ESG RESEARCH INSIGHTS REPORT

# L’atout XDR : une meilleure posture de sécurité

Les entreprises qui agrégent, corrèlent et analysent les signaux et données provenant de l’ensemble des couches de sécurité sont mieux outillées pour maîtriser les attaques et tempérer le stress qui pèse sur leurs équipes.

par Dave Gruber, Senior Analyst
Adam DeMattia, Director of Research

Septembre 2020

ESG Research Insights Report a été commandité par Trend Micro et est rendu public sous licence ESG.

## Sommaire

## Synthèse décisionnelle

L'avènement de l' XDR, à savoir l'extension des fonctions de détection et de réponse aux menaces à de multiples couches de sécurité, crée de nouvelles opportunités pour les équipes de sécurité. En capitalisant sur les enseignements de l'EDR (détection et menaces au niveau des Endpoints), la technologie XDR analyse les indicateurs provenant des fonctions de protection des Endpoints, du réseau, de la messagerie et des instances Cloud, offrant ainsi une visibilité plus large au cœur des attaques modernes et complexes. La promesse de l'XDR est d'assurer des gains de productivité. Cette technologie aide les analystes de sécurité juniors à traiter une part plus importante des attaques, de manière autonome et en faisant de moins en moins appel à leurs managers, certes plus expérimentés, mais peu nombreux et déjà fortement mobilisés.

Alors que la vague XDR s'accélère, les entreprises s'interrogent sur comment cette technologie peut les aider à simplifier leurs environnements. Pour répondre à cette question, Trend Micro et ESG ont conduit une enquête en identifiant les entreprises qui utilisent déjà une approche similaire à l'XDR. Une telle approche favorise l'agrégation, la corrélation et l'analyse automatisées de données issues de différentes fonctions de sécurité, avec pour objectif de détecter et de répondre aux menaces modernes. Cette étude met en exergue les réalisations business de ces entreprises mais se penche également sur les conséquences subies par celles qui ne mettent pas en œuvre de telles pratiques.

Pour cette étude, nous sommes partis de l'hypothèse que les entreprises ayant investi dans une automatisation de type XDR développeront de nouvelles capacités : identification rapide des menaces complexes, temps de réponse plus rapides, efficacité des équipes de sécurité et amélioration globale du niveau de sécurité. Ces hypothèses ont été validées par les résultats de notre enquête. Les équipes de sécurité qui ont déjà investi pour agréger, corréler et analyser les signaux et données provenant de toutes les couches de sécurité déclarent subir moins d'attaques réussies, maîtriser davantage leur niveau de sécurité et faire peser moins de stress sur leurs équipes. Ces dernières identifient et répondent plus rapidement aux menaces et savent gérer leurs alertes de manière pertinente.

**Les équipes de sécurité qui ont déjà investi pour agréger, corréler et analyser les signaux et données provenant de toutes les couches de sécurité déclarent subir moins d'attaques réussies, maîtriser davantage leur niveau de sécurité et faire peser moins de stress sur leurs équipes.**

Au sein de la plupart des entreprises, le cloisonnement des données est une réalité. 41% des entreprises interrogées indiquent que leurs données sont très fragmentées et 61% d'entre elles intègrent et agrègent de manière annuelle les données issues de leurs différentes fonctions de sécurité. Elles sont nombreuses à tenter d'abattre ces cloisons à l'aide d'un SIEM, mais 50% d'entre elles affirment être frustrées par le niveau de complexité, de redondance et de compétences expertes nécessaires pour opérer leur SIEM.

Nous avons demandé à celles qui ont le plus investi dans l'automatisation, la corrélation et le traitement analytique de nous indiquer le nombre de personnes en ETP ( équivalent temps plein) qui leur semble nécessaire pour remplacer leurs systèmes automatisés. La réponse ressort à une moyenne de 8 ETP, ce qui constitue, pour la majorité des entreprises, un investissement particulièrement lourd. D'autre part, nous avons constaté que les entreprises qui n'ont pas encore investi dans l'automatisation de l'agrégation, de la corrélation et du traitement analytique, ignorent près de deux fois plus d'alertes que leurs homologues ayant investi en ce sens, et qu'elles subissent ainsi une zone d'ombre et des risques inconnus ou non pris en charge.


L'XDR définit une toute nouvelle approche pour automatiser l'agrégation, la corrélation et l'analyse des données de sécurité, offrant ainsi davantage de fiabilité et d'efficacité aux équipes de sécurité qui luttent pour garder la main sur un univers des menaces complexe et en expansion. Plus que jamais, les équipes de sécurité doivent doper leur productivité en dépit d'une pénurie de compétences en cybersécurité et d'initiatives de transformation digitale qui s'accélèrent.

Ce document se penche également sur certaines données d'étude spécifiques et sur leur interprétation. Alors que l'adoption des solutions XDR progresse, nous nous attendons à ce que les indicateurs et résultats à venir valident nos conclusions.

## État des lieux

Les équipes de sécurité subissent 5 macro-tendances qui nourrissent leur transformation :

- L'univers des menaces devient plus sophistiqué et les cybercriminels s'investissent pour contourner les lignes de défense en place.
- La surface d'attaque des entreprises s'étend rapidement et les divers équipements utilisés sont autant de vecteurs potentiels d'attaque.
- Si une approche en profondeur favorise une sécurité robuste, la multiplication des fonctions de sécurité donne lieu à un volume important d'alertes et d'indicateurs : un vrai défi pour les professionnels de la sécurité qui doivent trier et classer ces alertes pour définir leurs priorités.
- La pénurie d'analystes en sécurité compétents et expérimentés ne permet pas aux entreprises de recruter et fidéliser les profils nécessaires.
- La pandémie mondiale de la COVID-19 accélère les initiatives de transformation digitale, celles-ci imposant des investissements non planifiés pour déployer de nouvelles fonctions de sécurité.

Ces cinq macro-tendances ont amené les équipes de sécurité à un point de rupture et elles doivent identifier de nouveaux moyens pour garder la main. L'XDR est justement l'un de ces moyens.

## L'essentiel sur l'XDR

L'XDR est une nouvelle étape dans l'automatisation de la détection et de la réponse aux menaces. Cette approche capitalise sur des concepts qui ont déjà fait leurs preuves avec l'EDR (Endpoint Detection and Response). L'EDR permet déjà aux analystes de détecter et de prendre en charge les menaces qui contournent les lignes de défense traditionnelles pour cibler les Endpoints. Les solutions XDR diffèrent de celles dédiées à l'EDR puisqu'elles intègrent des indicateurs de sécurité provenant de différentes couches de sécurité. La corrélation et l'analyse des signaux et des données permet d'identifier et d'isoler les menaces. L'XDR se substitue aux tâches complexes pour consolider ces données au sein de plateformes SIEM ou de lacs de données, ce qui permet aux équipes de sécurité de se focaliser davantage sur la détection et l'investigation, plutôt que sur la conception et la gestion d'outils d'agrégation et d'analyse de données.

Si les offres XDR sont relativement nouvelles sur le marché, leurs concepts sous-jacents ont fait leurs preuves et sont mis en œuvre depuis déjà plusieurs années par les équipes de sécurité les plus matures. L'XDR offre l'opportunité d'atteindre un tout nouveau niveau d'automatisation et de fiabilité qui permet aux équipes de sécurité de garder la main sur des menaces en évolution rapide.

### L'EDR est devenu un pilier pour la majorité des équipes de sécurité

Les architectes en sécurité travaillent sans relâche pour intégrer et pérenniser un panel de fonctions de sécurité protégeant les données, les applications et l'infrastructure. Les stratégies de défense en profondeur sont devenues monnaie courante pour de nombreuses entreprises, avec une volonté d'intégrer les fonctions autonomes constitutives de l'infrastructure de sécurité. Cette approche a fait ses preuves pour beaucoup d'entreprises, mais crée des défis supplémentaires chez d'autres, avec notamment un cloisonnement des données qui empêche toute corrélation, ainsi qu'une multiplication des alertes, devenues trop nombreuses pour être triées et traitées de manière efficace.

Traditionnellement, la fonction de détection tire parti d'indicateurs réseau pour surveiller les comportements suspects. Les équipes en charge des analyses post-incident doivent accéder aux données des Endpoints pour déterminer l'impact des attaques et leurs méthodes. Cette prise de conscience a encouragé l'émergence d'outils de détection et de réponse pour les Endpoints, capables de recueillir les indicateurs historiques permettant aux enquêteurs de « remonter le temps » pour étudier les attaques passées. La détection et la réponse aux incidents sur les Endpoints octroient un niveau de visibilité auparavant impossible via les techniques traditionnelles d'analyse réseau.

Si les outils EDR étaient dans un premier temps utilisés dans un contexte d'analyse post-incident, les équipes de sécurité se sont rendues compte que les fonctions primaires de sécurité (antivirus, pare-feu, sécurité email et autres) présentaient certaines limites dans leur capacité à prévenir les attaques : il suffisait qu'une infime partie de ces attaques réussisse pour compromettre l'infrastructure. Ce constat est à l'origine d'une méthode employée par les équipes de sécurité consistant à prévenir ce qui était possible de prévenir, et utiliser la détection et la réponse aux menaces dans le cas contraire. C'est ainsi que l'EDR s'est imposé auprès des équipes de sécurité.

Avec la sophistication des attaques, même les solutions EDR ont montré leurs limites face aux menaces ATP et furtives. Les équipes de sécurité matures et disposant des budgets adéquats ont su relever ce défi en agrégeant et corrélant les indicateurs de sécurité provenant de multiples fonctions de sécurité, et en utilisant un traitement analytique avancé pour offrir une visibilité rapide et fiable sur les attaques modernes. Notre étude indique que ces entreprises ayant utilisé cette approche sont moins confrontées à des attaques réussies, répondent plus rapidement aux menaces et savent traiter un maximum d'alertes. Cette approche affiche ainsi des résultats supérieurs dans la protection des données, des applications et de l'infrastructure. Elle exige néanmoins davantage de temps et de budget, ainsi que des compétences spécialisées pour pouvoir agréger, intégrer et analyser les signaux provenant de multiples fonctions de sécurité. Pour ces raisons, seules les équipes de sécurité les plus aguerries ont su mettre en œuvre cette approche avec succès.

