PRÉSENTATION D'ESG

Pourquoi la détection et la réponse managées (MDR) font partie intégrante des stratégies modernes de cybersécurité

Date : août 2022 **Auteur :** Dave Gruber, analyste principal, ESG

RÉSUMÉ : Personne ne nie l'importance des compétences de détection et d'intervention d'un programme de cybersécurité. L'enjeu majeur est de savoir comment assurer une détection et une réponse rapides, précises, fiables et cohérentes lorsque les menaces se multiplient et se complexifient trop rapidement pour le rythme d'adaptation de la plupart des entreprises. La détection et la réponse managées (MDR) en tant que service géré par de tierces parties sont une approche qui permet aux organisations de suivre la cadence.

Introduction : l'avènement des MDR

Toutes les organisations sont confrontées à une dure réalité : les menaces de cybersécurité augmentent rapidement, les surfaces d'attaque se multiplient et les procédés et les outils traditionnels pour détecter les menaces et y répondre ne suffisent plus. Les menaces elles-mêmes et les contrevenants sont plus habiles, agiles et persistants, ce qui crée ainsi une cible numérique mobile pour les professionnels de la sécurité et des TI chargés de protéger les actifs d'une entreprise.

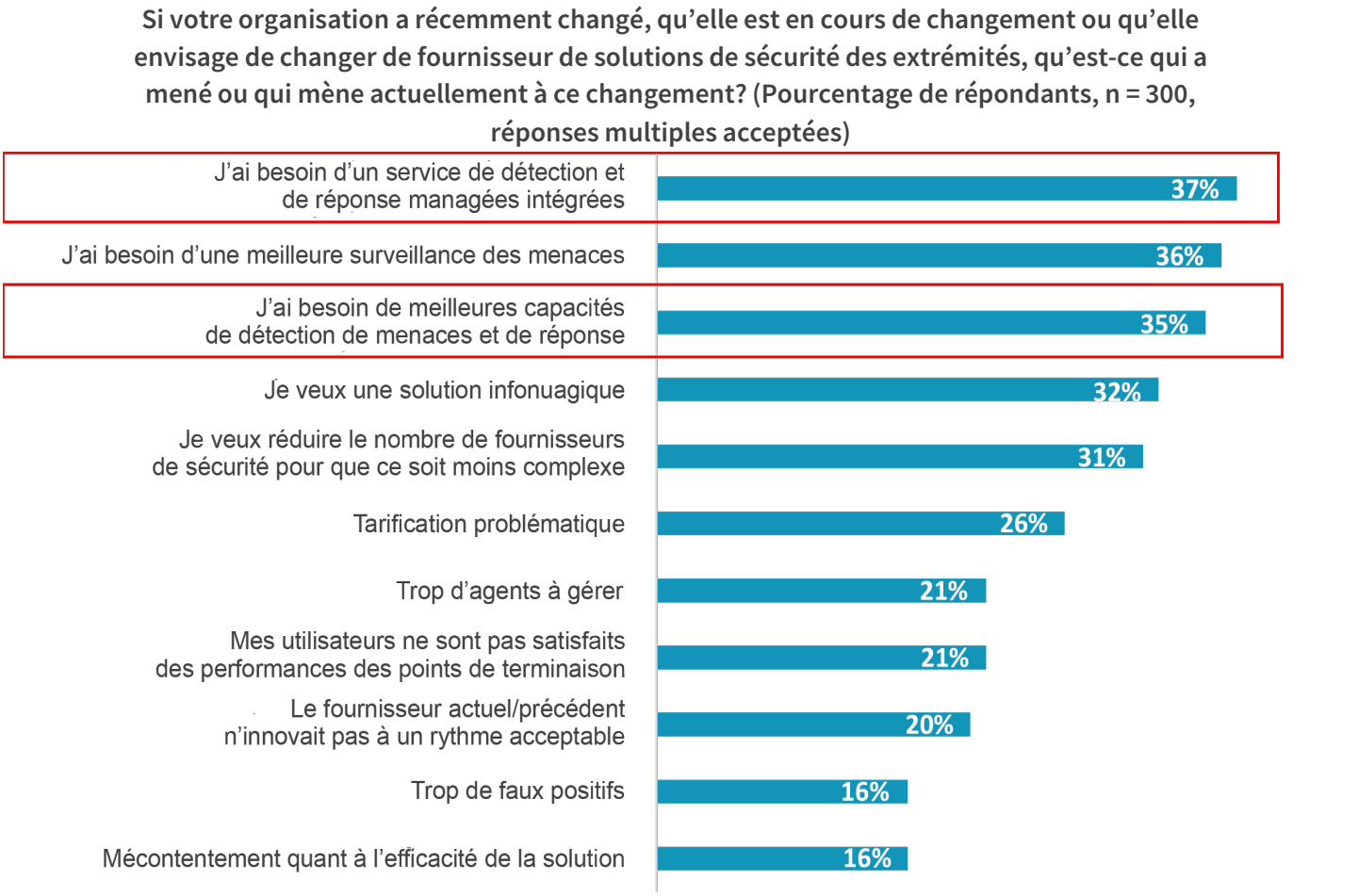
Une abondance de contrôles de sécurité ajoute des dépenses et de la complexité aux efforts de détection et d'intervention en exigeant des équipes de sécurité qu'elles procèdent au triage manuel d'une avalanche constante d'alertes pour trier les menaces valides des fausses alertes. La création d'un plus grand centre des opérations de sécurité avec plus d'outils et d'ingénieurs de sécurité est coûteuse. Cela présume que les entreprises peuvent trouver et embaucher suffisamment de professionnels de la sécurité pour faire face aux lacunes considérables et croissantes en matière de cybersécurité.

