SOPHOS

Guide d'achat de services MDR (Managed Detection and Response)

Peu d'entreprises disposent des ressources internes nécessaires pour gérer efficacement leurs programmes de sécurité tout en se défendant de manière proactive contre les menaces nouvelles et émergentes. Par conséquent, les entreprises recherchent des services MDR (Managed Detection and Response) pour mettre en œuvre leurs programmes opérationnels de sécurité.

Selon Gartner[1], 50 % des entreprises auront recours à des services MDR d'ici 2025 (contre moins de 5 % en 2019).

Toutefois, le marché des services de sécurité est relativement nouveau, et il est difficile d'y voir clair parmi toutes les offres sur le marché. Il est de plus en plus difficile de faire les bons choix pour votre organisation. Ce guide vous apporte un éclairage sur les éléments à prendre en considération au moment de choisir un service MDR. Il vous permet également de voir comment les fournisseurs de services MDR se positionnent les uns par rapport aux autres pour vous aider à prendre une décision éclairée.

Les opérations de sécurité nécessitent des professionnels qualifiés

L'industrie de la cybersécurité connaît une importante pénurie de compétences et de personnel expérimenté. Les organisations peinent ainsi à mettre en place des programmes efficaces pour les opérations de sécurité (SecOps) afin de détecter, d'analyser et de répondre aux menaces avant que des dommages ne se produisent.

Si des outils tels que l'EDR (Endpoint Detection and Response) sont conçus pour détecter les menaces et répondre aux incidents, il faut néanmoins l'expertise d'opérateurs qualifiés pour tirer pleinement profit de toutes leurs capacités. Dans une enquête menée en 2019 auprès de 2 300 responsables IT et professionnels de la cybersécurité[2], 54 % des répondants ont déclaré « ne pas être en mesure d'exploiter pleinement leur solution » à cause d'un manque de compétences.

Ce problème est tellement répandu que selon le cabinet d'analystes ESG[3], « pour 34 % des entreprises, leur plus grand défi est le manque de personnel qualifié pour analyser les incidents de cybersécurité impliquant un système d'extrémité afin de déterminer la cause profonde et la chaîne d'attaque ».

Face à l'augmentation du volume et de la sophistication des cybermenaces, comment les organisations peuvent-elles se maintenir à niveau sans renforcer massivement leur équipe en charge des opérations de sécurité ? Pour répondre à ce problème, une solution alternative est née : les services de sécurité managés. Plus précisément, les services managés de détection et de réponse (MDR).

Définition des services MDR (Managed Detection and Response)

Les services MDR correspondent à des opérations de sécurité externalisées, assurées par une équipe de spécialistes. Ils agissent comme une extension de l'équipe de sécurité du client, en combinant des opérations réalisées par des experts (investigations, traque des menaces, surveillance en temps réel et réponse aux incidents) avec un ensemble de technologies pour recueillir et analyser les données d'intelligence.

Pour identifier et neutraliser rapidement les menaces, les fournisseurs de services MDR associent souvent une combinaison de technologies de couche hôte-réseau avec des analyses avancées, l'intelligence sur les menaces, des données d'investigation et une expertise humaine. L'objectif des services MDR est de détecter et de répondre aux menaces qui ont réussi à contourner les contrôles de sécurité préventifs dans les environnements des clients. Ces contrôles préventifs, tels que les pare-feu, les antivirus et le filtrage de contenu, sont efficaces pour stopper les menaces basiques connues, mais peuvent être inefficaces face aux nouvelles cyberattaques sophistiquées. Les fournisseurs de services MDR se sont développés pour pallier les carences en matière de détection et de réponse aux menaces de ces outils.

