Guide du marché des services de détection et de réponse gérés

Publié le 14 février 2023 - ID G00 761083 - 24 min de lecture

Par Pete Shoard , Al Price , **et 3 de plus**

Les services MDR offrent aux clients des fonctions SOC modernes, clé en main, livrées à distance ; en fin de compte, la perturbation et le confinement des menaces. Les responsables de la sécurité et de la gestion des risques devraient utiliser cette recherche pour identifier les services MDR qui répondent à leurs exigences en matière de risques liés à l'entreprise.

Aperçu

Principales conclusions

- Les offres centrées sur la technologie mal nommées et les wrappers de services fournis par les fournisseurs (VDSW), qui ne parviennent pas à fournir des services de détection et de réponse gérés (MDR) pilotés par l'homme, posent des problèmes aux acheteurs qui cherchent à identifier et à sélectionner un fournisseur axé sur les résultats.
- Les capacités clés en main de détection, d'investigation et de réponse aux menaces (TDIR) sont une exigence essentielle pour les acheteurs de services MDR qui exigent des services fournis à distance déployés rapidement et de manière prévisible .
- Les acheteurs de MDR doivent se concentrer sur la capacité à fournir des informations contextuelles qui auront un impact direct sur leurs objectifs commerciaux, car la collecte à grande échelle de télémétrie et d'analyse automatisée est insuffisante face à des menaces peu courantes .
- Un nombre croissant de clients MDR exigent que les fournisseurs soient en mesure d'initier à distance des mesures de confinement actif ou de perturbation d'une menace , mais l'autonomie des fournisseurs varie encore. Des facteurs tels que la confiance, la géographie et la maturité de la sécurité de l'organisation consommatrice affectent l'adoption.

Recommandations

En tant que responsable de la sécurité et de la gestion des risques responsable des opérations de sécurité, vous devez :

- Utilisez les services MDR pour obtenir des capacités d'opérations de sécurité dirigées par l'homme, fournies à distance, 24 heures sur 24, 7 jours sur 7 , lorsqu'il n'existe aucune capacité interne existante ou lorsque l'organisation a besoin d' accélérer ou d'augmenter les capacités d'opérations de sécurité existantes .

- Évaluez comment l'approche de confinement et les rapports d'incidents du fournisseur MDR peuvent s'intégrer à votre organisation et si des actions peuvent être effectuées en votre nom pour s'aligner sur les exigences de l'entreprise ainsi que sur la conformité/la politique juridique/la réglementation gouvernementale.

- Tirez le meilleur parti des services MDR en préparant les processus de flux de travail de réponse et en intégrant les systèmes de gestion des tickets existants pour garantir une réponse centrée sur l'entreprise.

- Déterminez si le service du fournisseur MDR est en mesure de s'aligner sur les exigences de votre entreprise et fournissez des résultats exploitables auxquels les équipes internes peuvent réagir avec succès, plutôt que de se contenter de résultats technologiques régurgités sans analyse supplémentaire.

Hypothèse de planification stratégique

D'ici 2025, 60 % des entreprises utiliseront activement les capacités de perturbation et de confinement des menaces à distance fournies directement par les fournisseurs de MDR, contre 30 % aujourd'hui .

Définition du marché

Ce document a été révisé le 23 février 2023. Pour plus d'informations, consultez la page Corrections sur gartner.com.

Les services de détection et de réponse gérées (MDR) offrent aux clients des fonctions de centre d'opérations de sécurité (SOC) fournies à distance . Ces fonctions permettent aux organisations de détecter, d'analyser, d'enquêter et de réagir rapidement en perturbant et en maîtrisant les menaces. Ils offrent une expérience clé en main, utilisant une pile technologique prédéfinie qui couvre généralement les terminaux, le réseau, les journaux et le cloud. La télémétrie est analysée au sein de la plate-forme du fournisseur à l'aide d'une gamme de techniques. Ce processus permet une enquête par des experts qualifiés dans la chasse aux menaces et la gestion des incidents, qui fournissent des résultats sur lesquels les entreprises peuvent agir.

Les capacités de base incluent :

- Fonctions de détection et de réponse fournies à distance 24h/24 et 7j/7 .

- Une pile technologique exploitée par un fournisseur qui permet et coordonne la détection des menaces en temps réel, l'investigation et la réponse d'atténuation active. Qu'il soit développé par le fournisseur MDR, un ensemble intégré de technologies commerciales qui utilisent des techniques modernes (comme les API) pour échanger des données et des instructions, ou une combinaison des deux approches.

- Personnel qui interagit quotidiennement avec les données individuelles des clients et possède des compétences et une expertise dans la surveillance, la détection et la chasse aux menaces, la veille sur les menaces (TI) et la réponse aux incidents.

- Livraison clé en main, avec des processus et un contenu de détection prédéfinis et préréglés. Cela inclut un manuel standard de flux de travail, de procédures et d'analyses, et nécessite un ensemble minimum viable de télémétrie pour fournir des services ; offrant une intégration avec des technologies de détection et de réponse tierces au-delà des technologies appartenant au fournisseur.

- La disponibilité d'activités d'atténuation, d'investigation et de confinement à distance immédiates (telles que la mise en quarantaine des hôtes et la désauthentification des utilisateurs) au-delà de l'alerte et de la notification, fournies et coordonnées par le personnel du fournisseur de services.

