

# ÊTRE PRÉPARÉ AUX RISQUES OU Y ÊTRE EXPOSÉ

COHESITY

## Le fossé de la cyber-résilience dans les entreprises de taille moyenne

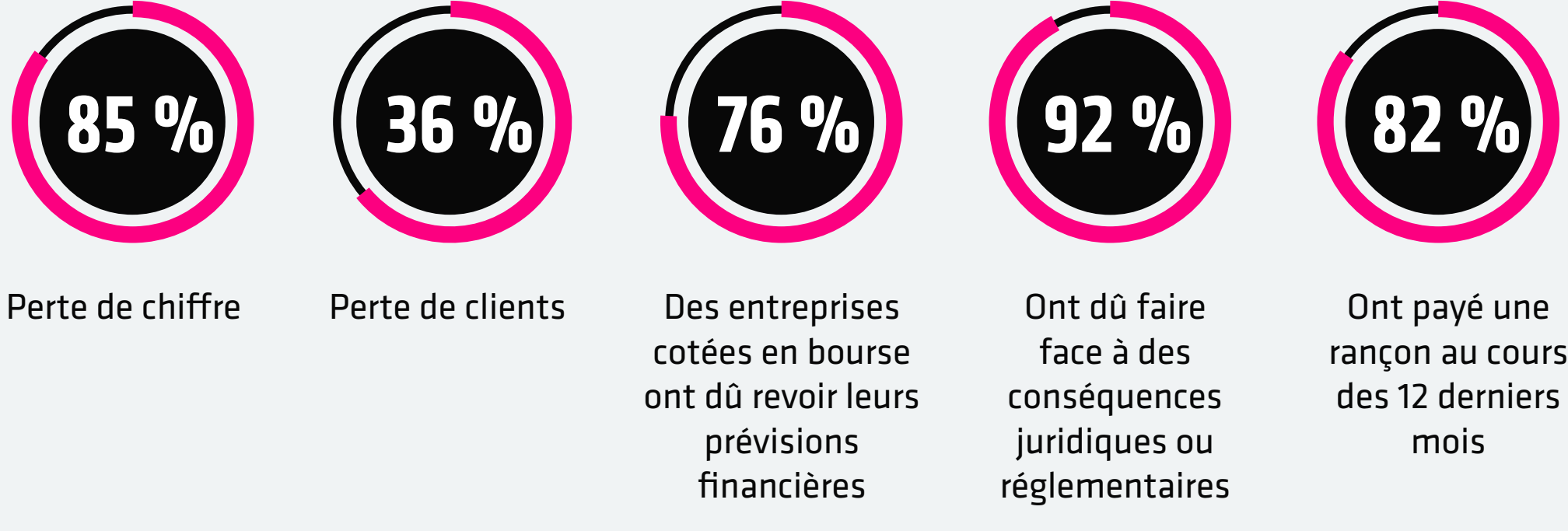


Les cyberattaques ne sont plus des événements isolés, mais une caractéristique inhérente à notre monde numérique. Chaque jour le confirme : à l'échelle mondiale, les entreprises de taille moyenne sont de plus en plus fréquemment prises pour cible. Aucune entreprise n'est à l'abri. La fréquence et la sophistication croissantes des menaces ont entraîné une augmentation du nombre de cyberattaques graves qui causent des dommages mesurables sur le plan financier, opérationnel et en termes de réputation.

**UNE ENQUÊTE MONDIALE MENÉE AUPRÈS DE PRÈS DE 1 000 DÉCIDEURS DANS LE DOMAINE DES OPÉRATIONS INFORMATIQUES ET DE SÉCURITÉ D'ENTREPRISES DE 1 000 à 1 999 EMPLOYÉS RÉVÈLE LA RÉALITÉ.**