### Mais n'est-ce pas ce que fait le SIEM justement ?

Depuis les cinq dernières années, les entreprises tentent de tirer le meilleur parti du SIEM. L'idée consiste à injecter autant de logs et d'indicateurs de sécurité que possible dans le SIEM, pour identifier et traiter les menaces. Cependant, les plateformes SIEM peinent à corréler les évènements de manière efficace, en déléguant cette tâche à des analystes en sécurité qui doivent consolider les signaux et indicateurs d'attaque.

Si le SIEM a été largement adopté, l'étude d'ESG montre que peu d'entreprises pensent que cette technologie tient toutes ses promesses. La majorité d'entre elles estime que le besoin en compétences expertes est trop important pour déployer et utiliser un SIEM de manière efficace au quotidien. Pour autant, le SIEM est majoritairement considéré comme un outil qui améliore les capacités des entreprises à enquêter sur les menaces. Les entreprises qui se sont investies dans la conception de règles personnalisées, l'intégration de données et le traitement analytique affichent les résultats les plus encourageants en matière de sécurité. Elles précisent néanmoins qu'il est nécessaire de former des experts pour atteindre un tel résultat.

## Comprendre toute la valeur de l'XDR

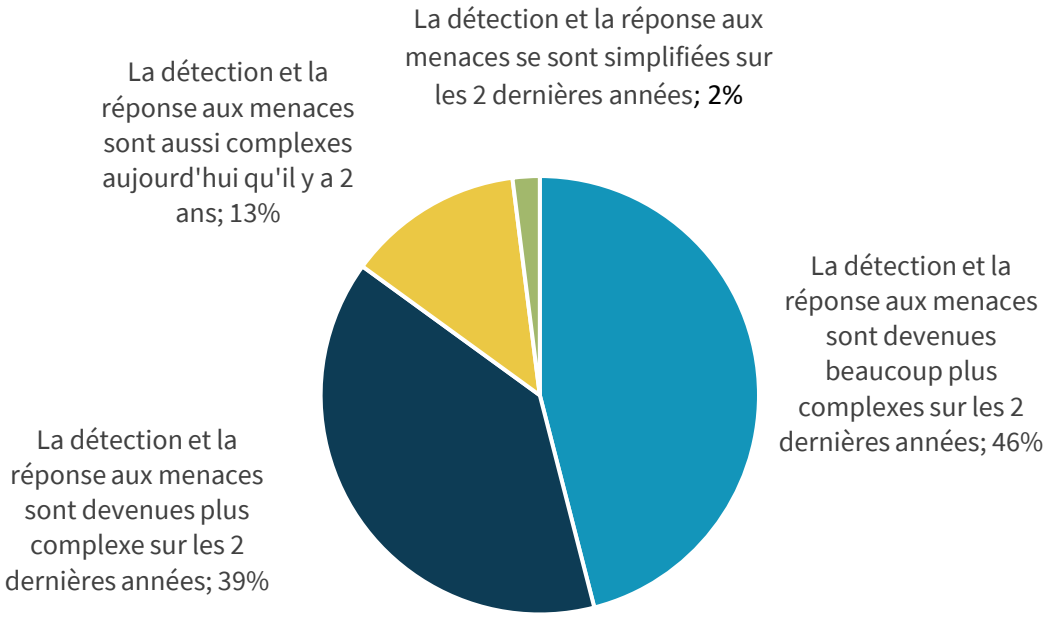
L'XDR étant une solution plutôt nouvelle, l'équipe d'ESG se base sur une comparaison de technologies pour identifier et mesurer la création de valeur de l'XDR. L'objectif est d'identifier les entreprises qui utilisent déjà des processus d'automatisation technologiques proches de l'XDR dans l'objectif d'évaluer des avantages spécifiques, et de les comparer avec celles qui n'ont pas pris cette orientation.

500 personnes, issues de différents secteurs d'activité, ont été interrogées en Amérique du Nord durant l'été 2020 pour identifier les approches actuelles en matière de détection et de réponse aux menaces, et notamment celles qui font appel à l'automatisation.

Notre étude révèle que 85% des entreprises indiquent que la détection et la réponse aux menaces deviennent plus complexes (voir illustration 1). De plus, 81% d'entre elles indiquent que l'amélioration de cette activité est une priorité à laquelle un budget a été alloué.

## Illustration 1. La détection et la remédiation aux menaces deviennent un vrai défi

**Laquelle de ces déclarations reflète au mieux votre opinion en matière de détection et de réponse aux menaces ? (en % des répondants, N=500)**



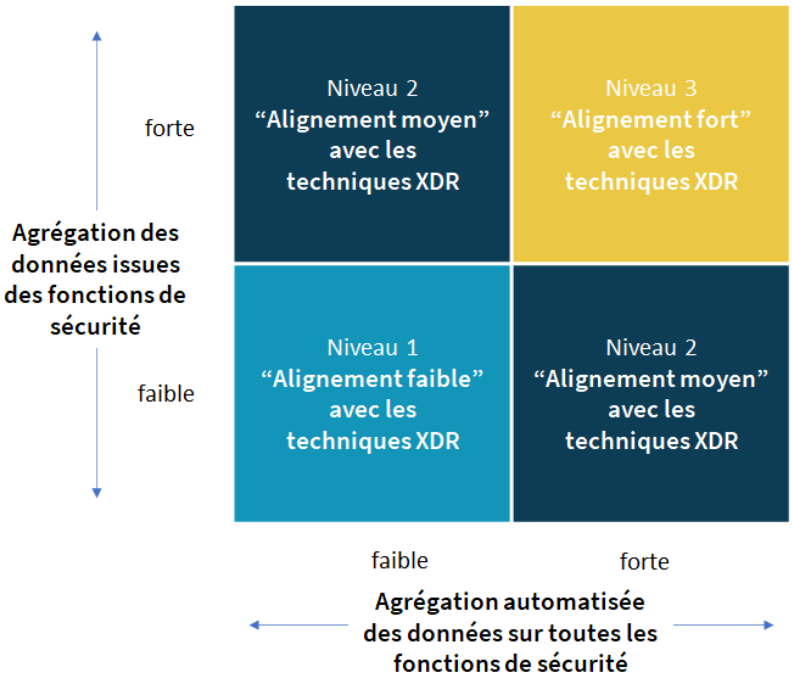

*Source: Enterprise Strategy Group*

57% des personnes interrogées déclarent que l'un des principaux défis constatés concerne la complexité croissante des menaces. 41% d'entre elles estiment que leur panel d'outils de sécurité devient particulièrement complexe. Enfin, c'est le recrutement de profils compétents en sécurité qui continue à être difficile pour 39% des entreprises.

### Les entreprises alignées sur une approche XDR affichent un meilleur niveau de sécurité

L'étude ESG a été initiée en créant un modèle qui évalue la valeur générée par les entreprises déployant une approche similaire à l'XDR. L'objectif était d'établir trois échantillons présentant différents niveaux de maturité, le niveau 3 regroupant les entreprises les plus en phase (alignées) avec l'XDR. Comme l'indique l'illustration 2, notre évaluation s'effectue selon 2 critères : le niveau d'agrégation et de corrélation entre plusieurs fonctions de sécurité et, d'autre part, le niveau d'automatisation qui s'applique à ce processus.

## Illustration 2. Modèle ESG d'évaluation de la valeur créée par l'XDR




Les personnes interrogées ont été réparties en 3 niveaux d'alignement avec XDR, selon leur réponse à 2 questions :

1. Comment décririez-vous les informations associées à vos différents outils de sécurité et de détection/réponse aux menaces ?
   Cloisonnées ← → Consolidées
2. Comment décririez-vous le processus d'intégration et d'agrégation des données issues de vos différents outils de sécurité et de détection/réponse aux menaces ?
   Manuel ← → Automatisé

ESG tire parti de ces attributs pour évaluer le niveau d'alignement avec l'XDR.

*Source: Enterprise Strategy Group*

Comme illustré ci-dessous, 21% de notre panel présente le plus haut niveau d'alignement avec l'XDR : ces entreprises automatisent l'agrégation, la corrélation et l'analyse des données issues des fonctions de sécurité.

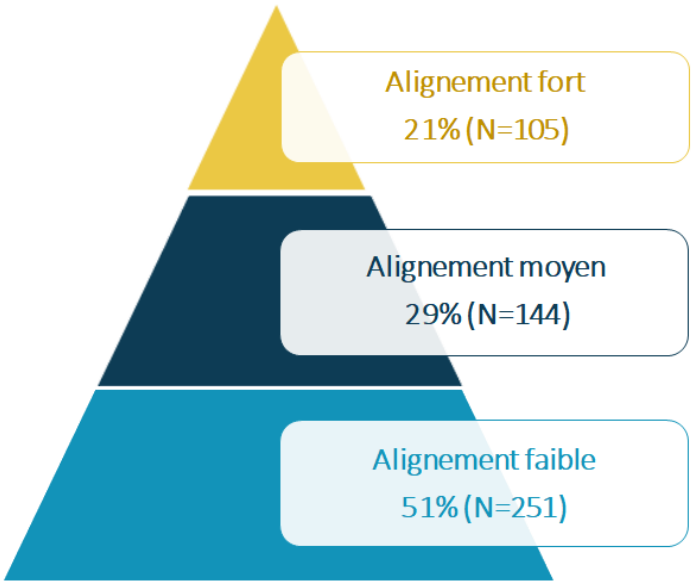
## Illustration 3. Modèle de maturité par rapport à l'XDR

Sur la base des réponses, ESG a classifié les entreprises de la façon suivante. Cette classification est cohérente, quelle que soit la taille des entreprises :

**Alignement fort (niveau 3) :**
- Agrégation automatisée des données à partir des différentes fonctions de sécurité
- 21% du marché actuel

**Alignement moyen (niveau 2) :**
- Des données de sécurité majoritairement cloisonnées et une agrégation partiellement automatisée, **OU**
- Des données agrégées à partir de toutes les fonctions de sécurité, mais avec de nombreux processus manuels
- 29% du marché actuel

