

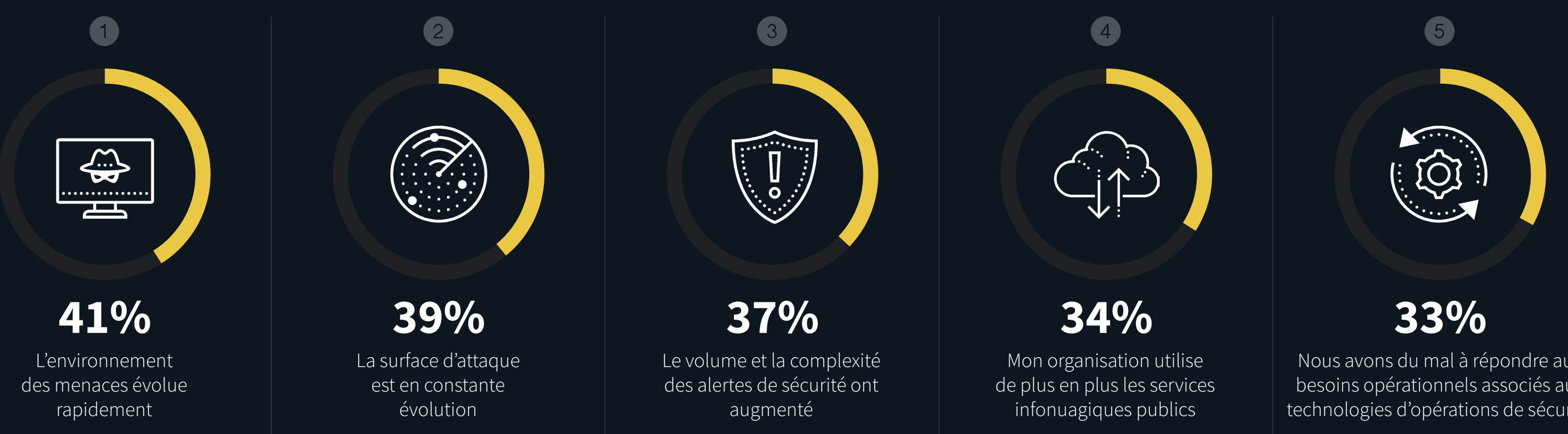
Comblant les lacunes des opérations de sécurité avec des services gérés de détection et d'intervention

Puisque le risque croissant de cyberattaques nuisibles détourne l'esprit et le budget des objectifs commerciaux principaux, les organisations doivent réagir en renforçant leurs programmes de cybersécurité. Les opérations de sécurité (SecOps) sont au cœur de tous les programmes de cybersécurité et sont responsables de la surveillance et de la protection de tous les aspects de la surface d'attaque numérique.

Malgré les investissements, les opérations de sécurité sont plus difficiles

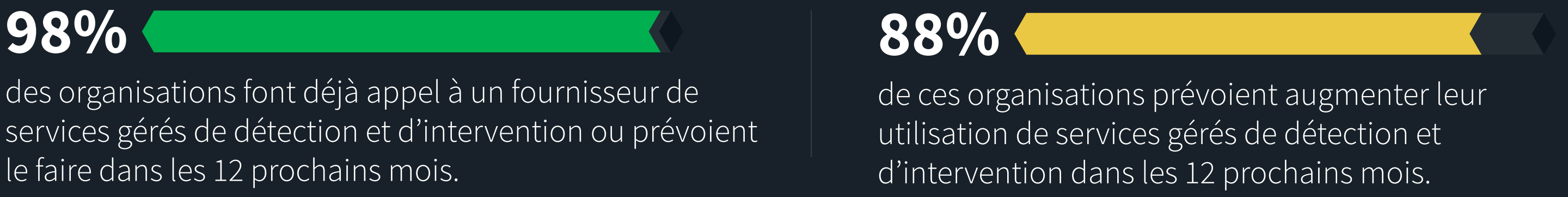


» Les cinq principales raisons qui expliquent pourquoi les opérations de sécurité sont plus difficiles.

