SOPHOS

Cinq raisons de choisir l'EDR

Les outils EDR (Endpoint Detection and Response) sont conçus pour complémenter la sécurité Endpoint en renforçant les capacités de détection, d'investigation et de réponse. Cependant, l'engouement suscité autour des outils EDR peut brouiller le message sur la manière de les utiliser et la raison de leur nécessité. Pour ne rien arranger, de nombreuses entreprises ont souvent des difficultés à voir la valeur ajoutée des solutions EDR, car celles-ci peuvent être difficiles à utiliser, limitées en capacité de protection et gourmandes en ressources.

Sophos Intercept X with EDR intègre dans une seule solution la fonctionnalité intelligente EDR avec la protection Endpoint et Serveur la mieux notée de l'industrie, ce qui en fait le moyen le plus facile pour les entreprises de relever les défis des menaces actuelles les plus complexes. Nous vous présentons ici les 5 principales raisons d'envisager une solution EDR.

Maintenir l'hygiène des opérations de sécurité IT et débusquer les menaces furtives

Selon les entreprises, le personnel chargé des opérations informatiques et celui chargé de la sécurité informatique peuvent soit faire partie de la même équipe, soit travailler de manière indépendante, soit encore être la même personne. Quelle que soit la configuration, un outil EDR doit pouvoir fournir des exemples d'utilisation différents pour ces deux domaines. Il doit être capable d'effectuer ces deux types de tâches et rester accessible sans compromettre la puissance.

Pour l'administrateur informatique, il est essentiel de maintenir le parc de l'entreprise en bonne santé. Il doit trouver les machines présentant des problèmes de performance, tels qu'un faible espace disque ou une forte utilisation de la mémoire, localiser les appareils dotés de programmes vulnérables qui ont besoin d'être corrigés, ou encore identifier les postes et les serveurs ayant des protocoles RDP activés inutilement ou dont les comptes invités sont toujours actifs. Sophos EDR donne aux administrateurs les outils permettant d'extraire les informations nécessaires pour répondre à toutes ces questions, et bien d'autres encore. Il offre aussi la possibilité d'accéder à distance aux appareils pour corriger les failles de sécurité en analysant les problèmes de performances, installant des correctifs et désactivant les protocoles RDP et les comptes invités.

Les spécialistes de la cybersécurité doivent pouvoir débusquer les menaces subtiles et évasives qui ne sont pas automatiquement identifiées par la protection Endpoint. Leur outil EDR doit repérer efficacement les indicateurs de compromission (IoC). Il doit par exemple identifier les processus qui tentent de se connecter sur des ports non standard, ceux qui ont modifié des fichiers ou des clés de registre, ceux qui se font passer pour autre chose, ou repérer les employés qui ont cliqué sur un lien dans un email de phishing. Sophos EDR permet de réaliser rapidement ce type d'investigation sur l'ensemble du parc informatique de l'entreprise. Il est ensuite tout aussi facile d'accéder à distance à un appareil pour l'examiner en profondeur, déployer des outils d'analyse et arrêter des processus suspects.