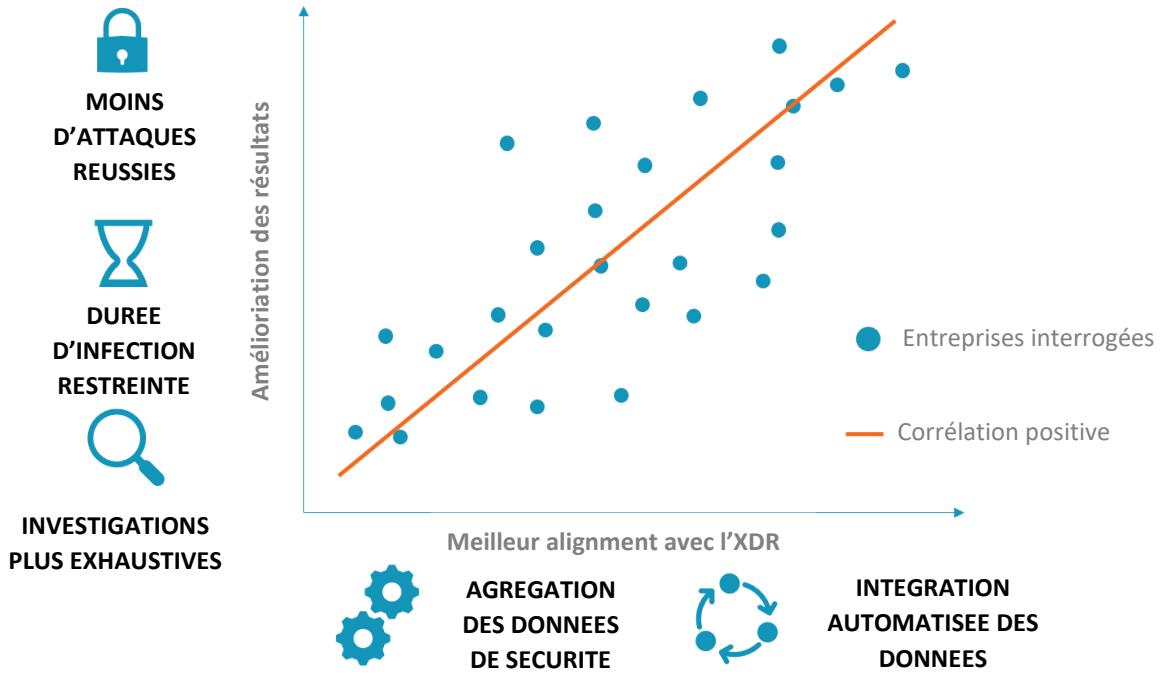
**Alignement faible (niveau 1) :**
- Des données de sécurité essentiellement/totalement cloisonnées et une agrégation 100% manuelle
- 50% du marché actuel




*Source: Enterprise Strategy Group*

L'hypothèse de notre enquête est que les entreprises qui automatisent l'agrégation, la corrélation et l'analyse des données de sécurité réduisent la durée d'infection (dwell time) des menaces et subissent moins d'attaques réussies.

**Illustration 4. Validation de l'hypothèse de maturité de l'alignement avec XDR**

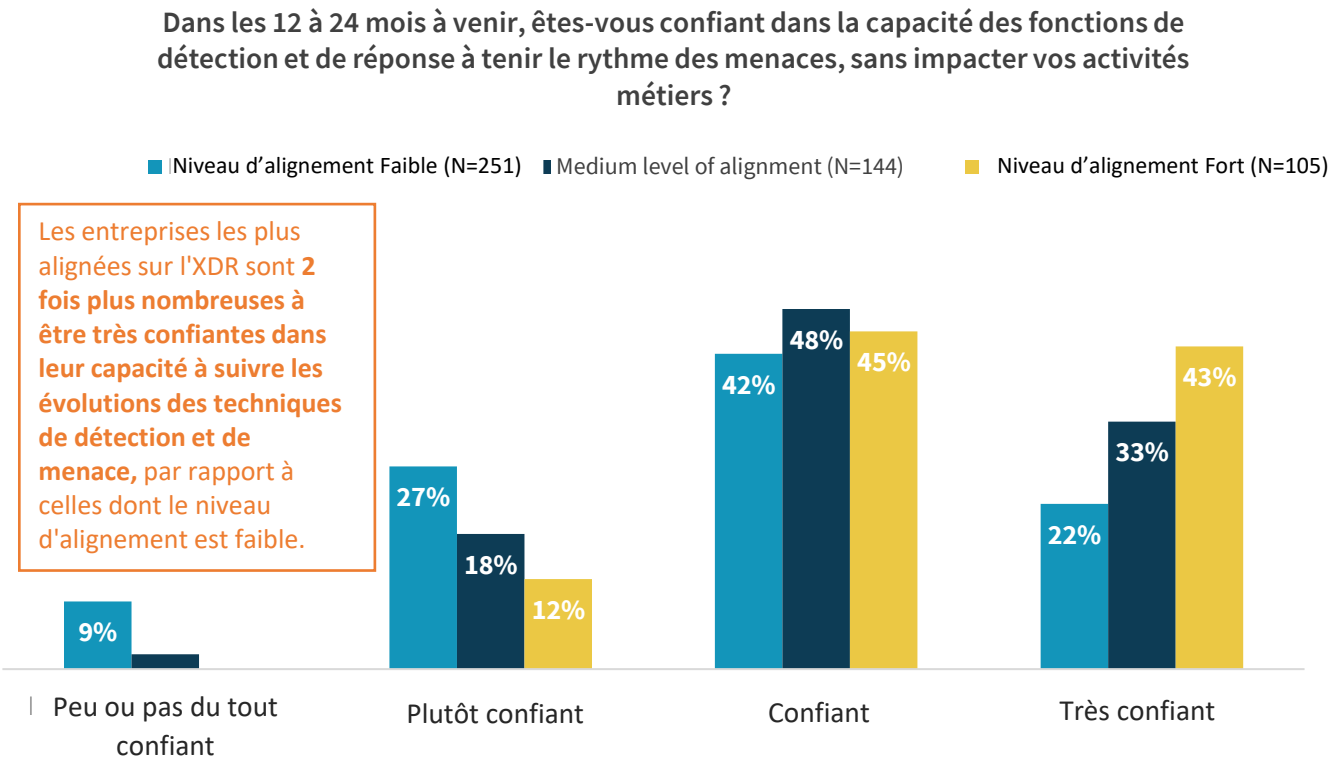



*Source: Enterprise Strategy Group*

## Les entreprises de niveau 3 subissent deux fois moins d'attaques réussies que les autres

Comme attendu, les entreprises de niveau 3, celles les plus alignées sur l'XDR, déclarent subir beaucoup moins d'attaques réussies. Elles ont aussi l'impression de bien s'en sortir en matière de détection et réponse aux menaces, surperformant leurs homologues de niveau 1 et 2. Ces entreprises de niveau 3 estiment également que la corrélation des données issues des différentes couches de sécurité aboutit à de nombreux avantages opérationnels et de sécurité.

## Illustration 5. Les capacités de détection et de réponse dépendent du niveau d'alignement avec l'XDR




*Source: Enterprise Strategy Group*

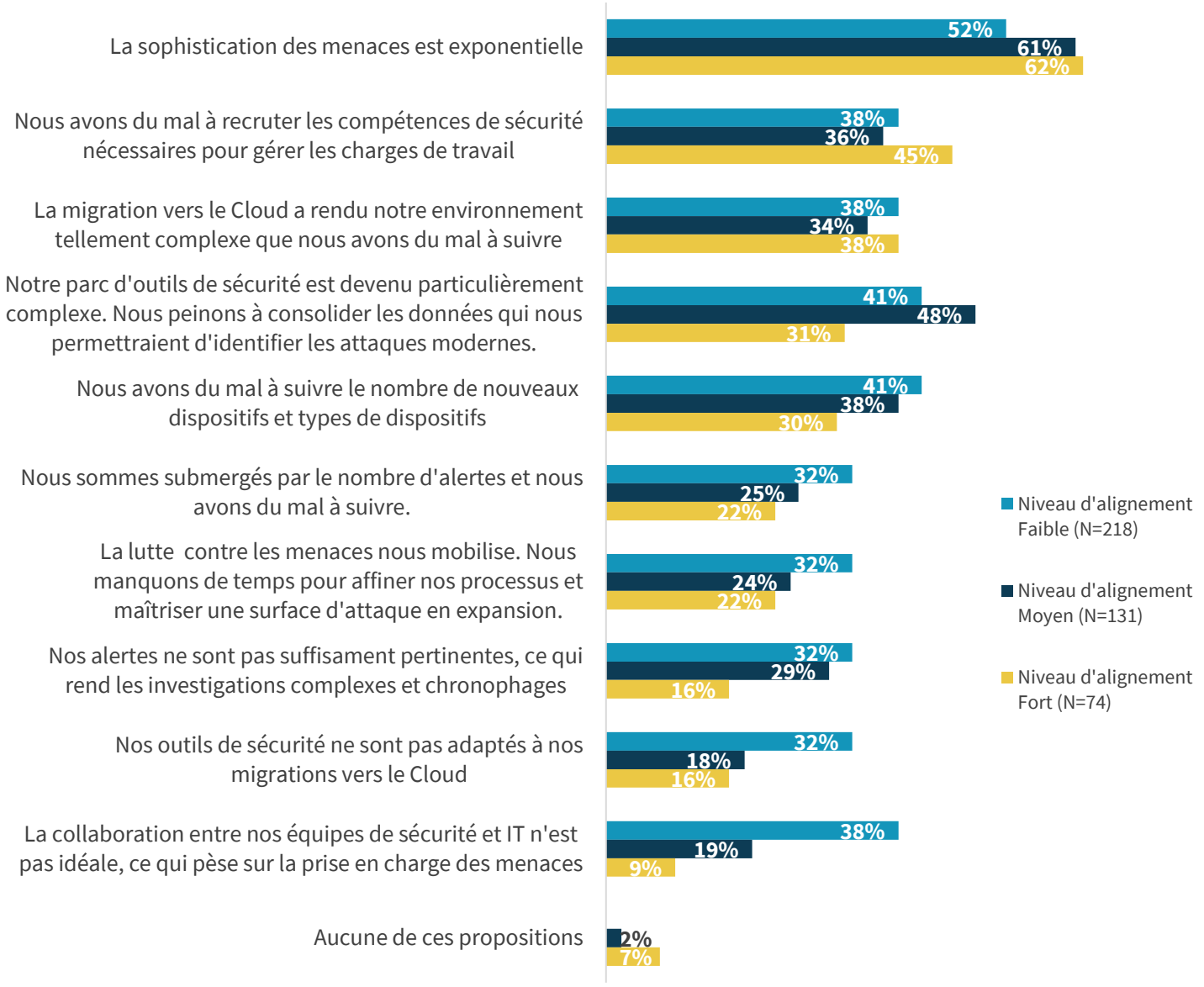
D'un point de vue quantitatif, les entreprises du niveau 3 ont subi deux fois moins d'attaques réussies sur les 12 derniers mois. Lorsqu'interrogées sur le nombre de personnes en ETP (équivalent temps plein) qui leur semble nécessaire pour remplacer leurs systèmes automatisés, la réponse ressort à une moyenne de 8 ETP, ce qui constitue, pour la majorité des entreprises, un investissement irréalisable. Les entreprises du niveau 1 ignorent deux fois plus d'alertes que celles du niveau 3, ce qui crée des zones d'ombre et génère des risques qui ne sont pas traités.

