Sophos Managed Detection and Response

Réponse aux menaces dirigée par des experts

Sophos MDR (Managed Detection and Response) est une offre de services de chasse aux menaces, de détection et de réponse, entièrement managés par une équipe d'experts, 24 h/24 et 7 j/7.

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

La plupart des entreprises ne disposent pas des outils, du personnel et des processus internes nécessaires pour se défendre contre les cybermenaces et gérer leur programme de sécurité. Sophos MDR assure la détection et la réponse aux menaces à toute heure du jour et de la nuit. Nous neutralisons les menaces sophistiquées 24 h/24, 7 j/7 et 365 j/an.

Sophos MDR est assuré par des chasseurs de menaces et des experts en réponse qui vont :

- Chasser de manière proactive et confirmer les menaces et incidents potentiels.
- Utiliser toutes les informations disponibles pour déterminer l'ampleur et la gravité des menaces.
- Fournir des informations sur le contexte et l'impact potentiel d'une menace.
- Prendre des mesures pour intercepter, contenir et neutraliser les menaces.
- Fournir des conseils pour remédier aux causes profondes des incidents récurrents.

Réponse humaine accélérée par machine

Tirant profit de Sophos XDR, Sophos MDR fusionne Machine Learning et analyse d'expert pour améliorer la chasse et la détection des menaces, l'investigation approfondie des alertes et les actions ciblées afin d'éliminer rapidement et précisément les menaces. Cette fusion entre la protection Sophos Endpoint avec XDR 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 MDR, vous contrôlez quand et comment les incidents potentiels sont escaladés, quelles actions de remédiation sont prises et qui est inclus dans les communications. Sophos MDR propose 3 modes de réponse ; vous choisissez comment vous souhaitez travailler avec notre équipe MDR si un incident se produit.

Notifier : Nous vous alertons si un incident potentiel se produit, vous fournissons le détail de l'événement et vous aidons à le prioriser et à y répondre en conséquence.

Collaborer : Nous travaillons avec votre équipe interne ou vos points de contact externes pour répondre à l'incident.

Autoriser : Nous contenons et neutralisons l'incident et vous informons des mesures que nous avons prises.

Avantages principaux

- Chasse aux menaces, détection et réponse avancées fournies sous forme de service managé
- Notre équipe de réponse aux menaces contient et neutralise les menaces à distance, 24/7/365
- Vous contrôlez quelles actions sont prises par l'équipe MDR en votre nom et comment les incidents sont gérés
- Accédez à une technologie de Machine Learning de pointe et une équipe d'experts de haut niveau
- Deux niveaux de services (Standard et Advanced) répondent aux besoins des entreprises de tous niveaux de maturité

SOPHOS

Niveaux de service Sophos MDR

Sophos MDR offre 2 niveaux de service (Standard et Advanced) pour répondre aux besoins des entreprises de toutes tailles et de tous niveaux de maturité. Quel que soit le niveau de service, les organisations peuvent utiliser l'un des trois modes de réponse (Notifier, Collaborer ou Autoriser).

Sophos MDR : Standard

Chasse aux menaces à partir d'indices 24/7

Les activités et artefacts malveillants confirmés (signaux forts) sont automatiquement bloqués ou supprimés. Cela permet à nos experts de chasser les menaces à partir d'indices, c'est-à-dire d'enquêter et d'analyser les facteurs de causalité et les événements connexes (signaux faibles) afin de découvrir de nouveaux indicateurs d'attaque (IOA) ou de compromission (IOC).

Diagnostic de sécurité

Nos examens proactifs vous permettent de rester à jour sur vos conditions de fonctionnement et vos configurations. Nous fournissons également des recommandations pour vous aider à maintenir les performances de Sophos XDR et des autres produits de Sophos Central à un niveau optimal.

Rapport d'activité

Nous fournissons un résumé des événements pour vous informer des menaces découvertes et des mesures de réponse prises entre chaque rapport.

Détections des adversaires

Nous utilisons des techniques d'investigation avancées pour distinguer les comportements légitimes des tactiques, techniques et procédures (TTP) utilisées par les cybercriminels.

Sophos MDR : Advanced inclut toutes les fonctionnalités du niveau Standard, plus :

Chasse aux menaces sans indices de départ 24/7

Nous utilisons la science des données et les renseignements sur les menaces pour anticiper les cyberattaques et identifier les IOA.

Données télémétriques améliorées

Nous enrichissons nos investigations avec des données provenant d'autres produits de Sophos Central afin d'aller au-delà des systèmes d'extrémité et d'obtenir une image complète de votre posture de sécurité.

Amélioration proactive de la posture de sécurité

Nous fournissons des conseils prescriptifs pour vous aider à optimiser votre posture de sécurité.

Interlocuteur dédié en cas d'incident

Un responsable de la réponse aux menaces est mis à votre disposition. Il collabore avec votre équipe interne et vos partenaires externes dès que nous identifions un incident et travaille avec vous jusqu'à la résolution de l'incident.

Assistance téléphonique directe

Votre équipe a un accès direct par téléphone à notre centre d'opérations de sécurité (SOC). Notre équipe MDR opérationnelle est disponible 24 h/24, 7 j/7 et 365 j/an, et s'appuie sur nos équipes du support technique réparties sur 26 sites dans le monde entier.

Découverte des ressources

Nous fournissons des informations sur vos actifs gérés et non gérés et sur la manière de les sécuriser.

Pack 'Onboarding Plus' pour les clients MDR

Notre offre Onboarding Plus est un service de prise en charge guidé à distance pour les clients qui ont acheté Sophos MDR. Ce service vous offre : un interlocuteur dédié au sein des Services professionnels de Sophos pour la prise en charge et la planification, une assistance pour le déploiement et la formation, et un diagnostic de sécurité pour s'assurer que vous tirez le meilleur parti de nos recommandations. Onboarding Plus inclut :

Jour 1 - Planification et exécution de l'implémentation

- Démarrage du projet.
- Configuration de Sophos Central.
- Examen des fonctionnalités de Sophos Central.
- Construction et test du processus de déploiement.
- Déploiement de Sophos Central dans votre organisation.

Jour 30 – Formation au XDR

- Formation pour apprendre à penser et à agir comme un centre d'opérations de sécurité (SOC).
- Chasse aux menaces pour identifier des CIO.
- Création de requêtes pour des investigations futures.

Jour 90 – Formation au XDR

- Examen de vos politiques de sécurité actuelles et mise à jour si nécessaire.
- Identification des fonctionnalités (le cas échéant) pouvant être utilisées pour améliorer davantage votre cyber protection.
- Réception de la documentation écrite avec nos recommandations tirées de notre diagnostic de sécurité.

Pour toute question, n'hésitez pas à contacter notre équipe des Services professionnels Sophos.

Amériques : ProfessionalServices@sophos.com

Région APJ : ProfessionalServicesAU@Sophos.com.au

Europe : ProfessionalServicesEmea@Sophos.com

Pour en savoir plus :

sophos.fr/mdr

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

© Copyright 2022. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

22-08-01 DS-FR (DD)

SOPHOS