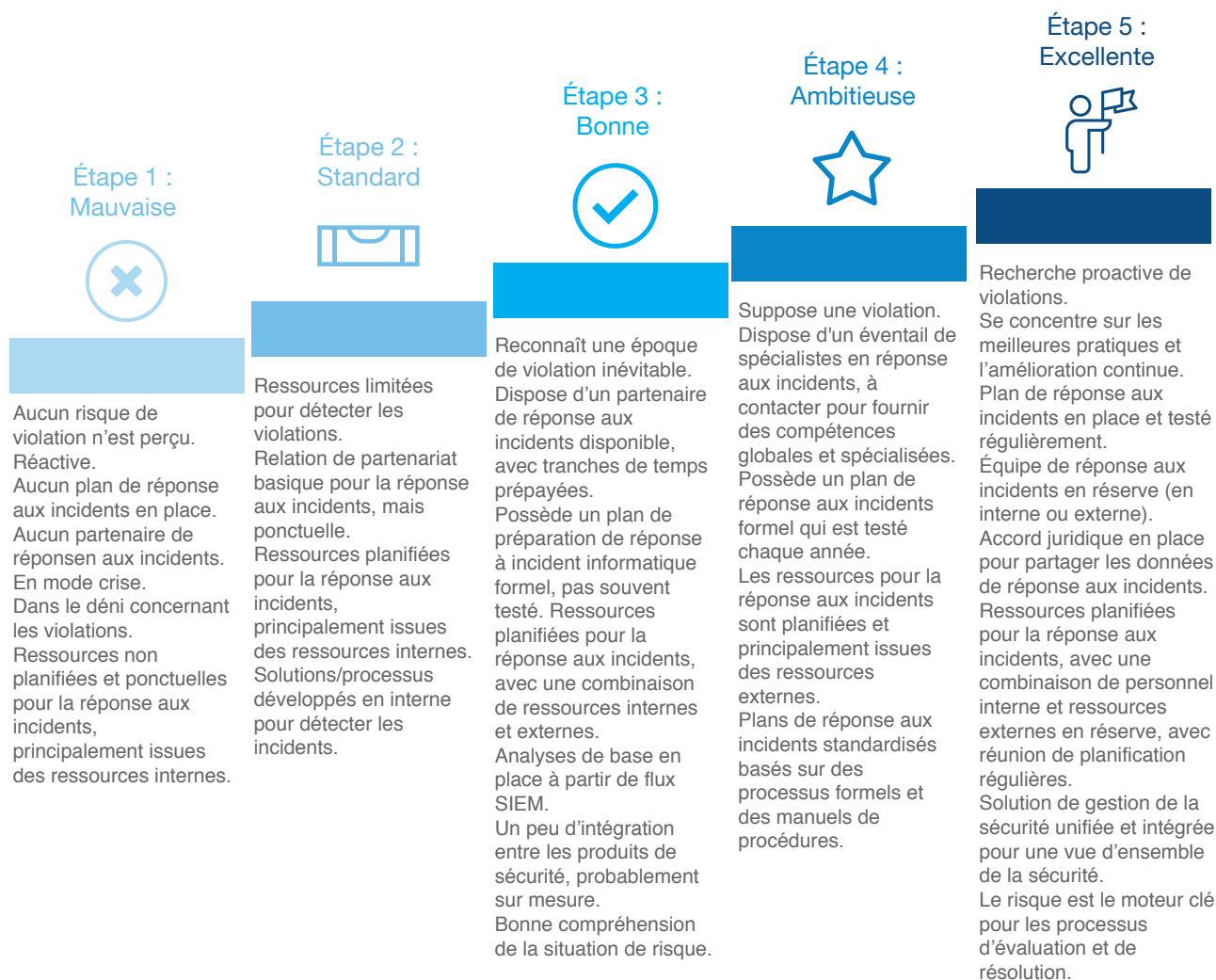


VOTRE ENTREPRISE EST-ELLE EN SÉCURITÉ ?