- Triez, enquêtez et gérez les réponses à toutes les menaces découvertes, quelle que soit leur priorité, sans limitation de volume ou de temps consacré au processus de découverte et d'investigation.

Les fonctionnalités facultatives incluent :

- Sources de données contextuelles supplémentaires fournissant des détails sur les expositions à la sécurité telles que les vulnérabilités, la visibilité de la surface d'attaque et l'analyse de la marque et de la réputation.
- Fonctionnalités d'investigation numérique et de réponse aux incidents (DFIR) offrant un personnel à distance ou déployable sur appel pour effectuer une analyse approfondie des incidents et des causes profondes.
- Des capacités d'évaluation et de validation de la sécurité, telles que la simulation de violation et d'attaque (BAS), qui analysent l'efficacité des contrôles de sécurité et des processus de réponse, et fournissent aux clients des conseils sur la manière d'améliorer leur posture défensive.
- Chasse aux menaces basée sur des hypothèses, où les clients sont en mesure d'identifier des cibles de chasse aux menaces spécifiques pour déterminer si un acteur de la menace était à blâmer. L'accent serait mis sur les utilisateurs d'intérêt ou lorsque des données privilégiées sont connues pour être entrées dans la circulation publique. Différent de la chasse aux menaces, qui est incluse dans le MDR et chasse les techniques de menace connues.

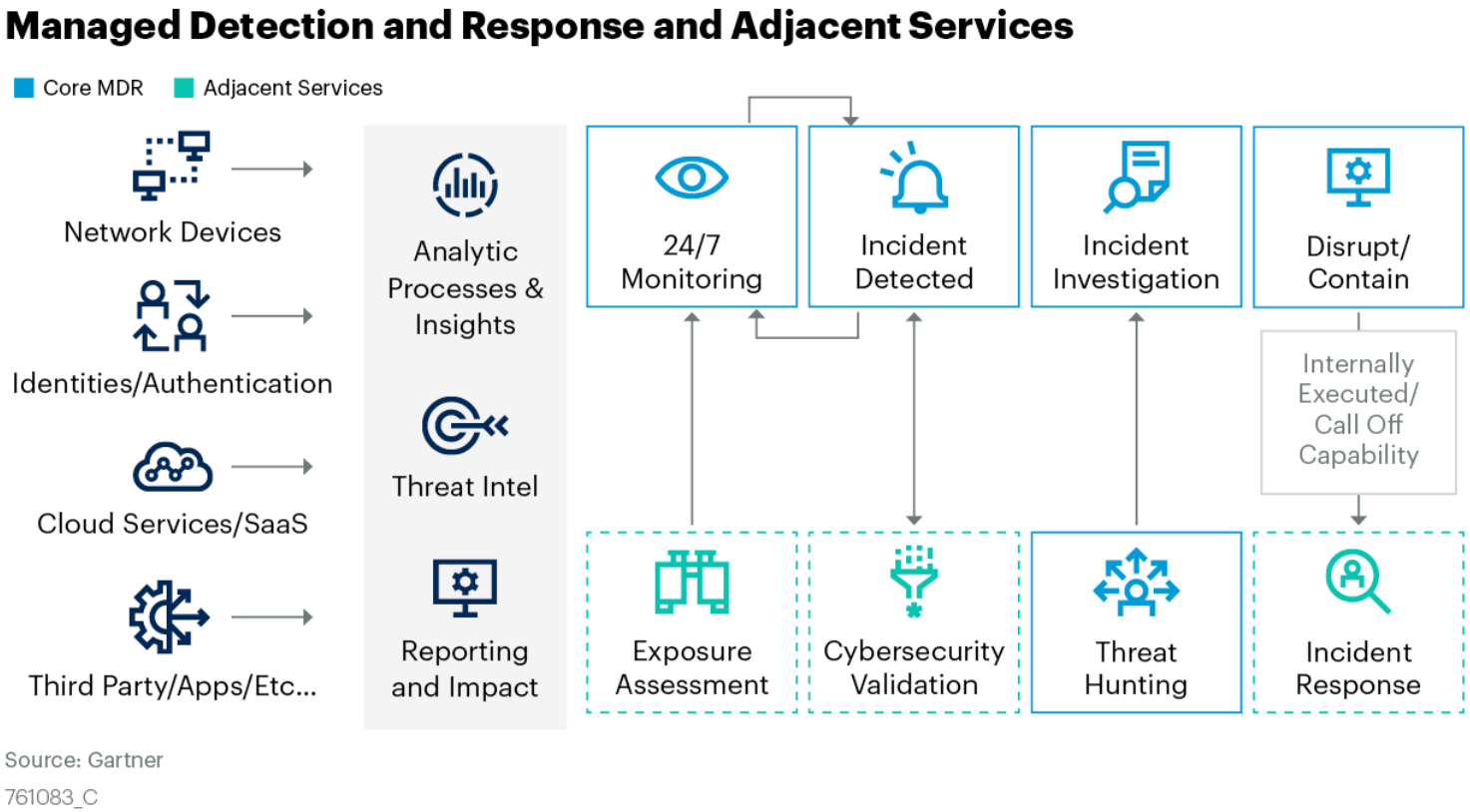
Description du marché

MDR fournit aux clients des fonctions SOC gérées par l'homme et fournies à distance à des fins de signalement, de détection rapide, d'analyse et d'investigation des menaces, ainsi que de réponse d'atténuation à distance à ces menaces (voir la remarque 1) .