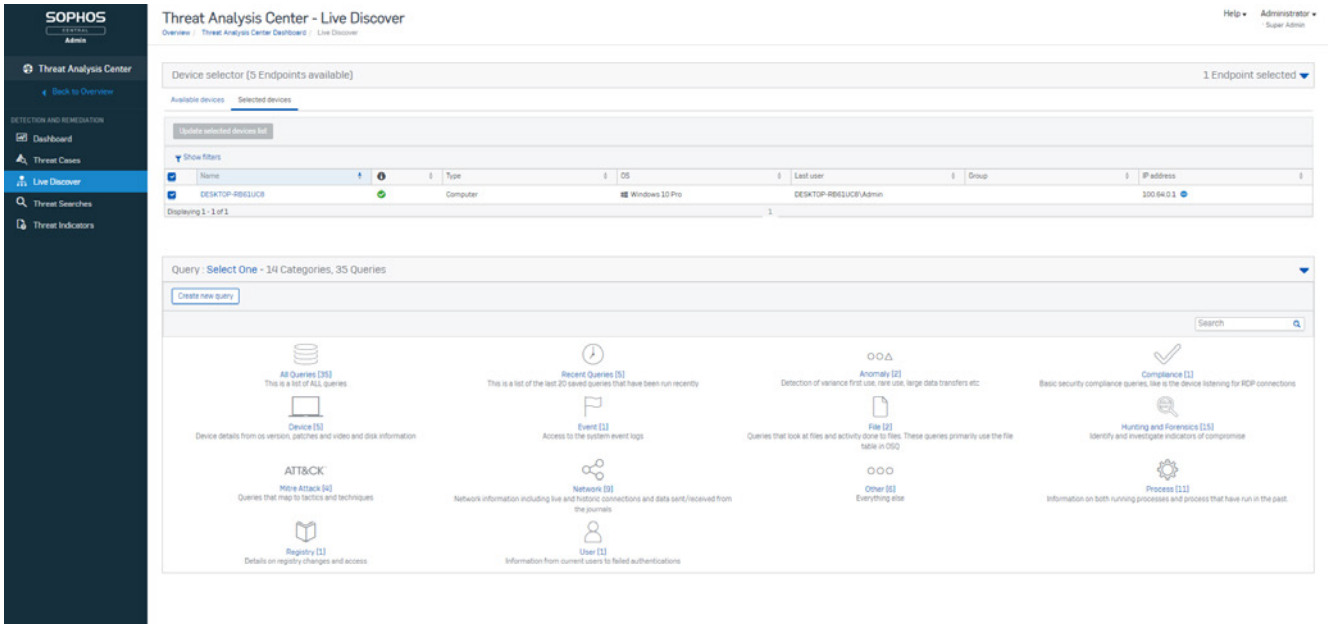

Figure 1 : Sophos Intercept X with EDR permet aux utilisateurs de lancer des requêtes détaillées pour obtenir des informations sur l'ensemble de leur parc

Détecter les attaques passées inaperçues

Quand il s'agit de cybersécurité, même les outils les plus avancés peuvent être piratés si les attaquants disposent de suffisamment de temps et de ressources, ce qui complique davantage la détection des attaques. Les entreprises se reposent entièrement sur la prévention pour rester protégées. Bien que cela soit primordial, l'EDR offre quant à lui un niveau supplémentaire de capacités de détection afin de trouver les incidents restés inaperçus.

Les entreprises peuvent ainsi exploiter l'EDR pour détecter des attaques en recherchant des indicateurs de compromission (IoC). C'est une manière simple et rapide de traquer toute attaque passée au travers des mailles de la protection. Le processus de recherche des menaces est souvent utilisé après un signalement par des entités de recherche tierces. Par exemple, une agence gouvernementale (comme US-CERT, CERT-UK ou CERT Australia) peut informer une entreprise qu'elle a détecté une activité suspecte sur son réseau. Cette notification peut être accompagnée d'une liste d'indicateurs de compromission, qui pourront être utilisés comme un point de départ pour déterminer ce qui est en train de se passer.

La fonction « Indicateurs de menaces » dans Intercept X fournit une liste des principaux événements suspects, pour que les analystes sachent exactement ce qu'ils doivent examiner. En faisant appel aux capacités de Machine Learning des SophosLabs, les principaux événements suspects sont présentés et classés dans une liste en fonction de leur score de menace. Cela permet aux analystes de prioriser leurs tâches et de se concentrer sur les événements les plus importants.

L'analyste sait ainsi par où commencer et peut retracer toutes les occurrences de cet objet suspect dans l'ensemble du parc, ce qui lui permet d'agir rapidement pour le nettoyer. De plus, il peut exploiter de puissantes requêtes SQL pour rechercher d'autres indicateurs de compromission, tels que les processus modifiant les clés de registre et ceux tentant de se connecter sur des ports non standard.

