Guide essentiel

9 ASPECTS À PRENDRE EN COMPTE DANS LE CHOIX D'UN SERVICE MDR

ESET Digital Security
Progress. Protected.

Un service MDR (Managed Detection and Response) peut aider à combler les lacunes en matière de capacité et d'expertise dans le domaine de la sécurité. Choisir le bon fournisseur est essentiel.

Les entreprises de toutes tailles admettent de plus en plus la nécessité d'une sécurité plus proactive. L'adoption croissante de l'informatique en nuage, de nouvelles pratiques de travail hybrides et d'une chaîne d'approvisionnement numérique ont augmenté la surface d'attaque, et les acteurs de la menace sont devenus plus inventifs pour trouver des moyens de s'infiltrer dans les réseaux.

Cependant, seules les grandes entreprises opèrent à une échelle qui leur permet de mettre en place un centre d'opérations de sécurité complet et de le doter d'analystes SOC à temps plein. Même si vous disposez des fonds nécessaires, les spécialistes de la cybersécurité se font rares. Si vous êtes une PME, vous devez probablement compter sur des informaticiens généralistes pour assurer la défense de l'environnement informatique.

Les services MDR (Managed detection and response) répondent aux besoins des entreprises qui doivent combler des lacunes en matière de capacité et d'expertise dans le domaine de la sécurité. Ils donnent accès à des services gérés par des professionnels de la cybersécurité et aux outils spécialisés dont ils ont besoin pour exercer leur métier.

Ceux qui emploient le terme MDR pour décrire leurs offres disposent toutefois d'une grande variété de modèles de prestation. Si vous estimez que le moment est venu de renforcer votre sécurité et de faire appel à un service MDR externalisé, vous devrez effectuer quelques recherches préalables afin de trouver le fournisseur qui conviendra le mieux à votre structure. Voici les questions que vous devriez vous poser.

1. QUEL EST LE PROCESSUS D'INTÉGRATION ET DE CONFIGURATION DU FOURNISSEUR ?

Les délais d'intégration varient, tout comme les outils de référence et les modèles de prestation des différents fournisseurs MDR. Faites le point sur le processus d'intégration et sur la mesure dans laquelle votre équipe informatique doit être impliquée afin qu'il n'y ait pas de surprises.

Les règles, exclusions et paramètres de détection doivent être personnalisés pour répondre aux besoins de votre environnement informatique et aux menaces auxquelles votre entreprise est confrontée. Une intégration plus rapide est certes toujours préférable, mais il faut faire quelques concessions pour trouver un équilibre entre la mise en place du service MDR le plus rapidement possible et l'obtention d'un fonctionnement optimal de la détection dès le premier jour.

De plus, gardez à l'esprit que la protection offerte par un service MDR s'améliore avec le temps. Il faut procéder à un certain nombre d'ajustements au fur et à mesure que les outils et les analystes humains gagnent en expérience pratique et assimilent ce qui est normal de ce qui ne l'est pas dans votre environnement.

2. LE SERVICE EST-IL DISPONIBLE 24H/24 ET 7J/7 ?

Les groupes adverses opèrent depuis des pays et des fuseaux horaires du monde entier, ce qui signifie qu'un service MDR doit être opérationnel 24h/24 et 7j/7. Les indicateurs de compromission et ceux d'attaque doivent être étudiés immédiatement, en temps réel, afin qu'une réponse appropriée puisse être engagée.

Un service local présente certains avantages, mais ceux-ci disparaissent rapidement si les effectifs ne couvrent pas suffisamment les besoins pendant la nuit. Votre meilleure option pourrait être un service qui peut mettre à votre disposition un représentant local et qui dispose également de centres d'opérations de sécurité dotés d'un personnel suffisant partout dans le monde, pour un fonctionnement 24h/24 et 7j/7.

3. QUELLE EST LA PILE TECHNOLOGIQUE ? QUELLES DONNÉES SONT UTILISÉES ?

Un service MDR repose sur une pile technologique fournie par le fournisseur qui gère la détection, l'enquête, l'atténuation et la réponse. Il peut s'agir d'un ensemble technologique développé par le fournisseur ou d'un ensemble d'outils de tiers reliés par des API.

Ces outils comprendraient très probablement, des solutions de détection et de réponse telles que, Endpoint Detection & Response (EDR) ou Extended Detection & Response (XDR), la gestion des informations et des événements de sécurité (SIEM) et l'orchestration, l'automatisation et la réponse aux alertes et incidents de sécurité (SOAR) et devraient s'intégrer à votre plateforme de protection des endpoints.

La caractéristique d'un système XDR par opposition à un système EDR est l'incorporation de données provenant de sources extérieures aux endpoints, y compris le trafic réseau et divers fichiers log. Demandez quelles données seront utilisées dans le cadre de la surveillance. L'un des avantages d'un service proposé par un éditeur de sécurité est que la plateforme des endpoints peut non seulement alimenter directement le XDR, mais peut également fournir une télémétrie qui recueille des données uniques sur les attaques.

