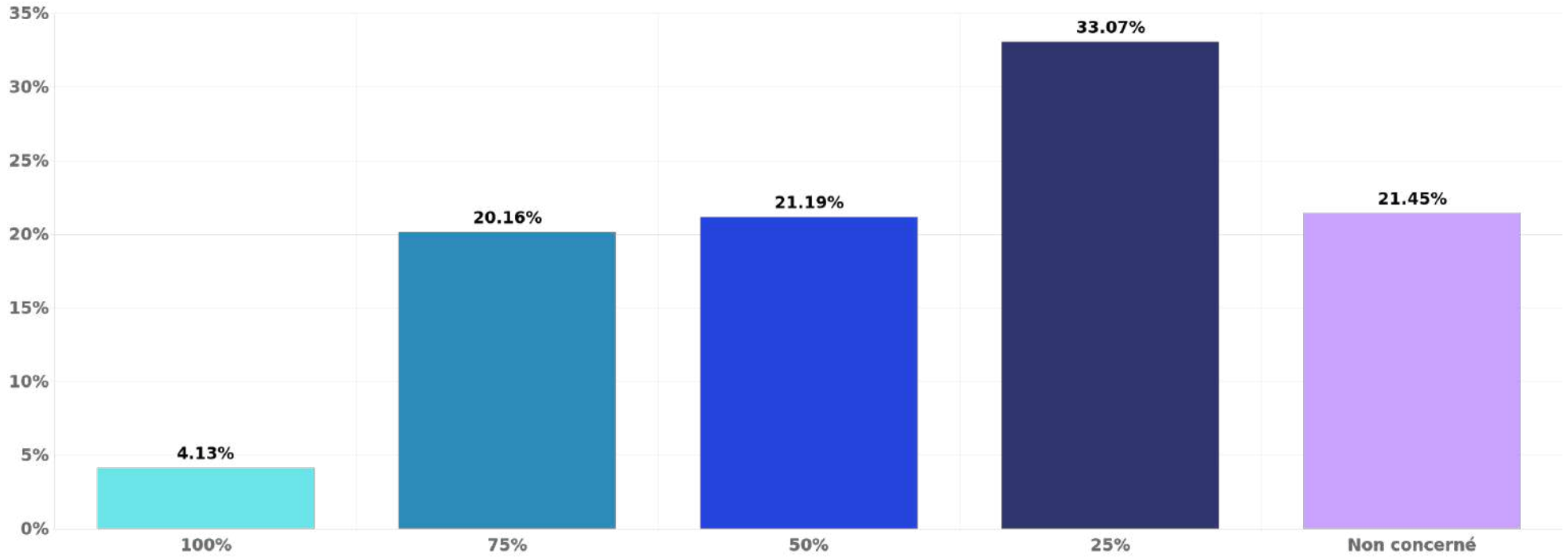
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

46.Dans votre travail quotidien, quel pourcentage de votre temps consacrez-vous à l'application du RGPD ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

47.Avez-vous participé à une formation à la cybersécurité au cours de l'année écoulée ?

Proposition des réponses	Effectif	Pourcentage
Oui, en présentiel	131	33.85%
Oui, en e-learning	159	41.09%
Non, ni en présentiel ni en e-learning	118	30.49%
Total	387	100.00%

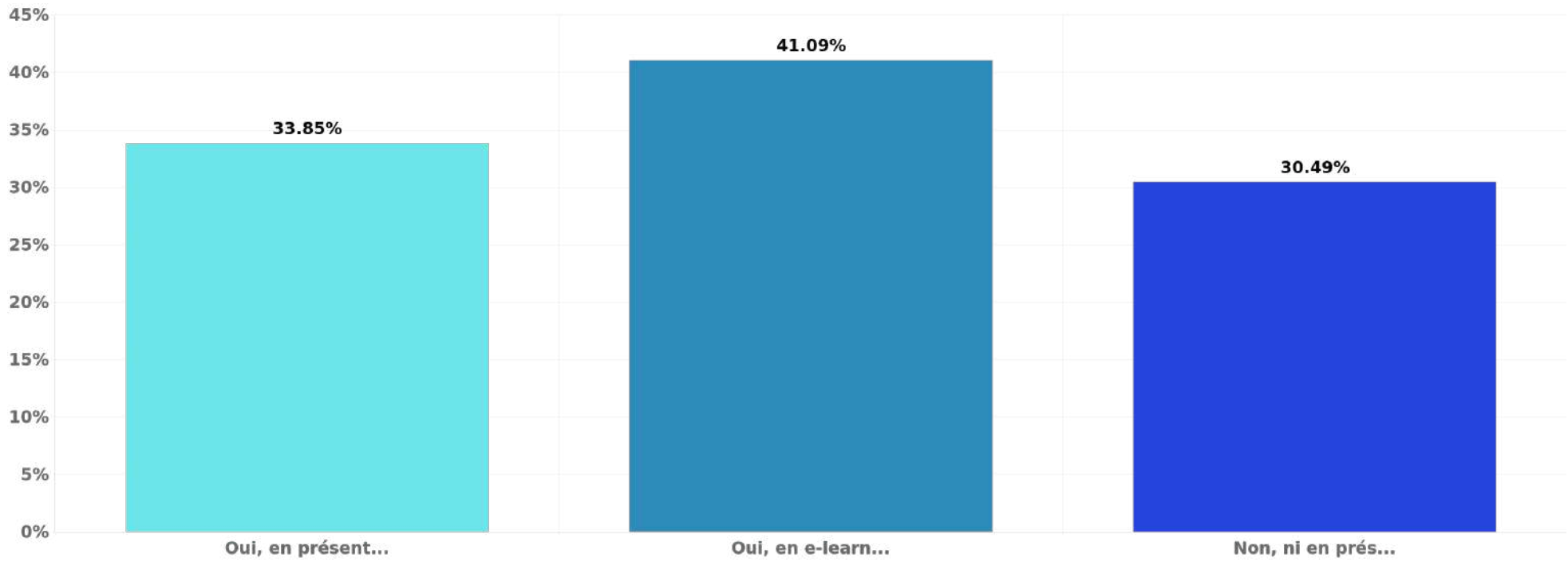
Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

47.Avez-vous participé à une formation à la cybersécurité au cours de l'année écoulée ?



Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

48.Si vous deviez suivre une formation à la cybersécurité dans les 6 prochains mois, que préféreriez-vous ?

Proposition des réponses	Effectif	Pourcentage
Une formation en présentiel	161	41.60%
Une formation en e-learning	179	46.25%
Aucun des deux	21	5.43%
Ne sait pas	26	6.72%
Total	387	100.00%

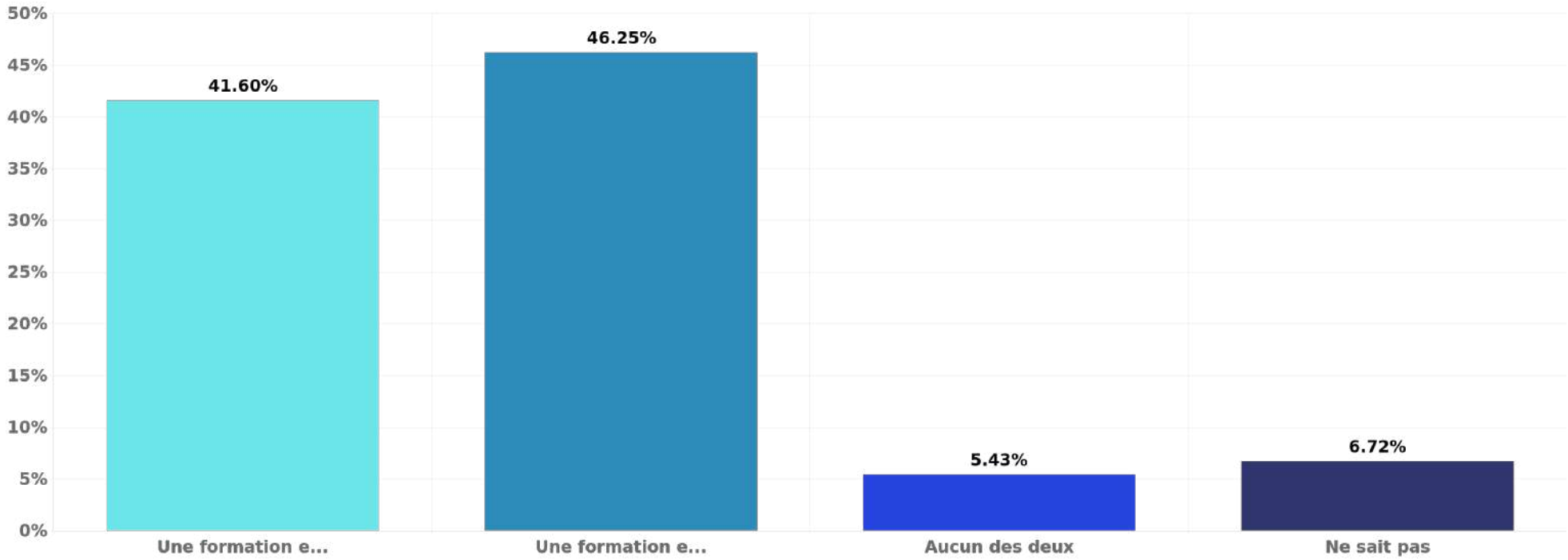
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

48.Si vous deviez suivre une formation à la cybersécurité dans les 6 prochains mois, que préféreriez-vous ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

49.Quelle serait pour vous la durée idéale d'une formation à la cybersécurité ?

