Enterprise Strategy Group | Getting to the bigger truth.™

Combler les lacunes des opérations de sécurité avec la solution MDR

À mesure que le risque de cyberattaque dévastatrice augmente et monopolise l'attention et le budget qui devraient être consacrés aux objectifs métier essentiels, les organisations doivent réagir en renforçant les programmes de cybersécurité. Les opérations de sécurité (SecOps), responsables de la surveillance et de la protection de tous les aspects de la surface d'attaque numérique, sont au cœur de tous les programmes de cybersécurité.

Malgré les investissements, les opérations de sécurité gagnent en complexité

PLUS DE LA MOITIÉ
des personnes interrogées pensent que les SecOps **ont gagné en complexité** au cours des deux dernières années.

» **Voici les cinq principales raisons pour lesquelles les SecOps ont gagné en complexité.**

1. **41%** Le paysage des menaces évolue rapidement
2. **39%** La surface d'attaque est en constante évolution
3. **37%** Le volume et la complexité des alertes de sécurité ont augmenté
4. **34%** Mon organisation utilise de plus en plus de services de Cloud public
5. **33%** Il est difficile de répondre aux besoins opérationnels des technologies d'opérations de sécurité

Repenser les stratégies du programme

La taille et la complexité des surfaces d'attaque et du paysage des menaces ont augmenté, tout comme l'utilisation des contrôles de sécurité, ce qui génère des milliers d'alertes et des quantités massives de données de sécurité. Les équipes de sécurité repensent les opérations globales du programme afin d'intégrer davantage les données, issues des équipes IT et de direction opérationnelle, sur les ressources et les risques. Elles peuvent ainsi se concentrer sur les menaces qui représentent le risque le plus important pour les objectifs organisationnels.

98% des organisations sont déjà engagées ou prévoient de s'engager auprès d'un fournisseur MDR au cours des 12 prochains mois.

88% ode ces organisations prévoient d'augmenter leur utilisation de la solution MDR au cours des 12 prochains mois.

» **Principaux moteurs de valeur pour l'engagement MDR.**

AMÉLIORATION OPÉRATIONNELLE ET EFFICACITÉ.
La solution MDR peut aider les organisations à réduire le coût total des opérations de sécurité de plusieurs manières, comme l'infrastructure, le personnel et la gestion. Elle peut également résoudre le problème de lassitude face au nombre trop élevé d'alertes, et améliorer la probabilité que les faux positifs soient considérablement réduits.

AMÉLIORATION DE L'EFFICACITÉ DE LA CYBERSÉCURITÉ ET RÉDUCTION DES RISQUES.
La solution MDR peut aider les organisations à stopper les menaces déjà en cours, à améliorer la détection des menaces potentielles et des attaques avancées persistantes, à favoriser une chasse aux menaces proactive et à renforcer les contrôles, afin d'identifier et de prévenir les futures attaques.

» **Principales raisons pour lesquelles votre organisation utilise ou prévoit d'utiliser des services managés.**

55% **Concentration:** Mon organisation souhaite que son personnel de sécurité se concentre sur des initiatives plus stratégiques, plutôt que de consacrer du temps aux opérations de sécurité.

52% **Services:** Mon organisation estime que les prestataires de services peuvent gérer les opérations de sécurité mieux que nous-mêmes.

49% **Complément:** Mon organisation estime qu'un prestataire de services peut compléter notre équipe SOC avec des opérations de sécurité.

42% **Compétences:** Mon organisation ne dispose pas des compétences adéquates pour les opérations de sécurité.

> **« De nombreuses solutions MDR de première génération ont été conçues et implémentées pour une autre époque :** il y avait moins de données, moins de menaces et les détections étaient plus simples. »
>
> *- Dave Gruber, ESG Principal Analyst*

Nouvelles exigences pour la solution MDR

De nombreuses solutions MDR de première génération ont été conçues et implémentées pour une autre époque : il y avait moins de données, moins de menaces et les détections étaient plus simples. La nouvelle génération de solutions MDR doit être équipée pour protéger une surface d'attaque plus diversifiée, détecter des menaces plus complexes et tirer parti d'une approche plus axée sur les risques en vue de hiérarchiser et d'atténuer les risques.

- Surveillance 24x7 des événements et des journaux.
- La surveillance continue et évolutive du réseau, et l'analyse des menaces.
- La création de rapport sur la conformité aux normes.
- Une analyse détaillée et en temps réel basée sur la détection des menaces, le tri, les procédures d'enquête et les analyses approfondies.
- Des informations rapides, à haute visibilité, sur les activités suspectes et les alertes par volume, emplacement et type.
- Des recommandations basées sur l'IA pour les options de réponse contextuelle.
- Des conseillers en sécurité « humains » en contact direct avec les équipes internes.
- Des évaluations, la hiérarchisation et des conseils sur l'atténuation des failles de sécurité.

Face au grand nombre de prestataires de services potentiels qui peuvent fournir une partie, la plupart, voire la totalité des fonctionnalités MDR sous-traitées, **les organisations doivent rechercher des partenaires capables de fournir les fonctions suivantes:**

- Une intelligence sur les menaces contextuelle.
- Des capacités démontrées en matière de chasse aux menaces.
- Des fonctionnalités étendues dans les environnements multicloud et de Cloud hybride, le Zero-Trust et le modèle de responsabilité partagée de la sécurité du Cloud.
- Une expérience éprouvée dans la zone géographique, le marché vertical et le profil réglementaire de l'organisation.
- Un engagement à long terme en faveur d'une solution MDR basée sur le Cloud.
- Une capacité éprouvée à faire évoluer leur service au fil du temps, avec une technologie innovante, des processus éprouvés et une expertise démontrée par ses collaborateurs.

Ce qu'il faut retenir

À mesure que le risque de cyberattaque dévastatrice augmente et monopolise l'attention et le budget qui devraient être consacrés aux objectifs métier essentiels, les organisations doivent renforcer les programmes de cybersécurité. Bien que les cas d'utilisation varient, la plupart d'entre elles s'appuient sur des prestataires de services MDR pour développer et faire évoluer leurs programmes.

L'approche de Dell Technologies en matière de détection et de réponse managées associe des technologies flexibles, intelligentes et évolutives à des professionnels expérimentés de la cybersécurité. Elle aide ainsi les organisations de toutes tailles et de tous profils de ressources à accélérer et à renforcer les programmes de sécurité.

EN SAVOIR PLUS

DELL Technologies

Source : *Résultats de l'enquête complète ESG, SOC Modernization and the Rule of XDR*, août 2022.