Note de synthèse

Merci d'avoir répondu à l'évaluation de "Security Response Readiness* d'IDC, sponsorisée par Splunk. Cet outil a été développé pour fournir aux entreprises des informations comparatives sur leur degré de maturité à répondre aux incidents de sécurité, soutenues par des recherches indépendantes. Le sondage a rassemblé les réponses de personnalités influentes dans le domaine de la sécurité ou en charge de budget dans 600 entreprises à travers le monde. L'objectif est de comprendre les différences entre les entreprises avancées en matière de stratégie de sécurité, détection des incidents et réponse aux incidents.

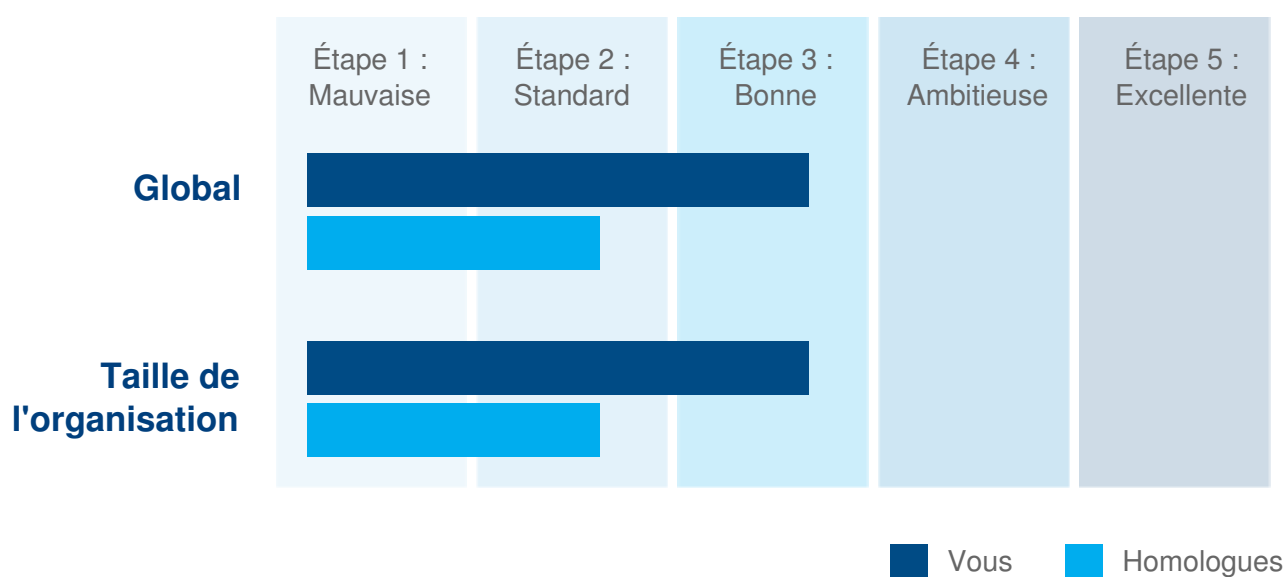
Sur la base de ce sondage, IDC a noté les réponses individuelles et a créé un cadre comparatif, élaboré en regroupant les entreprises en cinq niveaux de "Security Response Readiness"* basés sur leur approche de la stratégie de sécurité, ainsi que de la détection des incidents et de la réaction face à ceux-ci comme le montre la Figure 1. Les entreprises n'ont pas besoin d'être tout en haut de l'échelle pour commencer à percevoir des avantages. Toute amélioration peut apporter des bénéfices tangibles tant pour l'informatique que pour l'entreprise, en augmentant la réactivité, la pérennité et l'innovation grâce à une plus grande latitude. En effet, cela permet d'ajuster la stratégie pour répondre aux conditions changeantes du marché.



Overall Results

Sur la base de vos réponses, vous êtes situé avec **41%** des entreprises dans le groupe de préparation **Étape 3 : Bonne**, qui correspond au niveau **3rd** sur cinq.

Figure 2: Résultats de l'évaluation de Security Response Readiness* IDC



Sommaire général

Par rapport aux entreprises ayant les meilleures capacités, votre entreprise se trouve :

- 1 level ahead of the global leaders
- 1 level ahead of the leaders in companies of the same size

Vos performances en détail

Cet outil d'évaluation a été conçu pour vous aider à déterminer si votre entreprise est prête à faire face à l'évolution des menaces qui touchent les activités informatiques, aujourd'hui et à l'avenir.

