SOPHOS
Cybersecurity delivered.

Cinq raisons d'utiliser des services MDR

Un livre blanc Sophos. Septembre 2022

Introduction

Alors que les cybermenaces augmentent en volume, en complexité et en impact, les entreprises se tournent de plus en plus vers les services de détection et de réponse gérés (MDR) pour détecter et neutraliser les attaques avancées que les solutions technologiques seules ne peuvent empêcher. De fait, Gartner prévoit que 50 % des entreprises utiliseront des services MDR pour la surveillance, la détection et la réponse aux menaces d'ici 2025[1].

Toutefois, avec la profusion de solutions de cybersécurité sur le marché, il peut être difficile de comprendre ce qu'est exactement un service MDR, la façon dont il s'intègre dans votre écosystème de cybersécurité et les avantages de son utilisation. Ce guide répond à ces questions et offre des conseils pratiques sur les éléments à prendre en compte au moment de choisir un service MDR.

Sophos MDR

Sophos MDR est le service MDR le plus réputé au monde, sécurisant plus de 11 000[2] entreprises contre les menaces les plus avancées, notamment les ransomwares. Avec la meilleure note sur Gartner Peer Insights™[3] et la reconnaissance comme meilleur éditeur dans le G2 Grid® for Managed Detection and Response (MDR) 2022[4], vos cyberdéfenses sont entre de bonnes mains avec Sophos MDR.

Définition du MDR

Pour comprendre les avantages du MDR et ce qui se cache derrière la demande croissante de tels services, il est important de comprendre ce qu'est le MDR — et ce qu'il n'est pas.

La détection et la réponse gérées (MDR) est un service entièrement managé, disponible 24 h/24 et 7 j/7, assuré par des experts spécialisés dans la détection et la réponse aux cyberattaques que les solutions technologiques seules ne peuvent empêcher.

Il ne faut pas confondre MDR avec EDR (Endpoint Detection and Response) ou XDR (Extended Detection and Response). Les technologies MDR, EDR et XDR prennent toutes en charge et mettent en œuvre la chasse aux menaces. Les fonctionnalités EDR et XDR sont des outils qui permettent aux analystes internes de rechercher et d'analyser les compromissions potentielles, tandis qu'avec le MDR, ce sont les analystes du fournisseur de sécurité qui recherchent, investiguent et neutralisent les menaces au nom du client.

Comme leur nom l'indique, les outils EDR utilisent les points de données provenant des technologies de protection Endpoint, tandis que les outils XDR étendent les sources de données à toute l'infrastructure informatique (dont le pare-feu, la messagerie, le Cloud et les solutions de sécurité mobile) afin d'offrir une meilleure visibilité et un meilleur contexte. Chez Sophos, nous exploitons nos solutions EDR et XDR de pointe pour fournir notre service MDR.

Ce qui n'entre pas dans le champ du MDR, ce sont les actions de gestion quotidienne de la cybersécurité, telles que le déploiement de vos technologies de sécurité, la mise à jour des politiques, l'application de correctifs ou l'installation de mises à jour. Les fournisseurs de services managés (MSP) offrent des services de gestion de la sécurité informatique aux entreprises qui recherchent un soutien dans ce domaine.

Qui utilise des services MDR ?

Toute entreprise, dans tout secteur, peut utiliser des services MDR, qu'il s'agisse d'une petite entreprise aux ressources informatiques limitées ou d'une grande entreprise disposant d'un SOC interne. La question est en réalité : comment les entreprises travaillent-elles avec les services MDR ? Il existe trois principaux modèles de réponse MDR :

- L'équipe MDR gère entièrement la réponse aux menaces pour le compte du client.
- L'équipe MDR travaille avec l'équipe interne, en co-gérant la réponse aux menaces.
- L'équipe MDR alerte l'équipe interne et fournit des conseils de remédiation.

Chez Sophos, nous prenons en charge ces trois approches, en nous adaptant aux besoins individuels des clients.