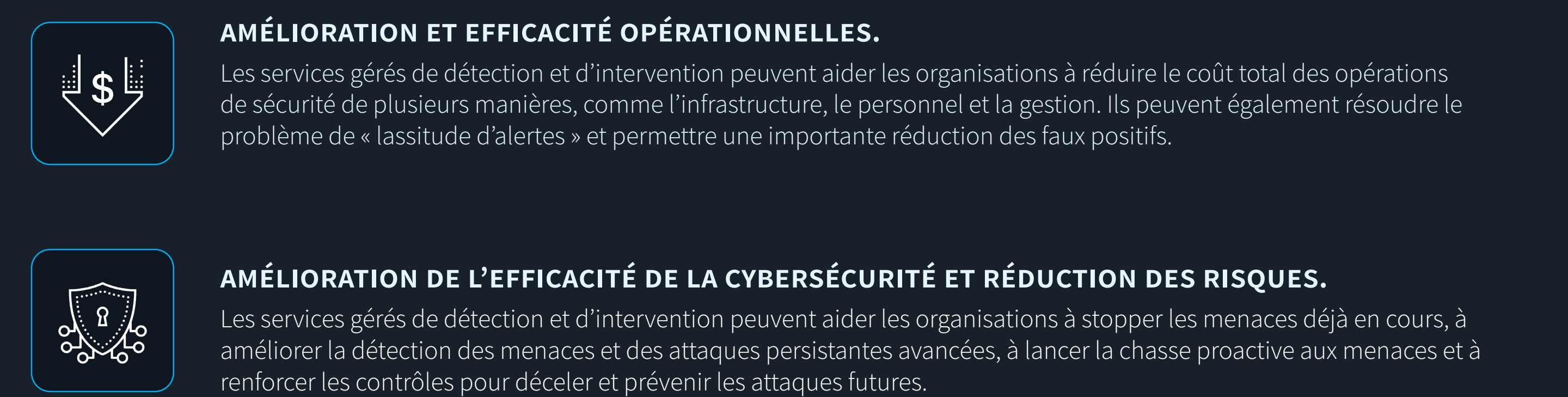


Repenser les stratégies du programme

Les surfaces d'attaque et l'environnement des menaces ont augmenté en taille et en complexité, de même que l'utilisation des contrôles de sécurité, qui génèrent des milliers d'alertes et de grandes quantités de données de sécurité. Les équipes de sécurité repensent l'ensemble des opérations de programmes afin d'incorporer davantage les données sur les actifs et les risques provenant des TI et des équipes du secteur d'activités afin de se concentrer sur les menaces qui posent le plus grand risque pour les objectifs organisationnels.



» Principaux générateurs de valeur de l'utilisation des services gérés de détection et d'intervention.



» Principales raisons pour lesquelles votre organisation utilise ou prévoit d'utiliser les services gérés.

