CESIN CAMPUS CYBER

RÉSULTATS
ETUDE

Evaluation des dépendances cyber 2026
CESIN x CAMPUS CYBER

Novembre 2026

DÉMARCHE ET
MÉTHODOLOGIE

ÉVALUATION DES DÉPENDANCES CYBER 2026
CESIN X CAMPUS CYBER

UNE DÉMARCHE COMMUNE POUR L'ÉCOSYSTÈME

1 Face à la multiplication des solutions et services de cybersécurité au sein des organisations, le CESIN et le Campus Cyber ont souhaité lancer cette enquête afin de mieux appréhender le niveau de dépendance des entreprises à leur écosystème de fournisseurs et d'outils cyber, ainsi que les évolutions de cette dépendance au fil du temps.

2 Cette étude a pour objectif d'établir un état des lieux des pratiques du marché et de construire un indicateur permettant de suivre les tendances observées. L'analyse s'appuie sur les cinq fonctions du référentiel NIST Cybersecurity Framework (Identifier, Protéger, Détecter, Réagir et Récupérer) tout en prenant en compte les dimensions de gouvernance, de pilotage de la sécurité et les facteurs qui influencent les choix d'investissement, d'architecture et d'organisation.

3 Le questionnaire adopte une approche par grandes familles de solutions de cybersécurité afin d'évaluer la couverture des besoins, le niveau de concentration ou de diversification des fournisseurs, ainsi que les stratégies mises en œuvre par les organisations.

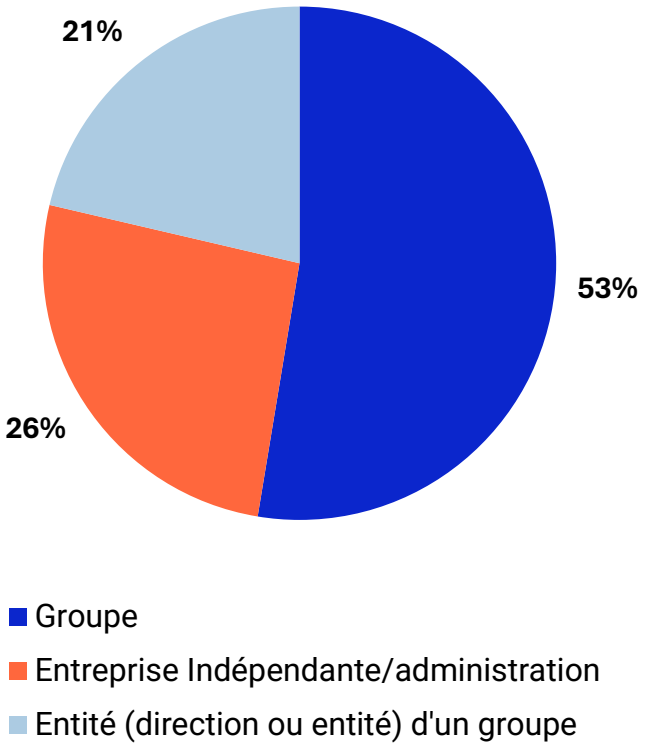
Echantillon de 192 membres du CESIN ayant tout ou partie répondu au questionnaire

L'échantillon de référence pour chaque question est précisé dans le rapport lorsque pertinent

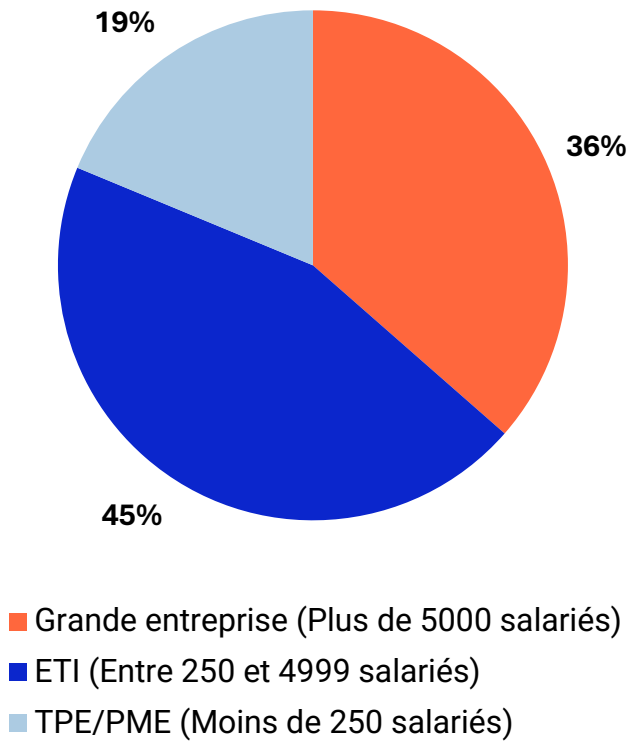
La consultation a eu lieu entre juin et septembre 2026

PROFIL DES RÉPONDANTS (1/2)

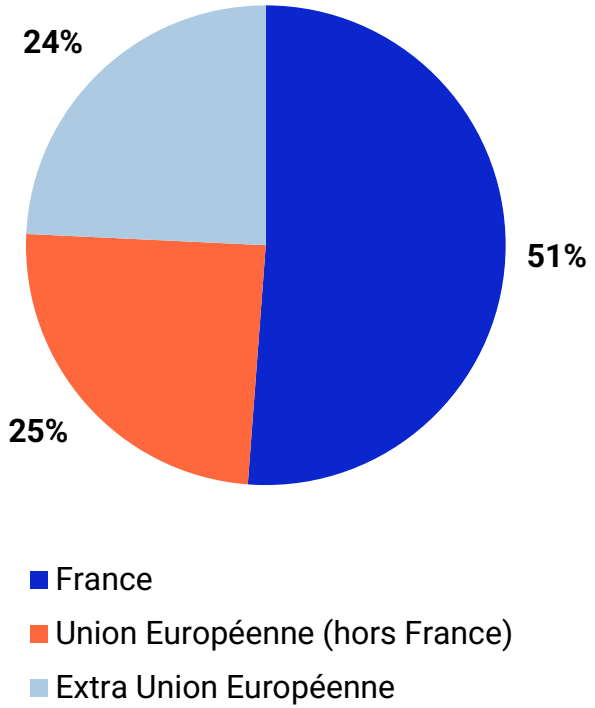
VOUS RÉPONDEZ EN TANT QUE :



QUELLE EST LA TAILLE DE VOTRE ENTREPRISE?