Les fournisseurs de services MDR offrent ces capacités à l'aide d'une combinaison variable de technologies - celles-ci sont généralement axées sur les terminaux et le réseau, mais impliquent de plus en plus des couches de services cloud, SaaS et des applications personnalisées. De plus, la connectivité aux capacités adjacentes fournit des informations contextuelles (par exemple, l'identité et l'utilisateur, l'exposition aux menaces et la criticité commerciale) pour améliorer et valider la détection des menaces. Les fournisseurs développent du contenu et des analyses axés sur les menaces, également connus sous le nom d'ingénierie de détection, et appliquent des informations sur les menaces, qu'elles soient développées en interne, achetées à des tiers ou une combinaison des deux approches. Les fournisseurs appliquent également des activités d'interruption et de confinement manuelles/automatisées, telles que l'isolement de l'hôte, le verrouillage de compte et le blocage du réseau (voir Figure 1).

La chasse aux menaces augmente la détection des menaces en temps réel. Il peut trouver des attaquants employant des tactiques, des techniques et des procédures (TTP) qui ont contourné les capacités de prévention et de détection des clients ou qui valident l'inexistence d'une menace dans un environnement . De plus, les demandes de chasse aux menaces plus ponctuelles et axées sur des hypothèses dirigées par les entreprises ont gagné en popularité. Ce type de chasse aux menaces ne doit pas être confondu avec la chasse aux menaces quotidiennes qui doit être incluse en tant que partie standard d'un service MDR. Au lieu de cela, il doit être considéré comme un service supplémentaire, motivé par les demandes des consommateurs pour des résultats spécifiques et aligné sur les modèles de tarification des conseils sur appel.

Figure 1 : Détection et réponse gérées et services adjacents



Les services MDR sont conçus pour réduire le délai entre la détection et la réponse aux menaces . Des fonctions d'opérations de sécurité supplémentaires ont vu le jour, notamment la gestion de l'exposition, la criminalistique numérique et la réponse aux incidents (DFIR) et les capacités de validation de la sécurité (telles que la simulation de violation et d'attaque [BAS]). Celles-ci complètent et enrichissent la détection des menaces, l'analyse, l'investigation ainsi que la réponse d'atténuation aux menaces.

Direction du marché

Le MDR est un marché établi à forte croissance (voir Part de marché : services de sécurité gérés, dans le monde, 2021, où le MDR est un segment distinct, le marché du MDR a augmenté de 48,9 % de 2020 à 2021).

Les fournisseurs de services MDR performants se concentrent sur la détection des menaces haute fidélité, l'investigation et la réponse d'atténuation avec une grande verbosité et des rapports interprétables par l'homme alignés sur les risques axés sur l'entreprise. Le fournisseur assume la responsabilité de déterminer comment les menaces sont détectées. Les clients peuvent avoir peu de possibilités de personnaliser les cas d'utilisation de la détection des menaces en fonction de leur environnement, mais sont encouragés à communiquer les exigences basées sur les risques pour s'assurer que les cas d'utilisation pertinents sont mis en œuvre. Ces exigences peuvent inclure l'identification des fonctions commerciales critiques et des actifs dont elles dépendent, ou du personnel ou des données importants et de l'impact que leur interruption ou leur compromission peut entraîner.

Les acheteurs ne doivent pas s'attendre à une personnalisation distincte ou spécifique qui serait disponible dans davantage de services de conseil dans le cadre du service MDR de base, car cela peut éventuellement être proposé en tant que capacité de service complémentaire ou adjacente. Pour atteindre l'échelle requise, une plate-forme de livraison commune pour tous les clients fournissant des rapports centralisés est essentielle. Une plate-forme de livraison commune garantit que tous les clients reçoivent un ensemble

commun de contenus TI et de détection et donc une expérience de service comparable. Cela offre à la fois une maturité aux capacités SOC établies au sein des organisations ou un niveau de maturité immédiat à ceux qui ont peu de capacités existantes.

D'autres éléments de MDR émergent sur le marché mais ne sont pas encore monnaie courante. Les caractéristiques suivantes peuvent attirer les acheteurs, en particulier lorsqu'ils recherchent une différenciation sur leurs marchés. Un modèle typique observé parmi les organisations moins matures dans leurs opérations de sécurité est de commencer par les capacités de détection et de réponse aux menaces, puis d'étendre les services utilisés par le fournisseur pour améliorer d'autres domaines des opérations de sécurité. Les domaines émergents comprennent :

- **Extension à d'autres fonctions d'opérations de sécurité, telles que la gestion de l'exposition , au-delà de l'analyse de vulnérabilité traditionnelle :**
  - Les capacités de gestion de l'exposition aident à prévenir les attaques grâce à une meilleure connaissance de leur surface d'attaque, une hiérarchisation efficace des expositions dans l'environnement du client, des comptes d'utilisateurs et des applications cloud, et la validation que ces expositions représentent réellement un risque.
  - La possibilité de surveiller l'infrastructure en tant que service (IaaS) et les plates-formes SaaS, ainsi que les applications en ligne populaires, en particulier les applications telles que Google Workspace, Microsoft 365, Salesforce, SAP et Workda y .
- **Compléments en libre-service de la plateforme commune , aussi appelée « co-gestion » :**
  - Celles-ci permettent aux organisations d'étendre leur maturité en matière de sécurité, d'abandonner l'utilisation d'un service MDR et d'inclure des fonctionnalités telles que l'investigation des données et les outils de création de rapports. Ces fonctionnalités permettent au personnel de sécurité interne du client d'utiliser les données collectées par le fournisseur pour des recherches et des fonctions personnalisées, telles que la chasse aux menaces ou les rapports de conformité.