Proposition des réponses	Effectif	Pourcentage
2 heures	94	24.29%
4 heures	95	24.55%
1 journée	108	27.91%
2 journées	52	13.44%
Plus de 2 journées	38	9.82%
Total	387	100.00%

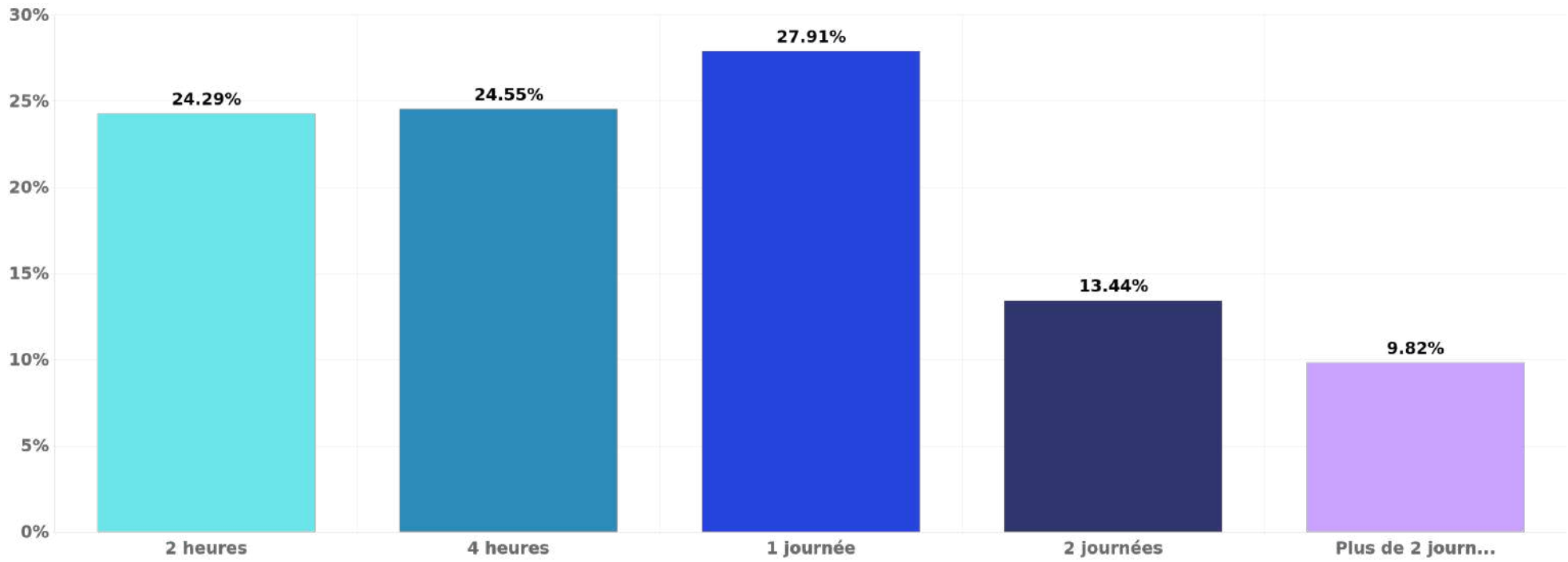
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

49.Quelle serait pour vous la durée idéale d'une formation à la cybersécurité ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

50.Pour vous former à la cybersécurité, êtes-vous favorable à :

Question 50	Oui, plutôt	Non, plutôt pas
Utiliser votre Compte Personnel de Formation (CPF)	51.94%	48.06%
Suivre la formation dispensée par mon entreprise	87.34%	12.66%
Suivre une formation certifiante	73.90%	26.10%
Vous former sur votre temps libre	40.83%	59.17%

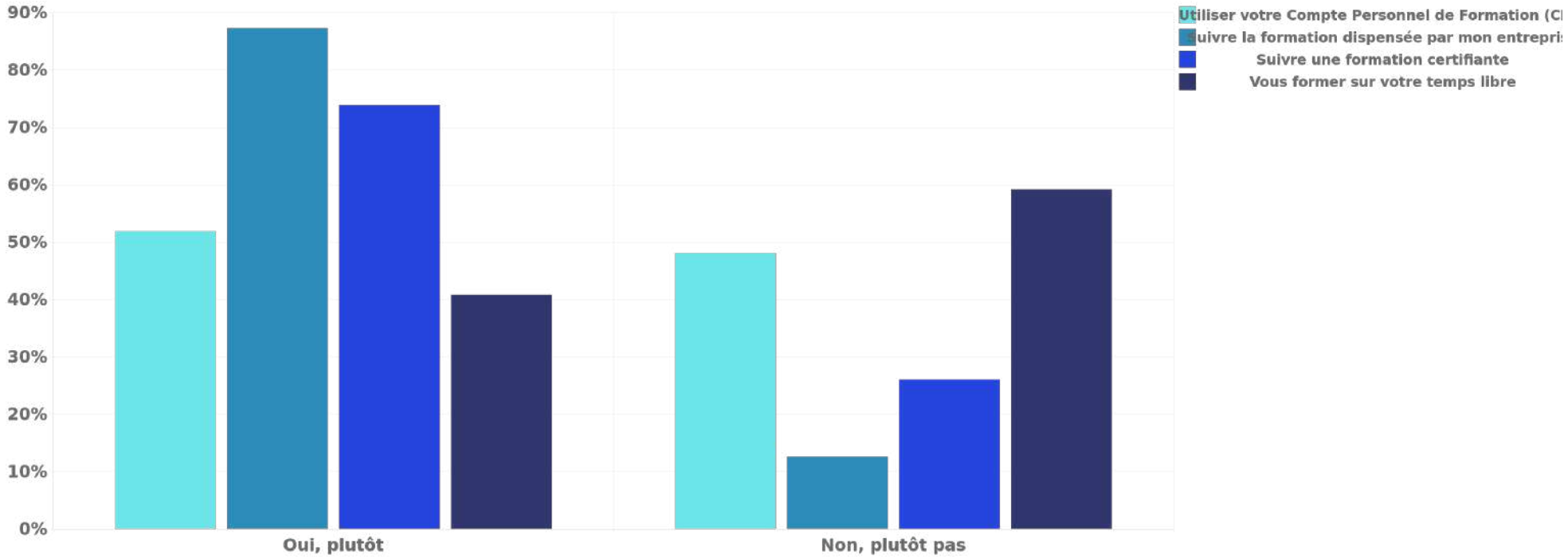
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

50.Pour vous former à la cybersécurité, êtes-vous favorable à :



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

51.Diriez-vous que votre environnement de travail favorise le développement de l'innovation ouverte ?

Proposition des réponses	Effectif	Pourcentage
Oui, tout à fait	75	19.38%
Oui, plutôt	197	50.90%
Ni oui, ni non	84	21.71%
Non, plutôt pas	22	5.68%
Non, pas du tout	9	2.33%
Total	387	100.00%

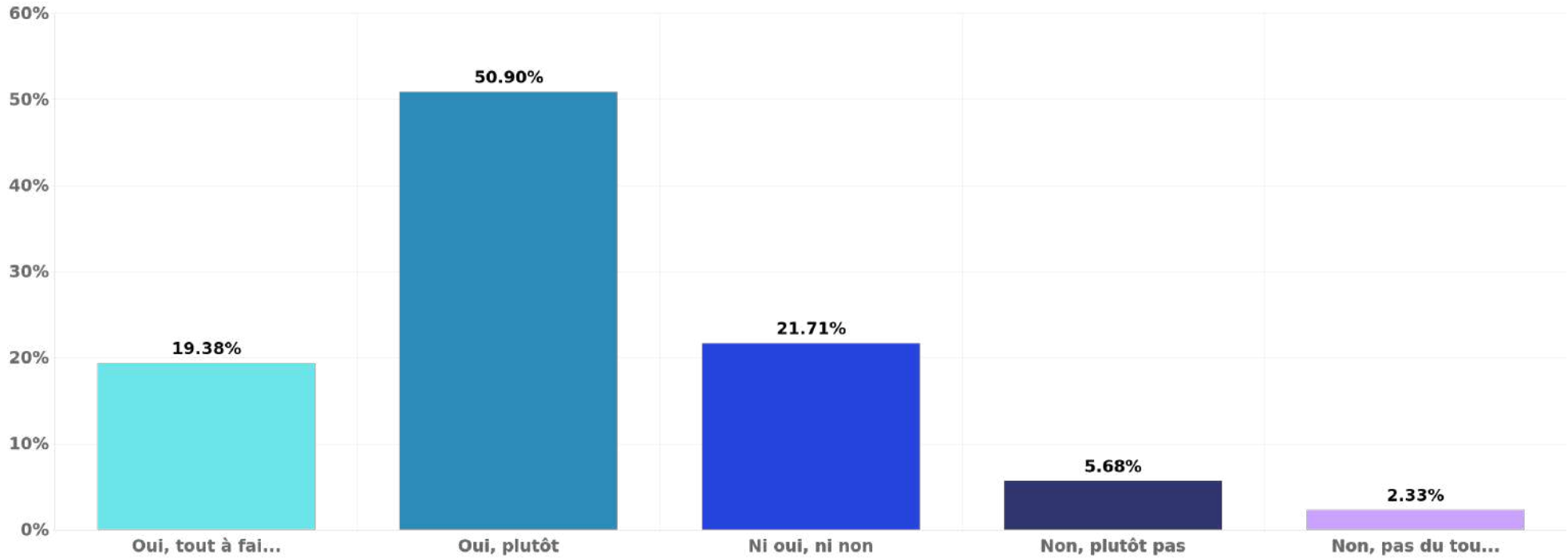
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

51.Diriez-vous que votre environnement de travail favorise le développement de l'innovation ouverte ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

52.Vous arrive-t-il de prendre l'initiative de partager des connaissances, des conseils sur la cybersécurité et d'encourager des pratiques sécuritaires dans votre entreprise ?

Proposition des réponses	Effectif	Pourcentage
Très souvent	86	22.22%
Parfois	191	49.35%
Rarement	67	17.31%
Jamais	43	11.11%
Total	387	100.00%

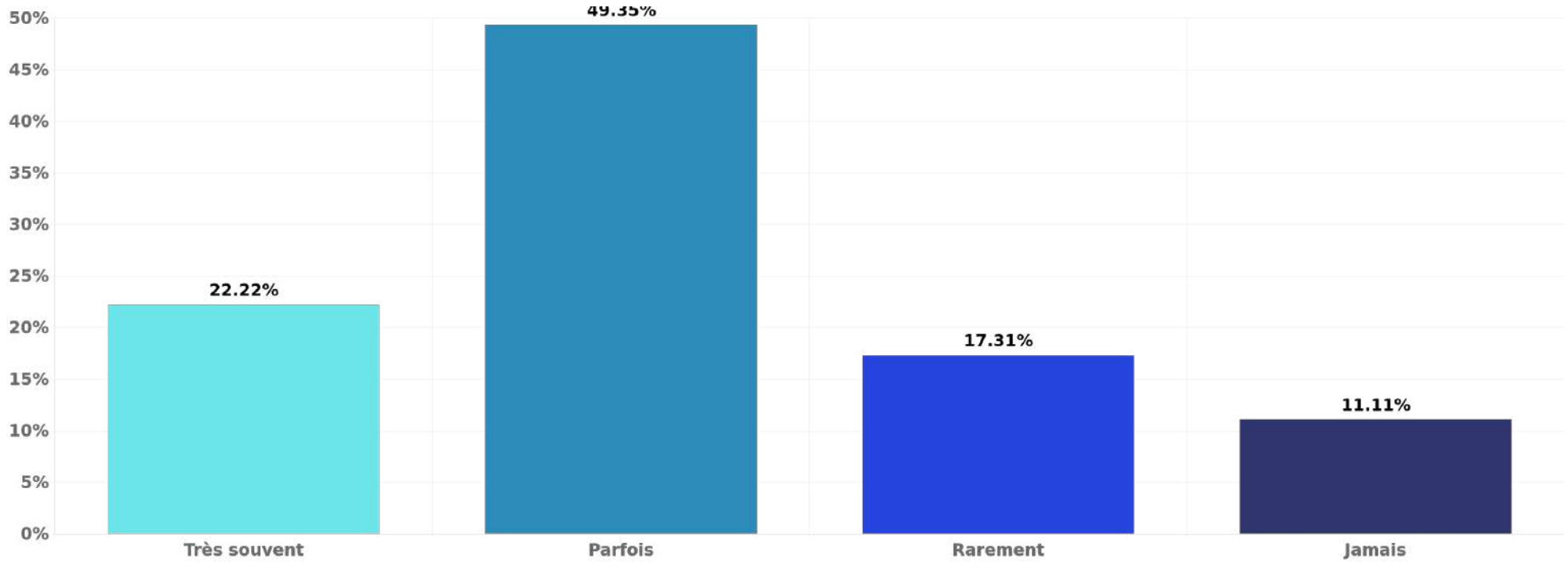
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

52.Vous arrive-t-il de prendre l'initiative de partager des connaissances, des conseils sur la cybersécurité et d'encourager des pratiques sécuritaires dans votre entreprise ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

53.Avec l'évolution des cyberattaques, il est important d'établir des points de contact au sein des entreprises pour sensibiliser à la sécurité informatique /cybersécurité. Seriez-vous prêt(e) à participer à cette initiative en tant qu'ambassadeur de la sécurité ?