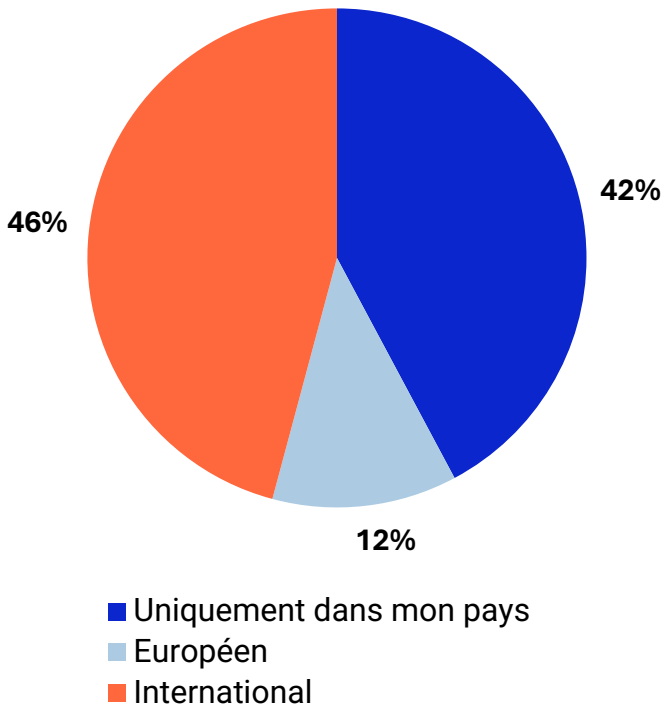


QUELLE EST LA ZONE D'IMPLANTATION DE VOTRE ENTREPRISE ?

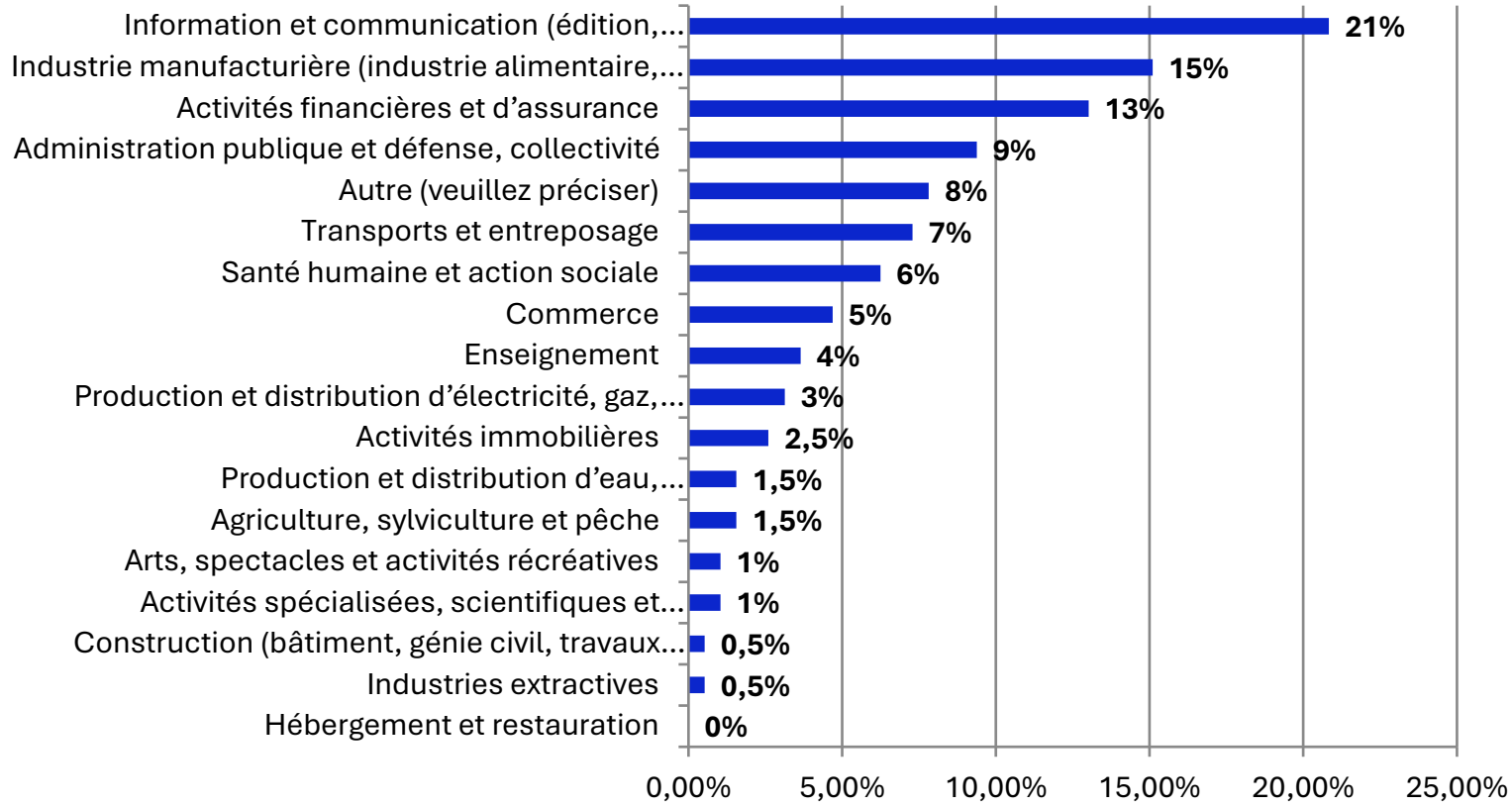


PROFIL DES RÉPONDANTS (2/2)

SUR QUEL PÉRIMÈTRE INTERVENEZ VOUS?



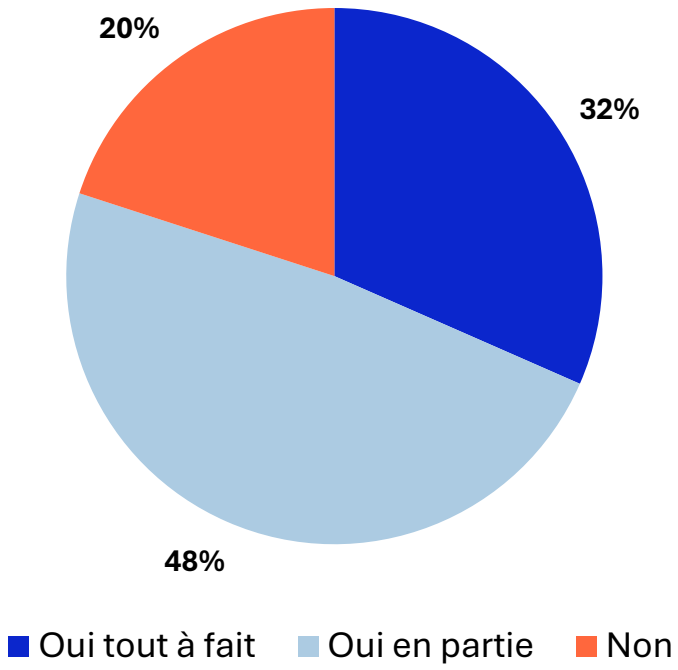
QUEL EST VOTRE SECTEUR D'ACTIVITÉ ?



