**Sophos ajoute Endpoint Detection and Response à Intercept X Advanced**

Une étude Sophos en Belgique et aux Pays-Bas démontre que :

*- 40% des ITDM belges et néerlandais dispose d’outils EDR faisant partie de leur protection endpoint  
- 46% des entreprises comptant entre 500 et 750 travailleurs ont EDR, contrairement à 28% des organisations à moins de 250 travailleurs  
- 7% des entreprises belges et néerlandaises estiment que EDR est inutile. Au sein des entreprises ayant moins de 250 travailleurs ce taux augmente même à 18%.*

Bruxelles – Le 9 octobre 2018 – **Sophos a annoncé aujourd’hui qu’il a ajouté Endpoint Detection and Response (EDR) à son portefeuille de protection endpoint Intercept X. Intercept X Advanced, alimentée par la technologie du deep learning offre la possibilité de découvrir plus vite et plus efficacement les maliciels et est disponible par un programme d’accès rapide global. Ainsi il apporte aux PME des capacités de réaction rapides et précoces. Le réseau neuronal de deep learning de Sophos est testé sur des centaines de millions d’échantillons pour chercher des caractéristiques suspectes de codes malveillants pour détecter des menaces inédites. Le réseau offre également une analyse approfondie et professionnelle d’attaques potentielles en comparant l’ADN de fichiers suspects aux échantillons des maliciels déjà catégorisés dans SophosLabs.**

**Pour ce qui est de la sécurité la taille ne dit pas tout**De récentes recherches de Sophos ont démontré qu’actuellement surtout les grandes entreprises profitent d’EDR. Deux ITDM (décideurs IT) sur cinq (40%) en Belgique et aux Pays-Bas disposent d’outils EDR faisant partie de leur protection endpoint. Ce pourcentage augmente avec la taille de l’entreprise. 46% des sociétés comptant entre 500 et 750 travailleurs ont des outils EDR dans le cadre de leur protection endpoint existante, alors que ce taux ne s’élève qu’à 28% pour les organisations ayant moins de 250 travailleurs. Les PME peuvent également s’exposer à des risques en sous-estimant l’importance d’EDR. Généralement 7% des entreprises belges ou néerlandaises pensent que les capacités EDR sont inutiles. Or si l’organisation compte moins de 250 travailleurs, le pourcentage augmente à une entreprise sur cinq (18%).

Jusqu’à présent, des recherches efficaces et les réponses aux incidents ont été accessibles dans les organisations disposant d’un centre de gestion de la sécurité (CGS) spécialisé ou d’une équipe de sécurité IT formée pour rechercher et analyser les cyberattaques. Avec Sophos Intercept X Advanced équipée d’EDR, toutes les entreprises, quelles que soient leur taille et leurs ressources, pourront ajouter la chasse aux menaces et disposer des capacités d’un CGS pour garantir leur sécurité. Ainsi les pirates informatiques criminels pourront se cacher beaucoup moins longtemps dans leur réseau.

**De multiples opportunités pour les pirates informatiques**Actuellement les possibilités pour les criminels informatiques sont légion, et dès qu’ils ont trouvé un point d’entrée, ils font appel à de multiples méthodes d’attaque pour intensifier leurs privilèges et avancer progressivement. Une étude de Sophos a démontré qu’un tiers des entreprises (34%), ont besoin de plusieurs jours, voire de mois pour corriger la situation, malgré qu’un tiers des sociétés reçoive un correctif/une mise-à-jour quotidiennement. Le résultat net est que les endpoints sont exposés aux cybercriminels qui peuvent entrer et circuler librement dans le réseau.

Avec Intercept X Advanced pourvue d’EDR, les managers IT peuvent voir dans Intercept X si un pirate bouge de façon latérale, et optimiser ainsi les programmes de protection et les capacités anti-exploitation. Intercept X est la solution de prévention endpoint la plus sophistiquée dans ce secteur d’activités. Sophos Intercept X avec EDR est intégrée dans Sophos Central, une console de gestion uniforme dans le nuage pour tous les produits de Sophos. Elle permet aux utilisateurs finaux et aux Managed Security Partners de prendre des décisions basées sur l’intelligence EDR à partir d’un point unique.

En un seul clic, les managers IT auront accès, sur demande, à l’intelligence conservée par SophosLabs, à des recherches accompagnées d’actions suspectes et à des étapes ultérieures recommandées. Pour avoir une vue globale sur toutes les menaces possibles et dans un souci de trouver toutes les nouveautés en matière de piratage informatique, SophosLabs dépiste, démantèle et analyse 400.000 attaques de maliciels uniques et inédites par jour. En ayant accès aux données du SophosLab, les managers IT de tous les niveaux bénéficieront dorénavant des dernières nouvelles en criminalistique à portée de main pour déterminer si une attaque a lieu et quelle en est la nature.

Erik Farine, directeur régional Benelux chez Sophos témoigne : « L’incidence énorme de maliciels, la fréquence des attaques et la facilité d’accès à des outils sur le dark web rendent les capacités EDR indispensables à chaque entreprise-surtout à celles ayant peu de ressources de sécurité IT. Sophos offre l’équivalent d’une équipe entière d’experts en cyber-sécurité et l’accès à la riche base de connaissance dont SophosLabs dispose concernant la réputation des fichiers et d’autres informations recueillies par le biais de téraoctets d’analyses de programmes malveillants. Les managers IT pourront désormais dépister et analyser rapidement les voies des attaques sans faire appel à la rétro-ingénierie des fichiers.

Intercept X Advanced avec le programme d’accès rapide EDR est accessible à tous. Plus de 300 organisations se sont déjà enregistrées. Pour rejoindre le programme et la communauté, visitez le programme d’accès rapide Sophos.

*Lisez les dernières nouvelles à propos de la sécurité et les avis sur notre Naked Security News primé et apprenez plus à propos Sophos sur notre Sophos News Channel.*

*Protégez chaque Mac et PC à votre domicile avec la nouvelle génération de logiciel internet gratuit et géré de façon centralisée, Sophos Home.*

***Connectez-vous avec Sophos où que vous soyez :***Twitter, LinkedIn, Facebook, Spiceworks, YouTube, Google+

**A propos de la recherche**L’étude a été menée par Sapio Research en utilisant des interviews en ligne en août et septembre 2018 auprès de 151 responsables IT dans des entreprises belges (50) et néerlandaises (101).

**Au sujet de Sophos**Sophos est un leader dans la sécurité Next-Generation des systèmes Endpoint et des réseaux. En tant que pionnier en matière de sécurité synchronisée, Sophos développe son offre innovante qui comprend des solutions pour les systèmes Endpoint, les réseaux, le chiffrement, le web, les emails et les mobiles, afin de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 39 000 partenaires enregistrés. Le siège social de Sophos se situe à Oxford (Royaume-Uni), et Sophos a été introduit à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts Presse :**Sandra Van Hauwaert, Square Egg, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816