Les services MDR sont disponibles auprès d'une gamme de fournisseurs (bien au-dessus de 300 fournisseurs à la date de cette recherche). Ces fournisseurs peuvent se concentrer spécifiquement sur l'opportunité du marché MDR et se consacrer à fournir uniquement des services de détection et de réponse, ou offrir une détection et une réponse ainsi que des services plus larges spécifiques à la sécurité informatique. Les services MDR sont également disponibles via des fournisseurs de services gérés (voir le Guide du marché pour les services de sécurité gérés), qui proposent le MDR dans le cadre d'un catalogue plus large de services ou de conseils en matière de technologie gérée, de sécurité et de gestion des risques.

De nombreux fournisseurs de MDR ciblent également des secteurs verticaux où ils peuvent offrir une expertise et des services spécifiques à l'industrie (tels que les infrastructures critiques et la fabrication, ou les soins de santé, qui ont tous des problèmes de confidentialité, de sécurité et de fiabilité). Pour plus d'informations, consultez Innovation Insight pour les plateformes de protection des systèmes cyber-physiques.

La détection d'une menace n'a aucun sens sans une réponse planifiée et opportune à cette menace.

Analyse de marché

La proposition de valeur clé du MDR est l'interprétation humaine des incidents de sécurité, en fournissant des conseils, ainsi qu'en effectuant les étapes d'atténuation initiales, qui seraient autrement complexes à comprendre et à mettre en œuvre. En fournissant une enquête, une analyse et une validation des menaces basées sur le contexte (et en prenant des mesures pour perturber ou contenir une attaque), le fournisseur de MDR peut gagner du temps pour que le client effectue une enquête plus approfondie et finalement corrige les problèmes découverts en utilisant ses processus de réponse standardisés internes .

Les capacités fournissant une réponse atténuante, pour perturber ou contenir les menaces, sont une capacité essentielle des fournisseurs de services MDR. Bon nombre de ces actions de réponse d'atténuation sont centrées sur l'utilisation de solutions EDR pour perturber ou contenir une menace, par exemple pour isoler un terminal ou tuer des processus malveillants. Cependant, les actions de réponse sont de plus en plus axées sur l'architecture d'entreprise moderne et les fonctions centrées sur l'identité (telles que les restrictions de compte dans les systèmes d'authentification) qui permettent à la réponse d'un fournisseur MDR d'être efficace sur toutes les plateformes, dans le cloud et le SaaS ainsi que sur site.

Les styles de prestation de services MDR varient, méfiez-vous des services de moindre importance qui imitent le MDR

Une variété d'approches de service MD R s'adresse à un éventail d'acheteurs. Les types d'acheteurs incluent :

- Les organisations qui ont des investissements dans la capacité de détection des menaces, d'investigation et de réponse (TDIR), mais qui se considèrent incapables de gérer ces investissements efficacement en raison d'une taille d'équipe ou de compétences inadéquates.
- Les organisations qui n'ont pas investi ou développé de capacités TDIR et qui ont besoin d'un soutien à la fois pour la configuration de base et la maintenance et la supervision à long terme d'une capacité.
- Les organisations qui disposent d'un SOC et souhaitent utiliser des services pour améliorer l'efficacité de leurs équipes et étendre la disponibilité des ressources existantes afin d'effectuer une défense contre les menaces plus axée sur l'entreprise .
- Les organisations qui ont une vision à long terme de posséder TDIR en interne mais qui doivent atteindre rapidement un niveau de maturité et qui souhaitent utiliser des services pour fournir une couverture provisoire pendant qu'elles embauchent, perfectionnent et développent les exigences pour les opérations SOC.

Les fournisseurs de MDR doivent exploiter la technologie de manière centralisée, de manière mutualisée pour atteindre l'échelle et la cohérence exigées par les acheteurs, et pour bénéficier des avantages de la visibilité mondiale du fournisseur concernant le contenu et la pertinence de la détection. Il n'y a pas de choix de type de technologie obligatoire, ni d'ensemble de télémétrie requis pour fournir un service MDR. Cependant, pour la plupart des engagements, une vaste expérience des plates-formes de détection et de télémétrie axées sur les points de terminaison, le réseau, le cloud SaaS et les applications est préférable pour la plupart. Des extensions à l'Internet des objets (IdO) et aux systèmes de sécurité cyber-physique (

CPS) ou à la technologie opérationnelle (OT) sont disponibles, mais rarement appelées séparément des exigences fondamentales de sécurité informatique ; les organisations reconnaissent que les cybermenaces sont des cybermenaces, quel que soit le système dans lequel elles résident.