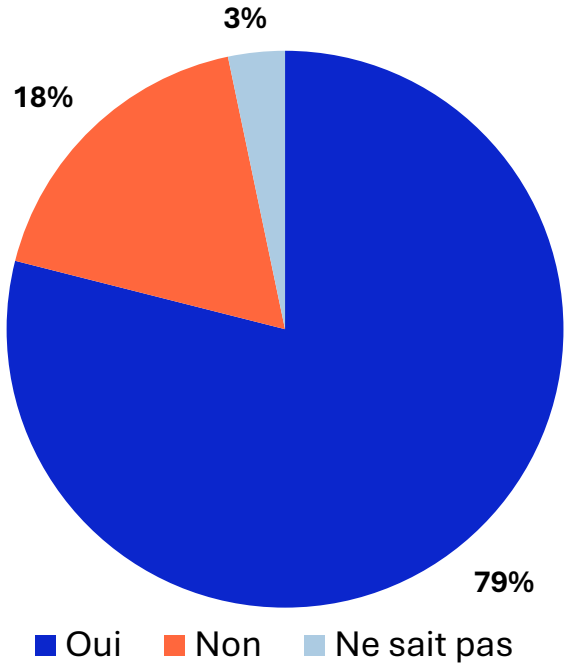
ÉTUDE DES DÉPENDANCES CYBER

LA SOUVERAINETÉ NUMÉRIQUE EST-ELLE UN AXE EXPLICITE
DE VOTRE STRATÉGIE NUMÉRIQUE D'ENTREPRISE ?

LA SOUVERAINETÉ NUMÉRIQUE (EMPLACEMENT DES DONNÉES, LOIS APPLICABLES, DÉPENDANCE À QUELQUES FOURNISSEURS) EST-ELLE UN AXE EXPLICITE DE VOTRE STRATÉGIE NUMÉRIQUE D'ENTREPRISE ?



SI OUI, EN FAITES-VOUS UNE DÉCLINAISON CYBERSÉCURITÉ?



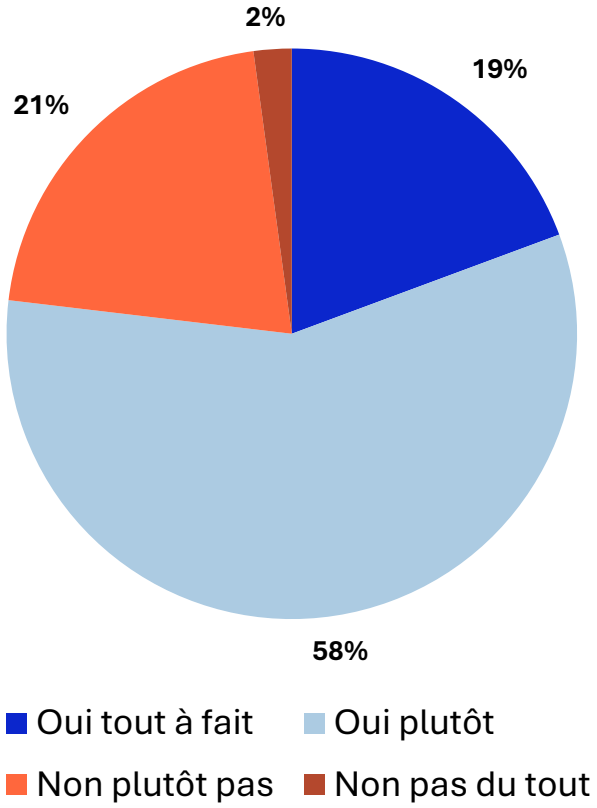
80 % Une prise en compte, au moins partielle déclinée comme telle :

- 32 % une priorité affirmée
- 48 % une intégration encore partielle

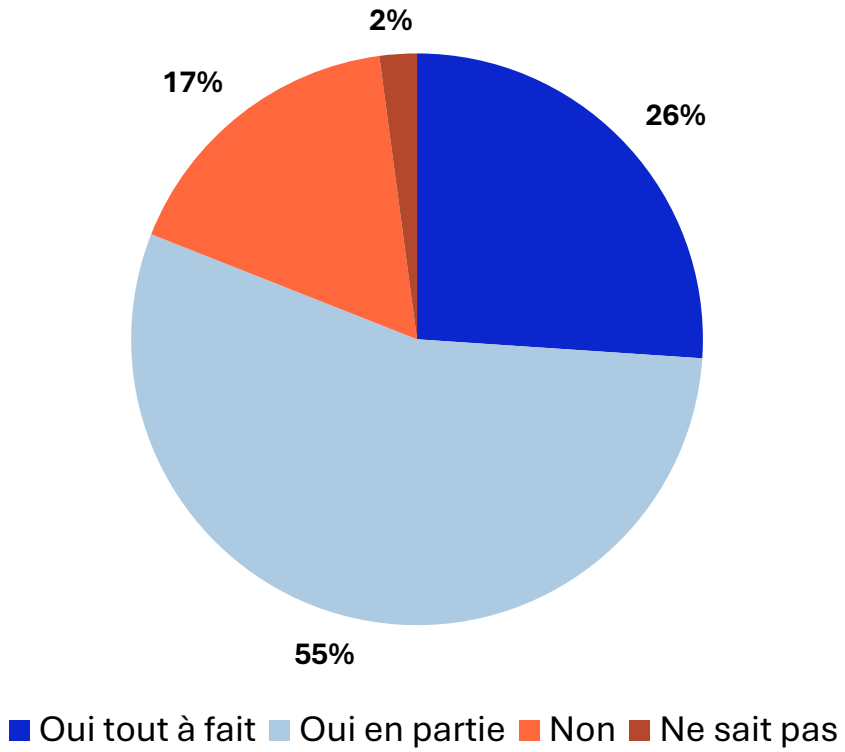
La souveraineté numérique est déjà prise en compte dans la stratégie numérique de la majorité des entreprises interrogées, et se **décline chez 80% d'entre eux dans leur stratégie cyber.**

AVEZ-VOUS UNE CARTOGRAPHIE IT DE L'ENSEMBLE DE VOS OUTILS, DONNÉES ET *INFRASTRUCTURES CRITIQUES, AINSI QUE DES FOURNISSEURS ET SOUS-TRAITANTS ASSOCIÉS?*

AVEZ-VOUS UNE CARTOGRAPHIE DE L'ENSEMBLE DE VOS OUTILS, DONNÉES ET INFRASTRUCTURES CRITIQUES, AINSI QUE DES FOURNISSEURS ET SOUS-TRAITANTS ASSOCIÉS?



CETTE CARTOGRAPHIE PERMET-ELLE D'IDENTIFIER SPÉCIFIQUEMENT LES DÉPENDANCES LIÉES À LA CYBERSÉCURITÉ ?