Pourquoi les organisations font appel à un service MDR

Voici quelques-uns des principaux facteurs qui incitent les organisations à recourir à un service MDR :

- **Capacités d'opérations de sécurité limitées en interne :** De nombreuses organisations ont du mal à aller au-delà d'une stratégie de sécurité axée sur la prévention et n'ont pas la capacité de mener et de maintenir leur propre programme opérationnel de cybersécurité.
- **Difficultés à tirer le meilleur parti des outils EDR :** Certaines organisations ont acheté une solution EDR, soit comme technologie réactive en cas d'incident, soit dans l'espoir de l'utiliser pour traquer les menaces et répondre aux incidents de manière proactive. Cependant, elles ne sont pas en mesure de développer pleinement leur propre programme opérationnel de cybersécurité et doivent faire appel à des experts externes.
- **Renforcement de l'équipe de cybersécurité interne :** Même les organisations qui disposent d'une équipe d'analystes de sécurité compétents ne couvrent pas toutes les plages horaires (c'est-à-dire la nuit, le week-end ou les jours fériés) et manquent de personnel spécialisé (analystes de malwares, spécialistes de la réponse aux incidents, etc.). De même, certaines équipes de sécurité s'appuient sur l'aide d'un SOC (Security Operations Center) externalisé pour pouvoir se concentrer sur les tâches informatiques et de sécurité plus générales qu'elles ont du mal à assurer.
- **Garantie de ne rien laisser passer de côté :** Même les SOC les plus expérimentés souhaitent souvent qu'une deuxième paire d'yeux surveille leur environnement pour s'assurer que rien ne leur échappe.

Bénéfices des services MDR

Équipe d'experts disponible 24/7/365

Les services MDR doivent également posséder l'expertise nécessaire pour détecter et répondre à tout type d'attaque. Les équipes MDR doivent non seulement recruter, former et maintenir en poste des professionnels difficiles à trouver, mais elles doivent également offrir une couverture continue. Cela signifie qu'elles surveillent en permanence votre environnement et peuvent répondre à toute menace à tout moment. Même la nuit, les week-ends et les jours fériés. C'est comme avoir une grande équipe d'opérations de sécurité qui ne prend jamais de vacances, de congés maladie et qui ne dort jamais.

Les services sont des facilitateurs

La plupart des organisations ont du mal à traquer eux-mêmes les menaces, à répondre aux incidents et à contrôler la sécurité. En externalisant les opérations de détection et de réponse, les membres de l'équipe interne peuvent se concentrer sur les tâches qui correspondent à leurs compétences. Pour les organisations plus avancées, l'ajout de services MDR permet également aux équipes de donner la priorité aux tâches critiques tout en se déchargeant d'une grande partie des tâches quotidiennes liées aux opérations de sécurité.

Solution économique

Les organisations qui cherchent à mettre en place leur propre programme opérationnel de sécurité se rendront rapidement compte de la difficulté et du coût induit par la consolidation d'un véritable SOC en interne. Même une organisation de taille moyenne aurait besoin d'au moins quatre analystes de cybersécurité pour maintenir une couverture 24 h/24, 7 j/7 et 365 j/an. Et les organisations plus larges auraient besoin d'embaucher plusieurs autres membres hautement qualifiés. Les organisations doivent également tenir compte du coût affecté aux ingénieurs requis pour personnaliser et maintenir les outils de l'équipe. Et il ne s'agit encore que de la rémunération des membres de l'équipe. Le budget devrait aussi prévoir le coût des outils dont l'équipe se sert, tels que la protection Endpoint, la protection Réseau, l'EDR, un SIEM, le traitement des flux de travail (SOAR), les flux de données d'intelligence, et bien plus encore.

Tranquillité d'esprit

Avec un service MDR adéquat, vous et votre organisation pouvez dormir sur vos deux oreilles en sachant qu'une équipe d'experts qualifiés surveille constamment votre organisation, traque les menaces, analyse les activités suspectes et répond aux incidents potentiels. Avec le panorama des menaces de cybersécurité qui ne cesse de s'étendre, vous pouvez travailler en toute tranquillité avec une équipe dont l'unique objectif est la cybersécurité.

Évaluation des fournisseurs de services MDR : les principales questions à poser

Critères généraux

Combien de clients le service MDR possède-t-il ?

