Sophos XDR

Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X consolide les fonctionnalités XDR puissantes avec une protection Endpoint incomparable. Traquez les menaces pour détecter les adversaires actifs et maintenez l'hygiène de vos opérations de cybersécurité. Lorsqu'un problème est détecté, répondez à distance avec précision. Étendez la visibilité au-delà de l'endpoint en intégrant les données des serveurs, du pare-feu et de la messagerie.

Lancez des requêtes pour les opérations IT et la traque des menaces

Obtenez rapidement les réponses à vos questions critiques. Les administrateurs informatiques et les professionnels de la cybersécurité verront une réelle valeur ajoutée pour leurs opérations informatiques et leurs actions de Threat Hunting quotidiennes.

Commencez par la meilleure protection

Intercept X bloque les attaques avant qu'elles ne surviennent. Vous bénéficiez ainsi d'une meilleure protection et vous passez moins de temps à analyser les incidents qui auraient dû être automatiquement bloqués. Vous avez également accès à des informations détaillées sur les menaces, vous permettant d'intervenir rapidement et avec discernement.

Explorez les données en profondeur et répondez rapidement

Lorsque vous identifiez un événement qui nécessite une investigation plus approfondie, vous pouvez accéder au Sophos Data Lake et explorer les données en temps réel directement depuis l'appareil, en plus des 90 jours de données historiques. Lorsqu'un incident est confirmé, accédez à distance à l'appareil et prenez les mesures nécessaires, comme la désinstallation d'une application ou le redémarrage.

Visibilité entre les produits

Sophos XDR va au-delà de l'endpoint et du serveur, permettant à Sophos Firewall, Sophos Email et d'autres sources de données* d'envoyer des données clés vers le Sophos Data Lake, vous offrant ainsi une vue incroyablement large de l'environnement de votre entreprise.

Obtenez des informations même lorsqu'un appareil est hors ligne

Sophos Data Lake, composant clé des fonctionnalités XDR, est un référentiel de données dans le Cloud. Il permet de stocker et d'accéder à des informations critiques provenant de vos solutions endpoint, serveur, pare-feu et messagerie, ainsi que d'utiliser les informations des appareils, même lorsque ces derniers sont hors ligne.

Avantages principaux

- Obtenez les réponses à vos questions critiques relatives aux opérations informatiques et à la traque des menaces
- Conçu pour les administrateurs IT et les analystes de sécurité
- Prenez des mesures correctives à distance sur les appareils qui vous intéressent
- Obtenez une vue d'ensemble de l'environnement informatique de votre entreprise et, si nécessaire, accédez à des informations plus détaillées
- Corrélez les données Endpoint, Server, Firewall, Email et autres*
- Requêtes SQL pré-écrites et entièrement personnalisables
- Disponible pour Windows, macOS et Linux

**Bientôt disponible avec Cloud Optix et Sophos Mobile*

SOPHOS

Démarrez en quelques secondes

Choisissez parmi une bibliothèque de requêtes SQL prédéfinies pour poser une grande variété de questions sur le système informatique et la sécurité. Si vous préférez, vous pouvez les personnaliser ou écrire les vôtres. Vous pouvez également vous référer à la communauté Sophos où les requêtes sont régulièrement partagées.

Cas d'usages

Opérations informatiques

- Pourquoi une machine est-elle lente ?
- Quels appareils ont des vulnérabilités connues, des services inconnus ou des extensions de navigateur non autorisées ?
- Des programmes en cours d'exécution devraient-ils être supprimés ?
- Identifier les appareils non gérés, invités et IoT
- Pourquoi la connexion au réseau du bureau est-elle lente ? Quelle application en est la cause ?
- Revenir 30 jours en arrière pour détecter toute activité inhabituelle sur un appareil disparu ou détruit

Threat Hunting

- Quels sont processus qui tentent d'établir une connexion réseau sur des ports non standards ?
- Afficher les processus qui ont récemment modifié des fichiers ou des clés de registre
- Lister les indices de compromission (IoC) mappés au cadre MITRE ATT&CK
- Prolonger l'investigation jusqu'à 30 jours sans remettre un appareil en ligne
- Utiliser les détections ATP et IPS du pare-feu pour analyser les hôtes suspects
- Comparer les informations de l'en-tête de l'email, les algorithmes de hachage SHA et autres IoC pour identifier le trafic vers un domaine malveillant

Que contient Sophos XDR ?

	XDR (Extended Detection and Response)
Sources de données inter-produits	✓
Requêtes inter-produits	✓
Requêtes endpoint et serveur	✓
Sophos Data Lake	✓
Durée de conservation du Data Lake	30 jours
Durée de conservation des données sur le disque	✓
Bibliothèque de requêtes SQL	✓
Capacités de protection Intercept X	✓

Pour plus de détails sur les licences, veuillez consulter les guides de gestion des licences pour Intercept X et Intercept X for Server.

Essayez-le gratuitement

Inscrivez-vous à une évaluation gratuite de 30 jours sur sophos.fr/intercept-x

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

21-07-08 DS-FR (PS)

SOPHOS