1 Rapport Gartner « Market Guide for MDR 2021 »
2 En août 2022.
3 Avis des 12 derniers mois au 1er août 2022. Le contenu de Gartner Peer Insights est constitué d'avis d'utilisateurs individuels basés sur leurs propres expériences avec les éditeurs répertoriés sur la plateforme. Ces avis ne doivent pas être interprétés comme des déclarations de faits et ne représentent pas les opinions de Gartner ou de ses affiliés. Gartner ne cautionne aucun fournisseur, produit ou service décrit dans ce contenu et n'offre aucune garantie, explicite ou implicite, quant à l'exactitude ou l'exhaustivité de ce contenu, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.
4 Sophos est reconnu comme Top Vendor dans le G2 Grid® for MDR Services 2022 servant le midmarket.

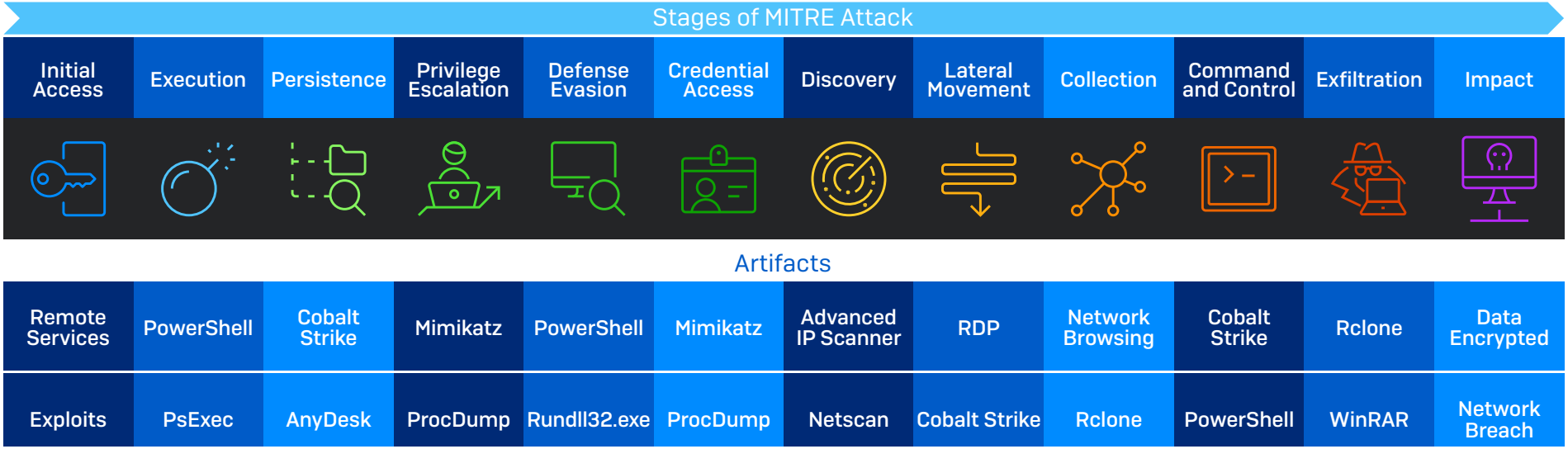
La nécessité de la détection et réponse aux menaces pilotée par des experts

Nous constatons aujourd'hui que les solutions technologiques ne peuvent à elles seules prévenir toutes les cyberattaques. Pour éviter d'être détectés par les solutions de cybersécurité, les acteurs malveillants utilisent de plus en plus d'outils informatiques légitimes ainsi que des identifiants et autorisations d'accès volés, sans oublier l'exploitation, dans leurs attaques, de vulnérabilités non corrigées. En imitant des utilisateurs autorisés et en profitant des failles des défenses des entreprises, les acteurs malveillants parviennent à éviter de déclencher les technologies de détection automatique.

L'image ci-dessous détaille les principaux artefacts (outils) utilisés par les attaquants à chaque étape de la chaîne ATT&CK de MITRE, tels qu'observés par les chasseurs de menaces de Sophos en 2021. Comme vous pouvez le constater, les outils usuellement utilisés par les équipes informatiques, tels que PowerShell, PsExec ou RDP, sont fréquemment exploités par les adversaires. Les technologies automatisées peinent à discriminer entre une personne légitime utilisant ces outils dans le cadre de ses fonctions et un attaquant les exploitant à l'aide d'identifiants volés.