Proposition des réponses	Effectif	Pourcentage
Oui	242	62.53%
Non	88	22.74%
Ne sait pas	57	14.73%
Total	387	100.00%

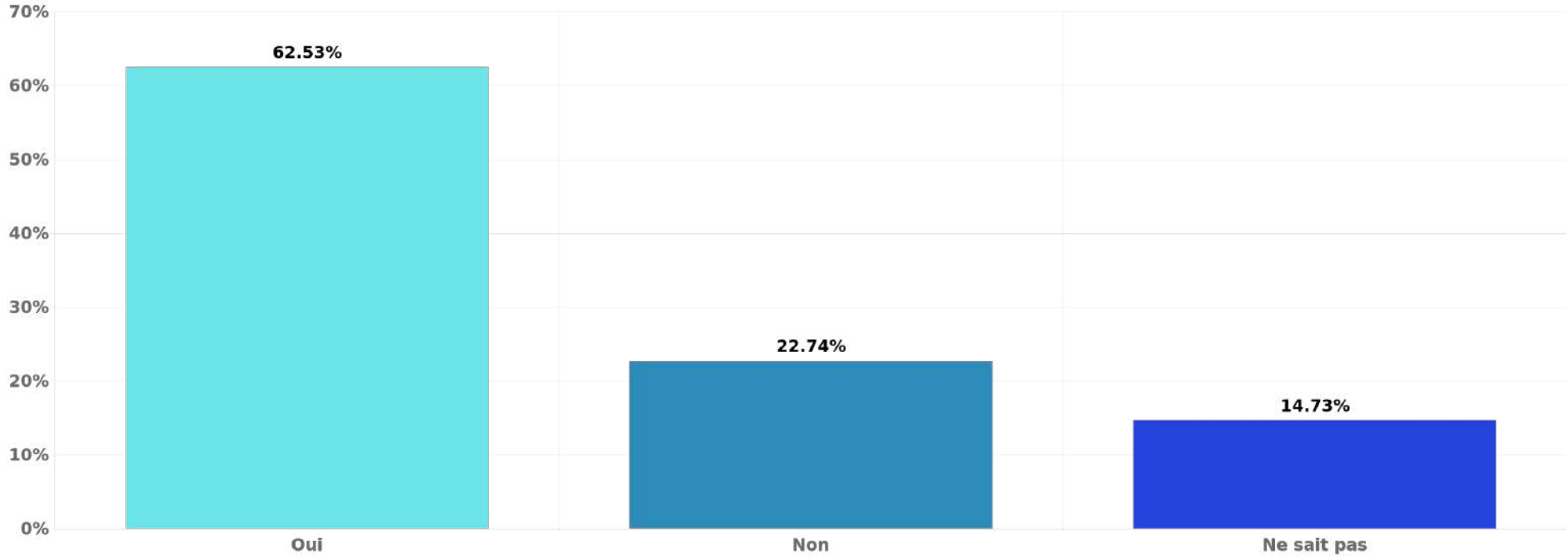
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

53.Avec l'évolution des cyberattaques, il est important d'établir des points de contact au sein des entreprises pour sensibiliser à la sécurité informatique /cybersécurité. Seriez-vous prêt(e) à participer à cette initiative en tant qu'ambassadeur de la sécurité ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

54.Comment évaluez-vous l'efficacité de vos managers et de la direction en tant qu'ambassadeurs de la cybersécurité dans votre entreprise ?

Question 54	1 - Très efficace	2 - Plutôt efficace	3 - Neutre	4 - Plutôt pas efficace	5 - Pas du tout efficace
Leur niveau de sensibilisation à l'importance de la cybersécurité	25.06%	43.93%	21.45%	6.72%	2.84%
Leur compréhension des menaces cybernétiques	20.67%	45.74%	23.26%	8.01%	2.33%
Leur capacité à distinguer entre des comportements sécurisés et risqués	19.64%	47.29%	23.26%	7.49%	2.33%
Leurs efforts pour sensibiliser les employés aux mesures de sécurité	19.38%	45.22%	22.48%	9.30%	3.62%
Leur implication dans la planification et la mise en œuvre de projets, avec une attention particulière aux risques de cybersécurité	23.77%	42.64%	24.29%	6.20%	3.10%
La qualité de leur coopération avec l'équipe de sécurité informatique	26.10%	43.93%	22.74%	5.17%	2.07%
Leur leadership influent et leur capacité à fournir des conseils pertinents en matière de cybersécurité	19.90%	42.89%	26.36%	7.75%	3.10%
Leur aptitude à répondre aux interrogations des employés ou à les orienter vers des experts	19.64%	49.10%	20.67%	8.53%	2.07%
Leur engagement continu envers les valeurs de la cybersécurité	23.26%	43.41%	24.55%	6.20%	2.58%
Leur encouragement envers le personnel pour l'apprentissage et l'application des techniques de cybersécurité	23.26%	45.22%	22.48%	6.20%	2.84%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

55.Quelles sont les stratégies à privilégier pour stimuler l'intelligence collective en matière de cybersécurité ?

Proposition des réponses	Effectif	Pourcentage
Instaurer une culture d'entreprise qui valorise la sécurité et la cybersécurité.	116	29.97%
Développer des programmes de formation en cybersécurité adaptés au profil de chaque employé.	112	28.94%
Sensibiliser spécifiquement chaque service de l'entreprise à la cybersécurité.	124	32.04%
Tisser des liens solides entre les équipes dédiées à la sécurité et tous les salariés.	92	23.77%
Assurer une veille technologique et réglementaire constante pour l'équipe de sécurité.	118	30.49%
Mettre en place une cellule de crise interdépartementale et interfiliale.	70	18.09%
Promouvoir le partage de savoir-faire en matière de sécurité avec les fournisseurs et partenaires.	84	21.71%
S'engager en faveur de la formation continue des équipes de sécurité et des prestataires externes.	101	26.10%
Encourager une ouverture d'esprit via des visioconférences dédiées à la sécurité.	72	18.60%
Stimuler la curiosité intellectuelle pour les meilleures pratiques en informatique.	88	22.74%

Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

55.Quelles sont les stratégies à privilégier pour stimuler l'intelligence collective en matière de cybersécurité ?

Proposition des réponses	Effectif	Pourcentage
Inculquer une vigilance permanente lors de l'utilisation de réseaux connectés.	87	22.48%
Clarifier les risques et conséquences liés aux différents usages informatiques.	113	29.20%
Établir des mesures de sécurité de base à mettre en place au domicile des employés.	98	25.32%
Concevoir des formations en cybersécurité qui intègrent les aspects de l'intelligence artificielle.	112	28.94%
Former les équipes en fonction des applications utilisées et de leur environnement numérique.	122	31.52%
Organiser des simulations d'attaques de phishing pour tester la réactivité des employés.	123	31.78%
Instituer une heure annuelle de « blackout » par service pour sensibiliser au risque de dépendance au numérique.	61	15.76%
Prévoir des journées dédiées à la sensibilisation à la sécurité et à la cybersécurité.	108	27.91%
Proposer des sessions informelles de formation à la sécurité pendant le déjeuner en télétravail (choix libre).	83	21.45%
Diffuser un podcast sur la sécurité et les cyberattaques, accessible lors des trajets quotidiens (choix libre).	51	13.18%

Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

55.Quelles sont les stratégies à privilégier pour stimuler l'intelligence collective en matière de cybersécurité ?

Proposition des réponses	Effectif	Pourcentage
Total	387	100.00%

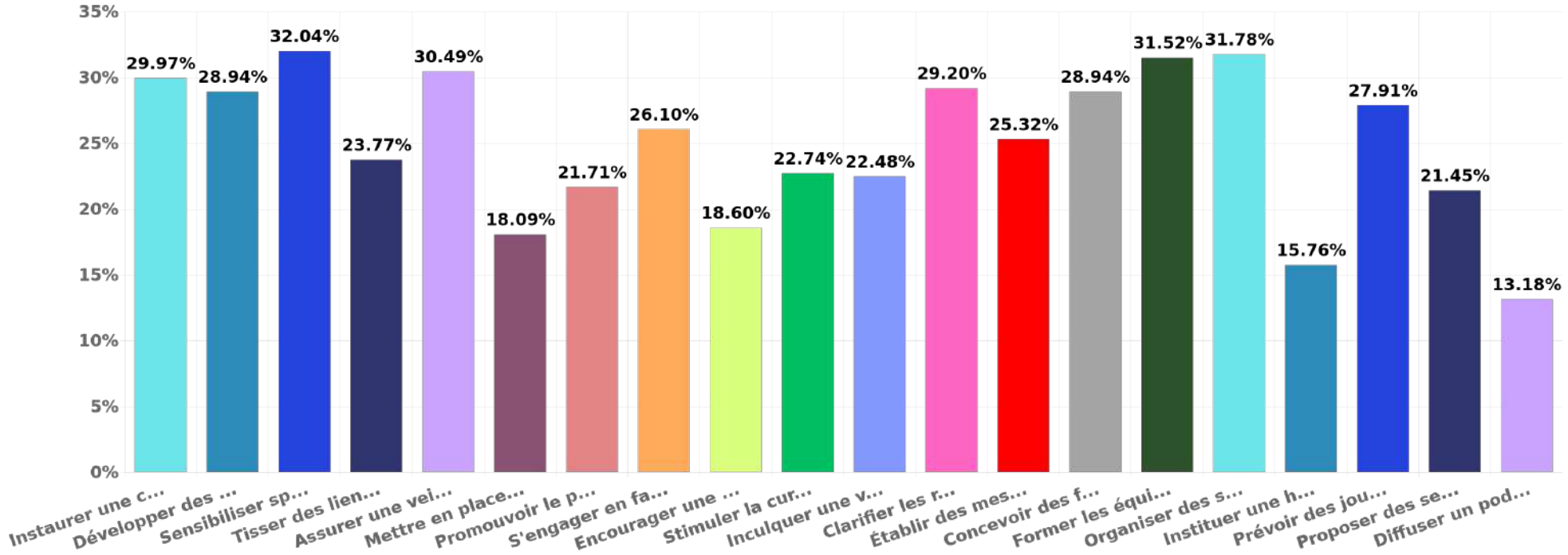
Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

55.Quelles sont les stratégies à privilégier pour stimuler l'intelligence collective en matière de cybersécurité ?