**Lorsqu'interrogées sur le nombre de personnes en ETP (équivalent temps plein) qui leur semble nécessaire pour remplacer leurs systèmes automatisés, la réponse ressort à une moyenne de 8 ETP.**

Notons que la sophistication grandissante des menaces est citée par toutes les entreprises interrogées comme étant le principal défi en matière de détection et prise en charge des menaces. Les entreprises du niveau 1 sont celles qui subissent le plus l'introduction de nouveaux dispositifs, les applications cloud, le nombre d'alertes et l'absence de données contextuelles dans les alertes (voir illustration 6).

## Illustration 6. Les entreprises en phase avec l'XDR s'en sortent le mieux face au niveau opérationnel

**Vous avez précisé que la détection et la réponse aux menaces sont devenues plus complexes sur les 2 années passées. Quels sont les principaux défis qui pèsent sur votre entreprise ? (en % des répondants)**

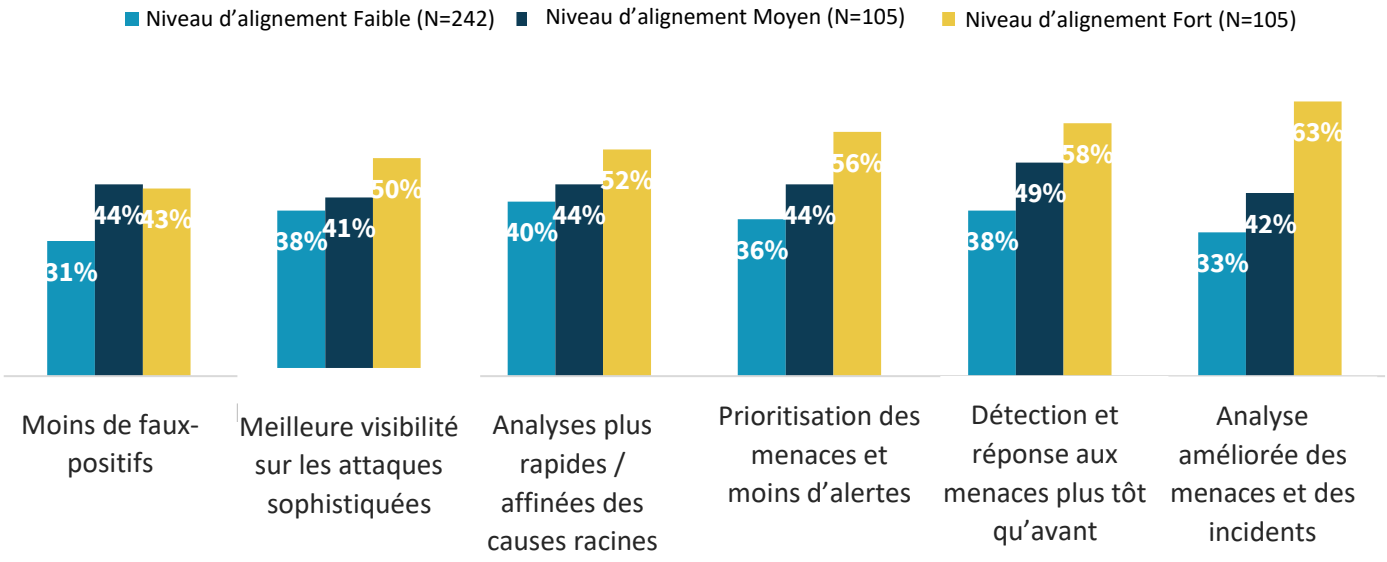



*Source: Enterprise Strategy Group*

En nous penchant sur les axes d'amélioration, nous constatons que les acteurs du niveau 3 affichent de meilleurs résultats sur l'ensemble des critères, avec de réelles améliorations en matière d'analyse des menaces/incidents, de prioritisation des alertes, de visibilité au sein des attaques sophistiquées et de temps de réponse et de détection. À noter également que les entreprises de niveau 2 superforment celles du niveau 1.

## Illustration 7. Les entreprises les mieux alignées avec l'XDR sont les plus susceptibles de s'améliorer

**Vous avez indiqué que votre entreprise est assez efficace pour corréler les données de menaces en matière de détection/réponse. Quelles sont les améliorations qui en résultent? (% des répondants)**

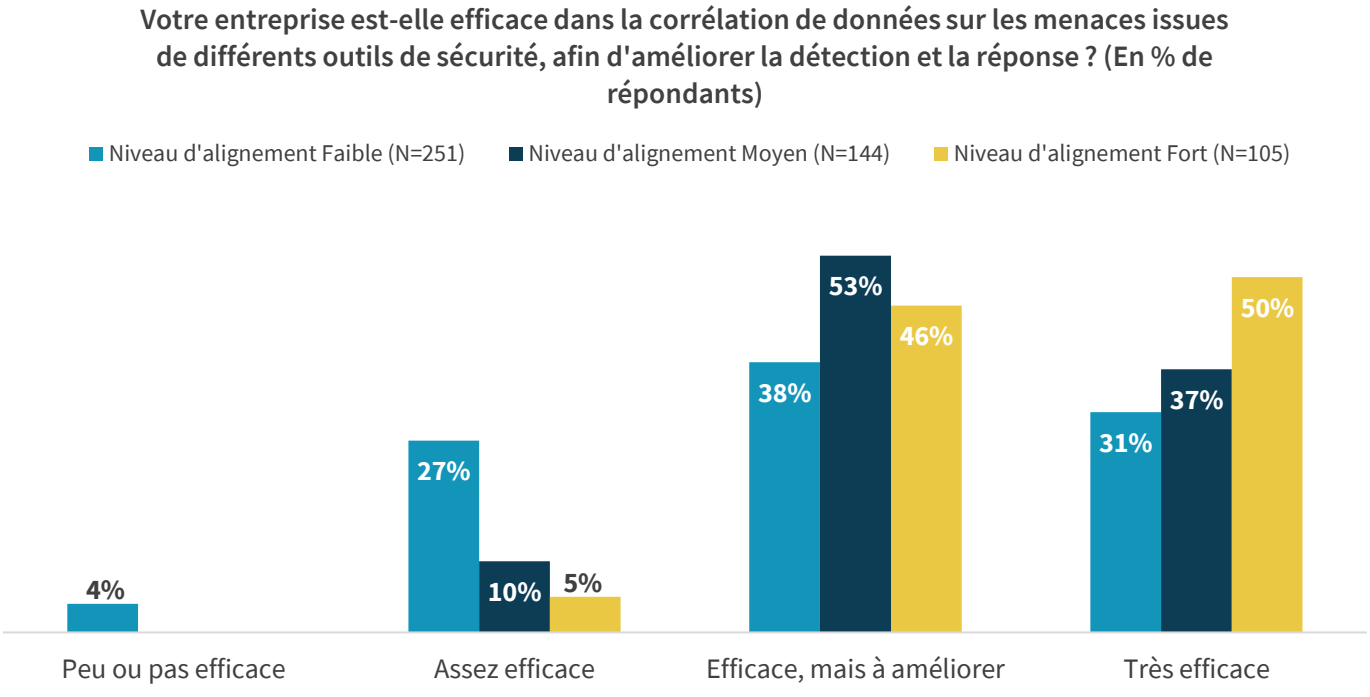



*Source: Enterprise Strategy Group*

### Meilleure corrélation = Meilleurs résultats

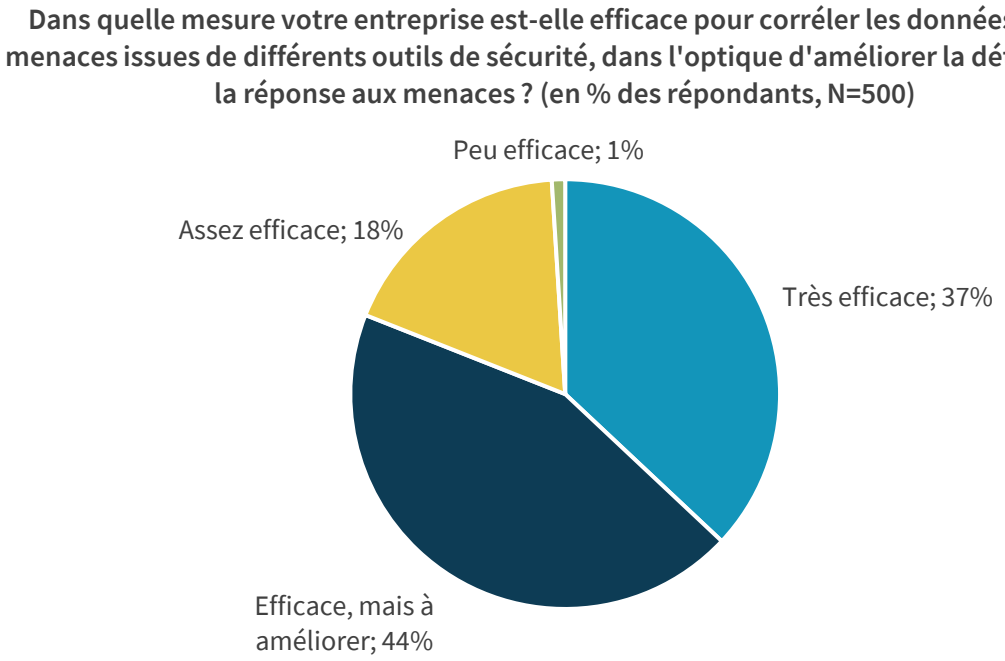
Les entreprises de niveau 3 ont 61% plus de chances d'être plus efficaces dans la corrélation de données issues des différents outils de sécurité, par rapport à celles de niveau 1 et 2. 50% d'entre elles se déclarent très efficaces (voir illustration 8). Même avec de tels résultats, 63% des personnes interrogées estiment pouvoir s'améliorer davantage sur le terrain de la corrélation de données (voir illustration 9). La volonté d'affiner la détection des attaques modernes implique de s'investir de manière permanente pour faire progresser la stratégie de corrélation, même lorsque l'automatisation est effective. Ce processus est facilité par nombre de solutions XDR dont la promesse est d'affiner de manière permanente et automatisée ces stratégies en tirant parti d'une veille sur les menaces fournies par l'éditeur de la solution.