Les cyberadversaires sont de plus en plus aptes à utiliser les services en nuage comme moyen d'attaque ou comme partie de la chaîne d'attaque, alors assurez-vous que votre fournisseur MDR est capable de détecter et de surveiller les activités dans le cloud.

4. QUELS RÔLES JOUE L'AUTOMATISATION DANS L'OFFRE ? QUELS RÔLES JOUENT LES ANALYSTES HUMAINS ?

Une pile technologique robuste est certes indispensable, mais ce qui fait la force d'un service MDR, c'est la présence d'analystes en cybersécurité dans la boucle.

L'intelligence artificielle peut jouer un rôle précieux dans l'identification des comportements anormaux et le filtrage d'actions à priori anodines pour reconnaître les corrélations et les signes de compromission ou d'attaque.
L'automatisation peut rapidement exécuter un ensemble d'actions qui isolent les systèmes ou stoppent une attaque. Ils servent d'assistance et ne remplacent pas l'expertise des analystes humains.

Dans leur hâte de commercialiser ou de rendre leurs services plus abordables, certains fournisseurs MDR privilégient de manière excessive l'automatisation pour une partie de leurs

offres (pour en savoir plus, voir plus bas « Qui s'occupe de l'atténuation et de la remédiation ?) Certains fournisseurs proposent des services à plusieurs niveaux, les plus élevés permettant d'accéder à des services plus spécialisés, tels que la participation de responsables chargés de la réponse aux incidents, digital forensic incident response (DFIR) et l'analyse des logiciels malveillants par des experts.

5. QUELLES SOURCES DE RENSEIGNEMENTS SUR LES MENACES SONT UTILISÉES ?

La mise à jour des renseignements sur les menaces concernant les activités des cyberadversaires mondiaux est un élément clé d'un service MDR d'une efficacité maximale. Réunies à partir de la télémétrie et organisées par les équipes de renseignements sur les menaces, ces mises à jour révèlent les méthodes d'attaque et présentent des contre-mesures.

Les données de renseignements sur les menaces peuvent être générées par le fournisseur de services MDR ou obtenus auprès d'un ou de plusieurs tiers. Il est important de comprendre les sources des renseignements du fournisseur, comment ils sont recueillis et comment ils sont rendus exploitables au sein du service.

Pour découvrir les menaces latentes dans votre environnement, il est essentiel de mettre à la disposition des analystes de la sécurité des renseignements actualisés et régulièrement mis à jour sur les menaces (thème n° 6).

À propos d'ESET Managed Detection and Response

Les services MDR d'ESET reposent sur une base solide : une protection ESET des endpoints primée ; Extended Detection and Response d'ESET, qui fournit des outils aux analystes de sécurité ; et des experts en sécurité humains qui gèrent les consoles. Ils travaillent au sein d'un réseau mondial de centres d'opérations pour surveiller et répondre aux menaces ; recueillir et organiser les renseignements sur les menaces ; et suivre avec vigilance les cyberadversaires internationaux et leurs tactiques, techniques et procédures.

Le service est disponible en deux niveaux, l'un conçu pour offrir une protection sophistiquée aux petites et moyennes entreprises et l'autre constituant efficacement un centre d'opérations de sécurité (SOC) de niveau entreprise. Les deux niveaux comprennent les éléments clés d'un service MDR, y compris la recherche proactive de menaces et la surveillance opérationnelle, l'endiguement et l'éradication des menaces. Le niveau supérieur offre un accès plus étendu aux services personnalisés ou spécialisés des cyberexperts d'ESET.

ESET MDR propose :

- Une chasse, surveillance et réponse aux menaces pour les clients de toute taille et de tout niveau de maturité en matière de sécurité
- Un service disponible 24h/24 et 7j/7. Une alliance entre l'automatisation pilotée par l'IA et l'expertise humaine
- Une bibliothèque pré-construite de modèles de détection de comportement, davantage personnalisée et adaptée à l'environnement du client
- Une équipe Global Threat Intelligence qui suit les incidents critiques actuels et prend des mesures coordonnées pour contrer les menaces

6. QUELS TYPES DE CHASSE AUX MENACES SONT PROPOSÉS ?

L'objectif de l'adversaire est d'établir une présence inconnue sur le réseau en utilisant des tactiques, des techniques et des procédures qui échappent aux mécanismes de détection existants. La recherche de ces menaces évasives et cachées relève de la chasse aux menaces proactive.

La prise en compte de la chasse aux menaces et l'étendue des services constituent l'un des principaux facteurs de différenciation parmi les services MDR. Vérifiez que la chasse aux menaces permanente et systématique fait bien partie de l'offre - elle doit être considérée comme une exigence fondamentale d'un service MDR.