Les acheteurs ont été confrontés à des défis avec la dénomination des services et le langage marketing qui ont souvent été trop promis et sous-livrés. Les capacités et les composants des services de base devraient être globalement les mêmes pour tous les fournisseurs de ce marché. Cependant, certains fournisseurs décrivent et proposent leurs services en tant que MDR, lorsqu'ils ne sont pas fournis comme un acheteur pourrait s'y attendre ou conformément à la manière dont le MDR est décrit dans ce guide. Il existe de nombreux domaines où une nouvelle terminologie, des mots à la mode et des acronymes ont fait surface et semé la confusion sur le marché :

- **Fournir simplement un service technologique géré -** Les services qui offrent une légère superposition aux investissements technologiques existants, tels que les technologies de détection et de réponse aux points finaux (EDR), sont souvent appelés MDR. Ces services offrent une expérience beaucoup moins humaine, en fonction de la technologie utilisée pour l'essentiel de la prestation. Bien que toujours valables, ces offres sont souvent promues comme étant plus engagées qu'elles ne le sont réellement, et seraient mieux décrites comme EDR gérées (MEDR). Généralement fournis par des fournisseurs de technologie, une dotation en personnel interne, des ensembles de compétences et un engagement accrus sont nécessaires pour tirer pleinement parti de ces services. Ces services sont également souvent fournis à l'aide de la technologie de gestion des informations et des événements de sécurité (SIEM) (voir Guide du marché de Gartner pour les services SIEM gérés) .

- **Détection et réponse étendues gérées -** Une tentative d'apparaître plus approfondie que les services MDR, la détection et la réponse étendues gérées sont généralement interchangées avec MDR en tant que terme de service, mais il n'est pas encore prouvé qu'il offre réellement plus de capacités ou de meilleurs résultats. Comme son nom l'indique, la technologie de détection et de réponse étendue gérée utilise une gamme de télémétrie plus large que, par exemple, l'EDR seul . Cependant, les services MDR utilisent généralement la télémétrie à partir d'un grand nombre de sources. Les acheteurs doivent examiner de plus près les offres de détection et de réponse étendues gérées pour s'assurer qu'on ne leur propose pas simplement une offre de technologie gérée (similaire à celle de MEDR) s'ils ont besoin des capacités MDR définies dans cette recherche.

- **Services renommés de détection des menaces historiques —** Certains fournisseurs proposent depuis un certain nombre d'années des services qui fournissent des capacités SOC en tant que service. Bon nombre de ces services pourraient être décrits comme étant plus alignés sur le SIEM géré ou fortement personnalisés en fonction du client. L'hétérogénéité de ces services et le manque d'offre clé en main peuvent parfois se camoufler derrière le changement de nom d'un service historique en MDR. Les acheteurs doivent évaluer ces services en fonction de leurs besoins. Ces services peuvent fournir des niveaux élevés de qualité et de détail dans les résultats, mais prennent régulièrement plus de temps à livrer, sont plus chers et nécessitent beaucoup plus de directives de la part de l'acheteur en ce qui concerne la portée et l'évolution.

Certains fournisseurs de MDR sont plus flexibles quant à l'utilisation des technologies de sécurité déjà détenues par les acheteurs. Ces fournisseurs auront un ensemble défini de technologies et de fournisseurs pris en charge, et dépendent généralement de la facilité d'intégration (par exemple, via des API) et de l' utilité

de cette technologie (par exemple, la capacité de produire une télémétrie utile, de détecter les menaces et de prendre en charge les incidents activités de réponse).

Cependant, il existe une tendance selon laquelle les organisations investissent dans leurs propres piles de technologies de sécurité, puis cherchent à adopter les services MDR. En réaction, la flexibilité des fournisseurs de services concernant les sources de données évolue vers un agnosticisme total des sources de données . Les acheteurs qui ne veulent pas ou ne peuvent pas remplacer les investissements qu'ils ont faits dans les technologies de sécurité ont besoin d'un fournisseur de MDR capable de s'adapter ou de s'intégrer aux technologies de sécurité qu'ils ont adoptées .

Il existe également un certain nombre de circonstances dans lesquelles les investissements de sécurité sont inclus dans le cadre d'une infrastructure plus large et d'abonnements SaaS. Celles-ci sont désormais courantes en tant que technologie principale prise en charge, certains fournisseurs de technologie développant spécifiquement des capacités pour permettre une gestion à plusieurs niveaux des plates-formes, donnant aux fournisseurs tiers un accès et un contrôle en plus de l'accès interne existant pour les équipes de sécurité.

La volonté d'utiliser des services plus indépendants de la technologie augmente la nécessité d'imposer un ensemble minimum de télémétrie pour permettre aux fournisseurs de fournir des services cohérents et de haute qualité. Les fournisseurs de MDR prenant en charge cette approche risquent de perdre le contrôle de la qualité et de la fidélité des sources de détection des menaces. Sans cela, ils seront incapables d'enquêter et de répondre efficacement aux menaces et donc incapables de répondre véritablement aux besoins de l'acheteur MDR.

Les services MDR doivent démontrer leur capacité à faire face aux menaces dans les infrastructures modernes

L'infrastructure moderne comprend l'utilisation de SaaS, IaaS, des abonnements tiers, des outils open source et une grande variété d'applications développées en interne. Le modèle traditionnel d'appareils sur site, de pare-feux de délimitation et d'appareils de point de terminaison spécifiques à l'entreprise commence à s'estomper. Les acheteurs de MDR doivent exiger la compatibilité pour les zones de leur infrastructure qui sont les plus critiques pour leur mission. Cela signifie non seulement une visibilité dans ces zones, mais également une réponse d'atténuation. "L'identité" devient rapidement une pièce importante du puzzle, et c'est l'un des rares points communs entre une soupe de technologies, de fournisseurs, d'applications et d'abonnements différents (voir Améliorer votre préparation aux cyberattaques avec la détection et la réponse aux menaces d' identité) .