## Illustration 8. Efficacité de la corrélation des données, selon le niveau d'alignement




*Source: Enterprise Strategy Group*

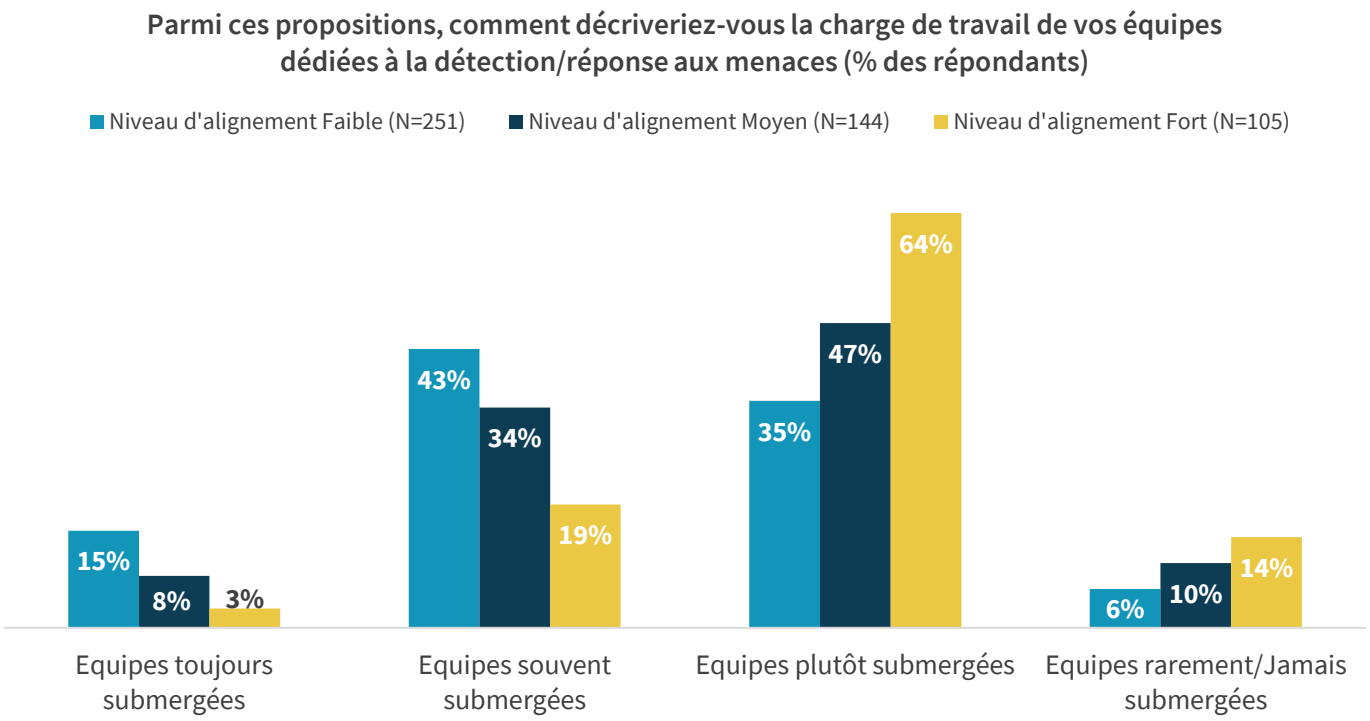
## Illustration 9. Efficacité de la corrélation des données, tous niveaux confondus




*Source: Enterprise Strategy Group*

Par rapport aux entreprises de niveau 3, celles de niveau 1 ont 2,6 fois plus de chances de déclarer que leur équipe dédiée à la détection et la remédiation des menaces est submergée (voir illustration 10). La corrélation manuelle des données est chronophage et exige un travail important : les analystes travaillant pour des entreprises de niveau 1 consacrent ainsi moins de temps aux activités d'investigation. Voilà qui pèse sur les équipes qui subissent des carences en compétences.

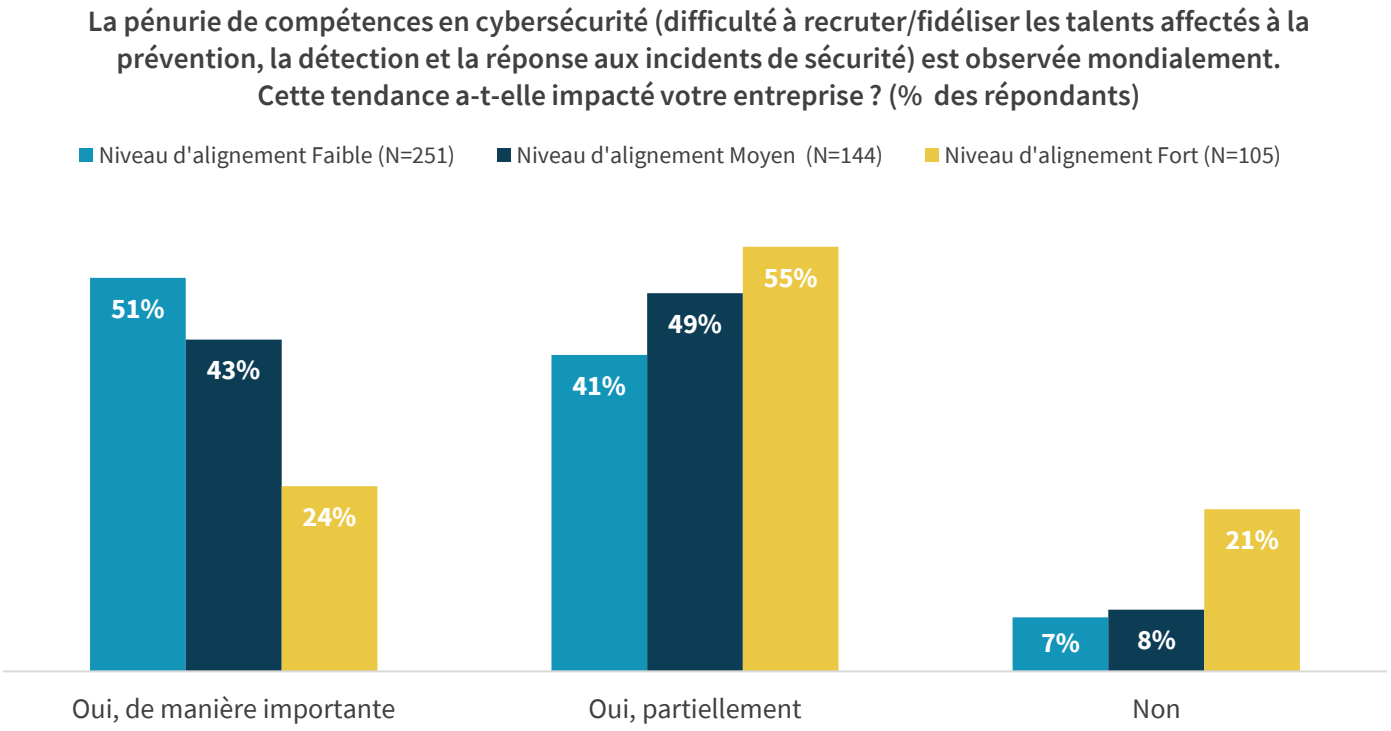
## Illustration 10. Charge de travail des équipes de détection et réponse, selon le niveau d'alignement




*Source: Enterprise Strategy Group*

Les acteurs du niveau 1 ont tendance à subir davantage la pénurie de compétences en cybersécurité.

## Illustration 11. Impact de la pénurie de compétences en cybersécurité, par niveau d'alignement



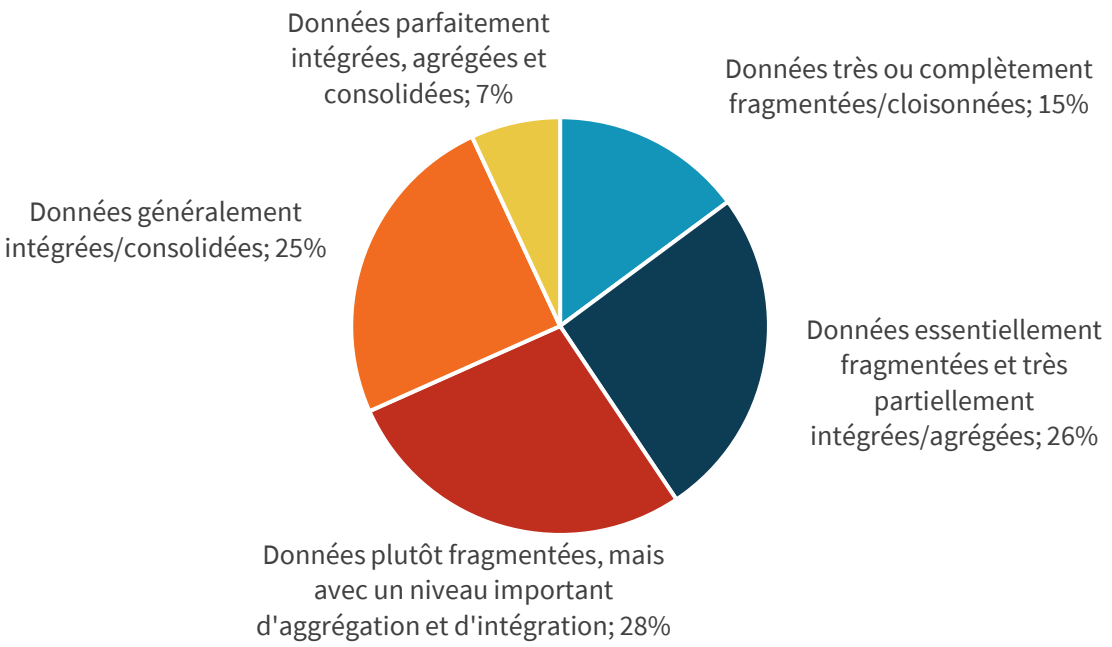

*Source: Enterprise Strategy Group*

## Des données généralement cloisonnées

Le cloisonnement des données est une réalité pour la plupart des organisations. Elles sont 41% à déclarer disposer de données fragmentées (Illustration 12) et 61% à opter pour une approche manuelle pour intégrer et agréger les données en provenance des différentes fonctions de sécurité. Il est ainsi complexe de garder la main sur la sophistication croissante des attaques modernes.