Pour bloquer ces attaques avancées, il faut une combinaison de technologies et d'expertise humaine. Chaque fois qu'un attaquant entreprend une action, il crée un signal. En combinant l'expertise humaine avec de puissantes technologies de protection et des modèles avancés de Machine Learning alimentés par l'IA, les analystes de sécurité peuvent détecter, investiguer et neutraliser les attaques humaines, mêmes les plus sophistiquées.

Alors que la chasse, l'investigation et la réponse aux menaces peuvent être effectuées en interne à l'aide d'outils EDR et XDR, l'utilisation d'un service MDR, aux côtés de votre équipe interne ou en tant que service entièrement externalisé, présente de nombreux avantages.



Principaux artefacts utilisés à chaque étape de la chaîne d'attaque de Mitre. Active Adversary Playbook 2022, Sophos

Les technologies de protection continuent de jouer un rôle essentiel dans les défenses d'aujourd'hui

Si les services managés de détection et de réponse sont un élément essentiel des cyberdéfenses, il reste indispensable de disposer de technologies de protection de haute qualité. Les technologies de sécurité Endpoint, réseau, messagerie et Cloud continuent de jouer un rôle essentiel dans les défenses d'aujourd'hui. L'utilisation de solutions de pointe augmente l'efficacité et l'impact d'un service MDR :

- Les technologies de protection automatisée permettent aux défenseurs de faire face au volume toujours croissant d'attaques face aux adversaires capables d'exploiter l'automatisation, l'IA et les malwares-as-a-service pour faire proliférer leurs menaces. Sophos Endpoint Protection bloque automatiquement 99,98 % des menaces avant qu'elles ne puissent avoir un impact sur l'entreprise.
- L'un des plus grands défis pratiques auxquels sont confrontés les chasseurs de menaces est le bruit de fond : avec un volume élevé de signaux, il peut être difficile de distinguer la forêt qui se cache derrière l'arbre. Les technologies de prévention supérieures réduisent le nombre d'alertes que les analystes doivent examiner. En permettant aux chasseurs de menaces de se concentrer sur des détections moins nombreuses et plus précises, les technologies de prévention de haut niveau accélèrent la réponse humaine aux menaces.
- Les analystes utilisent les détections et les signaux des technologies de prévention pour identifier et investiguer les activités suspectes. Plus la qualité des détections et la richesse des informations contextuelles sont élevées, plus l'investigation et la réponse sont rapides et efficaces.

En gardant cela à l'esprit, examinons maintenant les cinq principaux avantages des services MDR selon les entreprises qui y font appel.

1. Renforcez vos cyberdéfenses

L'un des principaux avantages du recours à un fournisseur de services MDR par rapport aux programmes internes d'opérations de sécurité est la protection accrue contre les ransomwares et autres cybermenaces avancées.

Avec un service MDR, vous bénéficiez de l'étendue et de la richesse de l'expérience des analystes du fournisseur. Un fournisseur MDR sera amené à gérer un volume et une variété d'attaques bien plus importants que n'importe quelle entreprise isolée, lui conférant ainsi un niveau d'expertise qu'il est presque impossible de reproduire en interne.

Les équipes MDR investiguent et répondent également aux incidents tous les jours, ce qui leur permet de mieux maîtriser les outils de chasse aux menaces. Elles peuvent ainsi répondre plus rapidement et plus précisément à toutes les étapes du processus, de l'identification des signaux importants à l'investigation des incidents potentiels et à la neutralisation des activités malveillantes.

Travailler au sein d'une grande équipe permet également aux analystes de partager leurs connaissances et leurs idées, ce qui accélère encore la réponse. L'équipe Sophos MDR compile des « runbooks » sur chaque menace ou acteur unique qu'elle rencontre. Lorsqu'un adversaire est identifié au cours d'une investigation, plutôt que de devoir effectuer des recherches approfondies au moment même de l'attaque, notre équipe peut se référer au runbook et passer directement à l'action.

Les runbooks sont continuellement mis à jour et les analystes enregistrent les informations importantes à chaque engagement, telles que :

- Les TTP (tactiques, techniques et procédures) communes ou spécifiques à une attaque particulière ou à un ou plusieurs acteurs de la menace.
- Les IOC (indicateurs de compromission) pertinents.
- Les preuves de concept (POC) connues pour les exploits liés aux vulnérabilités ouvertes.
- Des requêtes utiles pour la chasse aux menaces dans le cas d'une attaque ou d'un acteur malveillant particulier.