Les clients de Gartner considèrent les fournisseurs de MDR comme l' ensemble de leur cohorte d'analystes SOC Tier 1 et 2 ou comme une partie étendue de leur SOC existant. Les clients s'attendent à ce que leurs fournisseurs soient en mesure d'effectuer une enquête et un confinement en leur nom . Ceci est d'autant plus visible que les clients autorisent les fournisseurs de MDR à effectuer des activités d'interruption et de confinement à distance pour prendre en charge les processus internes de réponse aux incidents.

Les organisations qui dépendent des services MDR pour l'essentiel de leurs fonctions d'opérations de sécurité ont signalé qu'elles sont très susceptibles de

rejeter les fournisseurs MDR qui ne peuvent pas prendre des mesures d'atténuation des menaces en leur nom.

Lorsque les acheteurs ne sont pas à l'aise avec le fait que les fournisseurs exécutent directement les actions, ils veulent des mécanismes simples pour approuver ou initier eux-mêmes toute action de perturbation ou de confinement des menaces . La réponse complète à une menace n'est généralement pas effectuée par les fournisseurs de MDR . Cependant , les responsables de la sécurité et de la gestion des risques devraient exiger des menacesla perturbation et le confinement de leurs fournisseurs de services. Les activités de remédiation doivent être un ensemble logique de processus internes de suivi bien établis qui sont mis en œuvre une fois que les fournisseurs de MDR ont perturbé ou contenu les menaces. La correction doit être interne car il est difficile pour un fournisseur de MDR d'effectuer des activités de réponse complètes et de savoir, catégoriquement, qu'il n'aura pas d'impact inutile sur les fonctions commerciales légitimes. En tant que service supplémentaire, certains fournisseurs de MDR qui proposent des mandats de réponse aux incidents peuvent également aider à la phase de récupération, ce n'est pas la même chose que la réponse d'atténuation incluse dans le MDR.

Les processus des opérations de sécurité ne peuvent pas être entièrement externalisés

Le MDR peut être une offre intéressante, mais comme toutes les variétés de sécurité gérée, ce n'est pas une solution globale. Bien que certains des fournisseurs de MDR les plus progressistes soient en mesure d'être alignés sur les risques commerciaux, il est important de déterminer si le service qu'ils offrent découle des exigences spécifiques axées sur les risques de votre organisation et produit des résultats sur lesquels les équipes internes pourront agir.Concentrez-vous sur les détails des résultats offerts par les fournisseurs de MDR et identifiez la meilleure façon d'intégrer les sorties et la couverture d'un fournisseur de services MDR dans vos propres processus internes de réponse aux incidents. Il est essentiel d'affiner les processus de sécurité si vous espérez améliorer les résultats globaux. Il est également important de permettre aux ressources internes de travailler avec vos fournisseurs, car cela améliorera les résultats et aidera à maintenir de bonnes relations de travail avec les fournisseurs.

Évolution du marché MDR

Augmentation de la pertinence de l'exposition aux menaces

L'exposition d'une organisation aux menaces de sécurité est plus qu'une simple vulnérabilité, et avec l'expansion de l'infrastructure SaaS et IaaS, la gestion des problèmes découverts est plus difficile et plus volumineuse. Les fournisseurs de MDR ont commencé à chercher comment ils peuvent approcher une connexion entre la détection des menaces traditionnelles, la réduction de la surface d'attaque d'un client (voir Innovation Insight for Attack Surface Management) et la découverte des menaces et des expositions dans l'infrastructure moderne. La présentation d'une vue basée sur les risques des expositions aux menaces que les clients sont en mesure de hiérarchiser devrait être l'objectif principal d'une telle capacité. Cela devrait être exécuté par une communication efficace de l'impact commercial des scénarios de sécurité hypothétiques.Il y a encore une grande immaturité dans la visibilité de la plate-forme cloud, mais la pertinence d'inclure une analyse préventive axée sur l'exposition correspondra probablement et peut-être dépassera la nature réactive de la détection des menaces traditionnelles dans les prochaines années (voir Predicts 2023 : Enterprises Must Expand From Menace pour la gestion de l'exposition).

Adoption du MDR par des acheteurs plus matures

La cohérence dans la livraison est une caractéristique clé des services MDR, car cela leur permet d'évoluer. Mais cela permet également aux clients de mieux comprendre ce que le service fournira spécifiquement. La cohérence est quelque chose de bénéfique pour les acheteurs moins matures et matures. Pour les acheteurs moins matures, la cohérence permet d'utiliser les clients MDR existants comme référence pour la qualité et l'assurance du service, et pour les acheteurs plus matures, cela devient une garantie d'efficacité. Les services MDR n'ont pas besoin de fournir des capacités de détection de pointe ou d'être à l'avant-garde du marché des renseignements sur les menaces pour apporter de la valeur. Des livrables clairs et cohérents qui améliorent l'efficacité opérationnelle et la maturité de l'équipe de sécurité d'une entreprise sont souvent exactement ce qui est requis.