Alors que les programmes de cybersécurité sont reconstruits, les entreprises se tournent plus fréquemment vers des fournisseurs de détection et de réponse managées pour obtenir de l'aide.

Alors que les programmes de cybersécurité sont reconstruits, les entreprises se tournent plus fréquemment vers les fournisseurs de détection et de réponse managées pour affiner les procédés, combler les lacunes en matière de ressources et de compétences et moderniser les outils d'opérations de sécurité. Beaucoup associent la MDR à la sécurité des extrémités et des recherches d'ESG démontrent d'ailleurs que la nécessité d'un service de MDR intégré est l'une des raisons qui poussent les organisations à changer leurs fournisseurs de solutions de sécurité des extrémités (voir la figure 1).[1]

[1] Source : Résultats du sondage complet d'ESG, *Endpoint Security Trends*, décembre 2021. Toutes les références et tous les graphiques de la recherche d'ESG dans cette présentation ont été tirés de l'ensemble de résultats de ce sondage.

Figure 1. Motivations pour changer de fournisseur de sécurité des points de terminaison



Source : ESG, une division de TechTarget, inc.

Toutefois, alors que les équipes de sécurité étendent leurs programmes de détection et d'intervention et passent à des solutions de détection et d'intervention étendues (XDR) plus complètes, les offres de MDR permettent aux entreprises de mettre à jour à la fois la technologie et les modèles d'exploitation afin de couvrir une plus grande surface d'attaque et d'offrir une détection avancée des menaces. De nouvelles approches sont nécessaires et doivent combiner la surveillance en tout temps, une surveillance en direct des menaces dans le monde, l'automatisation et les analyses avancées de l'apprentissage automatique, et ce, en collaborant avec des quantités considérables de télémétrie de sécurité pour la détection rapide et la chasse aux menaces. Bien que les services de XDR continuent d'évoluer et de se développer, les services de MDR peuvent permettre aux organisations de toutes tailles et de tous niveaux de compétence en matière de sécurité d'effectuer des opérations de détection et d'intervention, ce qui permet d'atténuer les menaces avancées. Ceci est d'autant plus important puisque les organisations redéfinissent le champ d'application et les limites de la cybersécurité, du centre de données à la périphérie, en passant par le nuage. La MDR réunit les personnes, les procédés et les technologies nécessaires pour étendre la détection et la réponse aux menaces sur l'ensemble de l'entreprise distribuée.