Type de question : Choix multiples

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

Résultats

56.Les neurosciences cognitives sont le domaine de recherche dans lequel sont étudiés les mécanismes neurobiologiques qui sous-tendent la cognition (perception, motricité, langage, mémoire, raisonnement, émotions). Qu'en savez-vous ?

Proposition des réponses	Effectif	Pourcentage
Je connais bien ce sujet (connaissances précises)	80	20.67%
J'en ai entendu parler (connaissances vagues)	221	57.11%
Je ne sais pas de quoi il s’agit	86	22.22%
Total	387	100.00%

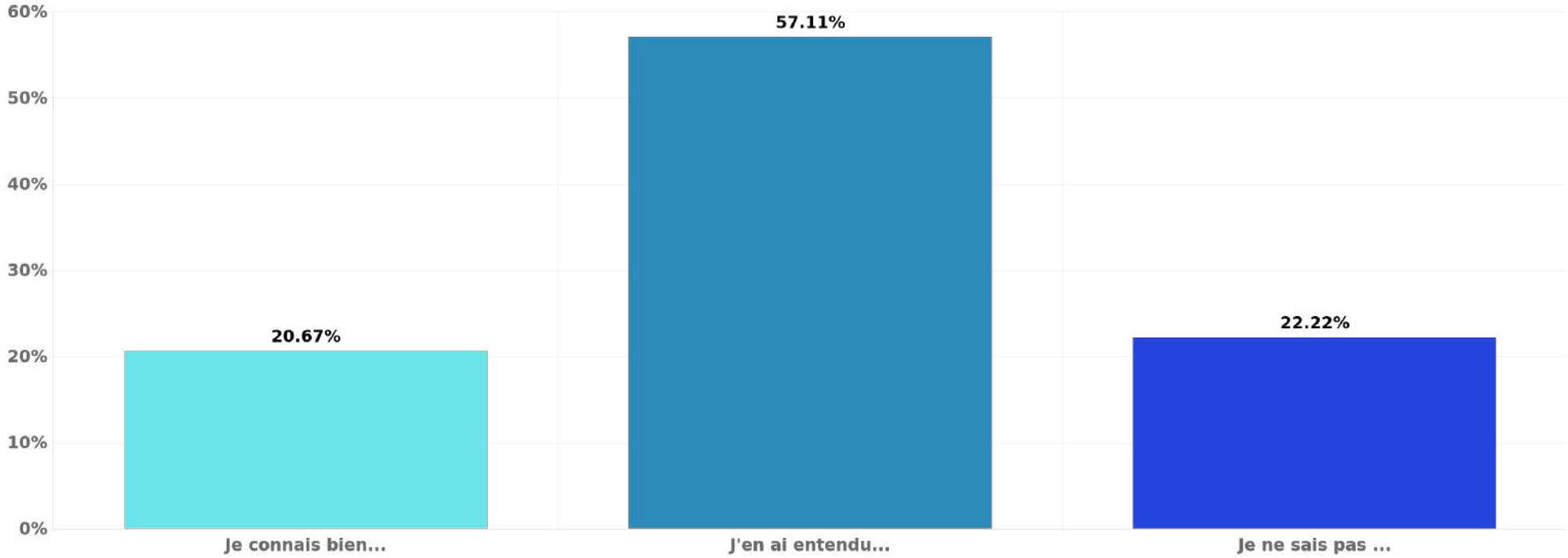
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

56.Les neurosciences cognitives sont le domaine de recherche dans lequel sont étudiés les mécanismes neurobiologiques qui sous-tendent la cognition (perception, motricité, langage, mémoire, raisonnement, émotions). Qu'en savez-vous ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

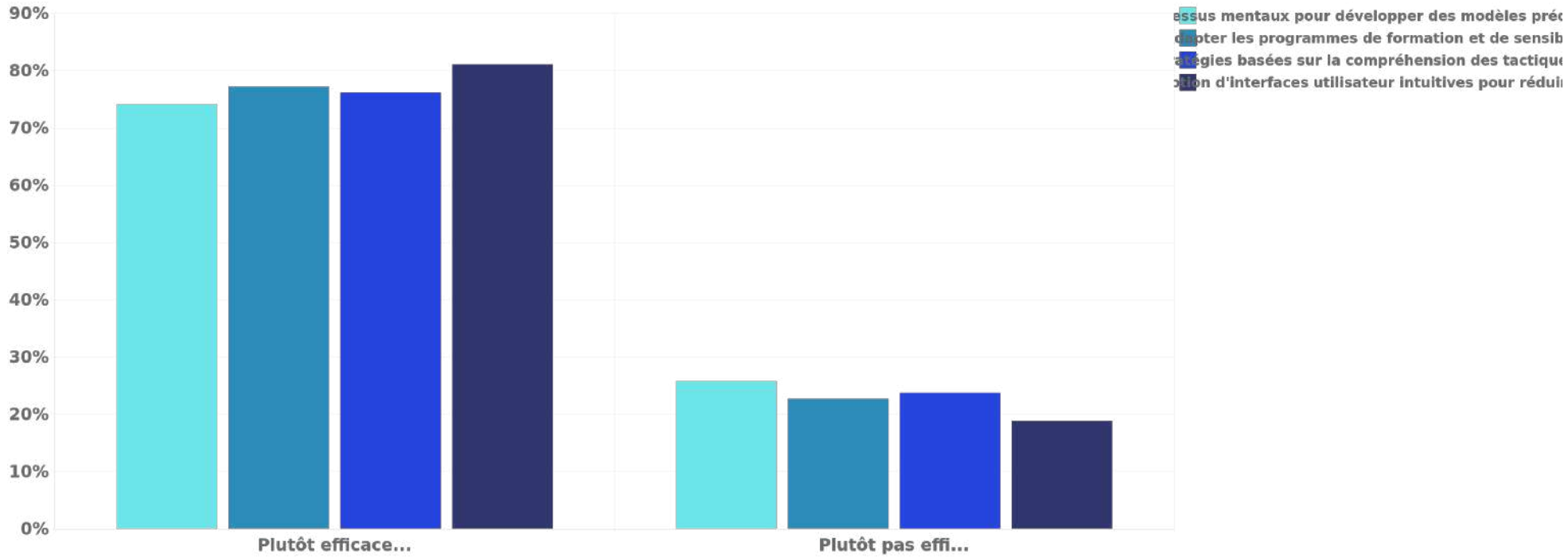
57.Comment évaluez-vous l'efficacité des stratégies suivantes basées sur les neurosciences cognitives en matière de cybersécurité ?

Question 57	Plutôt efficaces	Plutôt pas efficaces
Détection avancée des menaces : Comprendre les processus mentaux pour développer des modèles prédictifs qui identifient les comportements en ligne suspects.	74.16%	25.84%
Renforcement de la sensibilisation à la sécurité : Adapter les programmes de formation et de sensibilisation aux caractéristiques cognitives des individus.	77.26%	22.74%
Protection contre l'ingénierie sociale : Développer des stratégies basées sur la compréhension des tactiques de persuasion pour contrer les tentatives de manipulation.	76.23%	23.77%
Amélioration de l'expérience utilisateur sécurisée : Conception d'interfaces utilisateur intuitives pour réduire les erreurs humaines et les vulnérabilités en cybersécurité.	81.14%	18.86%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

57.Comment évaluez-vous l'efficacité des stratégies suivantes basées sur les neurosciences cognitives en matière de cybersécurité ?



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

58.Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant l'impact des neurosciences sur les programmes de formation en cybersécurité ?

Question 58	1 - Tout à fait d'accord	2 - Plutôt d'accord	3 - Ni d'accord, ni pas d'accord	4 - Plutôt pas d'accord	5 - Pas du tout d'accord
Les programmes basés sur les neurosciences permettent une personnalisation plus efficace de l'apprentissage, améliorant la rétention des informations et des compétences en cybersécurité.	23.51%	48.06%	24.29%	2.33%	1.81%
L'utilisation des principes neuroscientifiques augmente l'engagement et la motivation des apprenants en cybersécurité.	20.41%	43.15%	31.78%	3.62%	1.03%
Les techniques inspirées des neurosciences améliorent les compétences de résolution de problèmes dans des situations de cybersécurité complexes.	20.41%	46.77%	29.97%	2.07%	0.78%
Une meilleure compréhension du fonctionnement cérébral aide à réduire les erreurs humaines et les vulnérabilités comportementales en cybersécurité.	25.32%	46.51%	23.51%	3.62%	1.03%

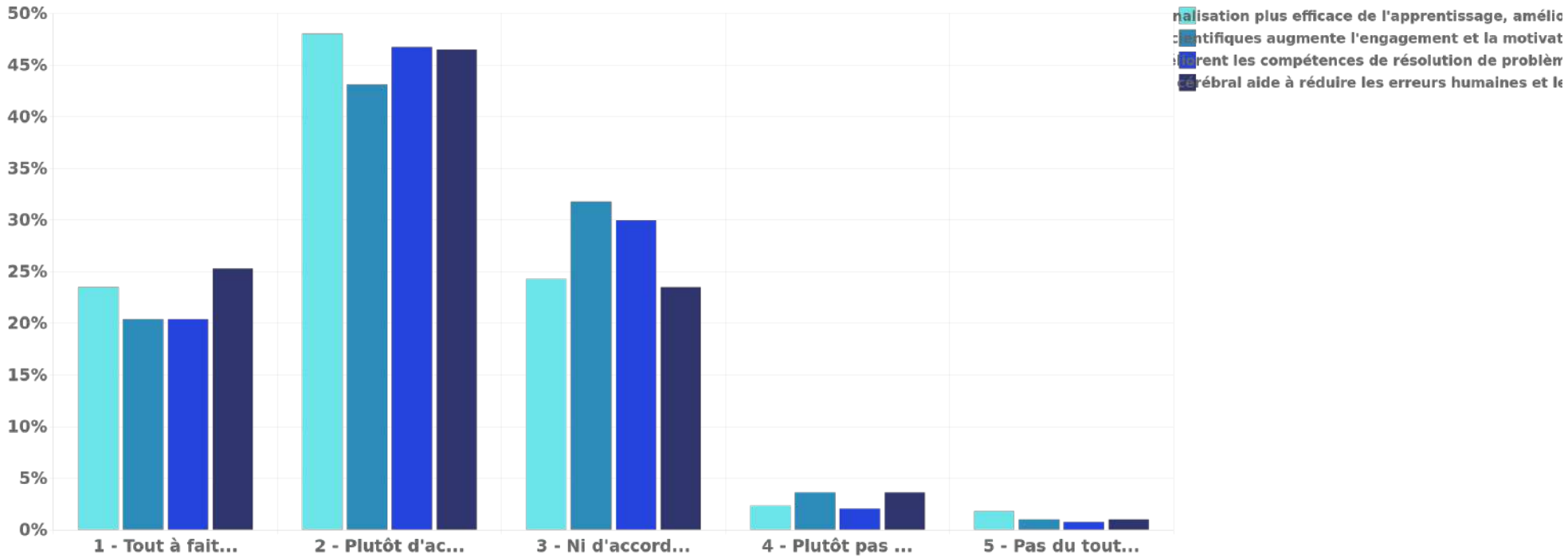
Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

58.Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant l'impact des neurosciences sur les programmes de formation en cybersécurité ?