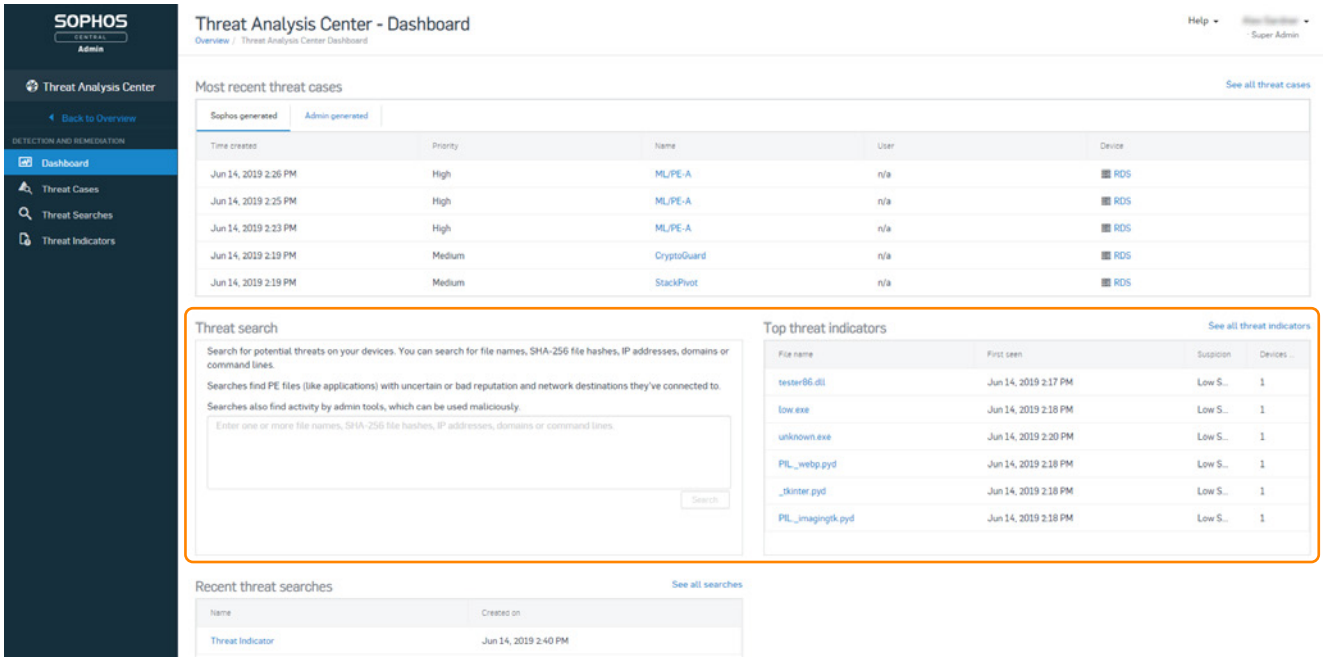

Figure 2 : Sophos Intercept X with EDR offre la capacité de chercher des indicateurs de compromission sur l'ensemble du réseau. Il fait aussi appel au Machine Learning pour identifier les principaux événements suspects qui doivent être analysés.

La capacité de lancer des requêtes détaillées combinée avec des conseils sur la manière de procéder et des informations sur les menaces facilite l'utilisation pour les administrateurs de Sophos EDR sans sacrifier la puissance ou la granularité.

Répondre plus rapidement aux incidents potentiels

Une fois les incidents détectés, les équipes IT s'efforcent généralement d'y remédier le plus rapidement possible afin de réduire le risque de propagation des attaques et de limiter les dommages potentiels. Naturellement, la question la plus pertinente à se poser est de savoir comment se débarrasser de chaque menace respective. En moyenne, les équipes passent plus de 3 heures à essayer de remédier à chaque incident. L'EDR peut accélérer ce processus de manière significative.

