SHOWCASE ESG

Pourquoi la solution MDR fait désormais partie intégrante des stratégies de cybersécurité modernes

Date : août 2022 **Auteur :** Dave Gruber, ESG Principal Analyst

RÉSUMÉ : Personne ne remet en question l'importance des fonctionnalités de détection et de réponse dans un programme de cybersécurité. Le problème est surtout de déterminer comment garantir une détection et une réponse rapides, précises, fiables et cohérentes, lorsque les menaces se multiplient et se complexifient à un rythme tel que la plupart des organisations ne peuvent s'y adapter. Une solution de détection et de réponse managées (MDR, Managed Detection and Response), en tant que service managé tiers, est une approche qui permet aux organisations de suivre le rythme.

Introduction : L'essor de la solution MDR

Toutes les organisations sont confrontées à une dure réalité : le nombre de menaces de cybersécurité augmente rapidement, les surfaces d'attaque s'étendent et les processus et outils traditionnels consacrés à la détection des menaces, ainsi qu'à la réponse apportée, ne suffisent plus. Les menaces elles-mêmes et les acteurs malveillants qui les lancent sont plus efficaces, agiles et persistants. Les professionnels de la sécurité et de l'informatique chargés de protéger les ressources de l'entreprise font donc face à une cible mouvante numérique.

Le fait de recourir à une pléthore de contrôles de sécurité augmente les coûts et la complexité liés aux efforts de détection et de réponse. En effet, les équipes de sécurité doivent trier manuellement un flux constant d'alertes pour faire la différence entre les menaces réelles et les faux positifs. La création d'un plus grand centre d'opérations de sécurité (SOC) et l'ajout d'autres outils et ingénieurs de sécurité coûtent cher. Cela suppose également que les organisations puissent identifier et embaucher suffisamment de professionnels de la sécurité, dans un contexte où le fossé en matière de compétences de cybersécurité se creuse de plus en plus.

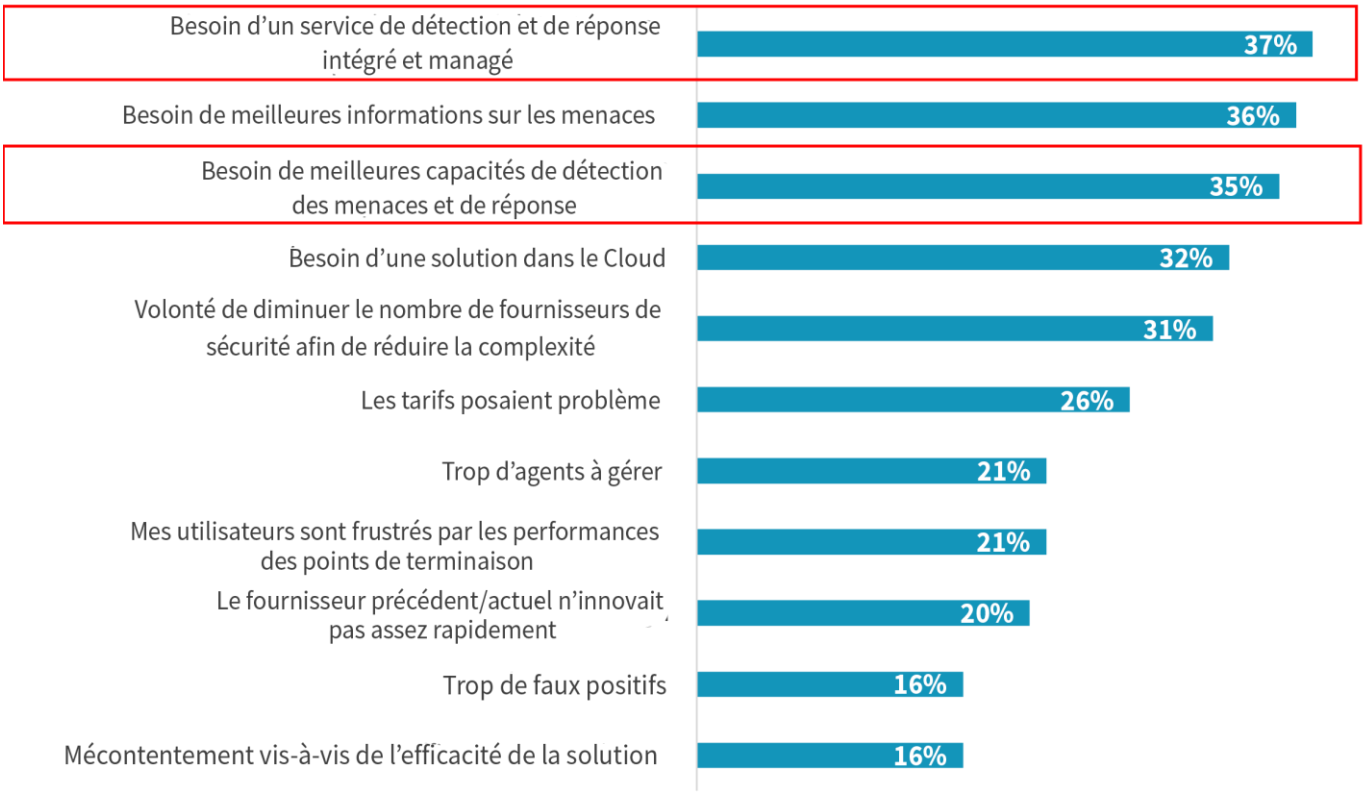
À mesure que les programmes de cybersécurité sont restructurés, les organisations se tournent plus fréquemment vers des fournisseurs de détection et de réponse managées.

