Présentation de la solution

Sophos NDR

Une visibilité de la criticité des flux réseaux

Sophos NDR (Network Detection and Response) est disponible à la fois pour Sophos MDR et Sophos XDR. La solution détecte en profondeur les activités réseau malveillantes que les postes et les pare-feux ne détectent pas. Sophos NDR analyse en continu le trafic à la recherche de modèles suspects, notamment les activités inhabituelles provenant d'appareils inconnus ou non gérés, d'actifs malveillants, de nouveaux serveurs C2 zero-day et de mouvements de données inattendus.

Cas d'usages

1 | VISIBILITÉ CRITIQUE

Résultats souhaités : Obtenir une visibilité critique sur les activités du réseau qui ne sont pas détectées par d'autres produits.

Solution : Sophos NDR, en collaboration avec vos solutions endpoint et pare-feu, surveille l'activité du réseau et détecte les modèles suspects et malveillants qui ne sont pas détectés par vos postes ou vos pare-feux. Il détecte les flux de trafic inhabituels provenant de systèmes non gérés et d'appareils connectés (IoT), d'actifs indésirables, de menaces internes, d'attaques zero-day inédites et de modèles inhabituels en profondeur dans le réseau.

2 | DÉTECTION PRÉCOCE

Résultats souhaités : Obtenir des résultats d'analyse de haute qualité pour identifier plus rapidement les menaces.

Solution : Sophos NDR utilise cinq moteurs de détection indépendants qui travaillent ensemble en temps réel pour identifier rapidement le trafic suspect et malveillant. Il mobilise des technologies telles que le Deep Learning, l'inspection approfondie des paquets (DPI), l'analyse des charges utiles chiffrées, l'analyse des noms de domaine et des technologies d'analyse puissantes. Grâce à Sophos NDR, vous ne recevez que des alertes de qualité pour ne pas vous submerger d'alertes en tout genre.

3 | RÉPONSE AUTOMATIQUE

Résultats souhaités : Stopper automatiquement les adversaires actifs et les menaces dans leur élan.

Solution : L'automatisation inter-produits entre Sophos NDR, Sophos XDR, Sophos MDR et Sophos Firewall permet une réponse immédiate pour stopper les menaces actives. Lorsque Sophos NDR identifie un indicateur de compromission, une menace active ou un adversaire, les analystes sont immédiatement alertés. Ils peuvent envoyer directement un flux de menaces à Sophos Firewall pour déclencher une réponse automatisée afin d'isoler l'hôte compromis.

4 | GESTION DANS UNE CONSOLE UNIQUE

Résultats souhaités : Passer moins de temps à gérer votre sécurité réseau.

Solution : Avec Sophos Central, vous disposez d'une plateforme de gestion unique dans le Cloud pour tous vos produits Sophos, y compris Sophos NDR, XDR, Endpoint, Firewall et bien plus encore. Vous bénéficiez d'outils riches et puissants qui exploitent notre Data Lake profond pour mener des actions de chasse aux menaces sur l'ensemble des produits, pour gérer la réponse de manière précoce, ou encore établir des rapports et des audits. Au final, vous passez moins de temps à gérer la sécurité de votre réseau.

Identifiez les actifs non protégés et malveillants

Révélez les mouvements de données inhabituels et les menaces internes

Détectez les attaques zero-day jusqu'alors invisibles

Pour en savoir plus et évaluer Sophos NDR
sophos.com/ndr

2023-11-06 DS-FR (MP)

SOPHOS