Lors de la réponse aux incidents, la première mesure qu'un analyste peut prendre est d'empêcher la propagation d'une attaque. Intercept X with EDR isole à la demande les postes et les serveurs, ce qui est une étape clé pour empêcher la propagation des menaces dans l'environnement. C'est souvent la première chose que font les analystes avant de commencer leur investigation. Cela leur permet de gagner du temps pendant qu'ils déterminent la meilleure ligne de conduite à adopter.

En effet, le processus d'investigation peut parfois être long et difficile. Cela suppose bien sûr qu'une investigation soit menée. La réponse aux incidents repose traditionnellement en grande partie sur des analystes hautement qualifiés. La plupart des outils EDR s'appuient également en grande partie sur les analystes pour savoir quelles questions poser et comment interpréter les réponses. Cependant, avec Intercept X with EDR, les investigations guidées permettent aux équipes de sécurité de tous niveaux de répondre rapidement aux incidents de sécurité, grâce aux instructions contextuelles qui offrent une suggestion d'étapes à suivre, des représentations visuelles claires des attaques et une expertise intégrée.

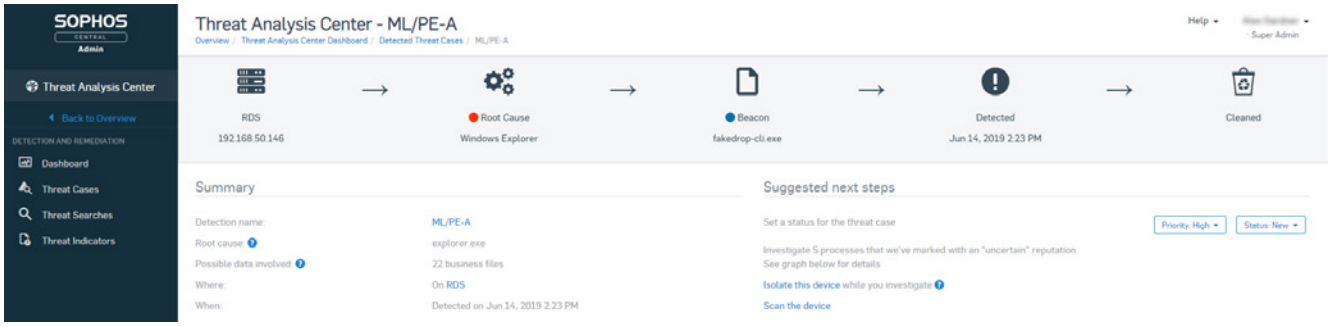

Figure 3 : La réponse guidée aux incidents propose une suggestion d'étapes à suivre et l'isolement à la demande des postes, afin de résoudre les incidents rapidement et en toute sécurité.

Sophos EDR permet aussi d'accéder à distance aux appareils via une interface de ligne de commande. C'est idéal pour pouvoir agir rapidement, lorsque l'employé n'est pas présent physiquement au bureau. En accédant à l'appareil, les administrateurs peuvent effectuer des recherches supplémentaires en déployant des outils d'analyse, installer/désinstaller des logiciels, arrêter des processus et redémarrer l'appareil.