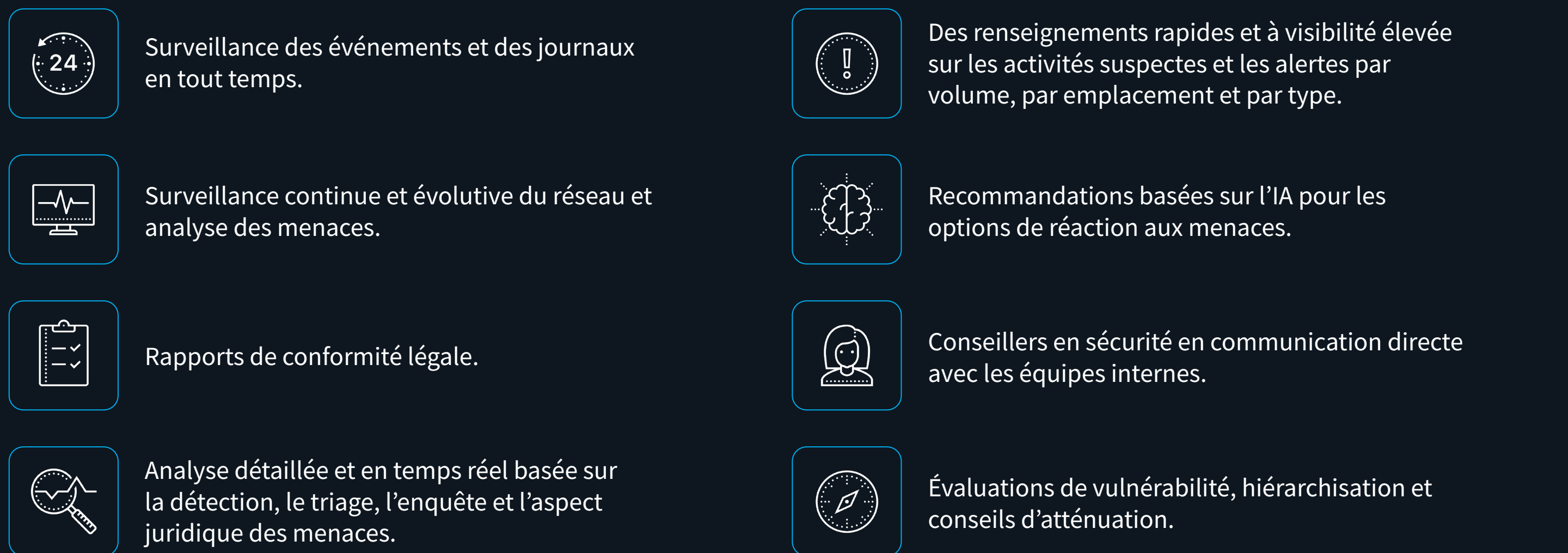


“ Plusieurs solutions de services gérés de détection et d'intervention de première génération étaient conçues et mises en œuvre pour une ère différente : moins de données, moins de menaces et des détections plus simples. ”

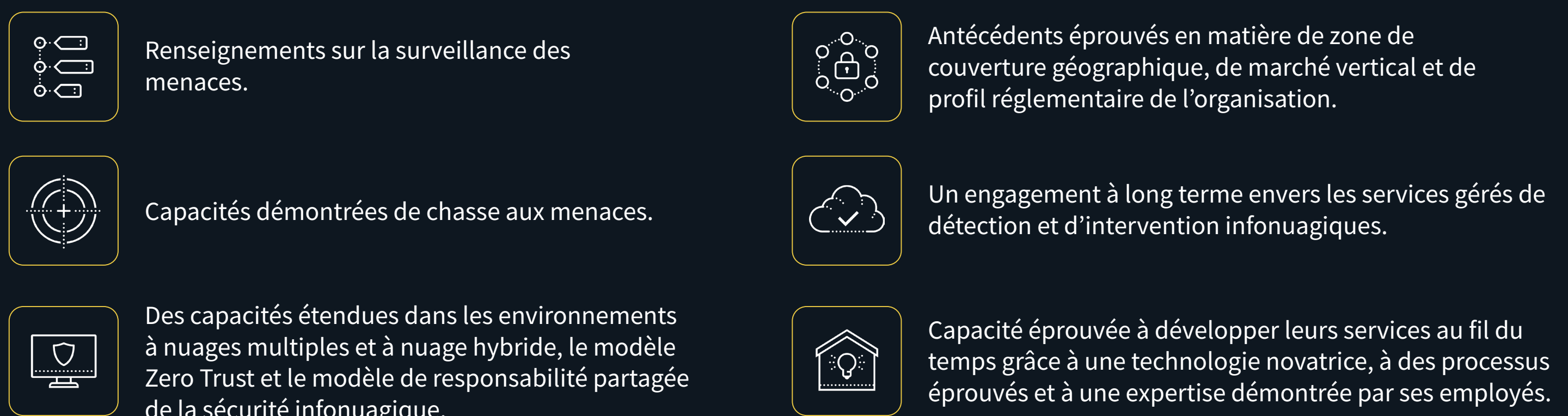
- Dave Gruber, analyste principal d'ESG

Nouvelles exigences pour les services gérés de détection et d'intervention

Plusieurs solutions de services gérés de détection et d'intervention de première génération étaient conçues et mises en œuvre pour une ère différente : moins de données, moins de menaces et des détections plus simples. La prochaine génération de solutions de services gérés de détection et d'intervention doit être en mesure de protéger une surface d'attaque plus diversifiée, de détecter des menaces plus complexes et de tirer le meilleur parti d'une approche axée sur les risques pour la hiérarchisation et l'atténuation.



Lorsque les organisations examinent le grand nombre de fournisseurs de services potentiels qui peuvent offrir certaines, la plupart ou même toutes les fonctionnalités de services gérés de détection et d'intervention en sous-traitance, **elles doivent rechercher des partenaires qui peuvent fournir les services suivants:**



La grande vérité

Puisque le risque croissant de cyberattaques nuisibles détourne l'esprit et le budget des objectifs commerciaux principaux, les organisations doivent renforcer leurs programmes de cybersécurité. Bien que les cas d'utilisation varient, la plupart des organisations ont appelé à des fournisseurs de services gérés de détection et d'intervention pour développer et adapter leurs programmes.

L'approche de Dell Technologies en matière de détection et d'intervention gérées combine des technologies flexibles, intelligentes et évolutives et des professionnels expérimentés en cybersécurité afin d'aider des organisations de toutes les tailles et de tous les profils de ressources à accélérer et à renforcer leurs programmes de sécurité.

EN SAVOIR PLUS