## LES DOMMAGES SONT CONSIDÉRABLES ET LES COÛTS S'ACCUMULENT RAPIDEMENT.

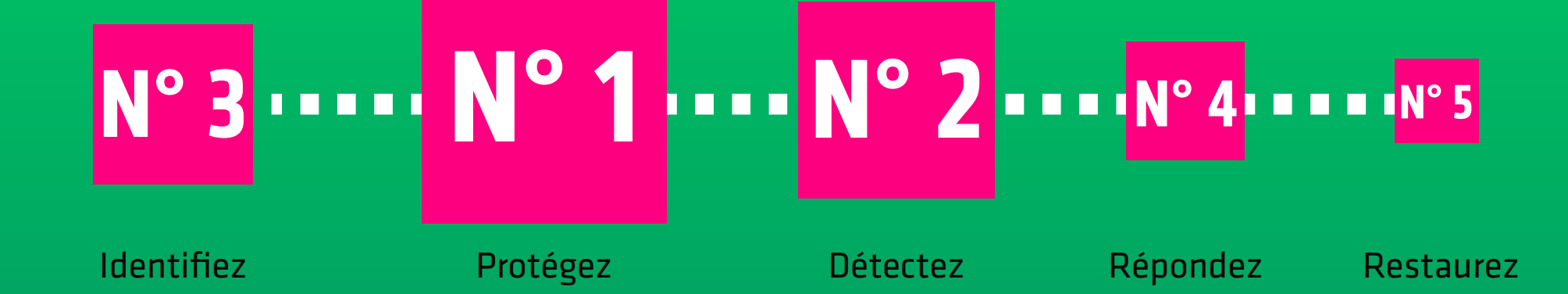


**DE NOMBREUSES ENTREPRISES SURESTIMENT LEUR RÉSILIENCE BIEN QU'ELLES AIENT DES PREUVES ÉVIDENTES QUE CE N'EST PAS LE CAS.**



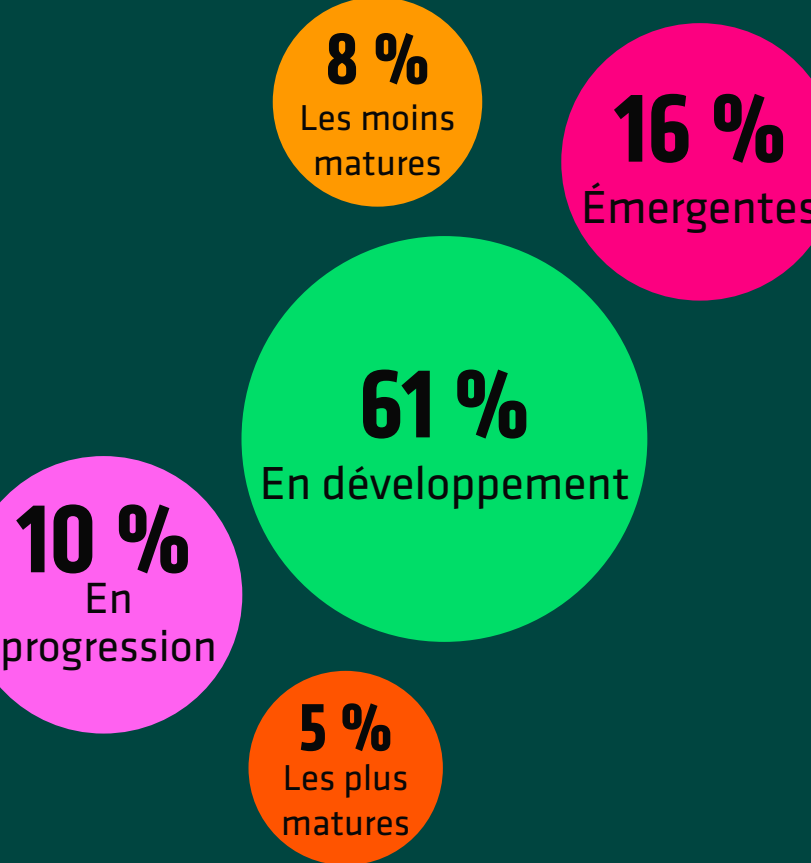
## LA PLUPART D'ENTRE ELLES CONTINUENT DE PRIVILÉGIER LA PRÉVENTION ET LA DÉTECTION PLUTÔT QUE LA RÉPONSE ET LA RESTAURATION, QUI SONT TOUT AUSSI CRITIQUES.

Ordre basé sur le cadre de cybersécurité du NIST.  
La taille des cases indique la proportion des investissements en matière de cyber-résilience, de la plus élevée à la plus faible.



## LA CONFIANCE ET LES HABITUDES DE CONSOMMATION NE REFLÈTENT QU'UNE PARTIE DE LA RÉALITÉ

La véritable résilience dépend des pratiques et des capacités qui la soutiennent. Si on l'évalue sur la base de critères de performance concrets, seules 5 % des entreprises font preuve de maturité dans cinq domaines essentiels : la **protection des données**, la **restauration des données**, la **détection et l'investigation des menaces**, la **résilience des applications** et l'**optimisation des risques liés aux données**.