Certains fournisseurs de MDR ciblent spécifiquement les acheteurs plus matures, en se concentrant sur la fourniture d'une solution sur mesure pour les organisations ayant déjà investi dans des outils de sécurité. Certains prestataires sont particulièrement agnostiques dans la manière dont ils délivrent leurs services. Cette approche commence à ressembler aux services SOC traditionnels des fournisseurs de services de sécurité gérés (MSSP), mais en mettant davantage l'accent sur les activités de perturbation et de confinement en plus des alertes et notifications typiques.

Validation complémentaire de la cybersécurité

Les acheteurs continuent de lutter pour tester les affirmations des fournisseurs de services de sécurité, en particulier ceux qui surprotègent la propriété intellectuelle (contenu de détection) qu'ils développent pour détecter les menaces pour les services proposés . Les capacités de BAS et de tests d'intrusion automatisés sont généralement considérées comme un moyen efficace de valider les affirmations des fournisseurs concernant la couverture et la complexité des mécanismes de détection. Une approche intéressante pour les acheteurs consiste à faire appel à un fournisseur tiers indépendant de tests et de simulations pour valider les capacités et renforcer la sécurité au cours d'un engagement.

Disponibilité de la technologie en libre-service

Une présence croissante sur le marché de la sécurité gérée et une augmentation des demandes « en tant que service » ont poussé un certain nombre de fournisseurs de MDR à proposer leurs plates-formes technologiques à des acheteurs plus matures ou plus matures. Cet ajout aux portefeuilles n'est pas une extension directe des capacités MDR. Cependant, cela montre la volonté et l'ouverture des fournisseurs de MDR de laisser les clients voir "sous le capot". Il soutiendra également une évolution naturelle de la maturité pour les clients qui souhaitent plus de contrôle et de visibilité sur leurs événements et problèmes de sécurité . Ces clients peuvent trouver que les options en tant que service prennent en charge une migration potentielle loin des outils et des technologies dont ils ne veulent plus la responsabilité de la gestion.

Activité de fusion et d'acquisition sur le marché MDR

Au cours des 12 derniers mois, il y a eu de nombreuses acquisitions sur ce marché .

Au 1T22 et 2T22 :

- Google rachète Mandiant
- Le groupe Herjavec et le groupe Fishtech conviennent de fusionner
- ReliaQuest achète Digital Shadows
- Logique d'alerte Fortra Buys

- Arctic Wolf achète Tetra Defense
- Forescout achète Cysiv

Au 3T22 et 4T22 :

- Open Systems achète Tiberium
- Security On-Demand achète/unifie avec le service MTS de Booz Allen Hamilton pour créer DeepSeas
- Allurity achète Aiuken
- CrowdStrike achète Reposify
- Logique d'alerte Fortra Buys

Les responsables de la sécurité et de la gestion des risques doivent être préparés au fait que, dans un marché en croissance rapide, les fournisseurs continueront d'être acquis.

Fournisseurs représentatifs

Les fournisseurs répertoriés dans ce guide du marché ne constituent pas une liste exhaustive. Cette section vise à mieux comprendre le marché et ses offres.

Présentation du marché

Gartner a inclus une gamme de fournisseurs dans cette recherche pour assurer une couverture d'un point de vue géographique, vertical et des capacités. Gartner estime que plus de 600 fournisseurs de ce marché prétendent proposer des services MDR. Ceux inclus dans ce guide du marché :

- Sont visibles pour les clients de Gartner (en fonction des demandes)
- Sont de taille et de distribution variables afin de refléter la population d'acheteurs
- Avoir une offre claire axée sur l'utilisateur final et les résultats, distincte des offres purement axées sur la technologie

Une liste des fournisseurs représentatifs est fournie dans le tableau 1 . Il ne s'agit pas d'une liste de tous les fournisseurs du marché des services MDR. Il ne s'agit pas, ni n'est destiné à être, d'une analyse concurrentielle des fournisseurs.

Tableau 1 : Fournisseurs représentatifs

Fournisseur	Nom du service	Quartier général
Accusé de réception	Détection et réponse gérées	Barcelone, Espagne
Aiuken	Détection et réponse gérées	Madrid, Espagne

Réseaux de loups arctiques	Détection et réponse gérées	Eden Prairie, Minnesota
Atos	Détection et réponse gérées	Bezons, France
Défense binaire	Détection et réponse gérées	Stow, Ohio
Bitdefender	MDR Avancé/Entreprise	Bucharest, Roumanie
BleuVoyant	Détection et réponse gérées	New York, New York
Aperçu critique	Détection et réponse gérées	Seattle, Washington
Démarrage critique	Détection et réponse gérées	Plan, Texas
FouleStrike	Faucon complet	Sunnyvale, Californie
Cyberaison	Cybereason MDR terminé	Boston, Massachusetts
CYBEROO	Détection et réponse gérées	Reggio d'Émilie, Italie
Cydère [2]	Détection et réponse gérées par l'entreprise	Kansas City, Missouri
Cysiv	SOC en tant que service	San José, Californie
Mer profonde [1]	Services de gestion des menaces (MTS)	McLean, Virginie
Deepwatch	Détection et réponse gérées	Denver, Colorado
eSenti	Détection et réponse gérées	Waterloo, Ontario

