Sophos MDR pour Microsoft Defender

Réponse aux menaces assurée par des experts pour les environnements Microsoft

Sophos Managed Detection and Response (MDR) pour Microsoft Defender renforce votre équipe avec des experts hautement qualifiés qui surveillent, investiguent et répondent aux alertes de la Sécurité Microsoft 24 h/24 et 7 j/7.

Optimisez votre investissement dans la Sécurité Microsoft

De nombreuses entreprises ont investi dans la suite de Sécurité Microsoft, mais ne disposent peut-être pas d'une expertise interne suffisante pour utiliser efficacement la gamme de technologies multi-produits de Microsoft afin de détecter, d'investiguer et de répondre à des centaines d'alertes de sécurité chaque jour :

- La pénurie mondiale de spécialistes de la cybersécurité a atteint 3,4 millions de personnes[1].
- 71 % des équipes de sécurité estiment qu'il est difficile de déterminer quelles alertes doivent être examinées parmi le bruit de fond généré par leurs outils de sécurité[2].
- Le délai médian de réponse aux menaces pour les entreprises disposant d'une équipe dédiée aux opérations de sécurité est de 16 heures, ce qui laisse aux attaquants un temps considérable pour opérer au sein du réseau[3].

Sophos MDR pour Microsoft Defender offre les capacités de détection, de chasse et de réponse aux menaces les plus robustes disponibles pour les environnements Microsoft. Nos analystes surveillent, investiguent et répondent aux alertes de la Sécurité Microsoft 24 h/24 et 7 j/7, et exécutent immédiatement des actions de réponse pour bloquer les menaces confirmées. Leur temps moyen de réponse aux menaces est de 38 minutes, soit 96 % plus rapide que le temps de référence de l'industrie.

Détecter et bloquer les menaces au-delà de Microsoft Defender

Avec Sophos MDR pour Microsoft Defender, nos experts en Sécurité Microsoft détectent, investiguent et répondent aux menaces en utilisant les données de sécurité des produits Microsoft suivants :

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Centre de sécurité et conformité O365
- Microsoft Sentinel
- Activité de gestion Office 365

De plus, nos détections propriétaires, nos renseignements sur les menaces de classe mondiale et nos chasses aux menaces assurées par des experts ajoutent des couches de défense supplémentaires qui nous permettent d'identifier et de bloquer plus de menaces que les outils de Sécurité Microsoft ne peuvent le faire à eux seuls.

Les entreprises peuvent également intégrer des outils de sécurité non Microsoft et des sources de télémétrie provenant des solutions Sophos ou de dizaines d'autres fournisseurs tiers, tels que Palo Alto Networks, Fortinet, Check Point, AWS, Google, Okta, Darktrace, et bien d'autres encore, pour une visibilité et une protection complètes.

