Sophos Network Detection and Response (NDR)

Surveillance et analyse en continu du trafic réseau afin d'identifier les actifs indésirables, les appareils non protégés, les menaces internes et les attaques de type zero-day.

Pourquoi utiliser NDR

- Sophos NDR détecte les activités malveillantes au cœur du réseau, là où les postes et les pare-feux n'ont pas de visibilité.
- Sophos NDR analyse le trafic à l'intérieur du réseau ; c'est un élément essentiel de toute stratégie de défense en profondeur.
- La solution détecte les activités provenant d'appareils inconnus ou non gérés, d'actifs malveillants, de nouveaux serveurs C2 zero-day et de mouvements de données inhabituels.

Présentation de Sophos NDR

- Sophos NDR est un produit complémentaire de Sophos MDR et Sophos XDR
- Il fonctionne parfaitement avec Sophos Firewall pour fournir un niveau de détection et de réponse incomparable.
- Les alertes sont transmises instantanément aux analystes de Sophos MDR et XDR en vue d'une investigation et d'une réponse grâce à la fonctionnalité de réponse aux menaces actives de Sophos Firewall.
- Sophos NDR est déployé sous forme d'appliance virtuelle qui se connecte à un commutateur physique ou virtuel sur le réseau de l'entreprise

Tarification par utilisateurs + serveurs

10 000 Utilisateurs

+ 1 000 Serveurs

= 11 000 Utilisateurs et Serveurs NDR

Prix inférieur à celui de solutions NDR autonomes

Logiciel de l'appliance virtuelle inclus dans l'abonnement

Remise sur volume intégrée

Pourquoi choisir Sophos NDR

- Intégration complète avec Sophos MDR, XDR et Firewall pour une détection et une réponse incomparables
- Cinq moteurs de détection différents pour une visibilité maximale sur les menaces sur le réseau
- Une approche unique et brevetée de Machine Learning qui identifie les malwares dans le trafic chiffré
- Détection par algorithme de génération de domaine (DGA) qui ne nécessite pas de renseignements supplémentaires sur les menaces
- De puissantes analyses de risques détectent les activités anormales et identifient les modèles qui justifient une investigation plus poussée

Sophos NDR : fournir des résultats de sécurité supérieurs

Sophos NDR renforce la protection en détectant les menaces et les activités malveillantes que d'autres produits ne détectent pas :

- Appareils malveillants : appareils non autorisés et potentiellement malveillants qui communiquent sur le réseau.
- Appareils non protégés : appareils légitimes pouvant être utilisés comme point d'entrée.
- Menaces internes : mouvements anormaux de trafic et de données à l'intérieur de l'entreprise.
- Attaques zero-day : détection des tentatives des serveurs C2 en se basant sur les modèles de comportement trouvés dans les paquets de session.
- Menaces IoT et OT : appareils médicaux, terminaux de paiement, etc.) - surveillance des données provenant de ces appareils.

Combiné à d'autres télémétries de sécurité, Sophos NDR permet aux analystes de dresser un tableau complet de l'attaque, ce qui permet une réponse plus rapide et plus profonde.

Exemples de scénario :

1. Sophos NDR détecte un appareil qui communique au niveau du réseau interne
2. La protection Endpoint n'a aucun appareil connu en gestion

INFORMATION : Appareil non géré communiquant sur le réseau

ACTION MDR : lancement d'une investigation pour savoir si une politique utilisateur a été violée ou si une action malveillante a été effectuée en interne

Questions exploratoires

- Disposez-vous actuellement d'une solution de surveillance du trafic réseau (par exemple, Darktrace, Security Onion, Thinkst Canary) ?
- Disposez-vous actuellement d'ordinateurs portables ou d'autres appareils sans protection Endpoint ? Par exemple : dans un laboratoire, des terminaux de paiement ou des appareils connectés (IoT) ?
- Surveillez-vous le trafic réseau derrière votre pare-feu ?
- Comment surveillez-vous le comportement des utilisateurs internes ?
- Comment surveillez-vous le mouvement « normal » des données ?
- Réalisez-vous régulièrement une découverte des actifs sur l'ensemble de votre réseau ?
- Pouvez-vous identifier les nouveaux systèmes ou les systèmes malveillants sur le réseau ?
- Avez-vous une visibilité sur le trafic chiffré sur votre réseau ? Êtes-vous actuellement en mesure de déterminer si ce trafic est malveillant ?

23-11-06 FR-DA-(MP)

SOPHOS