À mesure que les programmes de cybersécurité sont restructurés, les organisations se tournent de plus en plus vers des fournisseurs de détection et de réponse managées pour affiner les processus, combler les lacunes en matière de ressources et de compétences, et moderniser les outils d'opérations de sécurité. Beaucoup associent la solution MDR à la sécurité des points de terminaison ; l'étude d'ESG révèle en effet que la nécessité d'adopter un service MDR intégré est un facteur important qui pousse les organisations à changer de fournisseur de solutions de sécurité pour les points de terminaison (voir Figure 1).[1]

[1] Source : Résultats de l'enquête complète ESG, *Endpoint Security Trends*, décembre 2021. Toutes les références et tous les graphiques de la recherche ESG présentés dans ce showcase proviennent de cet ensemble de résultats d'enquête.

Figure 1. Facteurs poussant les entreprises à changer de fournisseur de sécurité des points de terminaison

Si votre organisation a récemment changé, projette activement de changer ou envisage de changer de fournisseur de solutions de sécurité des points de terminaison, qu'est-ce qui a motivé/motive ce changement ? (Pourcentage de personnes interrogées, N = 300, plusieurs réponses possibles)



Source : ESG, une division de TechTarget, Inc.

Toutefois, à mesure que les équipes de sécurité étendent les programmes de détection et de réponse, en procédant à une mise à niveau vers des solutions de détection et de réponse étendues (Extended Detection and Response, XDR) plus complètes, les offres MDR permettent aux organisations de mettre à jour la technologie et les modèles d'exploitation capables de fournir une couverture de surface d'attaque plus complète et une détection avancée des menaces. De nouvelles approches sont nécessaires et doivent associer une surveillance 24 h/24, une intelligence mondiale sur les menaces en temps réel, l'automatisation et l'analytique avancée de l'apprentissage automatique, le tout en pouvant traiter d'importantes quantités de télémétrie de sécurité pour soutenir la détection rapide et la chasse aux menaces. Bien que la solution XDR continue d'évoluer et de se développer, les services MDR peuvent permettre aux organisations, indépendamment de leur taille et de leur niveau de maturité en matière de sécurité, de mettre en œuvre la détection et la réponse, et ainsi d'atténuer les menaces avancées. Cela est d'autant plus important alors que les organisations redéfinissent le périmètre et l'échelle des limites de la cybersécurité, du datacenter à la périphérie, en passant par le Cloud. La solution MDR rassemble les personnes, les processus et les technologies nécessaires pour étendre les cas d'utilisation de détection et de réponse aux menaces à l'échelle de l'entreprise distribuée.