Type de question : Matrice

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

59.Dans quelle mesure êtes-vous satisfait du contenu des formations cybersécurité proposé par les RH/DSI ?

Proposition des réponses	Effectif	Pourcentage
Très satisfait	51	13.18%
Plutôt satisfait	213	55.04%
Neutre	87	22.48%
Pas vraiment satisfait	32	8.27%
Pas du tout satisfait	4	1.03%
Total	387	100.00%

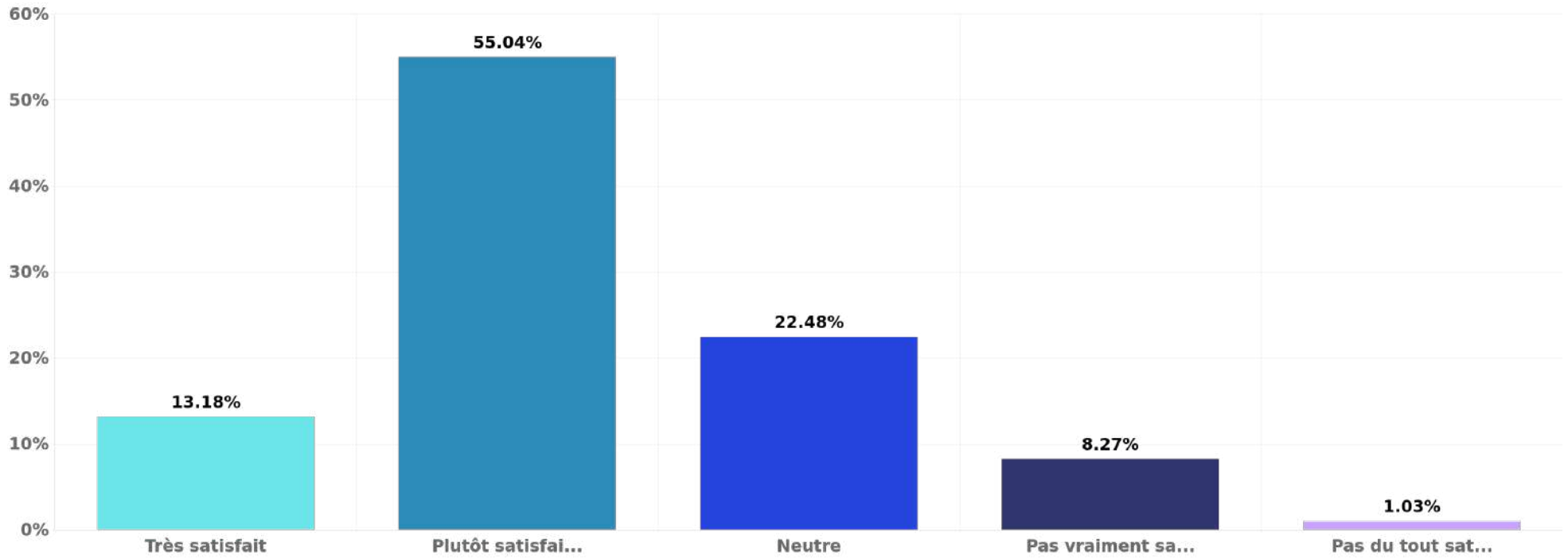
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

59.Dans quelle mesure êtes-vous satisfait du contenu des formations cybersécurité proposé par les RH/DSI ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

60.Dans votre quotidien, estimez-vous que vous mettez en œuvre efficacement les bonnes postures de cybersécurité pour vous protéger (contre les virus, le piratage, les arnaques en ligne, etc.) ?

Proposition des réponses	Effectif	Pourcentage
Tout à fait d'accord	85	21.96%
Plutôt d'accord	224	57.88%
Ni d'accord, ni pas d'accord	53	13.70%
Pas vraiment d'accord	23	5.94%
Pas du tout d'accord	2	0.52%
Total	387	100.00%

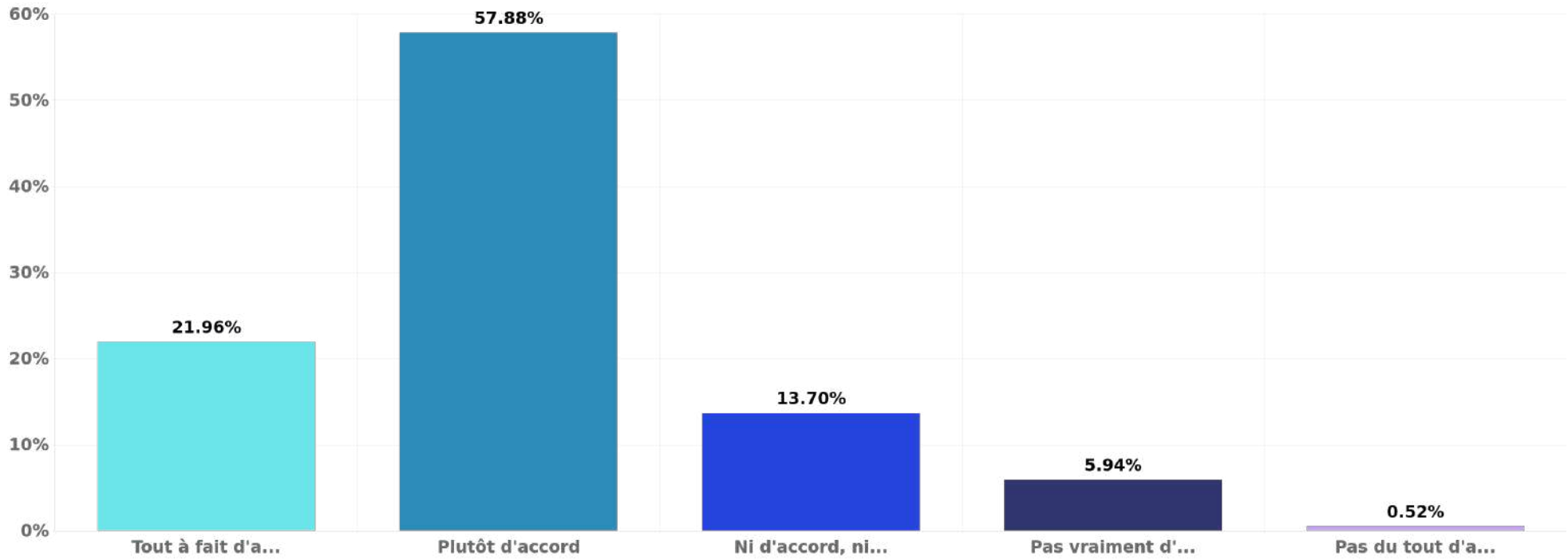
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

60.Dans votre quotidien, estimez-vous que vous mettez en œuvre efficacement les bonnes postures de cybersécurité pour vous protéger (contre les virus, le piratage, les arnaques en ligne, etc.) ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

61.Comment évaluez-vous l'efficacité de vos managers en tant qu'ambassadeurs de la cybersécurité dans votre service ?

Question 61	1 - Très efficace	2 - Plutôt efficace	3 - Ni efficace, ni pas efficace	4 - Plutôt pas efficace	5 - Pas du tout efficace
Leur niveau de sensibilisation à l'importance de la cybersécurité.	21.45%	44.70%	23.26%	7.75%	2.84%
Leur compréhension des menaces cybernétiques.	18.09%	44.96%	24.29%	9.30%	3.36%
Leur capacité à distinguer entre des comportements sécurisés et risqués.	22.22%	46.51%	19.90%	8.79%	2.58%
Leurs efforts pour sensibiliser les employés aux mesures de sécurité.	24.29%	41.86%	21.96%	8.27%	3.62%
Leur implication dans la planification et la mise en œuvre de projets, avec une attention particulière aux risques de cybersécurité.	22.48%	41.86%	25.32%	7.24%	3.10%
La qualité de leur coopération avec l'équipe de sécurité informatique.	22.74%	45.99%	20.16%	8.53%	2.58%
Leur leadership influent et leur capacité à fournir des conseils pertinents en matière de cybersécurité.	19.64%	40.57%	25.32%	10.08%	4.39%
Leur aptitude à répondre aux interrogations des employés ou à les orienter vers des experts.	20.41%	45.22%	21.19%	10.34%	2.84%
Leur engagement continu envers les valeurs de la cybersécurité.	19.38%	45.48%	25.06%	7.24%	2.84%

Type de question : Matrice Nombre de répondants à cette question : 387 Nombre de répondants à cette question : 0

Résultats

62.Si vous travaillez dans le domaine de la cybersécurité, vous considérez-vous comme un expert légitime dans ce domaine ?

Proposition des réponses	Effectif	Pourcentage
Oui	122	31.52%
Non	109	28.17%
Je ne travaille pas dans le domaine de la cybersécurité.	156	40.31%
Total	387	100.00%

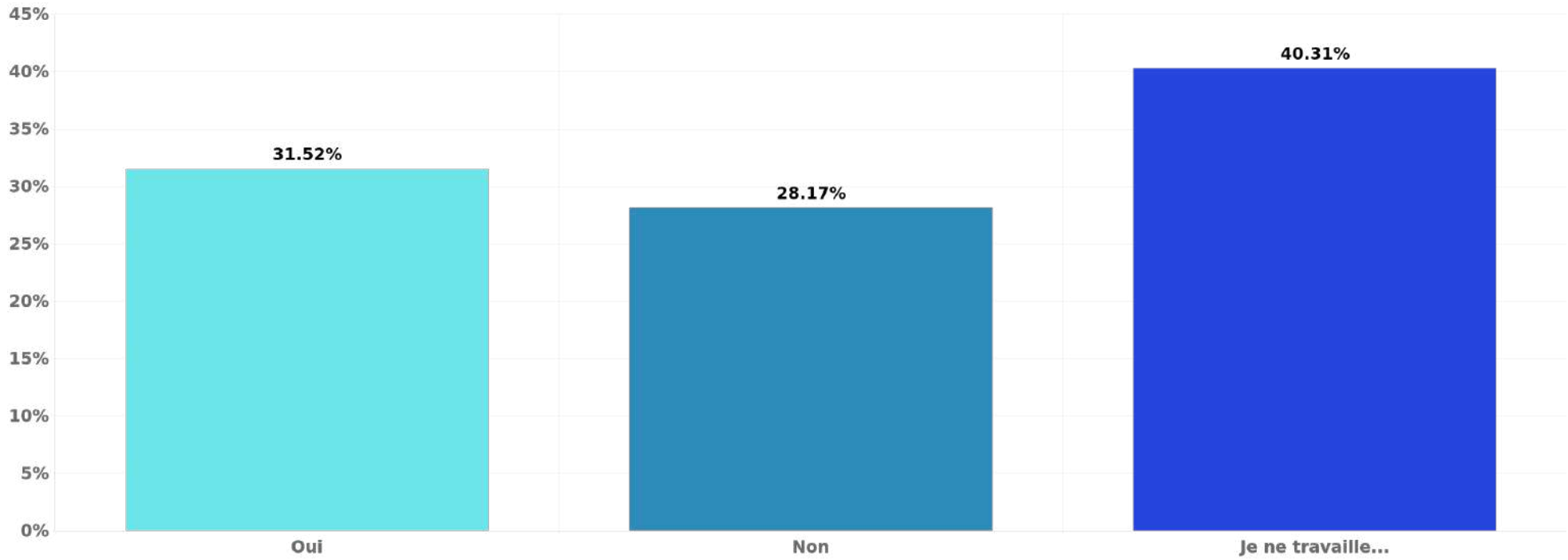
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

62.Si vous travaillez dans le domaine de la cybersécurité, vous considérez-vous comme un expert légitime dans ce domaine ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

63.Quel est votre niveau d'anglais ?