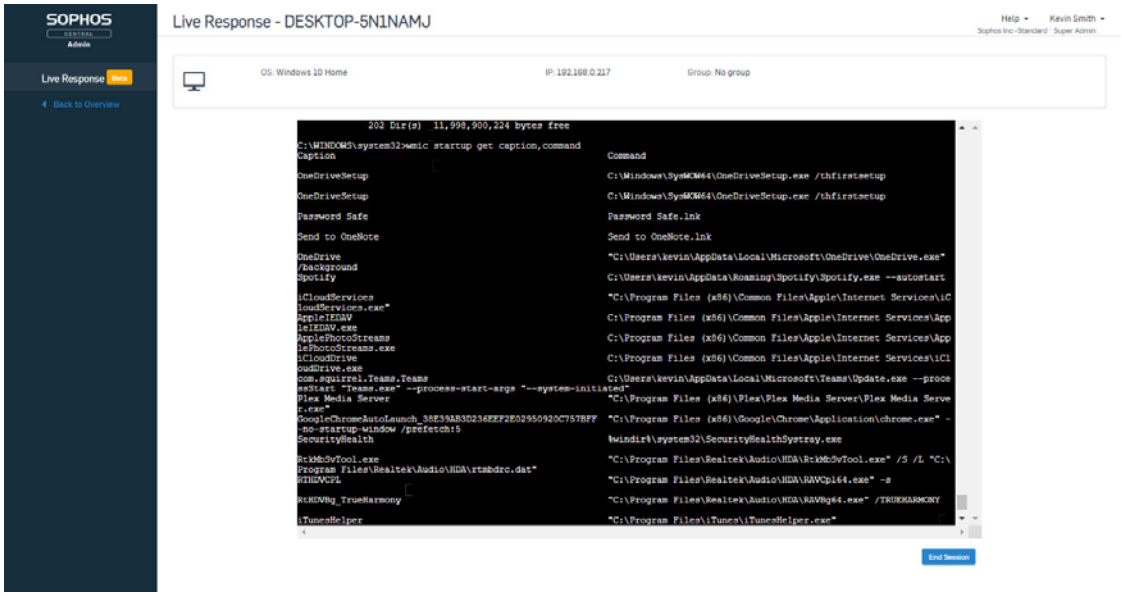

Figure 4 : Intercept X with EDR contient de nombreux boutons d'action offrant un grand choix d'options de remédiation, dont la plus courante est « Nettoyer et bloquer ».

Ajouter de l'expertise, pas des ingénieurs

De manière générale, les entreprises souhaitant ajouter des capacités EDR invoquent les « compétences du personnel » comme principal obstacle à leur adoption. Cela n'est pas très surprenant, car la pénurie de professionnels qualifiés dans le domaine de la cybersécurité est un problème récurrent depuis plusieurs années. Cet état de fait est particulièrement marquant dans les petites entreprises.

Principales raisons freinant l'utilisation de l'EDR par les entreprises

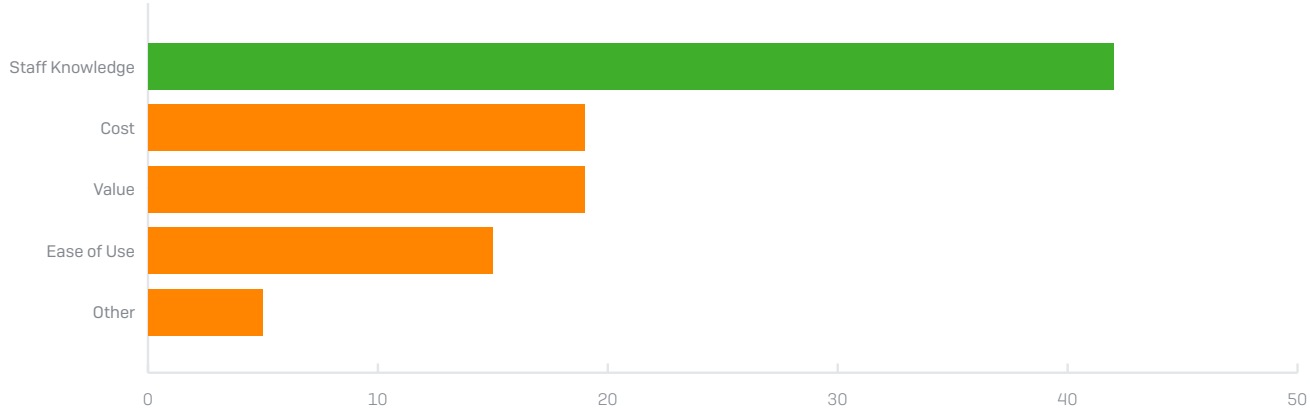

Figure 5 : Le manque de compétences du personnel est la principale raison invoquée par les entreprises pour expliquer pourquoi elles n'ont pas adopté de solution EDR. (Source : Étude Sapio en collaboration avec Sophos, octobre 2018)