**Illustration 12. Fragmentation des informations de sécurité, de détection et de réponse**

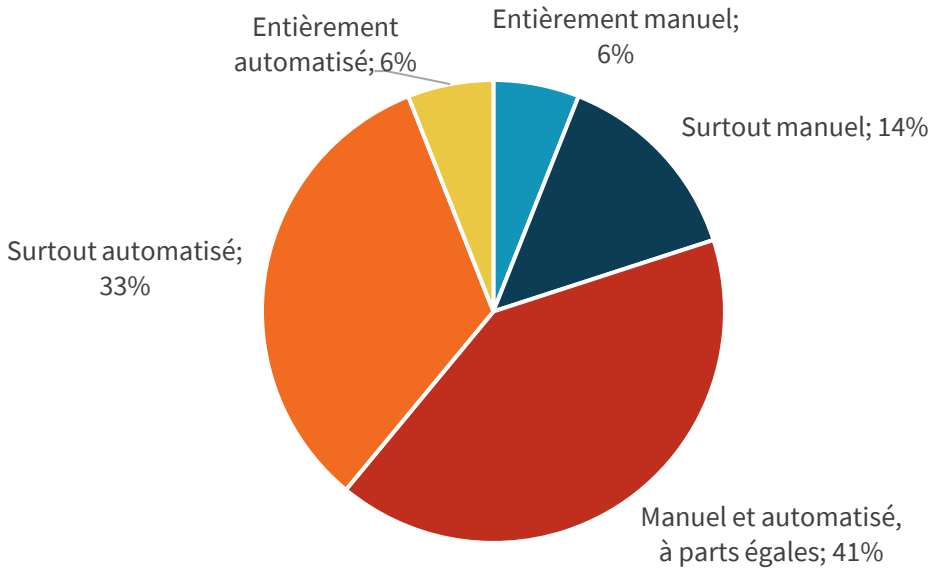
**Comment décririez-vous les informations/données issues de vos fonctions de sécurité et de détection/réponse aux menaces ? (% des répondants, N=500)**




*Source: Enterprise Strategy Group*

## Illustration 13. Intégration et agrégation des données de sécurité, de détection et de réponse

**Comment décririez-vous le processus d'intégration/d'agrégation des données issues de vos fonctions de sécurité, de détection de menace et de réponse ? (% des répondants, N=500)**




*Source: Enterprise Strategy Group*

Les entreprises qui assurent une corrélation efficace des données bénéficient d'améliorations opérationnelles majeures, parmi lesquelles des investigations plus rapides, une réponse accélérée aux menaces et une simplification des processus manuels. Les entreprises de niveau 3 sont 46 % plus nombreuses à avoir su accélérer les temps de réponse par rapport à leurs homologues moins alignés sur l'XDR.

## Illustration 14. Améliorations opérationnelles dues à une corrélation efficace des données de sécurité

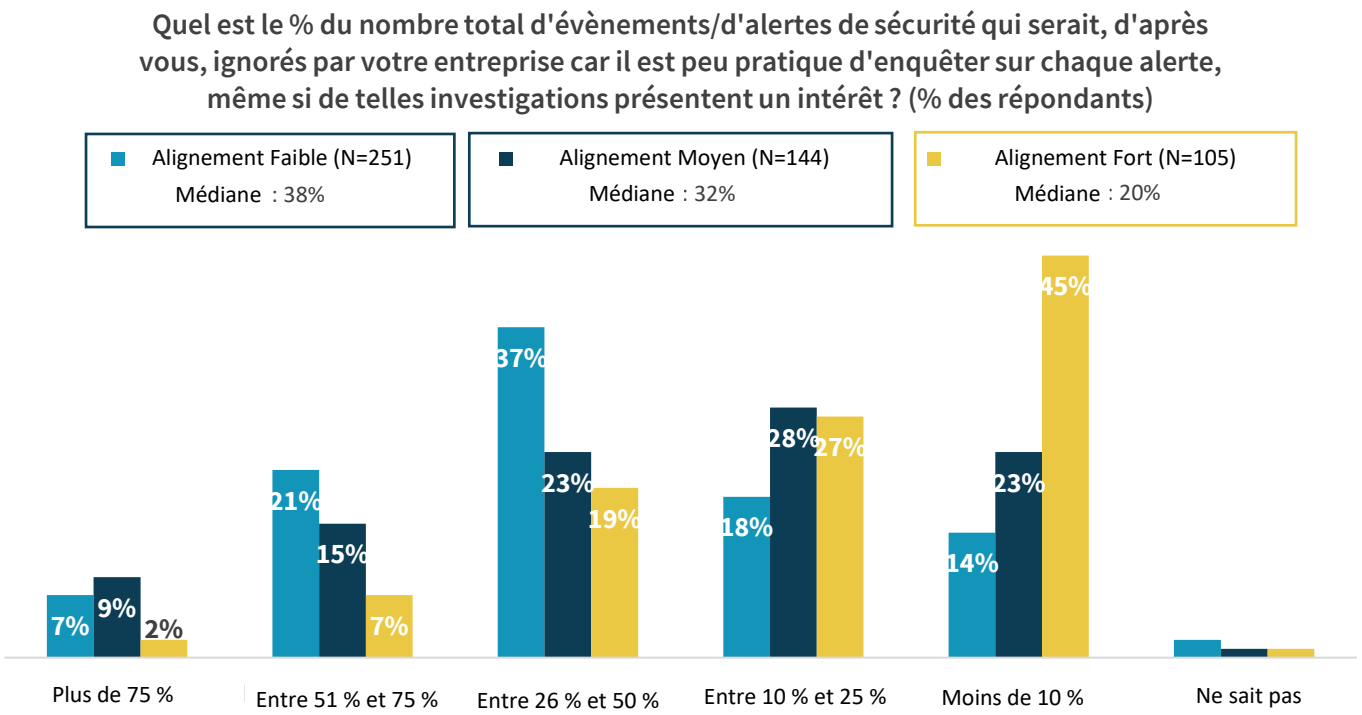

*Source: Enterprise Strategy Group*

### Les entreprises de niveau 3 ignorent bien moins d'alertes

72% des entreprises de niveau 3 ignorent moins de 25% des alertes alors que 65% des entreprises de niveau inférieur ignorent plus de 25% des alertes (voir illustration 15).

Cet écart important explique que les entreprises de niveau 1 et 2 subissent bien plus d'attaques.

## Illustration 15. Évènements/alertes de sécurité ignorés par les entreprises




*Source: Enterprise Strategy Group*

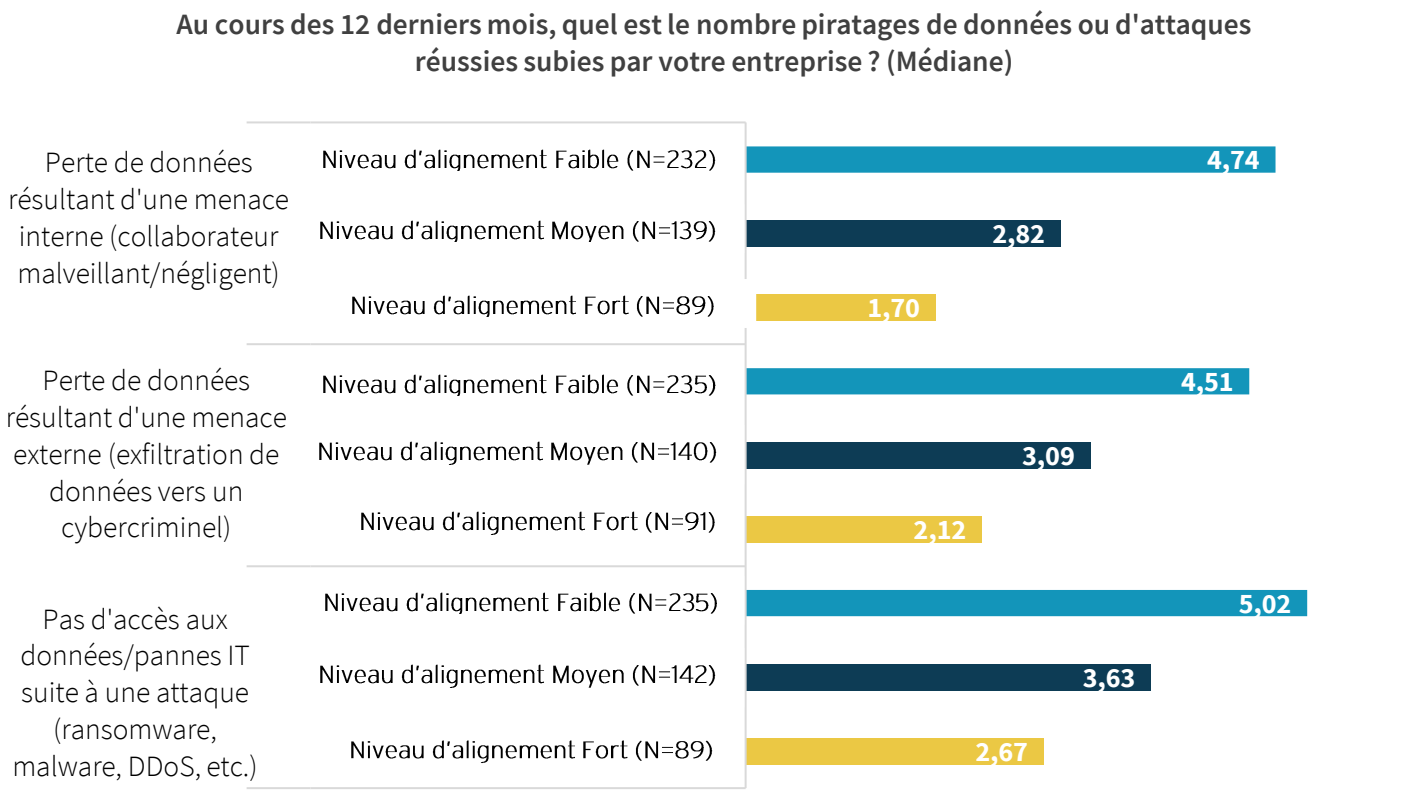
La durée d'infection (Dwell time) est un indicateur essentiel des attaques réussies. 65% des entreprises de niveau 3 indiquent des durées moyennes d'infection de quelques jours ou moins tandis que 45% des entreprises de niveau 1 déclarent que cette durée excède une semaine (voir illustration 16).