Un autre avantage des services MDR est qu'ils peuvent appliquer les données de renseignement obtenues auprès d'un client à d'autres clients dont le profil est similaire, leur permettant ainsi de prévenir de manière proactive des attaques similaires dans ce groupe sectoriel. Voici quelques exemples de scénarios dans lesquels l'équipe Sophos MDR réalise des investigations de manière proactive sur les parcs informatiques des clients :

- Un client dans un secteur vertical spécifique a été ciblé d'une manière particulière.
- Sophos X-Ops fournit des données de renseignements sur une attaque importante ciblant un certain profil d'industrie ou d'entreprise.
- Un événement important s'est produit dans le paysage de la sécurité et nous voulons vérifier si des clients sont affectés.

Si nos analystes détectent des signaux suspects, ils sont en mesure d'investiguer rapidement et de remédier à la situation, créant ainsi une immunité communautaire pour le groupe ciblé.

L'étendue et la richesse de l'expérience ainsi que la capacité à appliquer les connaissances acquises dans les environnements de nos clients permettent à l'équipe Sophos MDR d'élever les défenses des entreprises au-delà de ce qu'elles pourraient réaliser seules.

« Les retours mesurables de Sophos MDR incluent une réduction de 90 % du temps de détection des menaces à haut risque qui nécessitent une investigation, une réduction de 95 % du temps d'identification de la source de l'attaque et du type de menaces, et une amélioration de la précision des détections. »

Chitale Dairy, Inde

« Les pen-testeurs ont été choqués de ne pas pouvoir trouver un moyen d'entrer. C'est à ce moment-là que nous avons su que nous pouvions absolument faire confiance au service de Sophos. »

Université de South Queensland, Australie

« Avec Sophos MDR, nous avons réduit considérablement notre temps de réponse aux menaces. »

Tata BlueScope Steel, Inde

« Nous sommes informés de toute menace en temps réel. »

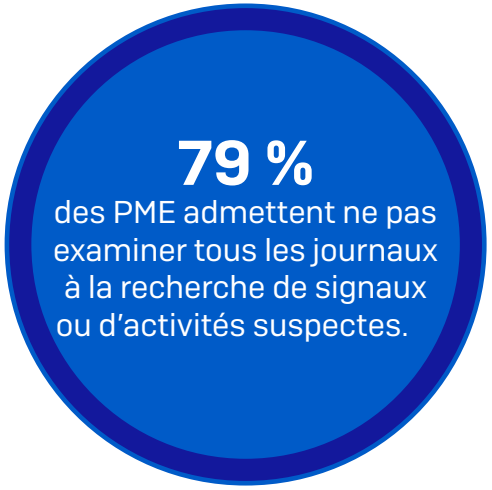
Bardiani Valvole, Italie

2. Libérez vos ressources informatiques

La chasse aux menaces prend du temps et est imprévisible. Pour les professionnels de l'informatique qui jonglent avec de multiples tâches et priorités, il peut être difficile de relever le défi : 79 % des équipes informatiques admettent ne pas examiner tous les journaux à la recherche de signaux ou d'activités suspectes[5].

Compte tenu de l'impact potentiel d'une attaque sur une entreprise, lorsque vous détectez quelque chose de suspect, vous devez souvent tout laisser tomber pour étudier la menace et y remédier immédiatement. La nature urgente du travail peut empêcher les équipes de se concentrer sur des défis plus stratégiques — et souvent plus intéressants.

Travailler avec un service MDR vous permet de libérer vos ressources informatiques pour soutenir des initiatives centrées sur l'activité de l'entreprise. Les entreprises utilisant Sophos MDR signalent systématiquement des gains considérables en matière d'efficacité informatique grâce à l'utilisation de notre service, leur permettant ainsi de mieux accompagner l'entreprise dans la poursuite de ses objectifs.