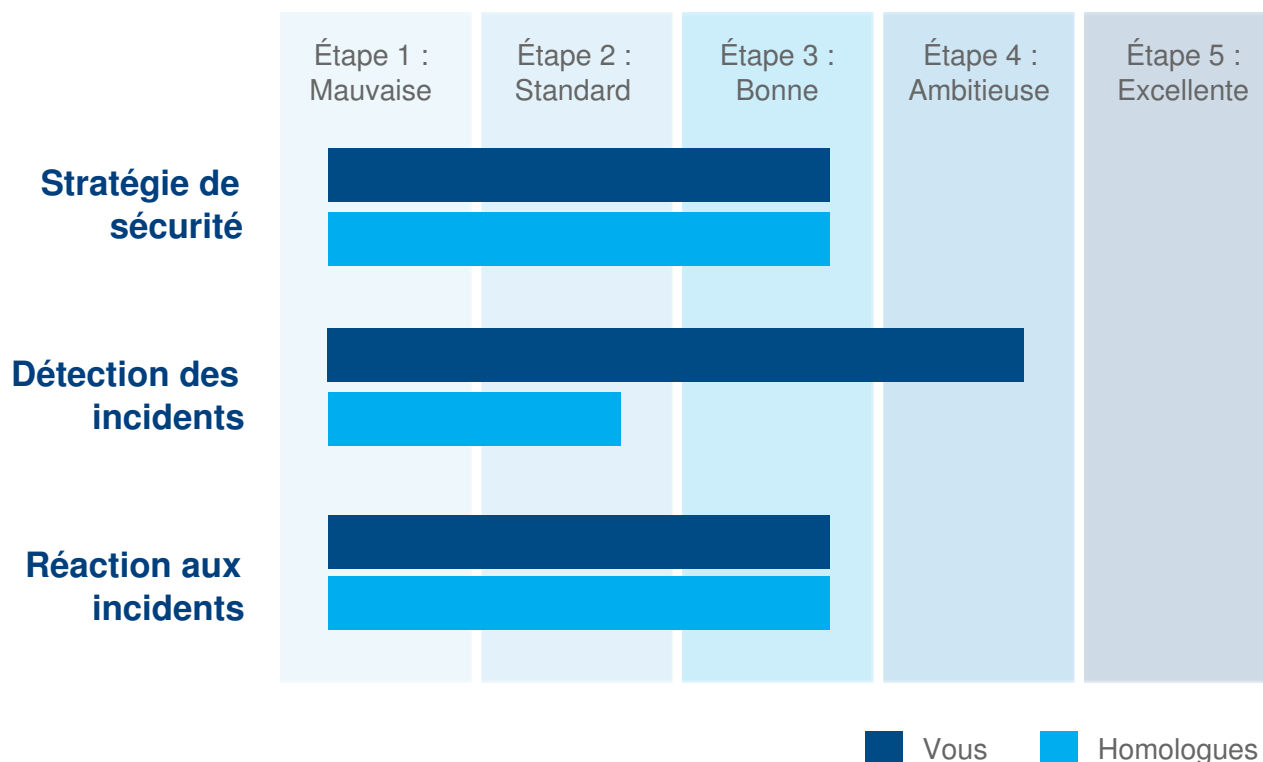
Nous nous sommes penchés sur les domaines clés suivants de la sécurité informatique :

- **Stratégie de sécurité**
- **Détection des incidents**
- **Réponse aux incidents**

Vos performances dans chaque domaine sont comparées à celles de vos homologues à la Figure 3.

Security Response Readiness* IDC par capacité

Figure 3: Security Response Readiness* IDC par capacité



Comment progresser ?