Certains fournisseurs proposent spécifiquement une chasse aux menaces personnalisée, planifiée ou régulière, qui se concentre sur les tendances actuelles en matière de menaces, ou une chasse aux menaces historiques fondée sur des hypothèses, qui s'appuie sur des données relatives à des détections et à des méthodes d'attaque antérieures.

7. QUI S'OCCUPE DE L'ATTÉNUATION ET DE LA REMÉDIATION ?

Parmi les fournisseurs MDR, il n'y a pas de vision partagée quant à qui — le fournisseur de services ou l'acheteur — est responsable de la partie « réponse » du service MDR. Si la détection des systèmes compromis et des attaques actives est un élément commun aux services MDR, les approches varient en ce qui concerne l'atténuation de la menace (endiguement pour prévenir d'autres dommages) et la remédiation (restauration des données et du fonctionnement du système).

Certains fournisseurs ne prendront des mesures correctives que si elles peuvent être automatisées — sinon, ils ne proposent que d'aider l'équipe informatique du client. D'autres offrent quant à eux une réponse dans le cadre d'un service de niveau supérieur, contrat d'engagement ou moyennant un prix supplémentaire.

Les clients diffèrent également quant à leur degré de tolérance à l'égard des changements apportés par des tiers. Vous pourriez être réticent à l'idée d'autoriser le service MDR à remédier à vos systèmes parce qu'ils manquent d'une connaissance approfondie de l'impact potentiel

sur les processus métier. Vous préférerez peut-être une approche qui repose sur le service MDR pour contenir la menace et la supprimer et laisser votre équipe informatique se charger de la restauration complète.

8. COMMENT L'APPROCHE DU FOURNISSEUR S'ALIGNE SUR VOTRE ENTREPRISE ?

Lorsque des incidents se produisent, l'impact du service MDR dépasse le cadre de la sécurité et touche d'autres parties de votre entreprise. Étudiez l'approche du fournisseur en matière de contrôle et réfléchissez à la manière dont les mesures prises s'aligneront sur les exigences de votre entreprise.

Sur le plan opérationnel, déterminez comment et si ses activités et ses résultats peuvent ou doivent être intégrés à vos systèmes de gestion des tickets et à vos flux de travail internes.

Le fournisseur doit également être en mesure de vous fournir ou de vous permettre de générer des rapports sur les incidents en attente et résolus, l'état de votre environnement et tout autre détail qu'il traite en votre nom.

9. SI VOUS AVEZ DES EXIGENCES RÉGLEMENTAIRES OU DE CONFORMITÉ PARTICULIÈRES, LE SERVICE PEUT-IL LES SATISFAIRE ?

Si vous avez des exigences en matière de confidentialité, de résidence ou de conservation des données, vérifiez que le fournisseur MDR est en mesure de les respecter. Il peut être nécessaire d'ajuster ou de faire des exceptions spéciales à ses processus standard pour se conformer à vos lois locales.

Si vous recherchez ou avez une couverture d'assurance cybersécurité, comparez les éléments du service du fournisseur avec les exigences en matière d'assurance. Les cybercontrôles supplémentaires qui font partie du service MDR peuvent vous permettre de bénéficier d'une couverture ou de réduire votre prime.

CONCLUSION

MDR est une catégorie de marché en pleine expansion. Selon Gartner, plus de 600 fournisseurs offrent des services MDR (ou des services qu'ils appellent MDR) ; 30 % des entreprises utilisent activement un service MDR, et ce nombre doublera d'ici 2025.

De manière générale, les fournisseurs MDR qui se sont mobilisés pour répondre à la demande croissante se répartissent en deux catégories : (1) les entreprises qui fournissent des services informatiques gérés sur une base externalisée et ont ajouté MDR à leurs offres et (2) les entreprises de logiciels de sécurité qui ont ajouté une composante de services. Au-delà de cette large catégorisation, il existe des modèles très différents sur la façon dont un service MDR devrait être conçu et mis en œuvre. Il est important de comprendre ces différences.

Le recours à un service MDR doit être étudié et pris plus qu'au sérieux et vous faites le bon choix en vous renseignant sur la nécessité de mettre en place un service MDR. Nous espérons que ce guide vous sera utile pour trouver la bonne solution pour votre entreprise.

Nous sommes ESET

Une défense proactive. Notre activité consiste à minimiser la surface d'attaque.

Gardez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre approche **axée sur la prévention, alimentée par l'IA et l'expertise humaine.**

Profitez d'une protection de premier ordre grâce à nos renseignements sur les **cybermenaces**, accumulés et analysés depuis plus de 30 ans. Notre réseau étendu de recherche et développement, dirigé par des **experts reconnus**, assure la sécurité de votre entreprise pour qu'elle puisse exploiter pleinement le potentiel de la technologie.

EN SAVOIR PLUS

ESET®
Digital Security
Progress. Protected.