

Sophos XDR

Défense contre les adversaires actifs avec EDR et XDR



Les adversaires font constamment évoluer leurs techniques pour exploiter les vulnérabilités et accélérer leurs attaques. Réduire les temps de détection et de réponse n'a jamais été aussi important. La plateforme XDR (Extended Detection and Response) unifiée de Sophos vous permet de détecter, d'investiguer et de répondre rapidement aux menaces multi-étapes et aux adversaires actifs dans votre écosystème de sécurité.

Cas d'usages

1 | ADOPTER UNE PROTECTION ROBUSTE DÈS LE DÉPART

Résultats souhaités : Bloquer plus de menaces en amont pour réduire la charge de travail.

Solution : Ciblez plus efficacement les investigations en bloquant davantage de violations de sécurité à la source. Sophos XDR inclut une protection inégalée pour stopper les menaces avancées rapidement avant qu'elles ne prennent de l'ampleur. Protégez les postes et les serveurs à l'aide de technologies sophistiquées, notamment l'IA, l'analyse comportementale et les technologies anti-ransomware et anti-exploit.

2 | ACCÉLÉRER LA RÉPONSE AUX MENACES

Résultats souhaités : Détecter, analyser et répondre aux menaces plus rapidement.

Solution : Les détections prioritaires par l'IA tirent parti des renseignements sur les menaces collectés par Sophos X-Ops. Elles permettent d'identifier rapidement et aisément les événements suspects qui nécessitent une attention immédiate. Chassez les menaces et répondez-y rapidement grâce à des workflows d'investigation optimisés, de puissantes capacités de recherche, des outils de gestion de dossier collaboratifs et des réponses automatisées.

3 | OBTENIR UNE VISIBILITÉ SUR LES SURFACES D'ATTAQUE

Résultats souhaités : Obtenir une visibilité et un aperçu complets des menaces évasives sur l'ensemble de vos principales surfaces d'attaque.

Solution : Utilisez les solutions Sophos — entièrement intégrées et compatibles XDR — pour obtenir une visibilité au-delà de vos postes ou pour exploiter vos investissements technologiques existants. Intégrez un vaste écosystème de solutions tierces de sécurité endpoint, pare-feu, réseau, messagerie, gestion d'identité et Cloud pour détecter et répondre aux menaces grâce à une plateforme XDR unifiée.

4 | IMPLÉMENTER UNE SOLUTION PUISSANTE POUR TOUS LES UTILISATEURS

Résultats souhaités : Les informaticiens généralistes et les analystes de sécurité peuvent aisément investiguer et répondre aux menaces.

Solution : Conçu à la fois pour les équipes SOC internes dédiées et les administrateurs qui s'occupent de la sécurité et d'autres responsabilités informatiques, Sophos XDR aide à optimiser l'efficacité des utilisateurs tout en fournissant une visibilité complète et des conseils pour vous aider à répondre aux menaces.

Gartner

Reconnu dans le Gartner Market Guide for XDR de 2023

MITRE ATT&CK

Résultats exceptionnels dans l'évaluation 2023 de MITRE Engenuity ATT&CK

G2 Leader

Classée solution XDR numéro 1 par les utilisateurs de G2 (Spring 2023)

Pour en savoir plus et évaluer Sophos XDR : sophos.fr/xdr