Quel que soit votre niveau, certains domaines continuent d'évoluer et méritent que l'on se concentre dessus plus que tout :

- **Intégration** – Prendre les incidents de sécurité sous tous les angles.
- **Approche proactive** – Réduire le temps entre la violation et la détection, passer de quelques mois à quelques heures (ou moins).
- **Rester en avance sur la conformité** – Il est suffisamment difficile d'arriver à la conformité pour nombre d'entreprises, sans parler de la conserver.
- **Best practice** – Reconnaître que les menaces ne s'arrêtent jamais et que les cadres de conformité et réglementaires sont souvent dépassés depuis des années, même au moment de leur instauration ; adopter une approche et de best practice constituent la meilleure manière d'atténuer les menaces. Avantage supplémentaire, si cela est effectué efficacement, la conformité sera obtenue naturellement.



Améliorations de la réponse aux incidents

Gérer votre réponse initiale à un incident de sécurité sera essentiel pour endiguer la menace et remédier à tout dommage potentiel, mais vous n'avez rien en place pour l'instant. Une plate-forme conçue pour standardiser et gérer cela peut s'avérer particulièrement utile, compte-tenu des exigences en matière de signalement des violations de la nouvelle législation comme la GDPR ou la conformité à l'Assurance contre les violations de sécurité informatique.

Un plan de réponse testé et bien défini est essentiel en cas de violation afin d'assurer le respect de toutes les obligations et exigences. Automatiser ce processus autant que possible sera très utile pour réduire les frais généraux d'exploitation continus.

Plus les personnes prennent de temps pour traiter un incident de sécurité, plus l'impact sur la productivité et le risque commercial sont élevés. Passer moins de temps en analyses et corrections doit être un objectif majeur, idéalement avec une approche visant la standardisation et l'automatisation de la réponse aux violations de sécurité.

Vous luttez pour faire face au volume d'incidents. Plutôt que de faire intervenir davantage de personnes pour essayer de faire face, envisagez des méthodes permettant de rendre la détection et la correction beaucoup plus efficaces (via des approches telles que l'automatisation et la priorisation).

Vous ne pouvez pas sécuriser efficacement ce que vous ne pouvez pas mesurer et vous ne mesurez pas suffisamment pour être à même de déterminer l'étendue et l'impact d'une violation. Suivre une approche proactive pour collecter et analyser les informations ne vous permettra pas seulement de détecter une violation plus rapidement et avec davantage de fiabilité. Cela vous aidera aussi à effectuer la rétro-ingénierie de la violation pour être en mesure d'améliorer votre réponse de sécurité et votre attitude face aux risques afin d'atténuer d'autres attaques.



Principes essentiels

La sécurité figure généralement tout en haut d'une liste de freins aux nouvelles initiatives informatiques, du développement et déploiement de nouveaux services et applications à l'exploitation de nouvelles architectures informatiques telles que le Cloud hybride. Une sécurité informatique en matière de suivi, de détection et de réaction (sur la base d'une plateforme avec automatisation et fonctions d'analyse) constituera l'un des facteurs permettant de différencier les entreprises numériques de haut niveau qui peuvent évoluer rapidement selon les conditions du marché. Le chemin pour y parvenir sera parsemé de risques et de pièges, parmi lesquels :

- **Se lancer sans stratégie** – La sécurité devant être à la fois délibérée et consciencieuse, il faut procéder consciemment pour éviter d'acheter des produits destinés à combler des lacunes en termes de capacités. Utilisez les compétences d'experts de sécurité externes qui possèdent une expérience durement acquise et des connaissances pour vous aider à bâtir des solutions éprouvées et gérables.
- **Vider l'océan à la petite cuillère** – Bien que cela puisse sembler être la meilleure solution, tout brûler pour recommencer est rarement une approche productive. Essayez plutôt d'améliorer vos capacités dans certains domaines, puis développez votre approche. Au fur et à mesure que l'adoption et l'expérience augmentent, une plus grande partie de l'infrastructure informatique peut être utilisée pour profiter des avancées.
- **Interopérabilité ouverte** – Nous ne savons pas ce que demain nous apportera et être bloqué avec des interfaces propriétaires entravera votre capacité à sécuriser votre parc informatique au fil de ses évolutions et changements. Recherchez des solutions qui s'intègrent bien en pile et prennent en charge une expansion via des API et interfaces ouvertes, bien définies et stables.