Proposition des réponses	Effectif	Pourcentage
Débutant	73	18.86%
Intermédiaire	172	44.44%
Avancé	120	31.01%
Langue maternelle ou bilingue	22	5.68%
Total	387	100.00%

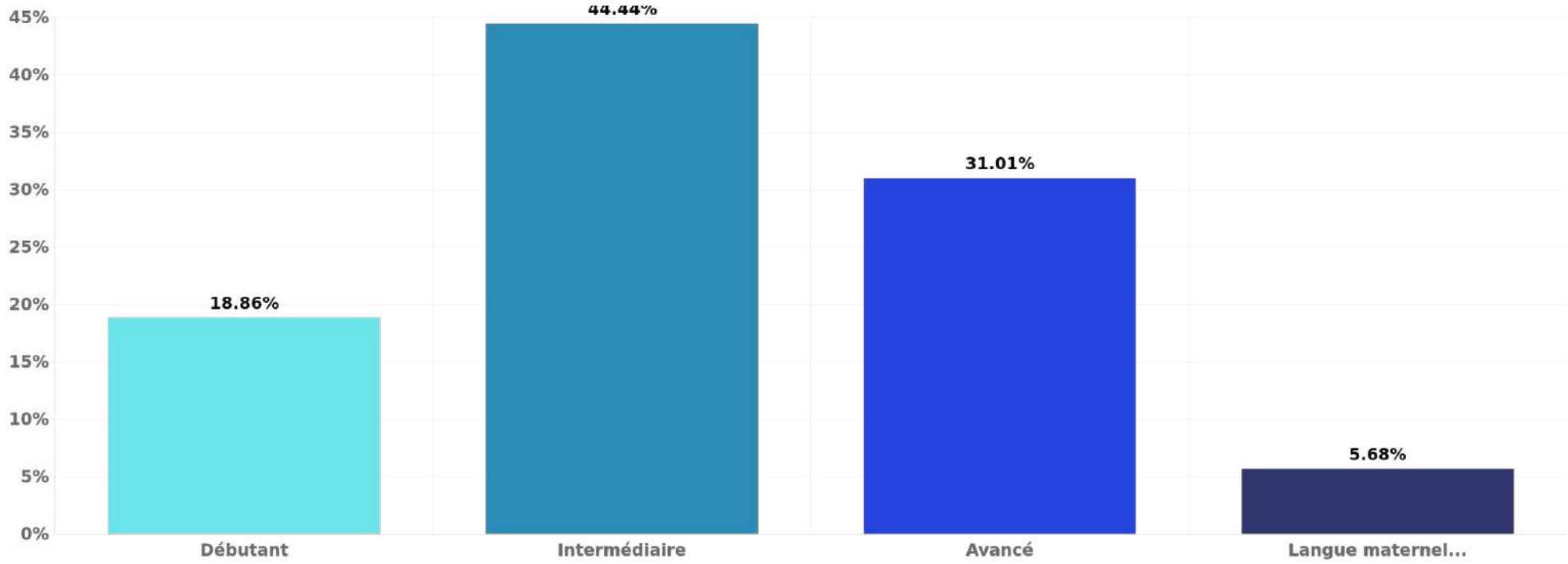
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

63.Quel est votre niveau d'anglais ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

64.Quel est le plus haut niveau de diplôme que vous avez obtenu ?

Proposition des réponses	Effectif	Pourcentage
Sans diplôme	0	0.00%
Diplôme National du Brevet (DNB)	3	0.78%
Baccalauréat	50	12.99%
Diplôme Universitaire de Technologie (DUT)	25	6.49%
Brevet de Technicien Supérieur (BTS)	53	13.77%
Licence (L1, L2, L3)	78	20.26%
Master (M1, M2)	156	40.52%
Doctorat	20	5.19%
Other	2	0.52%
Total	387	100.00%

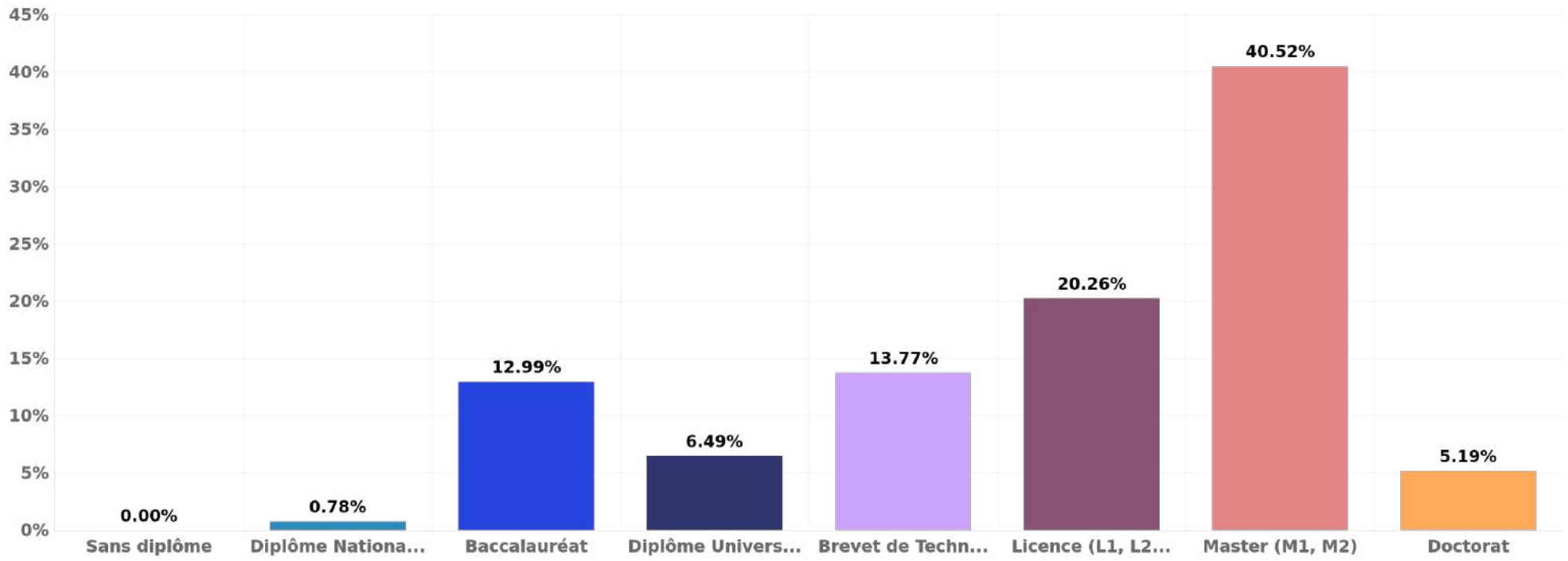
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

64.Quel est le plus haut niveau de diplôme que vous avez obtenu ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

65.Quelle est votre tranche d'âge ?

Proposition des réponses	Effectif	Pourcentage
19 ans ou moins	1	0.26%
20-39 ans	176	45.48%
40-59 ans	189	48.84%
60 ans ou plus	21	5.43%
Total	387	100.00%

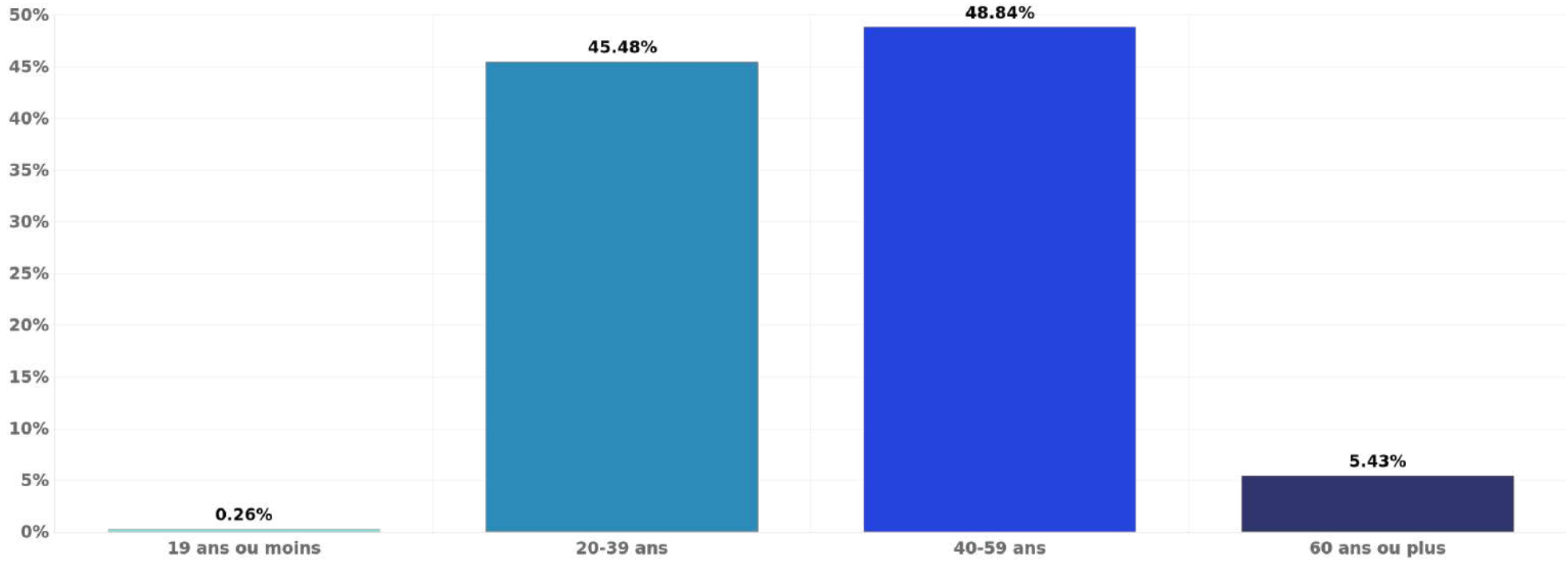
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

65.Quelle est votre tranche d'âge ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

66.Etes-vous ?