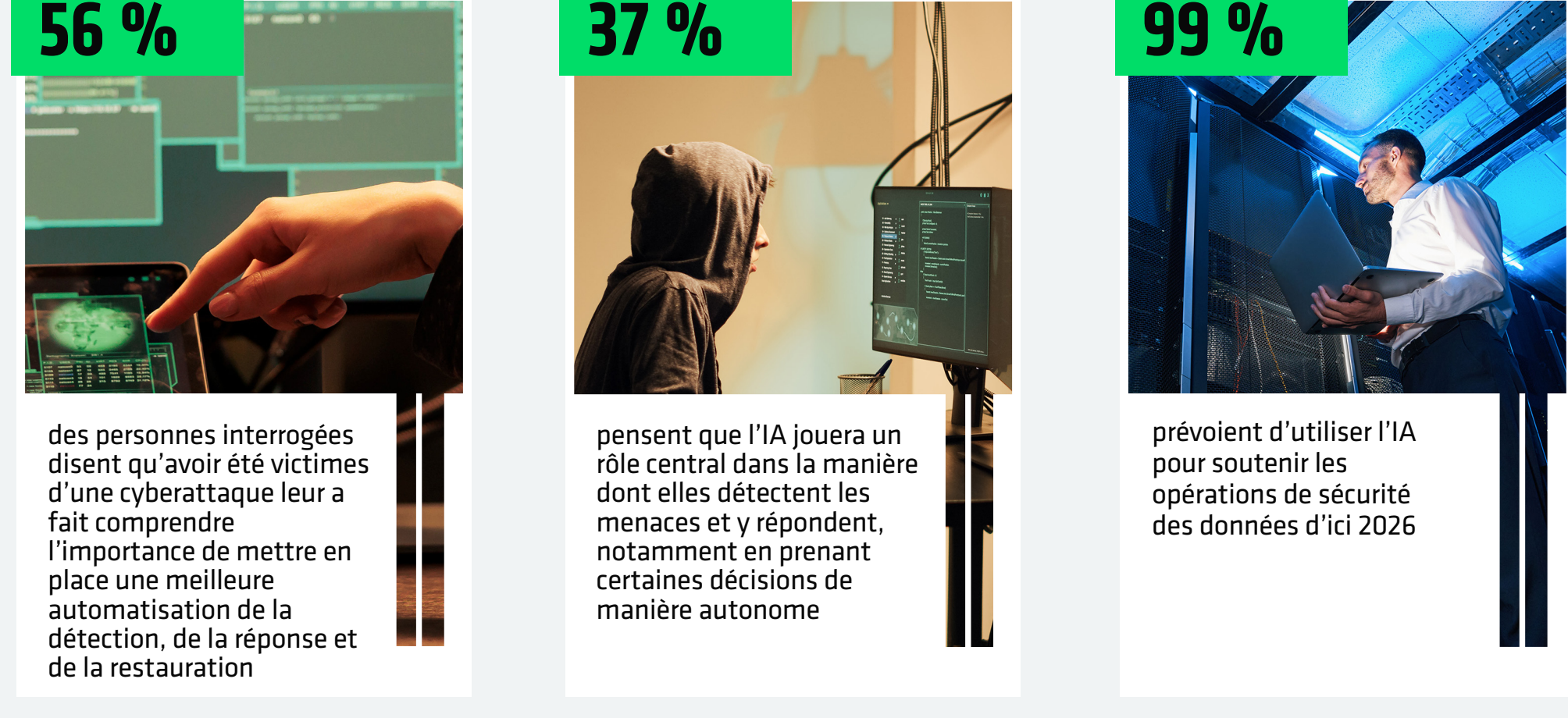


Pour les entreprises les plus cyber-résilientes, la résilience est systématique et complète. Entre autres bonnes pratiques, elles garantissent que les données sensibles sont sauvegardées à l'échelle mondiale, que l'authentification multifactor et les contrôles administratifs sont appliqués, que le renseignement sur les menaces est optimisé, que la restauration est sécurisée par des mesures correctives et que les mesures de protection de la conformité sont systématiquement respectées.

## MAIS LA MATURITÉ N'EST PAS STATIQUE.



La prochaine évolution nécessite de prendre conscience qu'il faut renforcer la résilience, et que celle-ci est alimentée par l'automatisation et l'IA. Les menaces sont de plus en plus rapides et complexes. L'automatisation est donc essentielle pour accélérer la détection, rationaliser la réponse et renforcer la restauration.



## ÊTES-VOUS PRÉPARÉS AUX RISQUES ?

- Découvrez **les solutions de cyber-résilience de Cohesity** pour les **entreprises de taille moyenne**.
- Évaluez votre **maturité en matière de cyber-résilience** avec cette **fiche d'évaluation de la résilience**
- Passez au niveau supérieur grâce à un **plan d'action en cinq étapes pour renforcer votre cyber-résilience**.

Vanson Bourne a interrogé 3 200 responsables informatiques et de la sécurité d'Amérique du Nord, d'Asie-Pacifique, d'Europe et d'Amérique latine, représentant des entreprises comptant 1 000 employés ou plus en 2025. Les répondants comprenaient 977 participants issus d'entreprises de taille moyenne comptant entre 1 000 et 1 999 employés.

**COHESITY** VansonBourne