Un élément qui différencie les fournisseurs de services MDR est l'expérience qu'ils ont acquise en matière de détection et de réponse aux incidents. Le nombre actuel de clients vous indiquera combien d'entreprises font véritablement confiance à ce fournisseur et quelle est sa réelle efficacité dans la réponse aux activités suspectes. Par ailleurs, assurez-vous que ce fournisseur a déjà collaboré avec des organisations au profil similaire au vôtre (taille, verticale, défis de sécurité).

Quel est le périmètre d'action du service ? La réponse aux menaces est-elle incluse ?

Tous les services MDR ne sont pas conçus de la même manière. Une exigence de plus en plus importante des clients (et que très peu de fournisseurs offrent aujourd'hui) est la capacité de prendre des mesures ciblées pour neutraliser les menaces au nom du client au lieu de simplement l'avertir de menaces potentielles ou imminentes. Malgré le « R » dans MDR, la majorité des fournisseurs se concentrent sur l'identification de la menace et la notification des clients, laissant à ces derniers la mise en œuvre de la réponse et de la remédiation. Pour que les services MDR soient efficaces, les analystes doivent mener des investigations méthodiques pour déterminer la validité et la portée des menaces, réduire les faux positifs, neutraliser les menaces confirmées, déterminer le contexte de l'attaque et fournir des recommandations supplémentaires pour améliorer la posture de sécurité globale de l'organisation.

Le service est-il disponible 24/7/365 ? Si un problème survient à 2 h du matin un dimanche, qui répondra ?

Assurez-vous que le service MDR surveille réellement votre environnement et soit capable de répondre à tout moment, de jour comme de nuit.

Quelles technologies le service utilise-t-il ? Sont-elles incluses dans le prix ?

Au moment d'évaluer un service MDR, il est important de savoir si les technologies utilisées par les opérateurs sont incluses dans le prix du service. Dans certains cas, vous devrez acheter séparément vos propres outils (tels que la protection Endpoint et l'EDR). D'autres offriront l'ensemble de technologies en plus des composants du service.

Le service est-il mis à disposition de manière proactive ou réactive ?

Les services MDR sont intrinsèquement proactifs. Contrairement aux services d'investigation numérique (Digital Forensics - DF) et de réponse aux incidents (Incident Response - IR) qui sont généralement proposés pour aider les clients à faire face à une crise déjà survenue (comme un incident ou une faille de sécurité), le MDR offre un service proactif, 24 h/24, qui surveille les environnements des clients pour détecter toute activité frauduleuse et, à mesure que les menaces apparaissent, guide, assiste ou neutralise les menaces en temps réel.

Comment allez-vous interagir avec l'équipe MDR ?

Il est important de comprendre le processus de communication avec votre prestataire de services. Existe-t-il une assistance téléphonique directe ? Pouvez-vous communiquer par email ? Pouvez-vous parler directement avec les analystes du SOC, ou bien devez-vous passer par un intermédiaire (par ex. un gestionnaire de compte) ? Dans certains cas, il peut y avoir une différence notable entre les fournisseurs de services MDR, entre ceux offrant une communication directe avec une personne contre ceux communiquant via un portail en ligne. Quel que soit le mode de communication, les fournisseurs de services MDR doivent toujours fournir une synthèse des activités afin de s'assurer que votre équipe sait quelles menaces ont été détectées et quels suivis doivent être effectués.

Méthodologie et critères d'efficacité

Quelle est la méthodologie des opérations de sécurité TDR (Threat Detection and Response) ?

Les fournisseurs de services MDR doivent avoir une méthodologie TDR bien définie. Si ce n'est pas le cas, ils auront probablement du mal à évoluer au fur et à mesure que leurs activités se développeront et seront plus susceptibles de passer à côté d'importants indicateurs censés révéler la présence d'activités suspectes.

Quelle est la rapidité du service ?

En matière de sécurité, chaque seconde compte. Les fournisseurs devraient être en mesure d'estimer :

- Délais moyens de détection
- Délais moyen de réponse
- Délais moyen de résolution

Quels types de mesures de remédiation les opérateurs MDR peuvent-ils prendre ? Peuvent-ils répondre activement pour vous ?