Principaux facteurs d'adoption de la solution MDR

L'utilisation des services MDR est en hausse, offrant aux équipes de sécurité un moyen d'étendre la couverture, de combler les lacunes en matière de personnel et de renforcer les objectifs globaux du programme. Les cas d'utilisation varient, mais les facteurs sous-jacents sont les suivants :

- Environnement de menaces : le nombre de cyberattaques et leur sophistication croissante ont fait peser une pression considérable sur les organisations, qui doivent les détecter et y répondre plus rapidement et de manière plus définitive.
- Intention de l'adversaire : les adversaires sont devenus plus intelligents, plus persistants et encore plus stratégiques dans la façon dont ils planifient et exécutent leurs attaques. Un puissant « écosystème criminel » est apparu, où les acteurs malveillants partagent des tactiques et collaborent même sur les attaques.
- Économie : l'engagement en matière de CAPEX pour la création et l'extension d'un SOC est important, généralement de l'ordre de sept chiffres, et parfois même plus.
- Actualisation des technologies de cybersécurité : la pile de contrôles de cybersécurité doit être actualisée plus fréquemment pour les organisations qui effectuent toutes ou la majeure partie de leurs activités d'opérations de sécurité en interne. Elles doivent notamment passer de la détection et de la réponse sur les points de terminaison de première génération à un cadre XDR/MDR plus complet.
- Pénurie de compétences : le manque de compétences en cybersécurité, qui a fait l'objet d'un grand nombre de discussions, est un problème récurrent. L'incapacité à pourvoir correctement les postes de cybersécurité en interne crée souvent des défis en matière d'objectifs de détection et de réponse, mettant ainsi les ressources en péril.

Les cyberattaques ciblent leurs victimes sans distinction. Les petites et moyennes entreprises, dont le personnel et le budget sont limités, avant même l'exposition à tout type d'attaques, sont menacées. Même les très grandes organisations ont besoin de personnel supplémentaire, de contrôles évolutifs et de conseils au niveau de la direction sur les stratégies favorisant la détection et la réponse face à l'évolution de l'environnement de menaces.

Éléments à rechercher dans un service MDR et chez un prestataire de services MDR

Toute organisation évaluant un service MDR doit définir des exigences importantes et non négociables, notamment :

- Intelligence sur les menaces contextuelle : prise en charge de l'intelligence et de la détection des menaces en temps réel, y compris la corrélation de plusieurs indicateurs pour identifier les menaces ou ignorer les faux positifs.
- Cas d'utilisation proactifs : prise en charge de la chasse active aux menaces connues.
- Télémétrie enrichie : mise en place d'investigations approfondies et d'une analytique sophistiquée, des points particulièrement importants pour identifier les nouvelles menaces émergentes.
- Mesures correctives : proposition de conseils de mesures correctives spécifiques à l'IA et contextuels.
- Atténuation des risques : évaluation et gestion des failles de sécurité.

Lorsqu'elles veulent sélectionner un prestataire de services MDR, les organisations doivent rechercher des partenaires capables de fournir des fonctionnalités spécifiques et démontrées, notamment :

- Couverture 24x7 : surveillance continue.
- Planification et consultation d'hypothèses.
- Expertise et expérience humaines du prestataire de services.
- Conseils pour les cadres dirigeants et les membres du conseil d'administration.
- Capacité à garantir la gouvernance, la conformité et la continuité d'activité.

En outre, les organisations doivent interroger les partenaires MDR potentiels sur les objectifs de niveau de service. Ces fonctions comprennent le temps moyen de réaction entre l'alerte et le lancement de l'investigation, le temps moyen de réponse entre le lancement de l'investigation et le moment où une analyse de l'incident est fournie à l'organisation, et le temps moyen de résolution entre le début de l'investigation et la résolution complète.

