SOPHOS

Managed Threat Response (MTR)

Réponse aux menaces dirigée par des experts

Sophos Managed Threat Response (MTR) 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.

Avantages principaux

- Capacités avancées de recherche, détection et réponse aux menaces offertes sous forme de service managé
- Collaborez avec une équipe d'intervention disponible 24/24 et 7 j/7 qui prend les mesures nécessaires à distance pour contenir et neutraliser les menaces
- Vous décidez et contrôlez quelles actions l'équipe MTR lance et comment les incidents sont gérés
- Symbiose entre technologie de Machine Learning de pointe et équipe d'experts de haut niveau
- Deux niveaux de services (Standard et Advanced) répondent aux besoins des entreprises de tous niveaux de maturité

Les notifications ne sont pas la solution, mais le point de départ

Peu d'entreprises disposent en interne des outils, des personnes et des processus adéquats pour gérer efficacement leur programme de sécurité 24 h/24, tout en assurant une défense proactive contre les menaces nouvelles et émergentes. 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.

Avec Sophos MTR, votre entreprise se dote d'une équipe d'experts en menaces de haut niveau qui va :

- Traquer de manière proactive et valider 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

Réponse humaine accélérée par machine

Développé pour renforcer notre technologie Intercept X Advanced avec EDR, Sophos MTR fusionne Machine Learning et analyse d'expert et améliore la recherche et la détection des menaces, l'investigation approfondie des alertes et les actions ciblées pour éliminer rapidement et précisément les menaces. Cette fusion entre la protection Endpoint de pointe de Sophos avec EDR intelligent et notre équipe d'experts en sécurité de haut niveau se traduit par ce que nous appelons la « réponse humaine accélérée par machine ».

Une transparence et un contrôle complets

Avec Sophos MTR, 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. Sophos MTR propose 3 modes de réponse afin que vous puissiez choisir la meilleure façon pour notre équipe MTR de travailler à vos côtés lors d'incidents :

Notifier : Nous vous informons de la détection et vous fournissons des informations qui vous aideront à définir les priorités et la réponse appropriée.

Collaborer : Nous travaillons avec votre équipe interne ou vos points de contact externes pour répondre à cette détection.

Autoriser : Nous gérons les mesures de confinement et de neutralisation et vous tenons informés des actions lancées.

Niveaux de service Sophos MTR

Sophos MTR offre 2 niveaux de service (Standard et Advanced) afin de répondre aux besoins des entreprises de toutes tailles et de tous niveaux de maturité. Quel que soit le niveau de service choisi, les entreprises peuvent tirer parti de l'un des trois modes de réponse (notifier, collaborer ou autoriser) pour répondre à leurs besoins particuliers.

Sophos MTR : Standard

Traque des menaces à partir d'indices 24h/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 *Toutes les fonctionnalités du niveau Standard + les éléments suivants :*

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 de threat hunters 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 système d'extrémité, 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 vos ressources 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.

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

2019-09-17 DSFR (GH)

SOPHOS