Les fournisseurs de services MDR doivent pouvoir expliquer ce qui se passe lorsque le service détecte une activité suspecte. Comme nous l'avons déjà indiqué, beaucoup d'entre eux se contentent de surveiller et de vous informer lorsqu'une activité suspecte se produit. L'opérateur MDR devrait pouvoir agir en votre nom, en fournissant une réponse proactive réalisée par un humain et non pas seulement un blocage automatisé par un outil.

La traque des menaces est-elle menée à partir d'indices (réponse aux alertes), sans indices de départ (recherche de nouveaux indicateurs d'attaque sans alertes), ou les deux ?

Il existe plusieurs sortes de traque des menaces. Bien que la traque des menaces soit par définition une activité humaine, certains vendeurs appellent la génération automatique d'alertes « traque des menaces » (alors que ce n'en est pas). Il est également important de savoir si les opérateurs MDR vont traquer de manière proactive les adversaires qui se cachent dans votre environnement, qu'ils aient détecté ou non un indicateur fort d'activité ou de compromission. Demandez-leur quel type d'activité déclencherait une investigation de la menace.

Quelles sources de données sont utilisées pour améliorer la visibilité ? Le service est-il simplement de type « EDR managé » ?

Alors que les données issues de la protection Endpoint sont essentielles pour un programme opérationnel de sécurité, certains fournisseurs de services MDR n'ont aucune visibilité supplémentaire au-delà des systèmes Endpoint. Ce ne sont pas de véritables fournisseurs MDR et ils s'apparentent davantage à des solutions « EDR managées » qui ont une visibilité limitée des menaces présentes dans votre environnement.

Le fournisseur de services MDR a-t-il accès aux données d'intelligence sur les menaces et aux chercheurs en menaces ?

Les fournisseurs de services MDR doivent avoir un niveau d'expertise qui aille au-delà de ce que la plupart des organisations peuvent construire par elles-mêmes. Cela comprend bien sûr des analystes de sécurité qualifiés. Toutefois, le fournisseur devrait également avoir accès à des données d'intelligence sur les menaces exclusives et collaborer avec des chercheurs en menaces lorsqu'un élément nouveau est détecté.

Comparaison des fournisseurs

Les fournisseurs de services MDR ont tendance à se répartir en trois catégories :

- **Surveillance uniquement :** Les services se concentrent sur la priorisation et la notification des clients lorsqu'une alerte automatique est générée par le produit. Ils ne proposent pas d'options de remédiation autres que des conseils sur ce que le client doit faire. En outre, ils ne font que tirer parti de la traque des menaces « automatisée » et ne procèdent pas à des investigations ou à une traque proactive au nom du client.
- **Réponse limitée ('r' minuscule) :** Les services comprennent des actions de réponse plus légères, mais se limitent à des actions automatisées. La traque des menaces est menée, mais uniquement lorsqu'une alerte déclenche l'investigation.
- **Réponse complète ('R' majuscule)** : Les services comprennent des capacités de réponse complètes. L'équipe MDR agit de manière proactive au nom du client grâce à une réponse manuelle et humaine. La traque des menaces n'est pas seulement menée à partir d'indices, mais l'équipe MDR traque systématiquement les menaces même lorsqu'un indicateur d'attaque n'est pas visible.

Capacités clés	Surveiller uniquement	Réponse limitée ('r' minuscule)	Réponse complète ('R' majuscule)
Surveillance 24/7	✓	✓	✓
Notification et priorisation	✓	✓	✓
Conseils de remédiation	✓	✓	✓
Rapport d'activité	✓	✓	✓
Traque des menaces 'automatisée'	✓	✓	✓
Réponse automatisée		✓	✓
Traque des menaces à partir d'indices		✓	✓
Traque des menaces sans indices de départ			✓
Réponse managée par des experts			✓