« Depuis l'implémentation de Sophos, nous avons réussi à libérer des heures opérationnelles importantes qui ont permis à nos équipes de se concentrer sur des initiatives qui ont augmenté la satisfaction de nos étudiants. »
London South Bank University, Royaume-Uni

« La capacité de Sophos MDR à remédier aux menaces ou à les supprimer rapidement et à les porter à notre attention nous libère pour nous concentrer sur des tâches à forte valeur ajoutée. »
Tomago Aluminium, Australie

« Parce que Sophos MDR est là, nous pouvons soutenir et développer d'autres secteurs de l'entreprise comme la gestion des vulnérabilités, les correctifs et la sensibilisation à la sécurité. »
The Fresh Market, États-Unis

« Sophos maîtrise parfaitement les dernières activités et menaces, nous permettant de nous concentrer sur la fourniture de services sécurisés et de qualité à nos clients et nos artistes. »
CD Baby, États-Unis

5 Enquête indépendante menée auprès de 5 600 responsables informatiques, janvier-février 2022. Commandée par Sophos et réalisée par Vanson Bourne.

3. Gardez l'esprit tranquille 24 h/24, 7 j/7

Avec des acteurs malveillants présents dans le monde entier, une attaque peut survenir à tout moment. Les adversaires sont plus actifs aux moments où votre équipe informatique est le moins susceptible d'être en ligne, comme les soirs, les week-ends et les périodes de fêtes. C'est pourquoi il est important que la détection et la réponse aux menaces soient effectuées 24 h/24 ; si vous ne le faites que pendant les heures de bureau, vous laissez votre entreprise exposée.

En proposant une couverture 24 h/24 et 7 j/7, les services MDR offrent une sérénité considérable. Pour les équipes informatiques, une telle tranquillité d'esprit leur permet tout simplement de passer de bien meilleures nuits. Elles peuvent se détendre en sachant que la responsabilité revient au fournisseur du service MDR.

Pour les dirigeants et les clients, une couverture 24 h/24 et 7 j/7 fournie par des experts et un niveau de cyber-préparation élevé et permanent offrent une puissante garantie que les données et l'entreprise seront bien protégées.

« Être soutenus par l'équipe Sophos MDR m'aide à dormir la nuit, car je sais que nous sommes protégés 24 h/24 et 7 j/7. »
Canucks de Vancouver, Canada

« L'équipe Sophos agit comme un gardien de but, se tenant derrière nous avec ses compétences et nous donnant l'assurance qu'il nous protège ».
Inspire Education Group, Royaume-Uni

« Nous avons désormais une confiance accrue dans la fiabilité, la robustesse et la nature complète de notre dispositif de sécurité. »
Aligned Automation, Inde

« L'entreprise est devenue beaucoup plus résiliente grâce à Sophos MDR. »
McKenzie Aged Care Group, Australie

4. Ajoutez de l'expertise, pas des ingénieurs

La chasse aux menaces est une opération très complexe. Les chasseurs de menaces doivent posséder un ensemble de compétences spécifiques et spécialisées, notamment :

- **Créativité et curiosité** : la recherche de menaces peut s'apparenter à la recherche d'une aiguille dans une botte de foin. Les chasseurs de menaces peuvent parfois passer des jours à chercher des menaces, utilisant de nombreuses méthodes pour les dénicher.
- **Expérience en cybersécurité** : la chasse aux menaces est l'une des opérations de cybersécurité les plus avancées. C'est pourquoi une expérience préalable dans le domaine et des connaissances fondamentales sont indispensables.
- **Connaissance du paysage des menaces** : il est indispensable de comprendre les dernières tendances en matière de menaces pour rechercher et neutraliser des entités inconnues.
- **Capacité à se mettre dans la peau des adversaires** : la capacité de penser comme un cybercriminel est essentielle pour lutter contre les approches humaines actuelles.
- **Capacité de rédaction technique** : les chasseurs de menaces sont tenus de consigner leurs découvertes dans le cadre du processus d'investigation. Il est donc essentiel que le chasseur puisse communiquer des informations complexes afin de mener la chasse à son terme.
- **Connaissance du système d'exploitation (OS) et des réseaux** : une connaissance pratique avancée des deux est essentielle.
- **Expérience du codage et de l'écriture de scripts** : cela est nécessaire pour aider les chasseurs de menaces à créer des programmes, à automatiser des tâches, à analyser les journaux (logs) et à effectuer des tâches d'analyse de données pour faciliter et faire progresser leurs investigations.

