SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

EDR conçu pour la traque des menaces et les opérations IT

Sophos Intercept X Advanced with EDR consolide la fonctionnalité EDR puissante avec une protection Endpoint incomparable. Traquez les menaces pour détecter les adversaires actifs, ou exploitez l'EDR dans vos opérations informatiques pour maintenir l'hygiène de la sécurité IT. Lorsqu'un problème est détecté, répondez à distance avec précision.

Avantages principaux

- Fonctionnalité EDR associée à la meilleure protection Endpoint
- Conçu pour les analystes de sécurité et les administrateurs IT
- Maintient de manière proactive l'hygiène informatique et traque les menaces avant qu'elles ne puissent produire des dégâts
- Posez n'importe quelle question sur un événement passé ou en cours
- Requêtes SQL préétablies et entièrement personnalisables
- Accès rapide aux données actuelles et historiques sur le disque jusqu'à 90 jours
- Répondez à distance avec précision avec un outil de ligne de commande
- Détectez, analysez et priorisez les incidents à l'aide du Machine Learning
- Accélérez les investigations et réduisez le temps d'impact des attaquants
- Disponible pour Windows, macOS* et Linux

**Bientôt disponible*

L'EDR commence avec la meilleure des protections

Pour empêcher toute violation, le maître mot est la prévention. Intercept X consolide en une seule solution la meilleure protection Endpoint sur le marché avec l'EDR. La plupart des menaces sont ainsi bloquées avant même de pouvoir occasionner le moindre dégât. Intercept X Advanced with EDR offre une plus grande assurance en matière de cybersécurité grâce à sa capacité à détecter les menaces, à les identifier et à y remédier.

Inclure l'EDR dans une suite de protection Endpoint la mieux notée du marché permet à Intercept X d'alléger considérablement la charge de travail consacrée à l'EDR. En bloquant davantage de menaces en amont, les analystes ne perdent plus de temps à analyser des faux positifs et un volume écrasant d'alertes.

Ajoutez de l'expertise, pas des ingénieurs

Détectez, priorisez et examinez automatiquement les menaces à l'aide de l'intelligence artificielle. Intercept X Advanced with EDR exploite le Machine Learning pour détecter et prioriser automatiquement les menaces. Si un fichier potentiellement malveillant est découvert, les utilisateurs peuvent se reposer sur le Deep Learning qui analyse automatiquement les malwares dans les moindres détails, décomposant les attributs des fichiers et les codes et les comparant à des millions d'autres fichiers.

Requêtes prêtes à l'emploi conçues pour les spécialistes, par des spécialistes : Les analystes de sécurité et les administrateurs IT peuvent utiliser Sophos EDR immédiatement grâce aux requêtes SQL prêtes à l'emploi et catégorisées par cas d'utilisation. Les requêtes peuvent être modifiées aisément pour personnaliser vos recherches, créées à partir de zéro ou obtenues auprès de notre communauté.

Obtenez des réponses aux questions complexes en reproduisant les compétences d'analystes qui vous font défaut. Intercept X Advanced with EDR reproduit les capacités d'analystes de haut vol, permettant ainsi aux entreprises d'ajouter de l'expertise sans avoir à augmenter leurs effectifs.

Conçu pour la traque des menaces et les opérations IT

Sophos Intercept X Advanced est la première solution EDR conçue pour les administrateurs IT et les analystes de sécurité. Elle vous permet de poser n'importe quelle question sur un événement passé ou en cours survenant sur vos postes. Traquez les menaces pour détecter les adversaires actifs, ou exploitez l'EDR dans vos opérations informatiques pour maintenir l'hygiène de la sécurité IT. Lorsqu'un problème est détecté, répondez à distance avec précision. L'EDR exploite pour cela deux fonctionnalités clés : Live Discover et Live Response.

Live Discover : Posez n'importe quelle question pour garder une longueur d'avance Live Discover offre aux analystes de sécurité et aux administrateurs IT la possibilité de poser et de répondre à presque toutes les questions auxquelles ils peuvent penser sur leurs postes et leurs serveurs. Découvrez rapidement les problèmes liés aux opérations informatiques afin de maintenir l'hygiène informatique, et posez des questions détaillées pour traquer les activités suspectes. Live Discover utilise des requêtes SQL puissantes, prêtes à l'emploi et entièrement personnalisables, qui permettent d'interroger rapidement jusqu'à 90 jours de données actuelles et historiques sur le disque. Exemples de scénarios d'utilisation :

Opérations informatiques

- Pourquoi une machine est-elle lente ? Doit-elle être redémarrée ?
- 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 ?
- Le partage à distance est-il activé ? L'appareil comporte-t-il des clés SSH non chiffrées ? Les comptes invités sont-ils activés ?
- L'appareil possède-t-il une copie d'un fichier particulier ?

Traque des menaces

- Quels sont processus qui tentent d'établir une connexion réseau sur des ports non standards ?
- Lister les indices de compromission (IoC) mappés au cadre MITRE ATT&CK
- Afficher les processus qui ont récemment modifié des fichiers ou des clés de registre
- Rechercher des détails sur les exécutions PowerShell
- Identifier les processus déguisés en services.exe

Live Response : Répondez à distance avec précision Lorsque des problèmes sont découverts, Live Response fournit aux utilisateurs un accès en ligne de commande aux postes et aux serveurs de l'entreprise. Accédez à distance aux appareils pour effectuer un examen plus approfondi ou résoudre tout problème. Les admins peuvent redémarrer les appareils, arrêter les processus actifs, exécuter des scripts, modifier le fichier de configuration, installer/désinstaller des logiciels, exécuter des outils d'investigation, etc.

Managed Detection and Response (MDR)

Sophos MTR (Managed Threat Response) est une offre de services de recherche, de détection et de remédiation des menaces, entièrement gérés par une équipe d'experts 24 h/24 et 7 j/7. Tandis que d'autres services MDR (Managed Service and Response) se contentent de vous notifier lorsqu'une attaque ou un événement suspect se produisent, avec le service MTR (Managed Threat Response) de Sophos, votre entreprise s'appuie sur une équipe d'experts de haut niveau spécialisés dans la recherche de menaces et leur remédiation, qui prend les mesures nécessaires en votre nom pour neutraliser les menaces, même les plus sophistiquées. Les clients qui choisissent de bénéficier du service Sophos MTR reçoivent aussi Intercept X Advanced with EDR.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Endpoint Protection
Techniques fondamentales	✓	✓	✓
Deep Learning	✓	✓	
Anti-exploit	✓	✓	
CryptoGuard anti-ransomware	✓	✓	
Endpoint detection and response (EDR)	✓		

Essayez-le gratuitement dès aujourd'hui

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

20-05-12 DS-FR (MP)

SOPHOS