Proposition des réponses	Effectif	Pourcentage
Un homme	208	53.75%
Une femme	179	46.25%
Total	387	100.00%

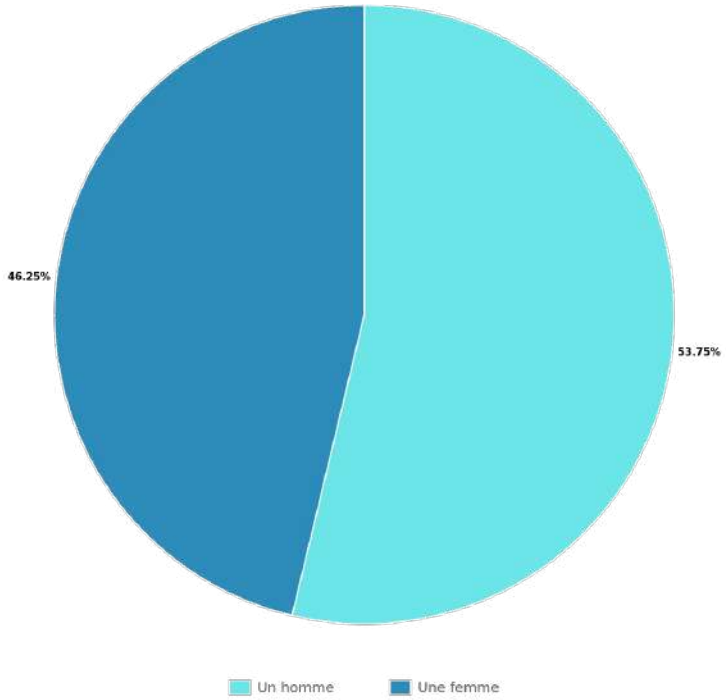
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

66.Etes-vous ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

67.Dans quelle région travaillez vous ?

Proposition des réponses	Effectif	Pourcentage
Auvergne-Rhône-Alpes	46	11.89%
Bourgogne-Franche-Comté	17	4.39%
Bretagne	13	3.36%
Centre-Val de Loire	7	1.81%
Corse	0	0.00%
Grand Est	31	8.01%
Hauts-de-France	40	10.34%
Île-de-France	106	27.39%
Normandie	17	4.39%
Nouvelle-Aquitaine	24	6.20%

Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

67.Dans quelle région travaillez vous ?

Proposition des réponses	Effectif	Pourcentage
Occitanie	42	10.85%
Pays de la Loire	18	4.65%
Provence-Alpes-Côte d'Azur	26	6.72%
Total	387	100.00%

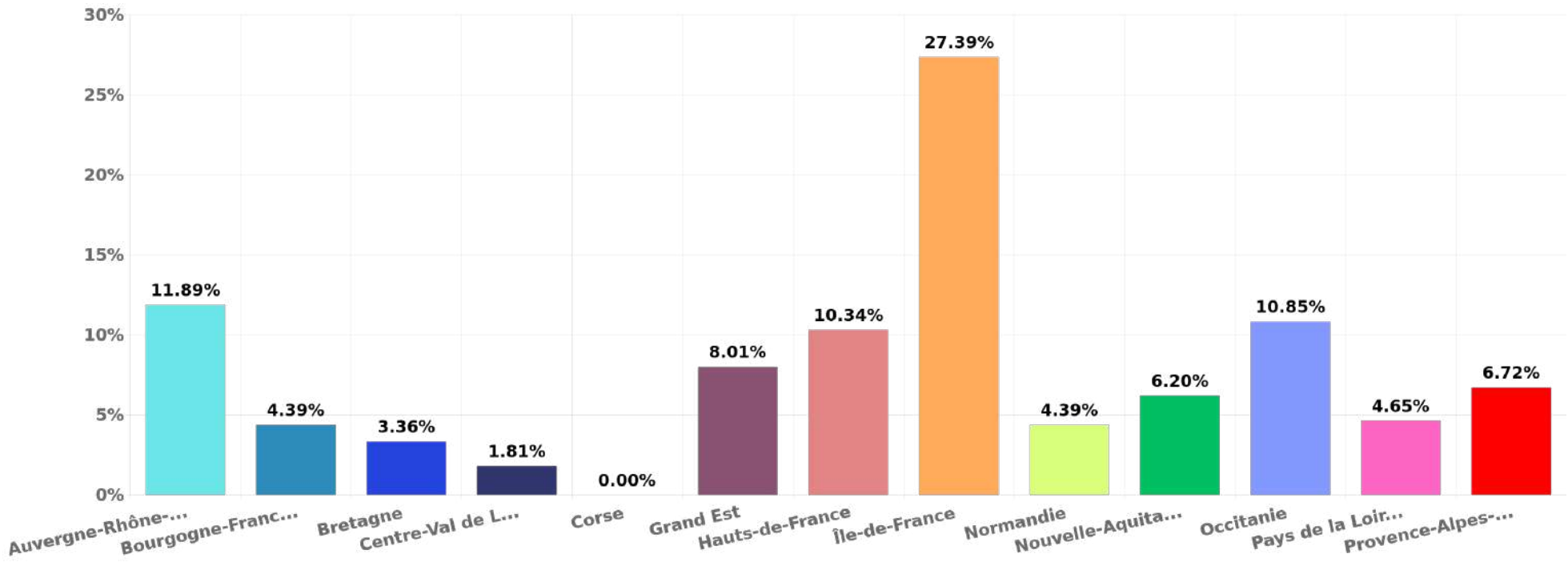
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

67.Dans quelle région travaillez vous ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

68.Quelle est votre ancienneté dans votre entreprise ?

Proposition des réponses	Effectif	Pourcentage
Moins d'un an	12	3.10%
De 1 à 3 ans inclus	62	16.02%
De 3 à 5 ans inclus	77	19.90%
De 5 à 10 ans inclus	85	21.96%
Plus de 10 ans	151	39.02%
Total	387	100.00%

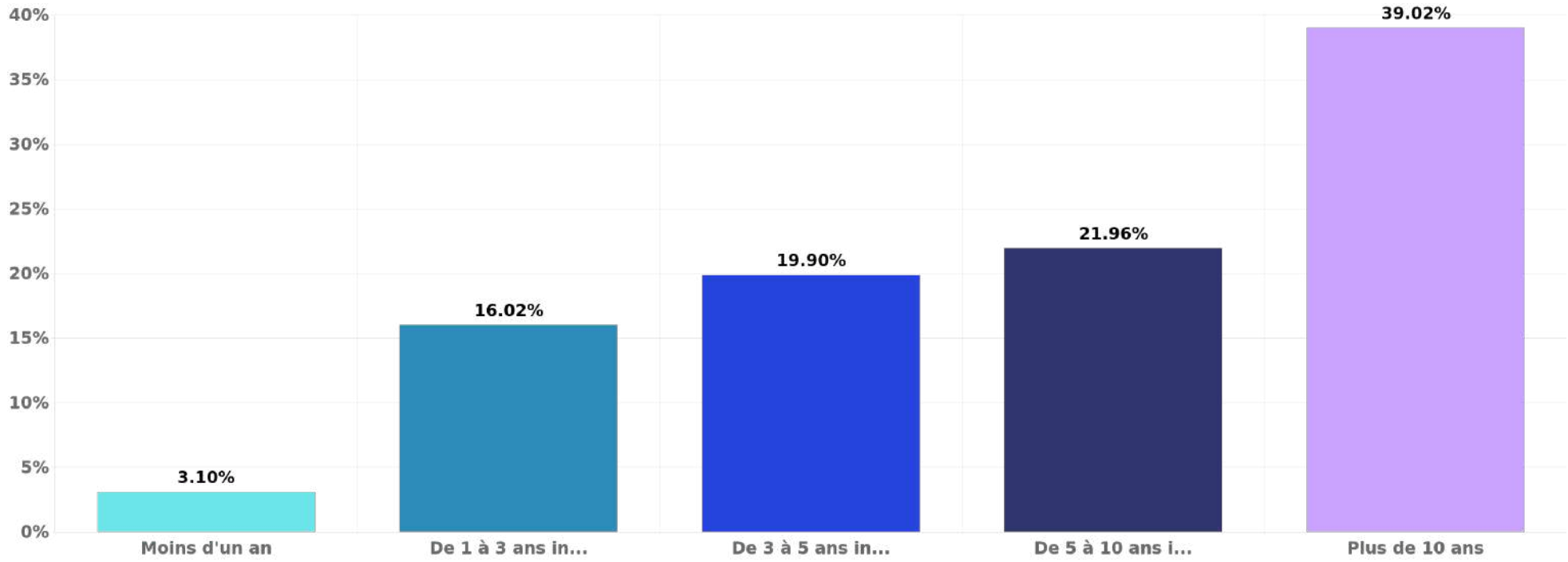
Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

68.Quelle est votre ancienneté dans votre entreprise ?



Type de question : Choix unique

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

69.Avez-vous des solutions ou suggestions pour booster la culture de la cybersécurité de votre entreprise ? C'est le moment de donner votre avis :