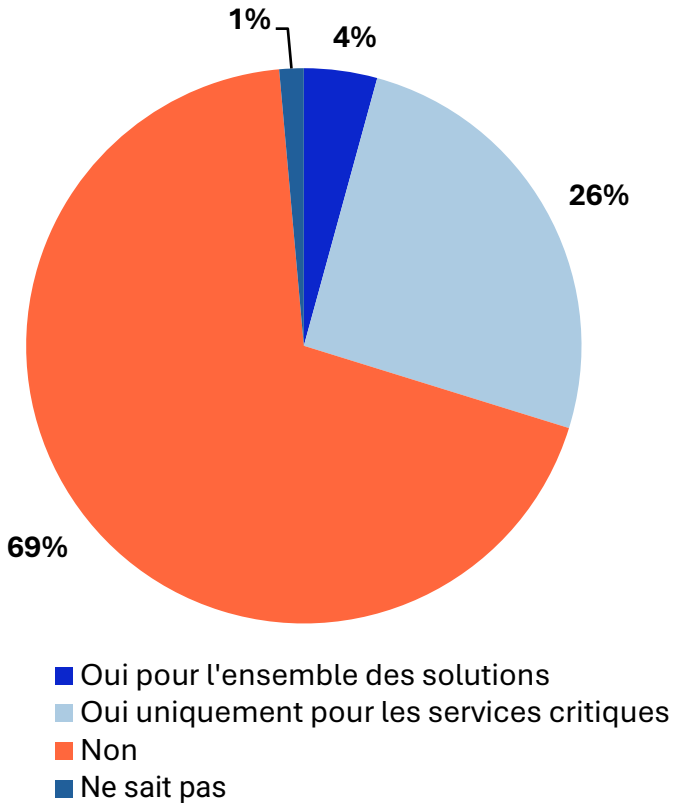


81 % des répondants indiquent que leur cartographie permet d'identifier ces dépendances, au moins en partie.

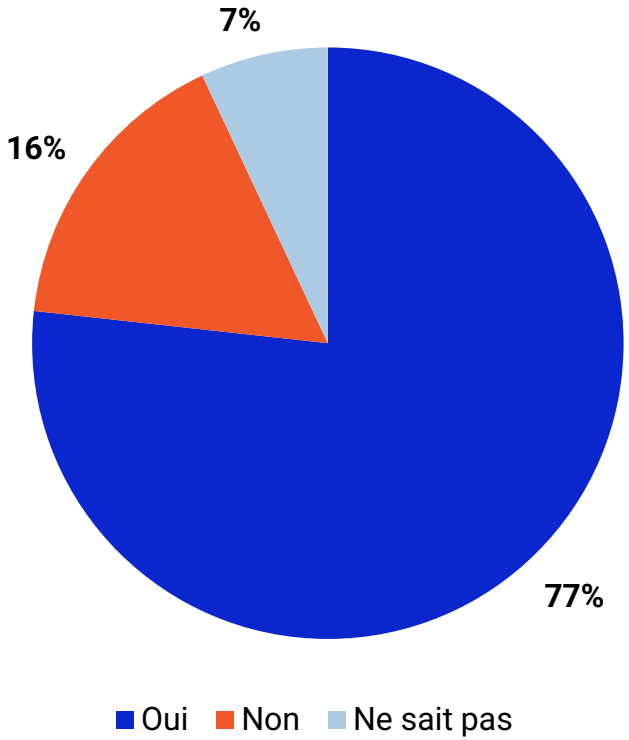
Seuls 26 % déclarent disposer d'une cartographie qui identifie pleinement les dépendances liées à la cybersécurité. Près de 55% n'en ont qu'une vision partielle.

DISPOSEZ-VOUS D'INDICATEURS DE SUIVI DE VOS *DÉPENDANCES NUMÉRIQUES OU CYBER?*

DISPOSEZ-VOUS D'INDICATEURS DE SUIVI DE VOS DÉPENDANCES NUMÉRIQUES OU CYBER ?



SI OUI, EST-CE QUE LE PROCESSUS "SÉCURISER LE SI" EN FAIT PARTIE ?



30% des répondants indiquent avoir des indicateurs de suivi des dépendances numériques ou cyber, au moins sur les services critiques.

Lorsque c'est le cas, « Sécuriser le SI » en fait partie pour plus de 76%.

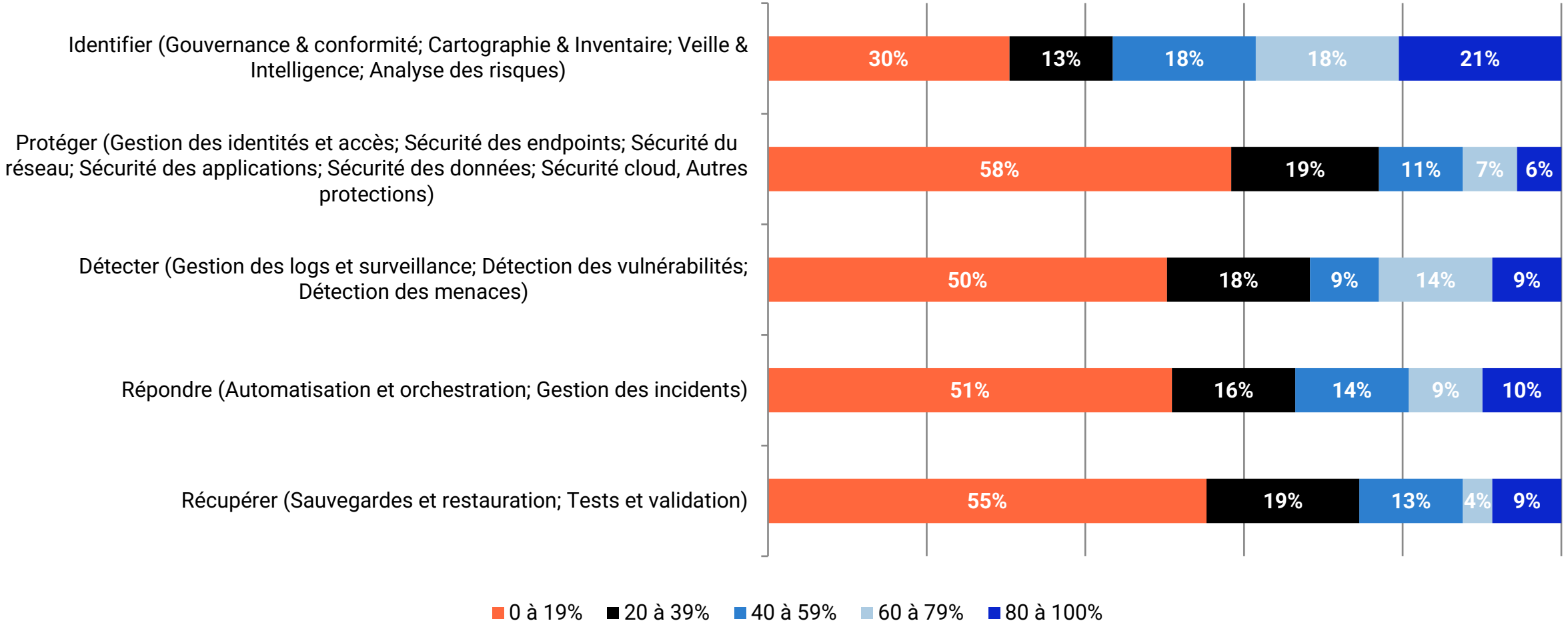
SI OUI, QUELS SONT VOS PRINCIPAUX INDICATEURS ?