Éditeurs représentatifs[4]		
Surveiller uniquement	Réponse limitée ('r' minuscule)	Réponse complète ('R' majuscule)
Carbon Black Managed Detection	Arctic Wolf	Sophos MTR Standard
CrowdStrike Falcon OverWatch	eSentire	Sophos MTR Advanced
Huntress	Expel	CrowdStrike Falcon Complete
Perch	Rapid7	
	Red Canary	
	SentinelOne Vigilance Respond	

Service Sophos Managed Threat Response (MTR)

Sophos MTR (Managed Threat Response) est une offre de services de recherche, de détection et de remédiation des menaces, entièrement gérés par une équipe d'experts, 24 h/24 et 7 j/7. L'équipe Sophos MTR ne se contente pas de vous notifier lorsqu'une attaque ou un comportement suspect sont identifiés, mais elle intervient à votre place pour neutraliser les menaces les plus sophistiquées et les plus complexes à l'aide d'actions ciblées.

L'équipe Sophos MTR, composée d'experts de haut niveau spécialisés dans la traque des menaces et leur remédiation, vont :

- Traquer de manière proactive et confirmer les menaces et incidents potentiels
- Utiliser toutes les informations disponibles pour déterminer l'ampleur et la criticité des menaces
- Prendre en compte le contexte professionnel approprié pour valider les menaces
- Lancer des actions pour intercepter, contenir et neutraliser les menaces
- Fournir des conseils pratiques pour remédier aux causes profondes des incidents récurrents

Capacités clés de Sophos MTR

Sophos MTR : Standard

Traque des menaces à partir d'indices 24 h/24 7j/7

Les activités et artefacts malveillants confirmés (signaux forts) sont automatiquement bloqués ou supprimés. Les analystes peuvent ainsi consacrer tous leurs efforts à traquer et à remonter la piste des menaces. Ce type de recherche consiste à agréger et à analyser les facteurs de causalité et les événements connexes (signaux faibles) pour découvrir de nouveaux indicateurs d'attaque (IoA) et indicateurs de compromission (IoC) qui n'étaient pas détectés auparavant.

Diagnostic de sécurité

Maintenez vos produits Sophos Central, en commençant par Intercept X Advanced avec EDR, à un niveau de performances optimales par un examen proactif de vos conditions d'exploitation et par des recommandations pour améliorer vos configurations.

Rapport d'activité

Les résumés des événements permettent d'établir les priorités et de vous informer, de sorte que votre équipe sait quelles menaces ont été détectées et quelles mesures ont été prises entre chaque rapport.

Détections contradictoires

Une grande partie des attaques réussies ont utilisé un processus semblant légitime pour tromper les outils de surveillance. En utilisant des techniques d'investigation exclusives, notre équipe détermine la différence entre un comportement légitime et les tactiques, techniques et procédures utilisées par les attaquants.

Sophos MTR : Advanced

Traque des menaces sans indices de départ 24h/24 7j/7

En se basant sur la science des données, l'intelligence sur les menaces et l'intuition d'experts chevronnés, nous prenons en compte le profil de votre société, vos ressources de grande valeur et vos utilisateurs les plus à risque pour anticiper le comportement des pirates et identifier de nouveaux indicateurs d'attaque (IOA).

Données télémétriques améliorées

L'investigation des menaces est complétée par des données télémétriques issues des autres produits Sophos Central, qui, en allant au-delà du poste de travail, fournissent une image complète des activités malveillantes.

Amélioration proactive de la posture de sécurité

Des recommandations vous aident à améliorer de manière proactive votre posture de sécurité et à renforcer vos défenses en corrigeant les lacunes de la configuration et de l'architecture, augmentant ainsi vos capacités de sécurité globales.

Interlocuteur dédié en cas d'incident

Lorsqu'un incident est confirmé, vous pouvez contacter un interlocuteur dédié dont la mission est de collaborer directement avec votre personnel sur site (équipe interne ou partenaire externe) jusqu'à ce que la menace active soit neutralisée.

Assistance téléphonique directe

Votre équipe peut appeler directement notre centre d'opérations et de sécurité (SOC). Notre équipe MTR opérationnelle est disponible 24 h/24 et s'appuie sur nos équipes du support technique réparties sur 26 sites dans le monde entier.