L'approche de Dell Technologies en matière de MDR

L'identification, l'évaluation et le partenariat avec un prestataire de services MDR obligent les organisations à se concentrer non seulement sur leurs besoins actuels en matière de détection et de réponse aux menaces, mais également sur la façon dont ces besoins sont susceptibles d'évoluer et de s'étendre à l'avenir. Il n'existe pas de boule de cristal permettant de prédire l'avenir des menaces de cybersécurité, mais les organisations doivent rechercher un partenaire MDR possédant une capacité éprouvée à faire évoluer son service au fil du temps, en s'appuyant sur des technologies innovantes, des processus éprouvés et une expertise démontrée par ses collaborateurs.

L'approche de Dell Technologies en matière de détection et de réponse managées associe des technologies flexibles, intelligentes et évolutives à des professionnels de la cybersécurité expérimentés. Son service basé sur abonnement est conçu pour offrir aux organisations à la fois une prévisibilité des coûts et une transition fluide vers un niveau de service supérieur, si nécessaire.

La plate-forme technologique de Dell Managed Detection and Response est Taegis XDR, un service Cloud natif entièrement managé développé par Secureworks, une division Dell. Taegis XDR détecte, analyse et traite les menaces entièrement vérifiées sur une surface d'attaque distribuée et diversifiée. Cette solution aide ainsi à protéger les organisations, qu'il s'agisse de grandes sociétés mondiales ou de petites entreprises.

La solution Taegis XDR est renforcée par les compétences d'un grand groupe d'analystes et d'ingénieurs de sécurité Dell, dont les connaissances collectives couvrent des décennies d'expertise. Elle contribue ainsi à protéger les organisations contre les menaces connues ou encore inconnues. Cette combinaison offre un moyen efficace d'unifier la détection et la réponse dans l'ensemble de l'architecture informatique, en grande partie grâce à la base de données d'intelligence sur les menaces mise à jour en continu. Dell Managed Detection and Response surveille, analyse et identifie également les comportements malveillants afin de réduire le temps moyen de détection et de réponse.

Dell Managed Detection and Response surveille, analyse et identifie également les comportements malveillants afin de réduire le temps moyen de détection et de réponse.

Enfin, étant donné qu'il est managé, le service Dell Managed Detection and Response réduit considérablement le besoin pour les organisations de rechercher et de recruter des professionnels de la sécurité, pour renforcer les équipes informatiques et d'opérations de sécurité internes déjà surchargées. Ce service est conçu pour compléter et étendre les capacités des organisations de manière à la fois économique et stratégique.

Ce qu'il faut retenir

L'expansion rapide de la surface d'attaque, les attaques de ransomware répétées et un paysage des menaces plus complexe de manière générale stimule l'investissement et la dynamique envers les solutions XDR et MDR, à mesure que les organisations modernisent les programmes de détection et de réponse aux menaces. Bien que les stratégies de sécurité individuelles varient, la nécessité de bénéficier d'une visibilité plus étendue sur la surface d'attaque, et la possibilité d'agréger, de corréler et d'analyser de grandes quantités de données de sécurité à partir des contrôles de sécurité individuels, constituent une étape importante pour maîtriser la situation.

Les services de détection et de réponse managées sont à la fois efficaces et facilement disponibles : les équipes de sécurité s'appuient sur les fournisseurs de MDR pour renforcer les compétences, les processus et les technologies de sécurité. L'étude d'ESG montre que les organisations qui investissent dans une solution XDR souhaitent que les services MDR complémentaires les aident à implémenter et à exploiter ces solutions. Elles doivent donc faire appel à des fournisseurs de solutions qui ont fait leurs preuves dans l'apport de solutions et de services de sécurité. Lorsque ces mesures sont appliquées au fil du temps, elles peuvent aider les équipes informatiques et de sécurité à développer et à faire évoluer leurs programmes de sécurité.

Pour aider les organisations à atteindre ces objectifs, ESG recommande d'explorer les solutions MDR de sociétés telles que Dell Technologies, proposant du personnel, des processus et des technologies.

Enterprise Strategy Group est une entreprise intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des données relatives aux marchés, des renseignements exploitables et des services de commercialisation à la grande communauté informatique.

www.esg-global.com contact@esg-global.com 508.482.0188