Les principaux indicateurs qui ressortent sont :

- Risque pays / souveraineté / localisation des données
- Conformité et réglementation
- Gestion des vulnérabilités
- Résilience opérationnelle
- Maîtrise du risque fournisseur
- Sécurité des développements et des actifs
- Détection et réponse

QUELLE EST LA PART DE SOLUTIONS EUROPÉENNES
PAR GRANDES CATÉGORIES du NIST.

Merci d'indiquer par grandes catégories de solutions la part en % de solutions européennes.



PART DE SOLUTIONS EUROPÉENNES
PAR GRANDES CATÉGORIES.

LES PRINCIPAUX ENSEIGNEMENTS :

- 49% des répondants, ont, toutes catégories confondues, déployé moins de 20% de solutions européennes.
- Globalement, seuls 20% des répondants déclarent avoir plus de 60% de solutions européennes sur l'ensemble des 5 piliers
- La plus forte propension de solutions européennes déployées est sur la partie « Identify » avec près de 40% de répondants qui ont déployé plus de 60% de solutions européennes
- La plus faible reste la partie "Protéger" avec près de 60% de répondants qui déclarent utiliser moins de 20% de solutions européennes

PILIER IDENTIFIER *(GOUVERNANCE & CONFORMITÉ, CARTOGRAPHIE & INVENTAIRE, VEILLE & INTELLIGENCE, ANALYSE DES RISQUES)*

IDENTIFIER

- **65%** des répondants déclarent une part de plus de **40% de solutions européennes** dans leurs solutions **« Gouvernance & conformité »**
- **51%** des répondants déclarent une part de plus de **40% de solutions européennes** dans leurs solutions **« Cartographie & inventaire »**
- **46%** des répondants déclarent une part de plus de **60% de solutions européennes** dans leurs solutions **« Veille & intelligence»**
- **84%** des répondants déclarent une part de plus de **40% de solutions européennes** dans leurs solutions **« Analyse de risques »**

PILIER PROTÉGER *(GESTION DES IDENTITÉS ET DES ACCÈS, SÉCURITÉ DES ENDPOINTS, SÉCURITÉ DU RÉSEAU, SÉCURITÉ DES DONNÉES, SÉCURITÉ CLOUD)*

PROTEGER

- Sur la partie « **Gestion des identités et des accès** » : **67%** des répondants déclarent déployer **plus de 80% de solutions extra-européennes**
- Sur la partie « **Sécuriser des endpoints** » : **78%** des répondants déclarent déployer **plus de 80% de solutions extra-européennes**
- Sur la partie « **Sécurité du réseau** » : **76%** des répondants déclarent déployer **plus de 80% de solutions extra-européennes**
- Sur la partie « **Sécurité des données** » : **63%** des répondants déclarent déployer **plus de 80% de solutions extra-européennes**
- Sur la partie « **Sécurité Cloud** » : **72%** des répondants déclarent déployer **plus de 80% de solutions extra-européennes**

PILIER DÉTECTER *(GESTION DES LOGS ET SURVEILLANCE; DÉTECTION DES VULNÉRABILITÉS; DÉTECTION DES MENACES)*

DÉTECTER

- Sur la partie « **Gestion des logs et surveillance**»,
  51% des répondants déclarent déployer une part de **plus de 40% de solutions européennes**.

- Sur la partie « **Détection des vulnérabilités**»,
  55% des répondants déclarent déployer une part de **plus de 40% de solutions européennes**

- Sur la partie « **Détection des menaces**»,
  55% des répondants déclarent déployer une part de **plus de 40% de solutions européennes**.

PILIERS RÉPONDRE (GESTION DES INCIDENTS, AUTOMATISATION ET ORCHESTRATION) **ET RÉCUPÉRER** (SAUVEGARDE ET RESTAURATION, TEST ET VALIDATION)

RÉPONDRE

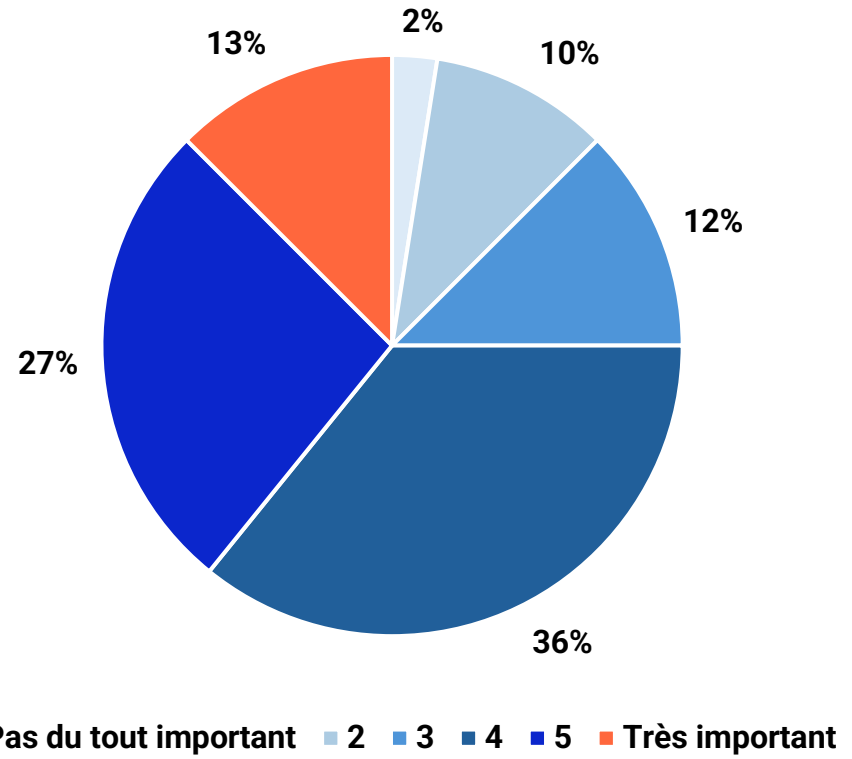
- Sur la partie « **Gestion des incidents», 61%** des répondants déclarent déployer une part de **plus de 40% de solutions européennes** et **36%** déclarent employer **plus de 80% de solutions open source**.