Cette combinaison rare de compétences associée à une pénurie notable de talents dans le secteur informatique, fait du recrutement d'experts en chasse aux menaces une tâche ardue — voire impossible — pour de nombreuses entreprises.

Les services MDR vous fournissent en réalité cette expertise. Chez Sophos, nous avons des centaines d'analystes experts qui fournissent des services MDR continus aux clients du monde entier. Sophos MDR permet aux clients d'étendre leurs capacités d'opérations de sécurité sans augmenter leurs effectifs.

« Nous bénéficions désormais d'une extension de notre pratique de sécurité existante sans avoir à mettre en place nos propres capacités internes. »
Hammondcare, Australie

« Sophos MDR nous a permis de faire face au volume croissant et à la sophistication des cybermenaces sans avoir à renforcer notre équipe de sécurité. »
Tourism Finance Corporation of India Limited, Inde

« Sophos nous évite d'avoir à recruter jusqu'à cinq nouveaux employés pour assumer cette tâche. »
AG Barr, Royaume-Uni

5. Améliorez votre ROI Cybersécurité

Maintenir une équipe de chasseurs de menaces 24 h/24 et 7 j/7 est coûteux. Pour assurer une couverture 24 h/24, vous avez besoin d'au moins cinq ou six personnes spécialisées dans la cybersécurité travaillant en équipes séparées. En tirant parti des économies d'échelle, les services MDR offrent un moyen rentable de sécuriser votre entreprise et d'optimiser votre budget de cybersécurité.

De plus, en améliorant votre protection, les services MDR réduisent également considérablement le risque d'être victime d'une violation de données coûteuse et évitent les coûts financiers liés à la gestion d'un incident majeur. Sachant que le coût moyen de remédiation d'une attaque de ransomware dans les entreprises de taille moyenne s'élève à 1,4 million de dollars en 2021[6], le fait d'investir dans la prévention est une décision financière judicieuse.

Si vous faites appel à un fournisseur MDR qui propose également des solutions de cybersécurité pour les systèmes endpoint, par exemple, vous pourrez alors profiter d'avantages considérables en termes de coût total de possession (TCO) grâce à un seul et unique éditeur et à la rationalisation de vos efforts en matière de gestion des fournisseurs.

Enfin, en choisissant un fournisseur qui s'intègre à vos technologies de sécurité actuelles, vous pouvez augmenter votre retour sur vos investissements existants. Chez Sophos, nous avons une approche du MDR non centrée sur Sophos qui vous permet d'exploiter vos produits tiers existants pour détecter, investiguer et répondre aux menaces, améliorant ainsi votre ROI. Avec Sophos MDR, vous pouvez utiliser nos outils de classe mondiale, des outils non Sophos, ou une combinaison des deux.

« Sophos propose une couverture et une charge de travail équivalentes à six employés à temps plein pour un coût inférieur à celui d'une seule personne ».
Detmold Group, Australie

« Le regroupement de tous nos produits de sécurité en un seul et même endroit nous a permis de réduire nos coûts et de gagner en efficacité ».
Independent Parliamentary Standards Authority, Royaume-Uni

« Sophos MDR est rentable à plus d'un titre. S'il permet d'éviter un incident majeur par an, il est rentabilisé dix fois, voire plus. »
Hammondcare, Australie

« Nous avons gagné 15 heures par semaine et multiplié notre productivité par un facteur de 2,6. »
Tourism Finance Corporation of India Limited, Inde

6 L'état des ransomwares 2022, Sophos. Enquête indépendante menée auprès de 5 600 professionnels de l'informatique dans 31 pays.

Quels éléments à prendre en considération au moment de choisir un service MDR ?

Les services MDR diffèrent d'un fournisseur à l'autre. Il y a de nombreux éléments à prendre en compte lors de l'évaluation des services, assurez-vous donc d'explorer les quatre domaines ci-dessous.