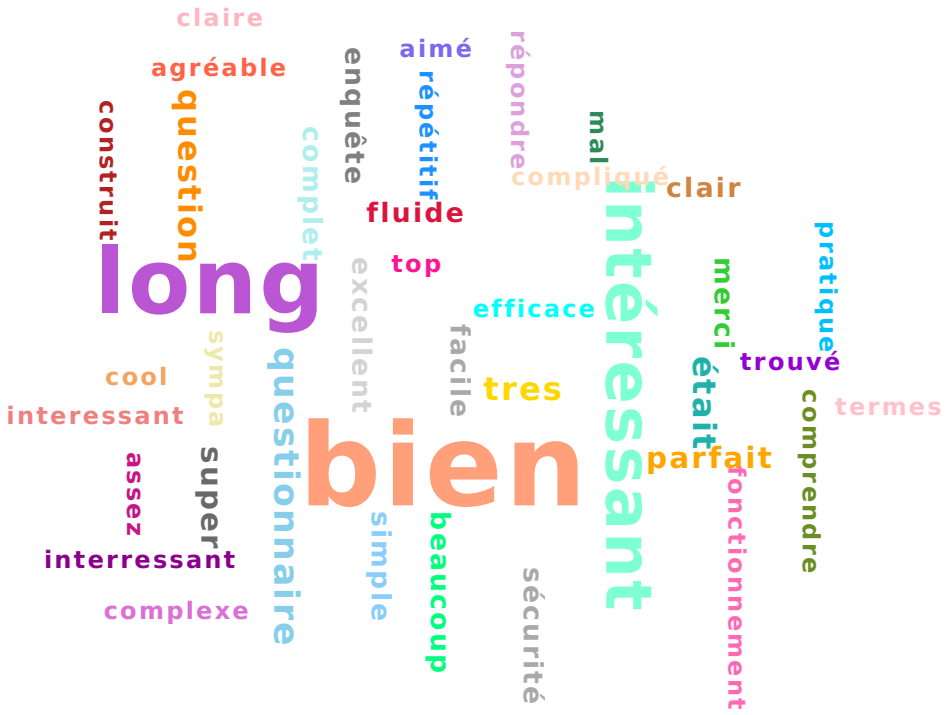
Type de question : Réponse ouverte

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0

Résultats

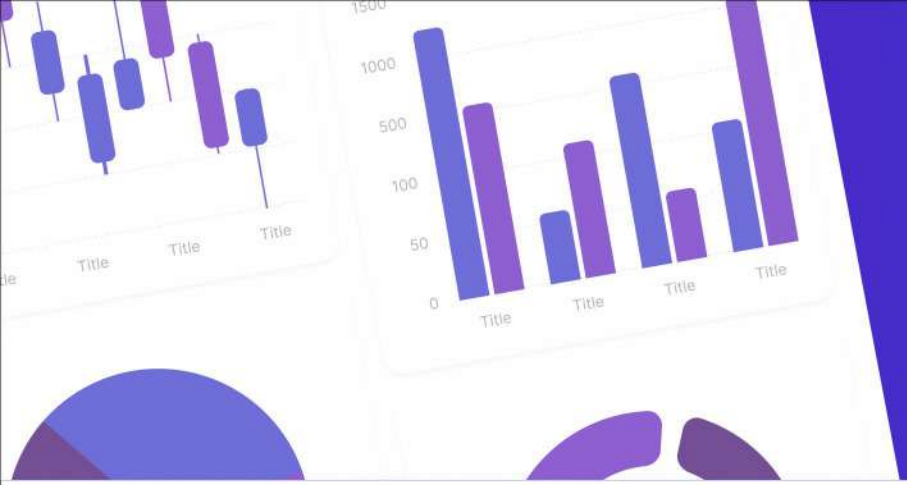
70.Qu'avez-vous pensé du fonctionnement de ce questionnaire ?



Type de question : Réponse ouverte

Nombre de répondants à cette question : 387

Nombre de répondants à cette question : 0



Mentions légales

Ce rapport a été généré automatiquement par la plateforme Selvitys. Il repose sur les données collectées lors de l'utilisation de notre solution de sondages en ligne. Grâce à nos algorithmes, nous analysons vos données et les mettons en forme pour produire des rapports qui offrent une vue d'ensemble précise et pertinente.

Pour toute question ou demande d'information, vous pouvez nous joindre aux coordonnées suivantes :

- Nom de la société : Selvitys
- Email : contact@selvitys.fr

L'administration du questionnaire a été effectuée entre le 25 septembre 2024 et 19 octobre 2024.

MÉTHODOLOGIE ET ÉCHANTILLONNAGE

TESTCYBER+ / QUALICREATIK

Selvitys

ÉCHANTILLON

Cette enquête a été réalisée auprès d'un échantillon **356 salarié(e)s du privé et du public, qui travaillent sur un ordinateur.**

CONTRÔLE QUALITÉ

Un **contrôle qualité** a été effectué sur l'ensemble des réponses collectées :

- Détection des réponses trop rapides
- Analyse de la cohérence des verbatims
- Analyse de la cohérence entre plusieurs variables
- Contrôle de l'adresse IP (afin d'éviter les doublons)

Les réponses jugées incohérentes ont été supprimées de la base de données de l'étude.

MODE DE COLLECTE

Sondage en ligne

DURÉE MOYENNE

26 minutes

DATES DE COLLECTE

Début : 25.09.24

Fin : 03.10.24

POUR TESTER LE SONDAGE

Veuillez cliquer ici.

PROFIL DES RÉPONDANTS

TESTCYBER+ / QUALICREATIK

Selvitys

SEXE

	%
Homme	55.34%
Femme	44.66%

TRANCHE D'ÂGES

	%
19 ans ou moins	0.28%
20-39 ans	45.22%
40-59 ans	48.88%
60 ans ou plus	5.62%

RÉGION

	%
Nord-Est	21.91%
Nord-Ouest	14.04%
Île-de-France	28.37%
Sud-Est	19.10%
Sud-Ouest	16.58%

NIVEAU DE DIPLÔME

	%
Sans diplôme	0.00%
Diplôme National du Brevet (DNB)	0.85%
Baccalauréat	11.58%
Diplôme Universitaire de Technologie (DUT)	6.50%
Brevet de Technicien Supérieur (BTS)	14.41%
Licence (L1, L2, L3)	21.47%
Master (M1, M2)	39.83%
Doctorat	5.37%
Other	0.56%

CATÉGORIE SOCIOPROFESSIONNELLE

	%
Salarié en entreprise (privé/public)	100%
Artisan, commerçant, profession libérale, indépendant	0.00%
Chef d'entreprise	0.00%
Etudiant	0.00%
Retraité	0.00%
Demandeur d'emploi	0.00%

PROFIL DES RÉPONDANTS

TESTCYBER+ / QUALICREATIK

Selvitys

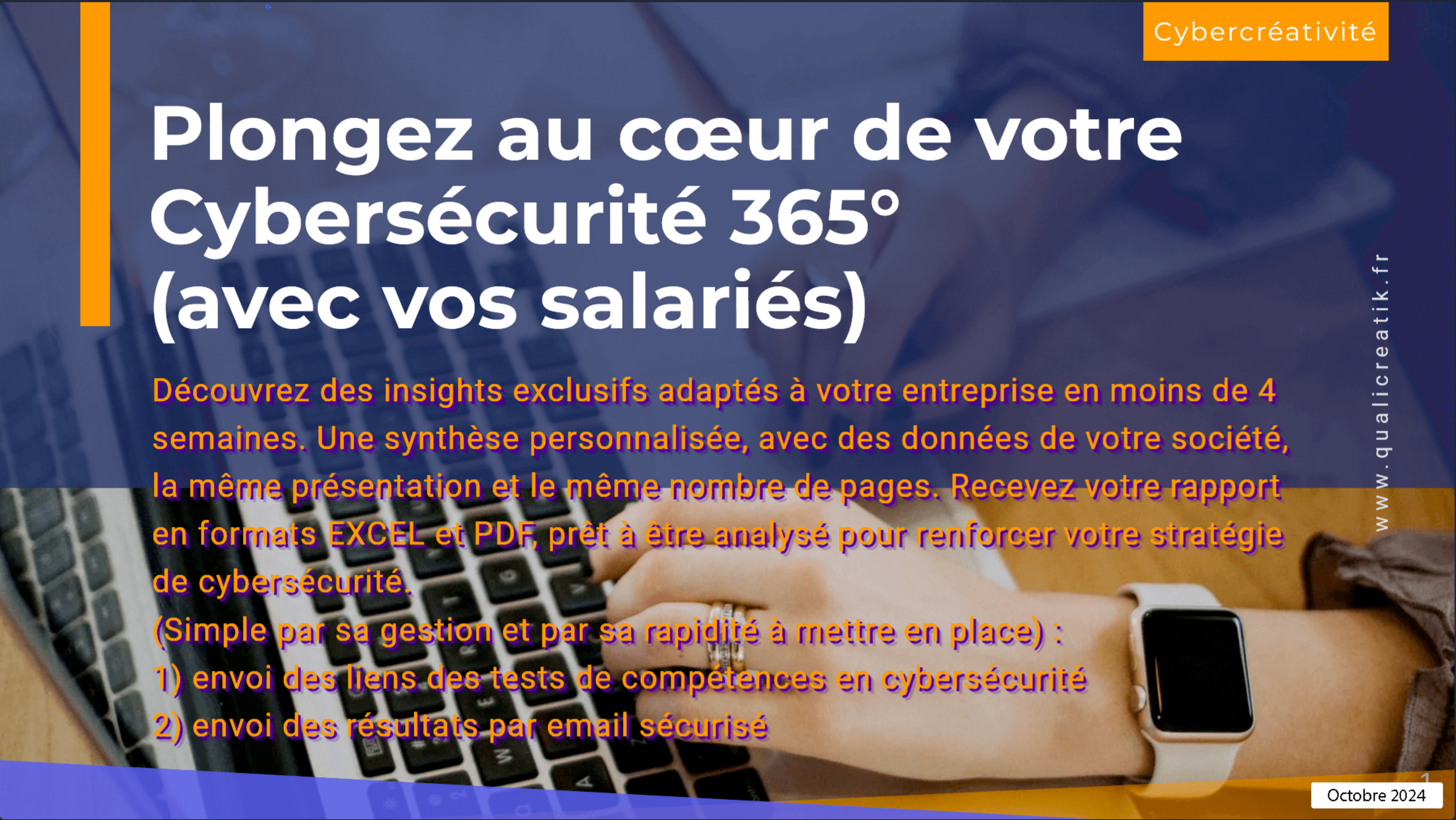
SECTEUR DE L'ENTREPRISE	%
DIRECTION	7.30%
COMPTABILITE	7.02%
RESSOURCES HUMAINES	5.90%
VENTES	5.34%
FINANCE	3.93%
LOGISTIQUE	7.02%
PRODUCTION	2.25%
ACHATS	0.28%
INFORMATIQUE	33.71%
COMMUNICATION	1.69%
SERVICE CLIENT	2.25%
SUPPORT DES VENTES	0.00%
MAINTENANCE	0.56%
SECRETARIAT	2.81%
QUALITE	1.40%
R&D	7.87%

SECTEUR DE L'ENTREPRISE	%
SERVICES GENERAUX	0.28%
ASSURANCE	0.00%
FORMATION	1.69%
BUREAU D'ETUDES	1.97%
GESTION DE PROJETS	1.97%
E-COMMERCE	1.12%
INTERNATIONAL	0.56%
SECURITE	1.12%
RELATIONS PUBLIQUES	1.40%

ANCIENNETÉ DANS L'ENTREPRISE	%
Moins d'un an	3.09%
De 1 à 3 ans inclus	15.73%
De 3 à 5 ans inclus	19.66%
De 5 à 10 ans inclus	22.19%
Plus de 10 ans	39.33%

Enquête réalisée entre le 25.09.2024 et le 03.10.2024 par Selvitys pour Qualicreatik.

Plongez au cœur de votre Cybersécurité 365° (avec vos salariés)



Découvrez des insights exclusifs adaptés à votre entreprise en moins de 4 semaines. Une synthèse personnalisée, avec des données de votre société, la même présentation et le même nombre de pages. Recevez votre rapport en formats EXCEL et PDF, prêt à être analysé pour renforcer votre stratégie de cybersécurité.

(Simple par sa gestion et par sa rapidité à mettre en place) :

1) envoi des liens des tests de compétences en cybersécurité

2) envoi des résultats par email sécurisé

www.qualicreatik.fr

Octobre 2024