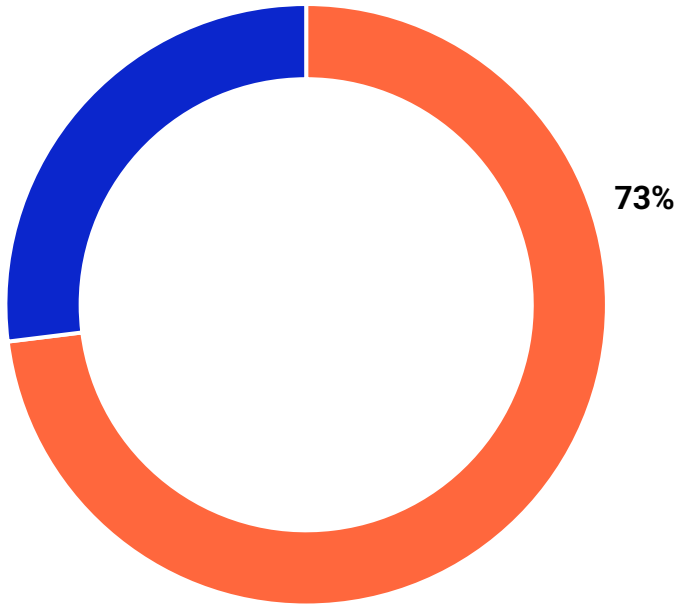
- Sur la partie « **Automatisation et orchestration** », **34 %** des répondants déclarent déployer une part de **plus de 40% de solutions européennes**.

RÉCUPERER

- Sur la partie « **Sauvegarde et restauration**», **70%** des répondants déclarent déployer **plus de 80% de solutions extra-européennes.**
- Sur la partie « **Test et validation**», **68%** des répondants déclarent déployer **plus de 40% de solutions européennes**.

COMMENT ESTIMEZ-VOUS LE NIVEAU D'IMPORTANCE QUE VOUS ATTACHEZ À LA DÉPENDANCE STRATÉGIQUE *(KILL SWITCH, ARRÊT DE SERVICE OU RISQUE SUR LA SUPPLY CHAIN) ?*



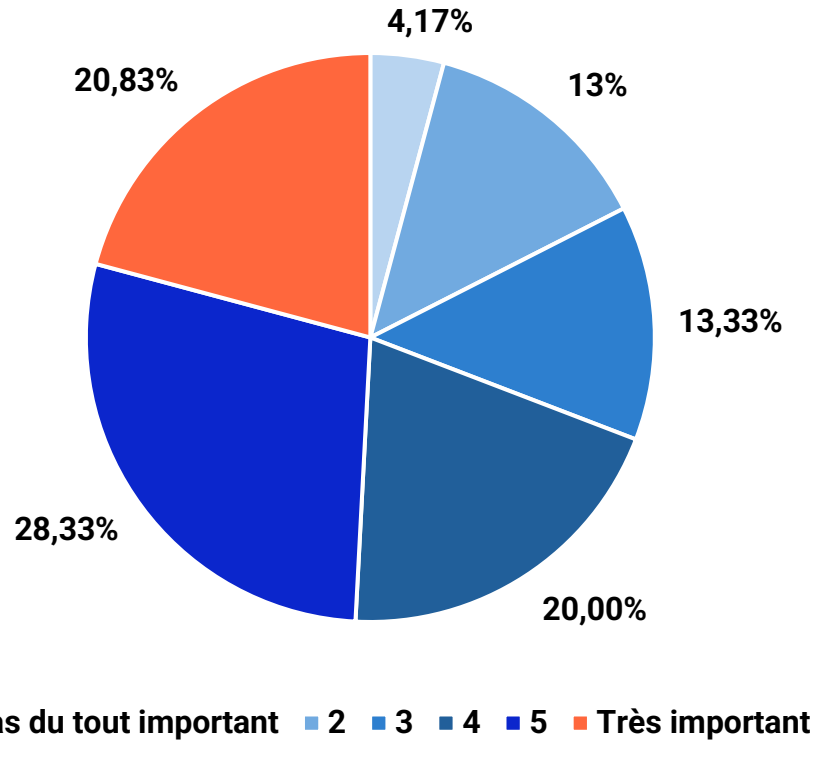


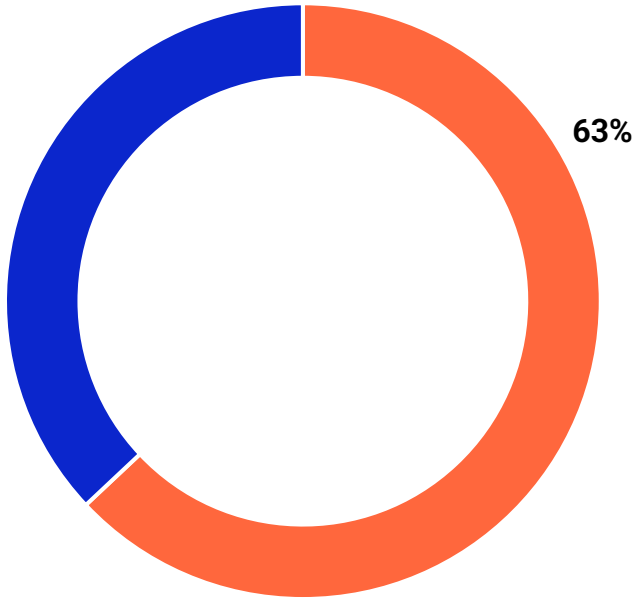
Sur une échelle de 0 à 6 (de « Pas du tout important » à « Très important »), la distribution montre que la dépendance stratégique est un sujet largement pris en compte par les répondants, même si elle n'apparaît pas encore comme une préoccupation critique pour tous.

Les répondants évaluent en moyenne leur niveau de dépendance stratégique à 73 sur 100, ce qui traduit une perception globalement élevée de leur dépendance vis-à-vis de certains fournisseurs, technologies ou services critiques.

1: Pas du tout important / 2 : très peu important / 3 : peu important / 4 : Assez important / 5 : Important / 6 : Très important