Pour combler le manque de compétences du personnel, Intercept X avec EDR reproduit les capacités d'analyse des ingénieurs qualifiés. Il exploite le Machine Learning pour intégrer des connaissances approfondies en matière de sécurité et s'enrichit de l'intelligence sur les menaces des SophosLabs, ce qui permet d'ajouter de l'expertise sans avoir besoin d'ajouter du personnel. Les capacités intelligentes de l'EDR aident à combler les lacunes dues au manque de compétences du personnel, reproduisant les fonctions de plusieurs types d'analystes :

- Analystes de la sécurité : Il s'agit des analystes de première ligne chargés de trier les incidents et de déterminer quelles alertes doivent être traitées immédiatement. Dans l'idéal, ils sont également capables de rechercher de manière proactive toute attaque qui serait passée inaperçue. Intercept X with EDR détecte et priorise automatiquement les menaces. Grâce au Machine Learning, les événements suspects sont identifiés et un score de menace leur est attribué. Les événements dont le score est le plus élevé sont ceux qui méritent une attention immédiate. Les analystes peuvent rapidement déterminer où concentrer leur attention et commencer leur investigation.
- Analystes de malwares : Les entreprises peuvent s'appuyer sur des experts en malwares spécialisés dans l'analyse des fichiers suspects par rétro-ingénierie. Cette approche est non seulement chronophage et difficile à réaliser, mais elle suppose un niveau de sophistication en cybersécurité que la plupart des entreprises ne possèdent pas. Les analystes de malwares sont nécessaires pour décider si un fichier qui n'a pas été bloqué est réellement malveillant. Ils peuvent aussi vérifier les fichiers identifiés comme suspects, mais pouvant être de simples faux positifs. Intercept X with EDR offre une meilleure approche de l'analyse des malwares grâce au Machine Learning. Grâce au moteur de détection des malwares le plus performant du marché, les malwares sont automatiquement analysés dans les moindres détails, en décomposant les attributs des fichiers et les composants du code, puis en les comparant à des millions d'autres fichiers. Les analystes peuvent facilement identifier les attributs et segments de code similaires aux fichiers de « bonne réputation » ou de « mauvaise réputation », afin de déterminer si un fichier doit être bloqué ou autorisé.
- Analystes de l'intelligence sur les menaces : Les investigations peuvent s'appuyer sur l'intelligence sur les menaces fournie par des organisations tierces (souvent à un coût supplémentaire) pour mieux comprendre les menaces et le contexte dans lequel elles s'inscrivent. Des analystes sont nécessaires pour interpréter et intégrer ces données afin de s'assurer qu'elles apportent une valeur ajoutée. L'intelligence sur les menaces peut servir de point de départ aux

investigations, de moyen de solliciter l'avis de la communauté sur un fichier suspect ou de déterminer si une attaque vise l'entreprise. Intercept X with EDR offre aux administrateurs IT et de sécurité la possibilité de recueillir davantage d'informations en ayant accès à la demande à l'intelligence sur les menaces des SophosLabs. Pour maintenir une visibilité totale sur le panorama des menaces, les SophosLabs suivent, déconstruisent et analysent chaque jour 400 000 attaques de malwares uniques et inédits, à la recherche constante des techniques d'attaque les plus récentes et les plus avancées. Cette intelligence est recueillie, regroupée et résumée pour en faciliter l'analyse, afin que les équipes n'ayant pas d'analystes dédiés ou n'ayant pas accès à des flux de données sur les menaces puissent bénéficier des recherches de l'une des meilleures équipes en cybersécurité dans le monde.