Découverte des ressources

De l'information sur les ressources, comprenant les versions du système d'exploitation, les applications et les vulnérabilités, à l'identification des ressources gérées et non gérées, nous fournissons des informations précieuses pour évaluer l'impact d'un incident, traquer les menaces et fournir des conseils pour améliorer de manière proactive la posture globale de sécurité.

Sophos Managed Threat Response (MTR) : Protection, EDR et MDR			
Capacités clés	Sophos Intercept X Advanced with EDR (technologie uniquement)	Sophos MTR Standard (technologie+ service managé)	Sophos MTR Advanced (technologie+ service managé)
Protection Endpoint	✓	✓	✓
EDR (Endpoint Detection and Response) pour les opérations IT	✓	✓	✓
EDR (Endpoint Detection and Response) pour la traque des menaces	✓	✓	✓
Service managé : Surveillance et réponse 24h/24		✓	✓
Service managé : Réponse proactive et manuelle		✓	✓
Service managé : Traque des menaces à partir d'indices		✓	✓
Service managé : Traque avancée des menaces sans indices de départ			✓
Service managé : Interlocuteur dédié			✓

Différentiateurs clés de Sophos MTR

Sophos agit en votre nom : Contrairement à Sophos MTR, d'autres services se contentent de surveiller et de notifier lorsque des activités suspectes sont détectées. L'équipe Sophos MTR intervient. Nous agissons à distance pour intercepter, contenir et neutraliser les menaces même les plus sophistiquées et les plus complexes.

Savoir-faire technique : Avec plus de 2 000 clients, Sophos a tout vu et tout arrêté. Notre équipe de spécialistes analyse en permanence les comportements anormaux et prend les mesures nécessaires contre les menaces.

Traque des menaces robuste Sophos traque les menaces à partir d'indices ou sans indices de départ, pour découvrir de nouveaux indicateurs d'attaque (IoA) et de compromission (IoC) qui n'étaient pas détectables auparavant.

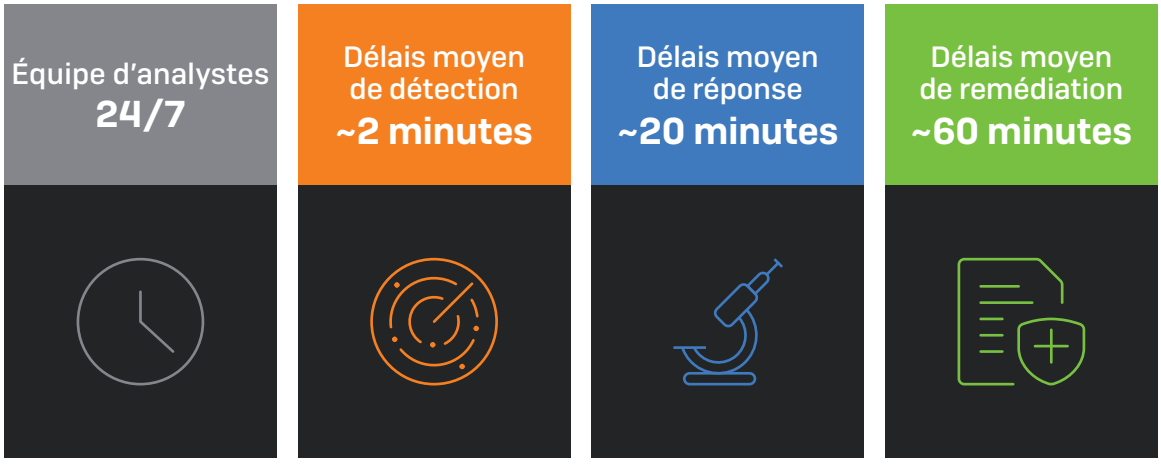
Détection de pointe : Allant au-delà des méthodes traditionnelles de détection, Sophos combine des modèles déterministes et de Machine Learning pour identifier les comportements suspects ainsi que les tactiques, techniques et procédures utilisées par les adversaires les plus avancés.