## Illustration 16. Durée d'infection moyenne avant détection d'un incident


*Source: Enterprise Strategy Group*

Cet impact est d'autant plus évident lorsque nous nous penchons sur le taux d'attaques réussies sur les entreprises de niveau 3. Celles-ci ont 3 fois moins de chances de subir des attaques réussies.

Illustration 17. Nombre moyen de piratages de données et d'attaques




*Source: Enterprise Strategy Group*

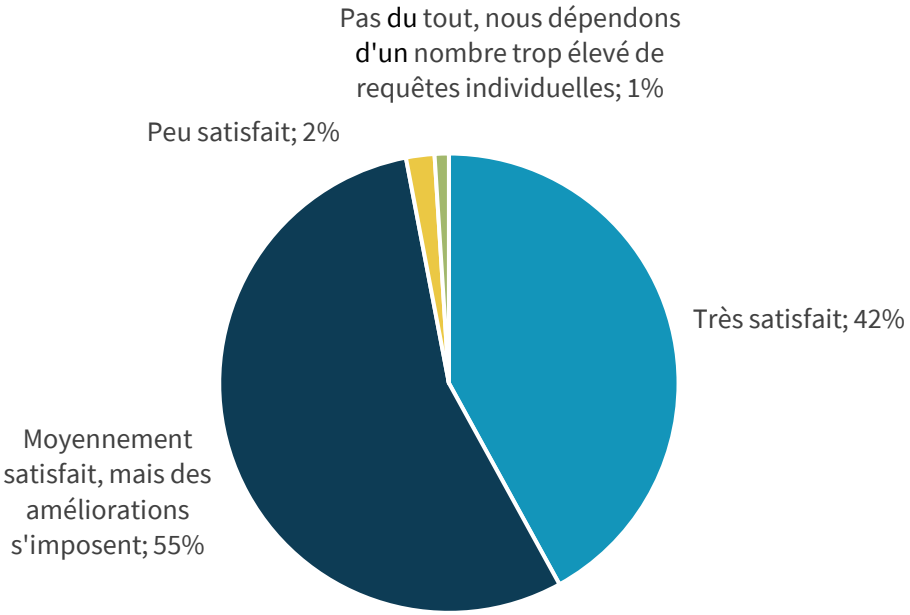
## Pourquoi le SIEM n'est-il pas une réponse suffisante ?

79% des équipes de sécurité actuelles font appel à une solution de gestion des informations et évènements de sécurité (SIEM) pour détecter et enquêter sur les menaces. Le SIEM est aujourd'hui largement adopté en tant qu'outil de sécurité. Pour autant, 57% des organisations utilisatrices se plaignent d'un niveau de bruit trop élevé tandis que seules 42% d'entre elles estiment que le SIEM est un outil efficace pour mener leurs investigations à bien. La raison ? Ce sont les fournisseurs de plateforme SIEM qui la donnent depuis des années.

L'intégration des données est une problématique complexe, comme en témoignent les statistiques ci-dessous. 83% des personnes interrogées déclarent devoir investir de manière continue et importante afin de pouvoir agréger les indicateurs. 55% des entreprises estiment que des progrès sont à faire en matière de corrélation de données (illustration 18).

## Illustration 18. La satisfaction des entreprises en matière de corrélation des SIEM

**Etes-vous satisfait du nombre de corrélations effectuées par votre SIEM pour encourager la détection de menaces et les investigations ? (% des répondants, N=393)**

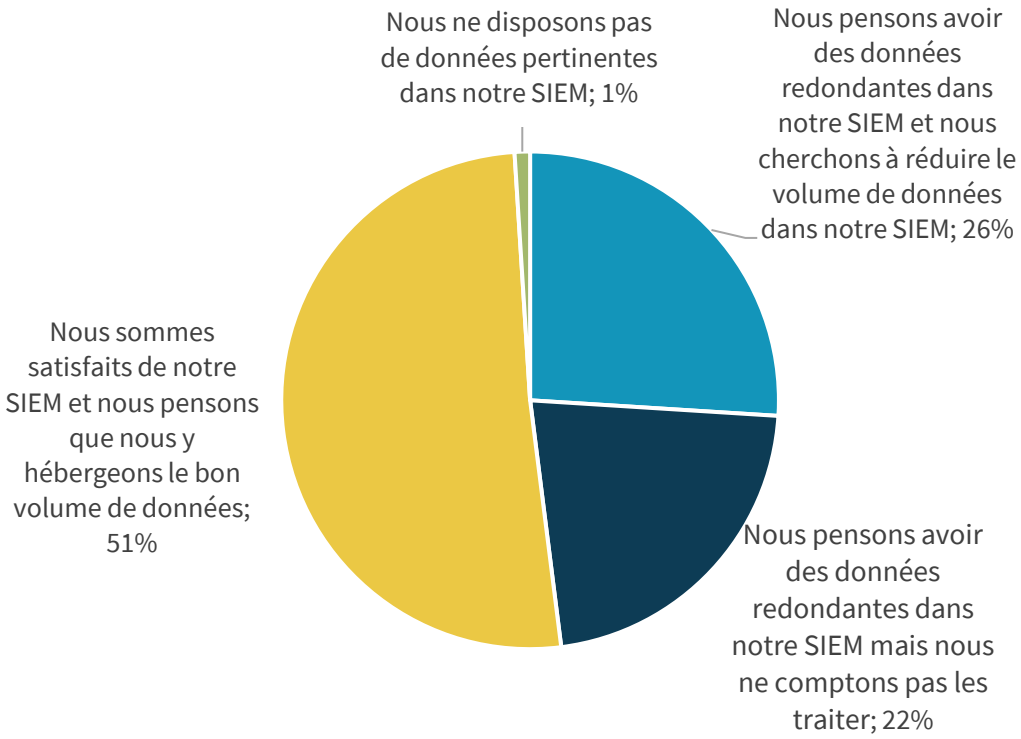



*Source: Enterprise Strategy Group*

50% des entreprises intégrant les données à partir de différentes fonctions de sécurité rencontrent une problématique de redondance de données associée à l'utilisation du SIEM (schéma 19). Compte tenu du coût élevé du SIEM et du fait que de nombreux fournisseurs de SIEM facturent en fonction de la quantité de données utilisées, la réduction de la quantité de données ingérées peut avoir un impact significatif sur les coûts opérationnels globaux.

## Illustration 19. L'opinion des entreprises sur le volume de données intégrées dans leur SIEM

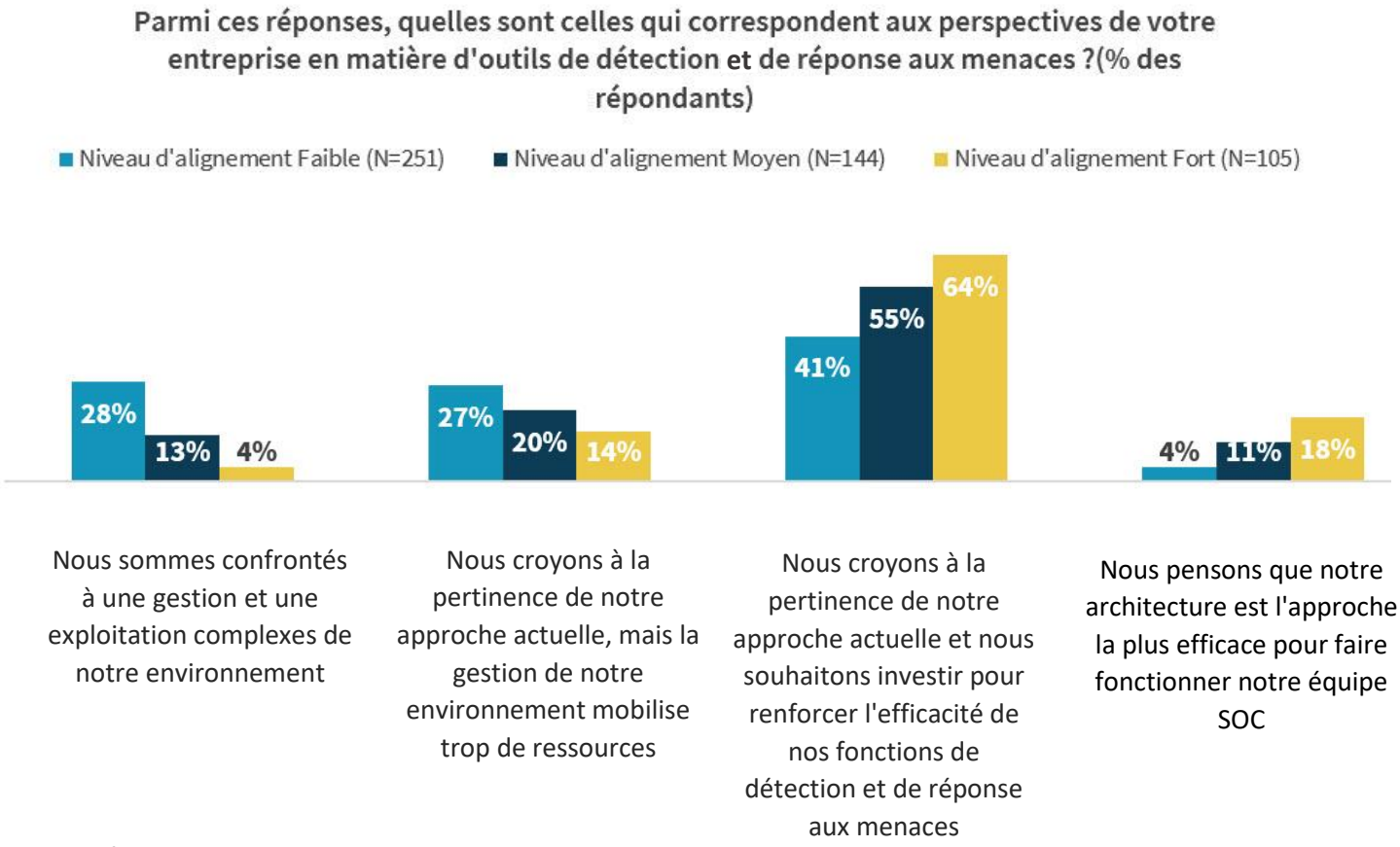
**Votre entreprise est-elle satisfaite du volume de données qui alimentent son SIEM dans une optique d'investigation sur les menaces ? (% des répondants, N=393)**