Principales motivations pour l'adoption de la MDR

L'utilisation des services de MDR est en hausse, ce qui offre aux équipes de sécurité un moyen d'étendre la couverture, de combler les lacunes dans le personnel et de renforcer les objectifs globaux du programme. Les cas d'utilisation varient, mais les motivations sous-jacentes comprennent :

- Le contexte des menaces : Le nombre de cyberattaques et leur augmentation ont mis une pression considérable sur les organisations afin qu'elles les détectent et y répondent plus rapidement et de façon plus définitive.
- L'intention de l'adversaire : Les adversaires sont devenus plus intelligents, plus persistants et encore plus stratégiques dans la planification et la réalisation de leurs attaques. Un puissant « écosystème criminel » est apparu dans lequel les contrevenants partagent des tactiques et collaborent même dans des attaques.
- L'économie : L'engagement de CapEx envers la création et l'expansion d'un centre des opérations de sécurité est considérable : il s'agit généralement de dépenses à sept chiffres, et parfois même plus.
- Le renouvellement des technologies de cybersécurité : Les contrôles en matière de cybersécurité doivent être renouvelés plus fréquemment pour les organisations qui effectuent toutes ou la majeure partie de leurs activités de sécurité en interne. Il s'agit notamment de passer de la détection et de la réponse des extrémités de première génération à un cadre XDR/MDR plus complet.
- La pénurie de compétences : Les lacunes en matière de compétences en cybersécurité constituent un enjeu perpétuel et bien connu. L'incapacité à trouver du personnel adéquat pour occuper des postes de cybersécurité internes entraîne souvent des difficultés en matière de détection et d'intervention, mettant les ressources en péril.

Les cyberattaques arrivent sans discernement. Les petites et moyennes entreprises, dont le personnel, le budget et les ressources sont limités, et qui ont déjà été exposées à tous types d'attaques, sont grandement à risque. Même les très grandes organisations ont besoin de personnel supplémentaire, de contrôles évolutifs et de services-conseils au niveau des cadres sur des stratégies afin de détecter l'évolution du contexte des menaces et de répondre convenablement.

Que rechercher dans un service de MDR et un fournisseur de service

Parmi les exigences importantes et insolubles pour toute organisation qui envisage à obtenir un service de MDR, on compte notamment :

- La surveillance des menaces contextuelles : Favoriser la surveillance et la détection des menaces en temps réel, y compris la corrélation de plusieurs indicateurs pour déceler les menaces ou rejeter les fausses alertes.
- Les cas d'usage proactifs : Encourager la chasse active des menaces connues.
- La riche télémétrie : Entreprendre des enquêtes judiciaires et des analyses approfondies. Elles sont particulièrement importantes pour déceler de nouvelles menaces émergentes.
- La remise en état : Offrir des conseils de remise en état propres au contexte pilotée par l'IA.
- La réduction des risques : Évaluer et gérer les points faibles.

Lorsque vient le temps de sélectionner un fournisseur de services de MDR, les organisations doivent rechercher des partenaires qui peuvent fournir des fonctionnalités précises et démontrées, notamment :

- Une couverture 24 h sur 24, 7 jours sur 7 : Rechercher une surveillance continue 24 h sur 24, 7 jours sur 7.
- La planification et la consultation concernant des scénarios hypothétiques.

- L'expertise humaine et l'expérience du fournisseur de services.
- Des conseils pour les cadres supérieurs et les membres du conseil d'administration.
- La capacité à assurer la gestion, la conformité et la continuité des affaires.

En outre, les organisations devraient demander aux partenaires potentiels de MDR quels sont leurs objectifs quant au service. Ces fonctions comprennent notamment le temps de réaction entre l'alerte et le lancement de l'enquête, le temps de réponse à partir du lancement de l'enquête jusqu'au moment où une analyse d'incident est fournie à l'organisation, ainsi que le temps de résolution des incidents à partir du début de l'enquête jusqu'au moment où la résolution complète a été effectuée.