COMMENT ESTIMEZ-VOUS LE NIVEAU D'IMPORTANCE QUE VOUS ATTACHEZ À LA DÉPENDANCE JURIDIQUE *(LOIS EXTRA-TERRITORIALES) ?*





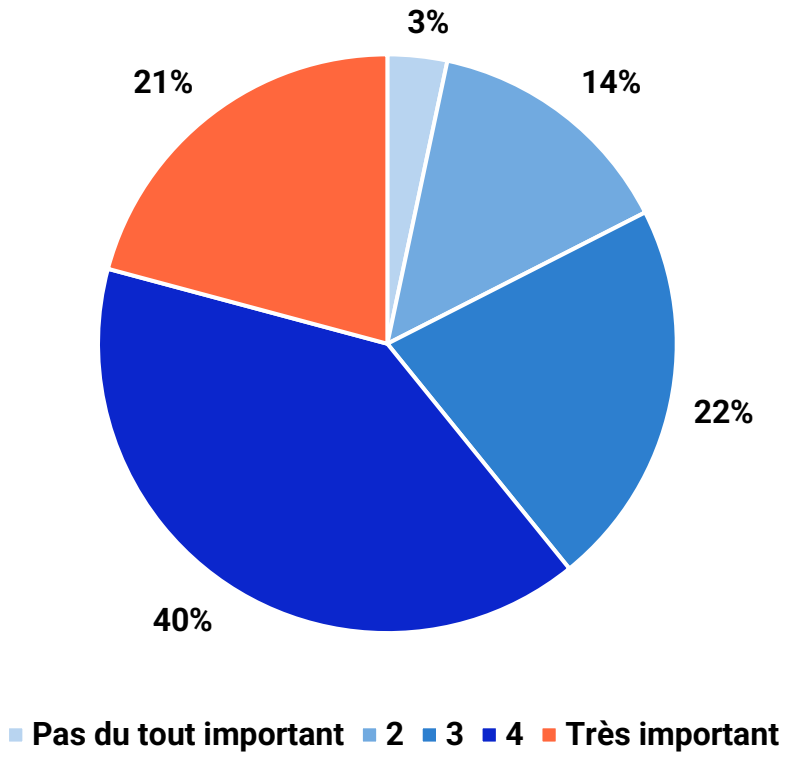
Comment évaluez-vous votre niveau de dépendance juridique?

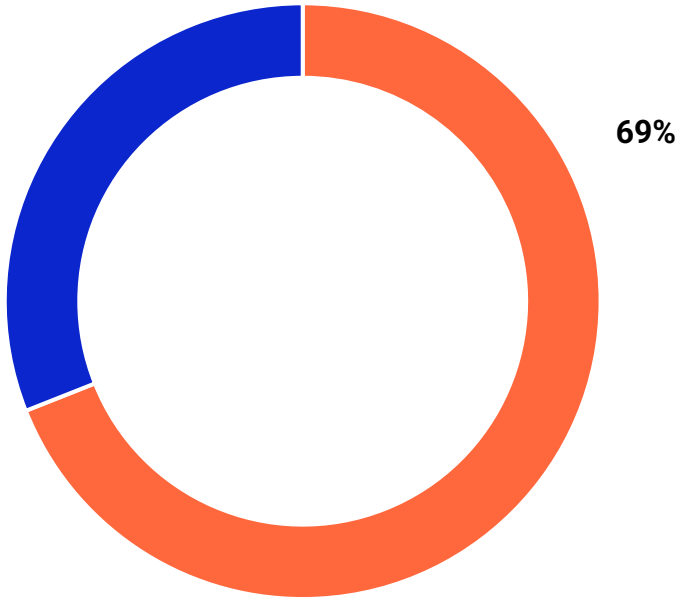
La dépendance juridique constitue un enjeu significatif pour une majorité des répondants : près de 7 sur 10 lui attribuent un niveau d'importance élevé (notes de 4 à 6), et près de la moitié la jugent très importante (notes de 5 ou 6).

Les répondants évaluent en moyenne leur niveau de dépendance juridique à 63 sur 100, ce qui traduit une perception globalement élevée de leur dépendance juridique.

COMMENT ESTIMEZ-VOUS LE NIVEAU D'IMPORTANCE QUE VOUS ATTACHEZ À LA DÉPENDANCE ÉCONOMIQUE ?

NOUS ENTENDONS ICI PAR DÉPENDANCE ÉCONOMIQUE LE PHÉNOMÈNE D'ENFERMEMENT VIS-À-VIS DE SOLUTIONS DIFFICILEMENT INTERCHANGEABLES



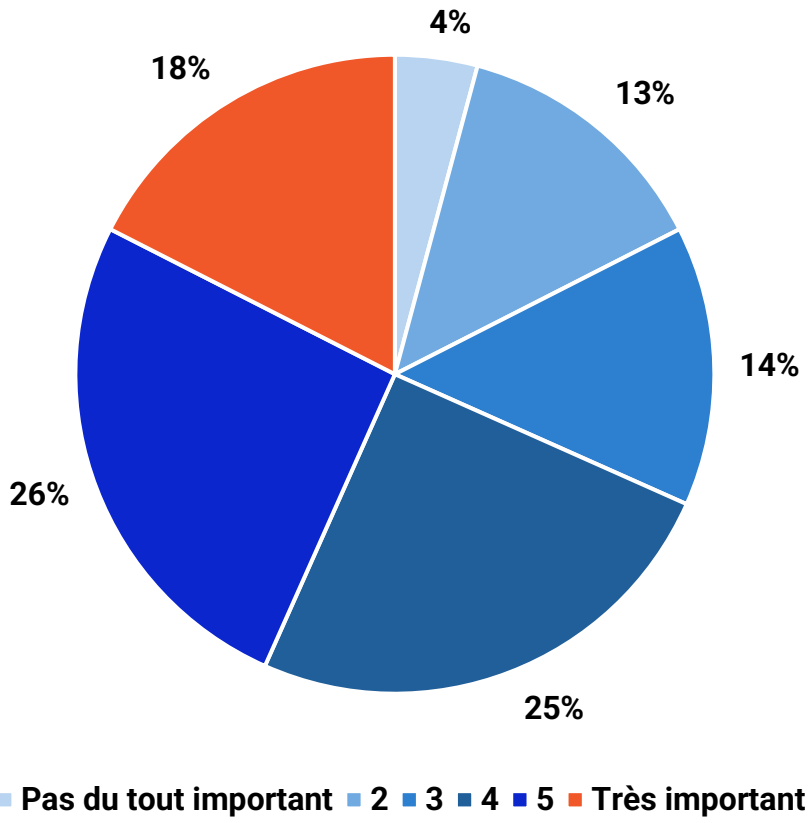


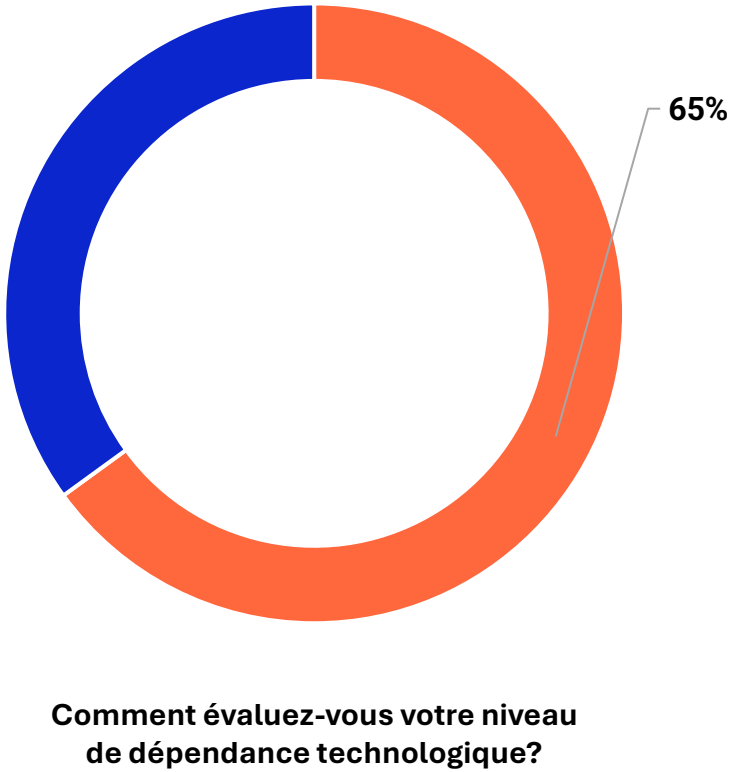
Comment évaluez-vous votre niveau de dépendance économique ?