Réponse humaine ciblée : Le service Sophos MTR inclut Intercept X Advanced with EDR, la meilleure protection Endpoint sur le marché. Cela signifie qu'il arrête automatiquement les menaces que d'autres laissent passer. Comme le service comprend une meilleure prévention proactive, l'équipe peut se concentrer sur la détection, la réponse et la réponse aux incidents les plus complexes.

Transparence et contrôle : Avec Sophos, vous restez le principal décideur et vous contrôlez quand et comment les incidents potentiels doivent être remontés, quelles actions de remédiation (le cas échéant) vous souhaitez que nous lancions et qui doit être inclus dans le processus de communication. Les entreprises peuvent tirer parti de l'un des trois modes de réponse (Notifier, Collaborer ou Autoriser) pour répondre à leurs besoins particuliers.

Outcome-Focused Security™ : Chaque action d'analyse, d'investigation ou de remédiation enrichit le service MTR de données décisionnelles qui optimiseront les configurations et les fonctionnalités de détection automatique.

Statistiques clés de Sophos MTR



Service Sophos Rapid Response

Piloté par une équipe d'experts en réponse aux incidents, le service Sophos Rapid Response identifie et neutralise de manière ultra-rapide les menaces actives ciblant une organisation. Le service Rapid Response est destiné aux organisations qui sont actuellement attaquées. Les clients Sophos MTR n'ont pas besoin du service Rapid Response, car la réponse aux incidents est intégrée dans le service Sophos MTR.

Le service Rapid Response agit immédiatement en cas d'incident actif. La prise en charge (onboarding) s'effectue en quelques heures et la majorité des clients font l'objet d'une priorisation (triage) sous 48 h.

L'équipe Sophos Rapid Response, composée d'experts en réponse aux incidents, d'analystes et de chasseurs de menaces, peut :

- Prendre rapidement des mesures pour trier, contenir et neutraliser les menaces actives
- Expulsion des adversaires de votre parc pour prévenir d'autres dommages
- Surveillance et réponse aux menaces 24h/24 et 7j/7 pour renforcer votre protection
- Recommandation en temps réel de mesures de prévention pour résoudre les causes profondes
- Fournir un compte-rendu post-incident de la menace détaillant notre investigation

Le service Sophos Rapid Response est disponible à la fois pour les clients Sophos actuels, mais aussi pour les clients non-Sophos.

Pour plus d'informations sur le service Sophos Managed Threat Response (MTR), visitez notre site web ou contactez un représentant Sophos.

Si vous préférez traquer vous-même les menaces, Sophos EDR vous donne les outils dont vous avez besoin pour les traquer et maintenir l'hygiène de vos opérations de sécurité. Commencez dès aujourd'hui un essai de 30 jours sans obligation d'achat.

Source :

1 Gartner, Market Guide for Managed Detection and Response Services, 26 August 2020, Analysts: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

2 Enquête 2019 auprès de 3 100 DSIhttps://secure2.sophos.com/fr-fr/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

3 https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

4 Cette comparaison et les informations contenues dans ce présent document sont basées sur l'interprétation de Sophos de données publiques à la date d'écriture du document. Ce document a été préparé par Sophos seul et non pas par les autres éditeurs listés ici. Les fonctionnalités ou caractéristiques des produits comparés, qui pourraient avoir un impact direct sur la précision ou la validité de cette comparaison, sont susceptibles de changer. Les informations contenues dans cette comparaison sont destinées à favoriser la compréhension et la connaissance d'informations factuelles sur divers produits et elles pourraient ne pas être exhaustives. Toute personne utilisant ce document devrait prendre ses propres décisions basées sur ses besoins, et devrait également faire des recherches en se basant sur les sources originales des informations et ne pas se baser uniquement sur cette comparaison pour choisir tout produit.

Pour plus d'informations sur
Sophos Managed Threat Response (MTR)

aller sur sophos.fr/mtr

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

2021-02-25 BG-FR (PC)

SOPHOS