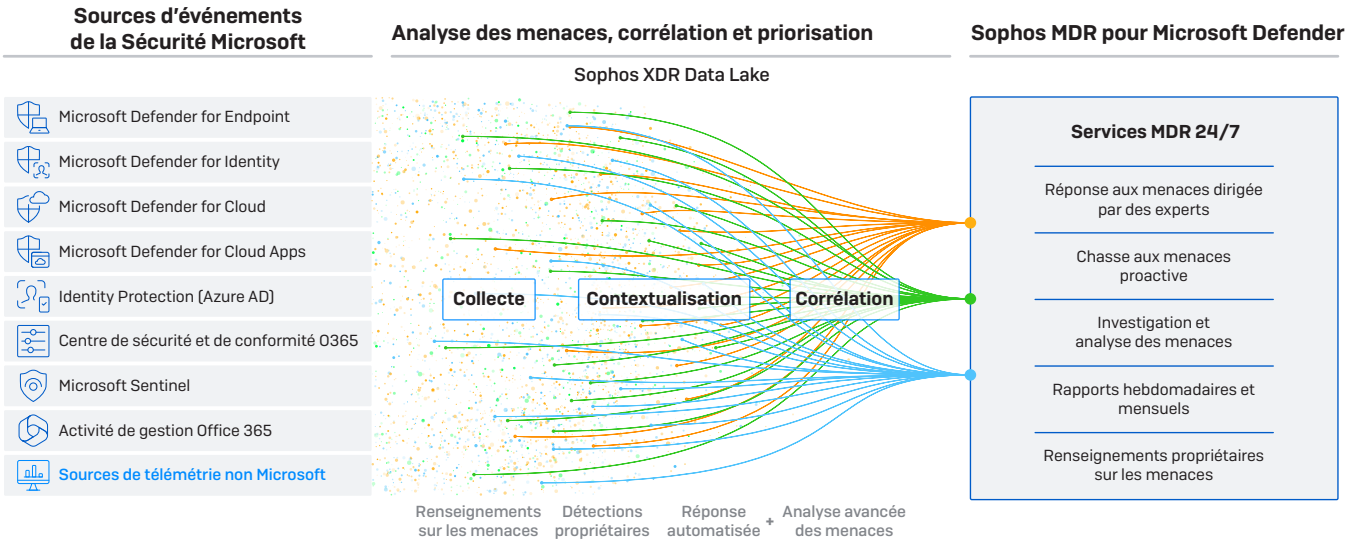
Avantages principaux

- Les analystes Sophos MDR surveillent, investiguent et répondent aux alertes de la Sécurité Microsoft, 24 h/24 et 7 j/7, en prenant des mesures immédiates pour bloquer les menaces confirmées.
- Les capacités du service s'étendent au-delà de Microsoft Defender for Endpoint et de Microsoft Sentinel pour couvrir l'ensemble de la plateforme de la Sécurité Microsoft.
- Lorsqu'une menace active est identifiée, l'équipe Sophos MDR peut exécuter un ensemble complet d'actions de réponse aux menaces en votre nom.
- Les détections propriétaires de Sophos, les renseignements sur les menaces et les chasses aux menaces assurées par des experts ajoutent des couches de défense supplémentaires.
- Intégration d'outils et de sources de télémétrie non Microsoft pour bloquer les attaques ciblant votre réseau, vos utilisateurs et vos clients.

1 2022 Cybersecurity Workforce Study, (ISC)2
2 L'état de la cybersécurité en 2023 : l'impact des cyberattaques sur les entreprises, Sophos
3 Gartner Cybersecurity Business Value Benchmark database, 2022

SOPHOS

Sophos MDR pour Microsoft Defender : Capacités de service clés



Surveillance 24/7 des menaces

Nos experts en Sécurité Microsoft détectent et bloquent les menaces avant qu'elles ne compromettent vos données ou ne causent des interruptions de service. Soutenu par six centres d'opérations de sécurité (SOC) mondiaux, Sophos assure une couverture 24 h/24.

Réponse aux menaces assurée par des experts

L'équipe Sophos MDR peut exécuter en votre nom un ensemble complet d'actions de réponse aux menaces pour interrompre, contenir et éliminer les attaquants. Parmi les actions de réponse aux menaces, figurent :

- Isoler le ou les hôtes utilisant Sophos Central
- Mettre en place le blocage d'IP de pare-feu basé sur l'hôte
- Arrêter des processus
- Forcer la déconnexion de sessions utilisateur
- Désactiver des comptes utilisateur
- Supprimer des artefacts malveillants
- Ajouter des hachages malveillants aux éléments bloqués dans Sophos Central

Chasse aux menaces proactive dirigée par des experts

Les chasses aux menaces proactives effectuées par des analystes hautement qualifiés permettent de découvrir et d'éliminer rapidement les menaces et de détecter les comportements des attaquants qui ont réussi à contourner la détection des outils déployés.

Compatible avec les outils de sécurité non Microsoft

Sophos MDR peut intégrer des outils de sécurité et des sources de télémétrie non Microsoft pour détecter et bloquer les attaques dans votre environnement.

Rapports hebdomadaires et mensuels

Les alertes en temps réel, les rapports et les options de gestion sont facilement accessibles dans Sophos Central, tandis que les rapports hebdomadaires et mensuels fournissent des informations sur les investigations de sécurité, les cyber menaces et la posture de sécurité de votre entreprise.

Briefings de renseignement mensuels

Fourni par l'équipe Sophos MDR, le « Sophos MDR ThreatCast » est un briefing mensuel qui donne un aperçu des derniers renseignements sur les menaces et des meilleures pratiques de sécurité.

Détections propriétaires

Les détections propriétaires, les analyses avancées des menaces et les renseignements sur les menaces de classe mondiale intégrés dans la plateforme Sophos ajoutent des couches de défense supplémentaires qui permettent d'identifier plus de menaces que les outils de Sécurité Microsoft ne peuvent le faire seuls.

Pour en savoir plus :

www.sophos.com/microsoft-defender

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

23-07-10 DS-FR (DD)

SOPHOS