La dépendance économique aux solutions de cybersécurité, définie comme la difficulté à substituer ou remplacer certaines technologies critiques, constitue une préoccupation majeure pour les organisations interrogées. Plus de six répondants sur dix (60,8 %) jugent cette dépendance importante ou très importante, tandis que plus de huit sur dix lui attribuent un niveau d'importance au moins moyen.

Les répondants évaluent en moyenne leur niveau de dépendance économique à 69 sur 100.

COMMENT ESTIMEZ-VOUS LE NIVEAU D'IMPORTANCE QUE VOUS ATTACHEZ À LA DÉPENDANCE TECHNOLOGIQUE *(PAS D'ALTERNATIVE SUR LE MARCHÉ) ?*

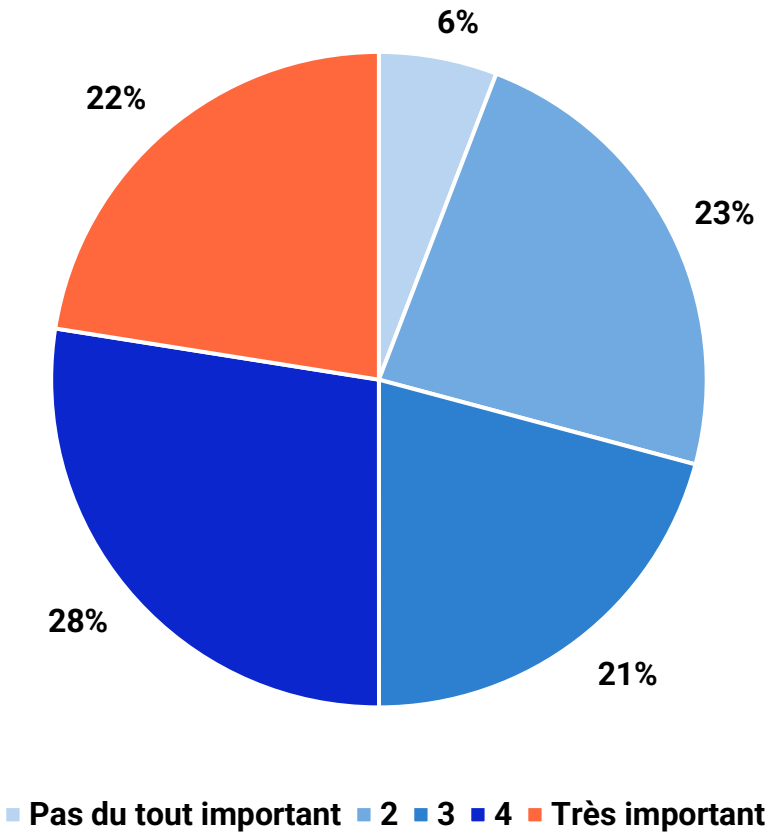


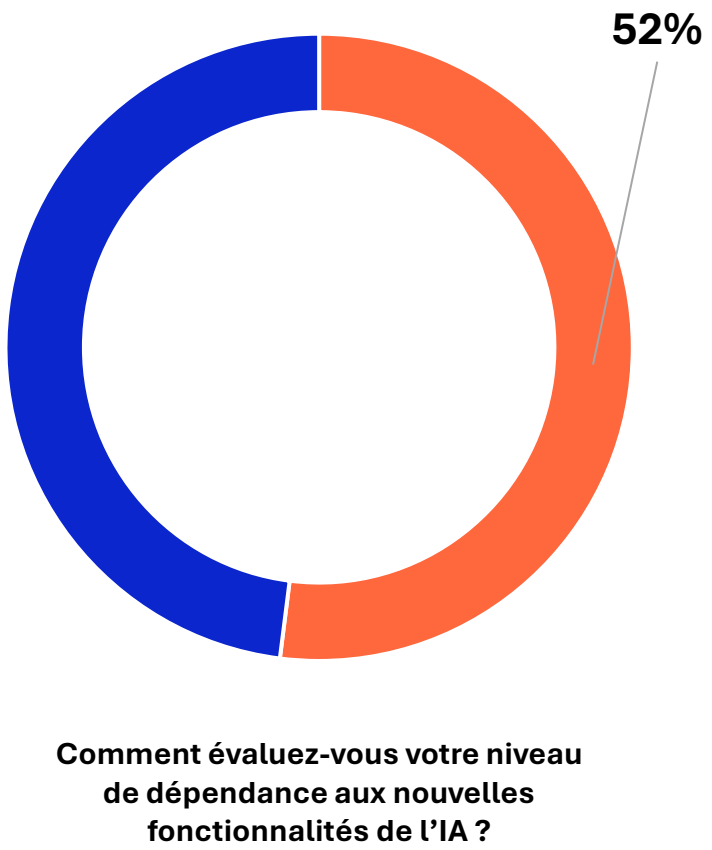


Les résultats montrent que la dépendance technologique constitue une préoccupation majeure pour les organisations interrogées. Plus des deux tiers des répondants (68 %) lui attribuent un niveau d'importance élevé, tandis que 43 % la jugent importante à très importante. Ce critère apparaît comme un facteur de risque significatif dans les choix de solutions cybersécurité.

Les répondants évaluent en moyenne leur niveau de dépendance technologique à 65 sur 100.

COMMENT ESTIMEZ-VOUS LE NIVEAU D'IMPORTANCE QUE VOUS ATTACHEZ À LA DÉPENDANCE AUX NOUVELLES FONCTIONNALITÉS DE L'IA *(AGENTIQUE, ...) ?*





Une organisation sur deux considère déjà que la dépendance aux innovations IA constitue un enjeu important ou très important.

Cependant, on note des perceptions contrastées : près de 30 % accordent une importance faible à cette question.

QUELS ONT ÉTÉ LES PRINCIPAUX CRITÈRES AYANT MOTIVÉ VOS CHOIX DE SOLUTIONS ? *(PLUSIEURS CHOIX POSSIBLES)*

Les principaux critères qui ressortent sont :

- Les performances techniques de la solution
- Le prix
- Le manque d'alternatives identifiées ou de connaissance de solutions françaises ou européennes pour répondre aux besoins

Et, dans une moindre mesure :

- La souveraineté
- L'interopérabilité
- Les contraintes d'achat