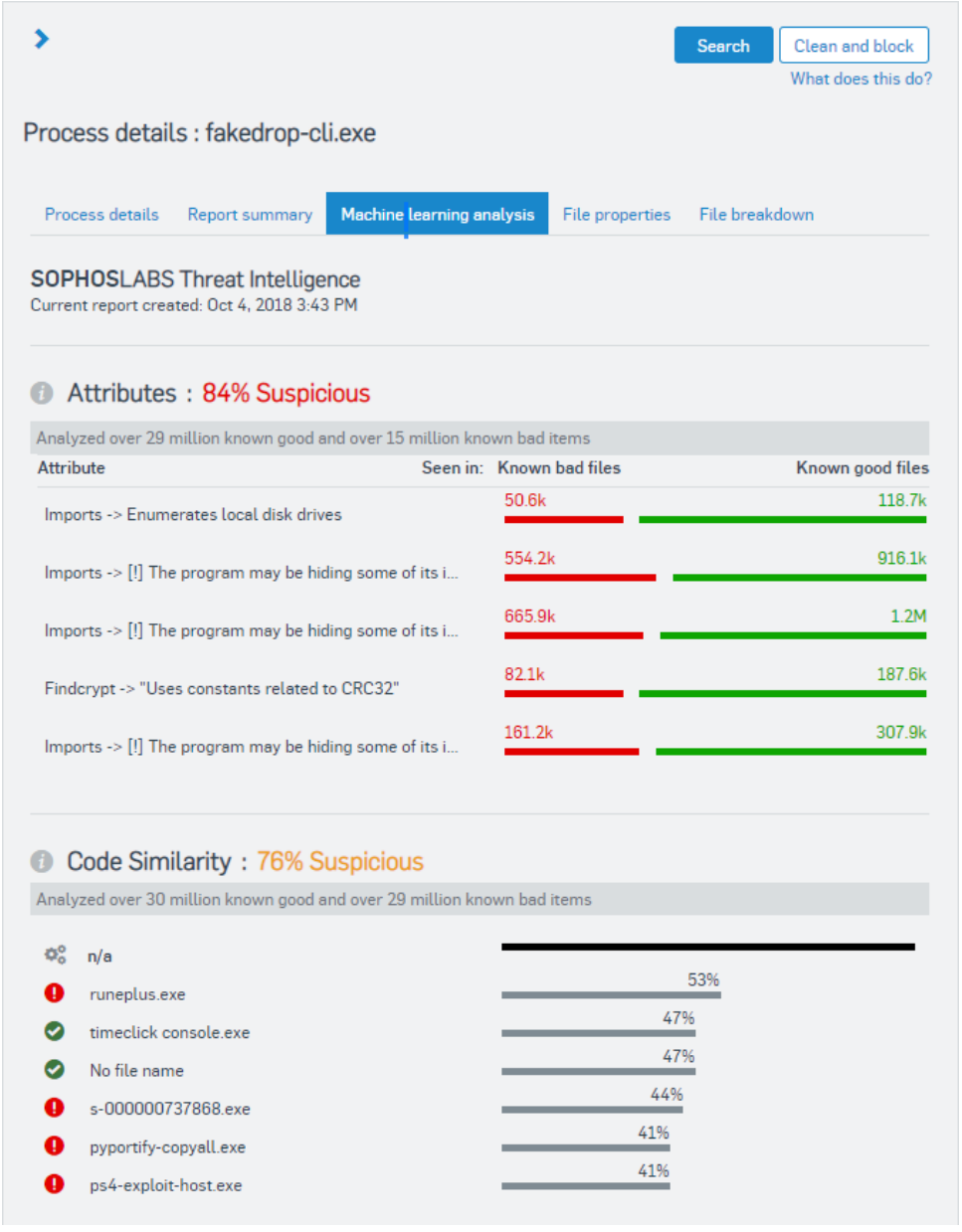

Figure 6 : L'analyse par Machine Learning affiche les attributs, les similarités de code et le chemin du fichier, pour une analyse simple, mais puissante.