L'approche de Dell Technologies quant aux MDR

L'identification, l'évaluation et le partenariat avec un fournisseur de services de 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. Bien qu'aucune organisation n'ait de boule de cristal qui lui permette de prédire l'avenir des menaces de cybersécurité, elles devraient tout de même chercher un partenaire de MDR qui a fait ses preuves en faisant évoluer son service au fil du temps par ses technologies novatrices, ses procédés éprouvés et l'expertise démontrée par ses employés.

L'approche de Dell Technologies en matière de détection et de réponse managées combine des technologies flexibles, intelligentes et évolutives, ainsi que des professionnels expérimentés en cybersécurité. Son service par abonnement est conçu pour offrir aux organisations une prévisibilité des coûts et un changement harmonieux vers un niveau supérieur de service, si nécessaire.

La plateforme technologique pour la détection et la réponse managées de Dell est Taegis XDR, un service infonuagique entièrement géré et développé par Secureworks, une unité commerciale de Dell. Taegis XDR détecte et analyse des menaces entièrement contrôlées, en plus d'agir contre celle-ci sur une surface d'attaque distribuée et diversifiée pour aider à protéger toutes les organisations, des grandes entreprises mondiales aux entreprises relativement petites.

Taegis XDR est renforcé par les compétences du vaste groupe d'analystes et d'ingénieurs en sécurité de Dell, dont les connaissances collectives représentent des décennies d'expertise, qui aident à protéger les organisations contre les menaces connues, mais également celles 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 sa base de données de surveillance des menaces continuellement mise à jour. La détection et la réponse managées de Dell surveillent, analysent et décèlent les comportements d'attaque, ce qui réduit le temps de détection et de réponse.

La détection et la réponse managées de Dell surveillent, analysent et décèlent les comportements d'attaque, ce qui réduit le temps de détection et de réponse.

Enfin, comme il s'agit d'un service géré, la détection et la réponse managées de Dell réduisent considérablement le besoin des organisations de rechercher et de recruter des professionnels de la sécurité pour des équipes d'opérations informatiques et de sécurité internes déjà surchargées. La détection et la réponse managées de Dell sont conçues pour compléter les propres compétences des organisations, ainsi que pour les étendre d'une manière économique, mais stratégique.

La grande vérité

Une surface d'attaque en pleine expansion, des attaques répétées par rançongiciel et un contexte de menaces généralement plus complexe stimulent les investissements dans les systèmes de XDR et de MDR, ce qui pousse également les organisations à moderniser leurs programmes de détection et de réponse aux menaces. Bien que les stratégies de sécurité individuelles varient, la nécessité d'un aperçu plus étendu de la surface d'attaque, ainsi que la capacité d'agréger, de corréler et d'analyser des quantités massives de données de sécurité provenant des contrôles de sécurité individuels qui les protègent sont importantes pour prendre le contrôle.

Les services de détection et de réponse managées sont à la fois efficaces et facilement accessibles, car les équipes de sécurité tirent parti des fournisseurs de MDR pour renforcer les compétences, les procédés et les technologies de sécurité. Une étude d'ESG démontre que les entreprises qui investissent dans la XDR recherchent des services de MDR complémentaires pour les aider à mettre en œuvre et à faire fonctionner ces solutions. Cela représente une collaboration avec des fournisseurs de solutions qui ont fait leurs preuves en matière de prestation de solutions et de services de sécurité. Appliquées au fil du temps, ces solutions peuvent aider les équipes de TI et de sécurité à développer et à faire évoluer leurs programmes de sécurité.

ESG recommande d'explorer les solutions de MDR d'entreprise comme Dell Technologies qui sont fournies avec du personnel, des procédés et des technologies afin d'aider les entreprises à atteindre ces objectifs.

Enterprise Strategy Group est une entreprise intégrée d'analyse technologique, de recherche et de stratégie qui fournit des renseignements commerciaux, des renseignements exploitables et des services de contenu de commercialisation à la communauté informatique mondiale.

www.esg-global.com contact@esg-global.com 508 482-0188