Expulser	Expulser le MDR	Herndon, Virginie
Fortra	Détection et réponse gérées	Eden Prairie, Minnesota
Intégrité360	Détection et réponse gérées	Dublin, Irlande
IBM	Détection et réponse gérées	Armonk, New York
Kroll	Répondeur Kroll	New York, New York
Sécurité Kudelski	Détection et réponse gérées	Cheseaux-sur-Lausanne, Suisse ; et Phoenix, Arizona
Mandiant	Défense gérée _	Alexandrie, Virginie
mnémonique	Défense gérée par Argus	Oslo, Norvège
Groupe CNC	Détection et réponse gérées	Manchester, Royaume-Uni
Obrela Sécurité Industries	Détection et réponse aux menaces gérées	Londres, Royaume-Uni
Ontinue (la division MDR d'Open Systems)	Détection et réponse gérées	Zurich, Suisse
Optiv	Détection et réponse gérées	Denver, Colorado
Orange Cyberdéfense	Détection et réponse gérées	Paris, France
Pondurance	Détection et réponse gérées	Indianapolis, Indiana
Professionnel	Détection et réponse gérées	Carlsbad, Californie

Quorum Cyber	Azure Sentinel SOC et MDR	Édimbourg, Royaume-Uni
Rapide7	Détection et réponse gérées	Boston, Massachusetts
Canari rouge	Détection et réponse gérées	Denver , Colorado
Secureworks	Détection et réponse gérées	Atlanta, Géorgie
Sophos	Détection et réponse gérées	Santa Clara, Californie
Trustwave	Détection et réponse gérées	Chicago, Illinois
Verizon	Détection et réponse gérées	New York, New York
AvecSecure	Détection et réponse gérées par Countercept	Helsinki, Finlande

[1] Anciennement Booz Allen Hamilton

[2] Fusion entre Herjavaec et Fishtech

Source : Gartner (février 2023)

Recommandations du marché

- Les services MDR ne conviennent pas à toutes les organisations. Comme indiqué dans la section Analyse du marché, il existe une variété de styles de prestation pour les services MDR et certains n'ont de MDR que le nom. Dans le cadre d'une volonté d'accroître la maturité, les organisations doivent déterminer si elles bénéficieront d'une combinaison de capacités de service à la fois à l'intérieur et à l'extérieur du MDR, y compris des engagements cogérés, SOC-as-a-service ou une approche interne de bricolage.

- Définissez les résultats spécifiques requis (structure des tickets d'incident, rapports) et les objectifs qui traitent des cas d'utilisation définis, avant de vous engager avec un fournisseur. Comme pour toute initiative d'externalisation, si les résultats ne sont pas définis, quel que soit le fournisseur de services utilisé, les chances de succès seront réduites (voir Qu'est-ce qui fait qu'un appel d'offres pour un service de sécurité réussi ?) . Les acheteurs doivent également veiller à ne pas trop insister sur la valeur des SLA dans le cadre de services axés sur la détection et la réponse.

- Comme les services MDR sont « consommables », les acheteurs doivent développer et appliquer leurs propres politiques et procédures internes de réponse aux incidents, afin de s'assurer que la pleine valeur du service MDR peut être obtenue. Une compréhension pertinente et interne de l'entreprise est essentielle

pour la « bonne » réponse à une menace découverte. Certains fournisseurs de MDR sont bien placés pour aider leurs clients à développer des politiques et des processus s'ils n'existent pas ou nécessitent une mise à jour. Les services internes, tels que les ressources humaines et le service juridique, peuvent être impliqués, tout comme les prestataires de services de réponse aux incidents (voir le Guide du marché pour la criminalistique numérique et la réponse aux incidents).

- Les organisations doivent effectuer une diligence raisonnable suffisante sur les fournisseurs de MDR avant de signer un contrat. Utilisez un appel d'offres et une preuve de concept (POC) et demandez des exemples de livrables pour valider les revendications et l'adéquation aux besoins avec les exigences de votre organisation. Utilisez également d'autres sources, telles que votre réseau de pairs et Gartner Peer Insights.

- Si vous avez des exigences de résidence des données et de confidentialité ou d'autres exigences de conformité, confirmez que les fournisseurs de MDR peuvent s'y conformer. Concentrez-vous sur les fournisseurs de MDR de votre région géographique ou sur ceux qui utilisent une architecture de collecte de données qui respecte les exigences de résidence des données . Une conservation séparée des journaux peut être requise en complément de tout service MDR pour garantir l'alignement sur les exigences réglementaires.

Clé d'acronyme et termes du glossaire

BAS	simulation de brèche et d'attaque
TCAC	taux de croissance annuel composé
CASB	courtier en sécurité d'accès au cloud
CIPS	infrastructure cloud et services de plate-forme
CNAPP	plate-forme de protection des applications cloud native
CWPP	plate-forme de protection de charge de travail cloud
DFIR	criminalistique numérique et réponse aux incidents
EDR	détection et réponse aux points finaux
PPE	plate-forme de protection des terminaux
IdO	Internet des objets
MDR	détection et réponse gérées
MSSP	fournisseur de services de sécurité gérés

NSM	surveillance de la sécurité du réseau
OT/ICS	technologie opérationnelle et systèmes de contrôle industriels
MONTER	orchestration de la sécurité, automatisation et réponse
COS	centre des opérations de sécurité
TI	renseignements sur les menaces
PTaaS	test d'intrusion en tant que service
TTP	tactiques, techniques et procédures

Remarque 1 : détection et réponse gérées

La réponse d'atténuation à distance est définie comme une interruption ou des actions de confinement, telles que la mise en quarantaine des hôtes et la désauthentification des utilisateurs.

Gartner