Managed Threat Response (MTR)

Vous souhaitez être assisté pour gérer l'EDR ? Le service MTR de Sophos fusionne technologie et analyse d'experts pour améliorer la recherche et la détection des menaces, l'investigation approfondie des alertes et les actions ciblées afin de répondre aux menaces.

Comprendre comment une attaque s'est produite et empêcher que cela ne se reproduise

La hantise des analystes de la sécurité est d'être victimes d'une attaque et de devoir rendre des comptes à leur supérieur sans pouvoir leur donner d'explications. Identifier et supprimer les fichiers malveillants résout le problème une fois l'attaque identifiée, mais cela ne permet pas de savoir comment ils sont arrivés là ou ce que l'attaquant a fait avant que celle-ci ne soit bloquée.

La fonctionnalité « Dossiers Menaces », incluse dans Intercept X with EDR, met en lumière tous les événements qui ont conduit à une détection, ce qui permet de comprendre facilement quels fichiers, processus et clés de registre ont été touchés par le malware et de déterminer l'impact d'une attaque. Elle fournit une représentation visuelle de l'ensemble de la chaîne d'attaque, assurant la fiabilité du rapport et détaillant la manière dont l'attaque a commencé et où l'attaquant est allé. Plus important encore, en comprenant la cause profonde d'une attaque, l'équipe d'informaticiens sera beaucoup plus à même de l'empêcher de se reproduire.

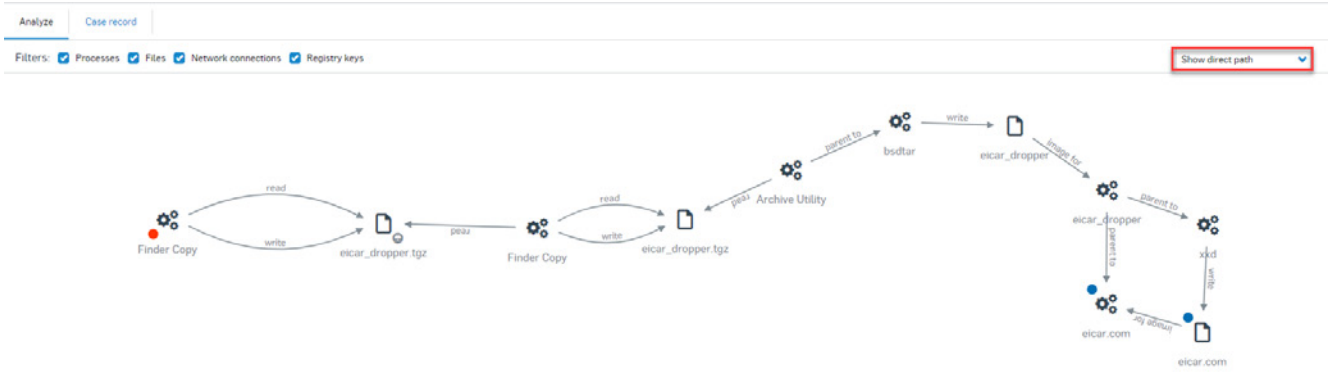

Figure 7 : La fonctionnalité « Dossiers Menace » fournit une représentation visuelle de l'ensemble de la chaîne d'attaque.

Visibilité sur l'ensemble votre environnement de cybersécurité

Sophos offre à la fois des capacités EDR et XDR (Extended Detection and Response), ce qui vous donne une visibilité inégalée sur vos endpoints et serveurs, ainsi que sur les données du réseau et de la messagerie. Vous pouvez rapidement passer d'une vue d'ensemble de votre environnement à une vue granulaire des domaines qui vous intéressent. Il complémente ainsi une protection de pointe qui stoppe les dernières menaces telles que les ransomwares, bloque les techniques utilisées par les exploits et neutralise les hackers.

Découvrez-en plus et démarrez votre évaluation gratuite à la page sophos.fr/interceptx

Essayez-le dès aujourd'hui

Demandez une évaluation gratuite de 30 jours sur **sophos.fr/intercept-x**

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

2021-04-19 (MP)

SOPHOS