*Source: Enterprise Strategy Group*

Les organisations de niveau 3, celles les plus en phase avec les pratiques XDR, sont persuadées de la pertinence de leur approche et comptent investir davantage pour améliorer l'efficacité globale de leur activité de détection et réponse aux menaces (Illustration 20). L'amélioration des résultats est un vecteur de confiance. Ce sont les entreprises de niveau 1 qui sont le plus à la peine face à la gestion complexe de leurs environnements.

Illustration 20. Les entreprises envisagent un investissement continu




## Perspectives

La technologie XDR est un vecteur d'automatisation et de fiabilité pour les équipes de sécurité qui ont du mal à garder la main sur des menaces toujours plus nombreuses et complexes. La pénurie de compétences en cybersécurité et l'accélération des initiatives de transformation numérique incitent les équipes de sécurité à identifier de nouveaux leviers de productivité.

Comme en témoignent les résultats présentés dans ce rapport, les entreprises qui ont investi dans l'agrégation et la corrélation des données issues de plusieurs couches de sécurité sont en mesure de détecter et de répondre plus rapidement aux menaces, de gérer davantage d'alertes et de renforcer leur sécurité. Elles sont également moins sujettes aux piratages de données.

Alors que de nombreuses entreprises ont tenté d'obtenir un effet de levier de type XDR à l'aide de leur plateforme SIEM, plus de la moitié d'entre elles s'estiment frustrées par le niveau de complexité, de redondance et d'expertise nécessaires pour exploiter cette technologie.

L'XDR apporte cette approche éprouvée à toutes les équipes de sécurité, sans le coût élevé et la complexité associée à des infrastructures personnalisées de support. Pour les entreprises qui ont du mal à s'en sortir contre les menaces, l'XDR devient un levier pour améliorer la visibilité et les performances. Pour les entreprises qui ont déjà investi dans la définition de pipelines de données personnalisés et d'outils d'analyse, l'XDR offre une nouvelle voie pour obtenir des résultats similaires, mais avec un processus bien plus simple.

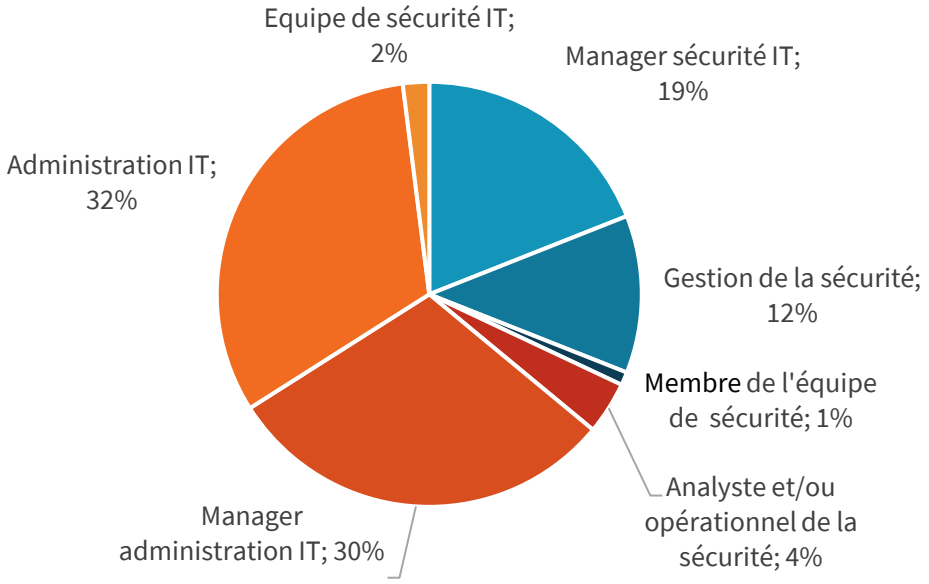
## Méthodologie et segments

Pour recueillir des données pour ce rapport, ESG a mené une enquête exhaustive auprès des professionnels de la sécurité et des responsables des stratégies, des processus et des technologies de détection et d'intervention de leur organisation. Tous les répondants sont basés en Amérique du Nord (États-Unis et Canada) et travaillent pour des organisations de 500 employés ou plus. L'enquête a été réalisée entre le 15 juin 2020 et le 30 juin 2020. Tous les répondants ont été motivés financièrement à répondre au sondage.

Après avoir appliqué les meilleures pratiques en matière de contrôle qualité des données et examiné les réponses restantes (sur plusieurs critères d'intégrité des données), il restait un échantillon final de 500 répondants. Les illustrations 21 à 23 présentent les données démographiques et les critères de segmentation du panel de répondants. Remarque : les sommes des totaux des chiffres et des tableaux dans le présent document sont susceptibles de ne pas représenter 100% en raison des arrondis.

### Illustration 21. Fonctions occupées par les répondants

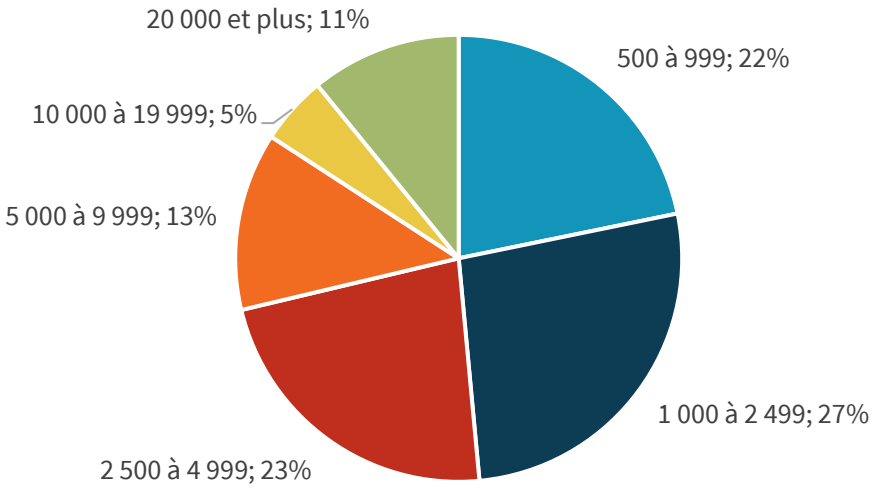
**Quel est, parmi ces intitutlés de postes, celui qui corrrespond le mieux à vos reponsabilités au sein de votre entreprise ? (% de répondants, N=500)**




*Source: Enterprise Strategy Group*

## Illustration 22. Effectif d'entreprise

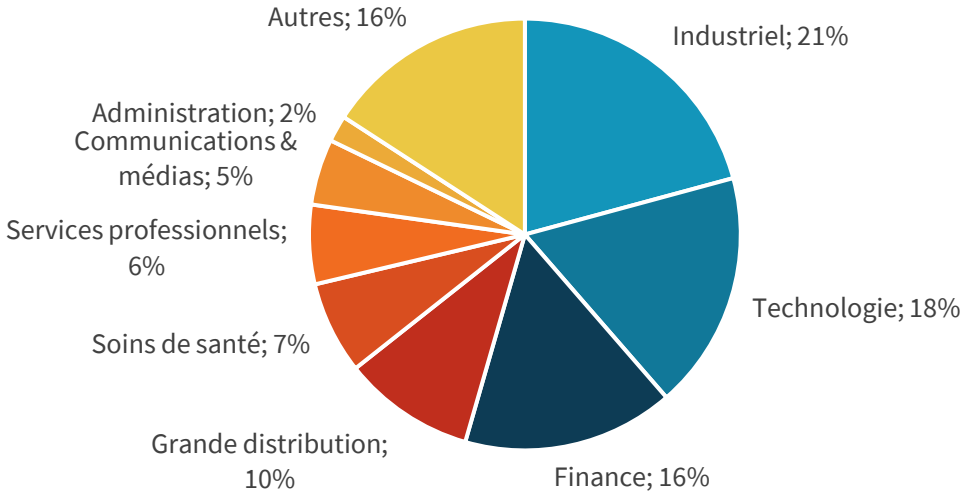
**Quel est l'effectif total de votre entreprise dans le monde ? (% des répondants, N=500)**




*Source: Enterprise Strategy Group*

## Illustration 23. Secteur d'activité principal des entreprises interrogées

**Quel est le secteur d'activité principal de votre entreprise ? (% des répondants, N=500)**




*Source: Enterprise Strategy Group*

**Enterprise Strategy Group** est un cabinet d'analyses stratégiques et d'études du marché de l'informatique, qui offre des services de veille et une visibilité pertinentes aux acteurs de l'informatique dans le monde.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188