1. **Niveaux de support et d'interaction offerts**

   Souhaitez-vous qu'un fournisseur MDR gère entièrement votre réponse aux menaces, qu'il la cogère avec votre équipe ou qu'il alerte votre équipe pour qu'elle puisse agir ? Identifiez le niveau de support et d'interaction qui vous intéresse et voyez comment les fournisseurs se positionnent les uns par rapport aux autres.

   Chez Sophos, nous agissons comme une extension de l'équipe informatique de nos clients, quelle que soit la capacité dont ils ont besoin. Qu'il s'agisse d'un support entièrement géré 24 h/24 et 7 j/7 ou du soutien d'une équipe interne, nous nous adaptons à votre situation.

2. **Ampleur et richesse de l'expérience acquise dans la lutte contre les menaces**

   Avoir une expérience vaste et approfondie de la réponse aux cybermenaces permet de mieux se défendre. Ayez une bonne compréhension du niveau d'expérience des analystes MDR du fournisseur et la manière dont ils appliquent leur savoir collectif aux parcs informatiques de leurs clients.

   Explorez également la profondeur de l'expertise en matière de sécurité de l'équipe MDR du fournisseur et la qualité des informations contextuelles fournies pour aider les analystes à prioriser et à investiguer les alertes.

   Sophos MDR sécurise plus de 11 000 entreprises dans le monde, travaillant dans des secteurs tels que la santé, l'éducation, la production, la distribution, la technologie, la finance, l'administration publique, les services, et bien d'autres encore. L'ampleur et la richesse de cette expérience nous permettent d'offrir une protection inégalée à nos clients.

   Derrière Sophos MDR se trouve l'équipe Sophos X-Ops. Avec plus de 30 ans d'expertise sur les malwares et des capacités d'IA de pointe, Sophos X-Ops fournit des informations et des analyses approfondies pour aider les agents MDR à identifier et à neutraliser rapidement les attaques.

3. **Expérience client au quotidien**

   Un fournisseur de services MDR efficace devient une extension de votre propre équipe. Assurez-vous que c'est un fournisseur avec lequel vous voulez travailler une fois le contrat signé. Parlez à leurs clients actuels pour comprendre leurs expériences et consultez les sites d'évaluation indépendants pour connaître les avis des clients.

   Sophos MDR est le fournisseur de services MDR le plus évalué et le mieux noté sur Gartner Peer Insights au 1er août 2022, avec une note moyenne de 4,8/5*. Lisez les témoignages de clients indépendants ici.

4. **Variété et richesse de la télémétrie**

   Les adversaires ne suivent pas un chemin technologique unique et la chasse aux menaces de votre fournisseur MDR ne doit pas non plus suivre un tel chemin. Plus la visibilité est grande sur votre environnement, mieux les analystes peuvent détecter les activités malveillantes et y répondre. Interrogez les fournisseurs sur leurs intégrations de sécurité et sur l'étendue de leur capacité à intégrer des signaux provenant de l'ensemble de votre environnement informatique.

   Sophos MDR offre des intégrations pour l'ensemble de l'environnement informatique, y compris des intégrations natives et tierces avec les technologies Endpoint, réseau, Cloud, messagerie et Microsoft 365. Notre approche agnostique (qui intègre des produits tiers) permet à nos analystes d'avoir une visibilité étendue sur l'ensemble de l'environnement du client, ce qui permet d'améliorer la détection, l'investigation et la réponse aux menaces.

Résumé

Alors que les cybermenaces continuent d'évoluer, les services MDR deviennent rapidement une protection indispensable pour les entreprises de toutes tailles. Travailler avec un fournisseur de services MDR fiable et éprouvé offre de multiples avantages, que vous souhaitiez externaliser entièrement votre chasse aux menaces ou compléter et améliorer vos services internes :

1. Renforcez vos cyberdéfenses.
2. Libérez vos ressources informatiques.
3. Gardez l'esprit tranquille 24 h/24, 7 j/7.
4. Ajoutez de l'expertise, pas des ingénieurs.
5. Améliorez votre ROI Cybersécurité.

Pour plus d'informations sur Sophos MDR, contactez votre partenaire Sophos ou consultez la page www.sophos.fr/mdr

www.sophos.fr/mdr

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2022-09-16 FR-WP (DD)

SOPHOS