SOPHOS

Las cinco principales razones por las que necesita EDR

Las herramientas de detección y respuesta para endpoints (EDR) están diseñadas para complementar la seguridad de endpoints con mayores funciones de detección, investigación y respuesta. Sin embargo, el revuelo que rodea a las herramientas de EDR puede hacer que resulte difícil comprender cómo se pueden utilizar exactamente y por qué son necesarias. Para colmo, a las soluciones de EDR actuales a menudo les cuesta proporcionar valor a muchas empresas, ya que pueden ser difíciles de usar, carecen de suficientes funciones de protección y consumen muchos recursos.

Sophos Intercept X with EDR integra la detección y respuesta inteligentes para endpoints con la mejor protección de endpoints y servidores del sector en una única solución, siendo la forma más fácil para las empresas de responder a las difíciles preguntas sobre incidentes de seguridad. He aquí algunas razones adicionales para considerar una solución EDR.

Mantenga la higiene de las operaciones de seguridad TI y detecte las amenazas furtivas

Dependiendo de la empresa, el personal de operaciones de TI y de seguridad TI puede formar parte del mismo equipo, funcionar de forma independiente o incluso tratarse de la misma persona. Sea cual sea el sistema, las dos áreas requieren distintos casos de uso de una herramienta EDR, de modo que esa herramienta debe ser capaz de realizar ambos grupos de tareas y permanecer accesible sin comprometer la potencia.

Para el administrador de las operaciones de TI, mantener la infraestructura de la empresa en buen estado es fundamental. Por ejemplo, detectar equipos con problemas de rendimiento, como la falta de espacio en disco o un uso de memoria excesivo; buscar dispositivos que tengan programas vulnerables que requieren parches, y localizar endpoints y servidores que tengan el RDP habilitado sin ser necesario o que aún tengan cuentas de invitado activadas. Sophos EDR brinda a los administradores las herramientas necesarias para formular todas estas preguntas y muchas más, así como la capacidad de acceder de forma remota a los dispositivos para cerrar brechas de seguridad mediante la investigación de problemas de rendimiento, la instalación de parches y la desactivación del RDP y las cuentas de invitado.

Los especialistas en ciberseguridad deben poder detectar aquellas amenazas esquivas que no logre descubrir su sistema de protección para endpoints. Su herramienta EDR debe ser eficaz a la hora de rastrear indicadores de peligro (IOC), por ejemplo, identificar procesos que intentan conectarse a puertos no estándar, procesos que tienen archivos o claves de registro modificados y procesos que se hacen pasar por otros, así como detectar qué empleados han hecho clic en un enlace de un correo electrónico de phishing. Con Sophos EDR, resulta sencillo realizar este tipo de investigaciones rápidamente en toda la infraestructura de la empresa. Y, posteriormente, es igual de fácil acceder remotamente a un dispositivo específico para investigarlo más a fondo, desplegar herramientas forenses y finalizar procesos sospechosos.

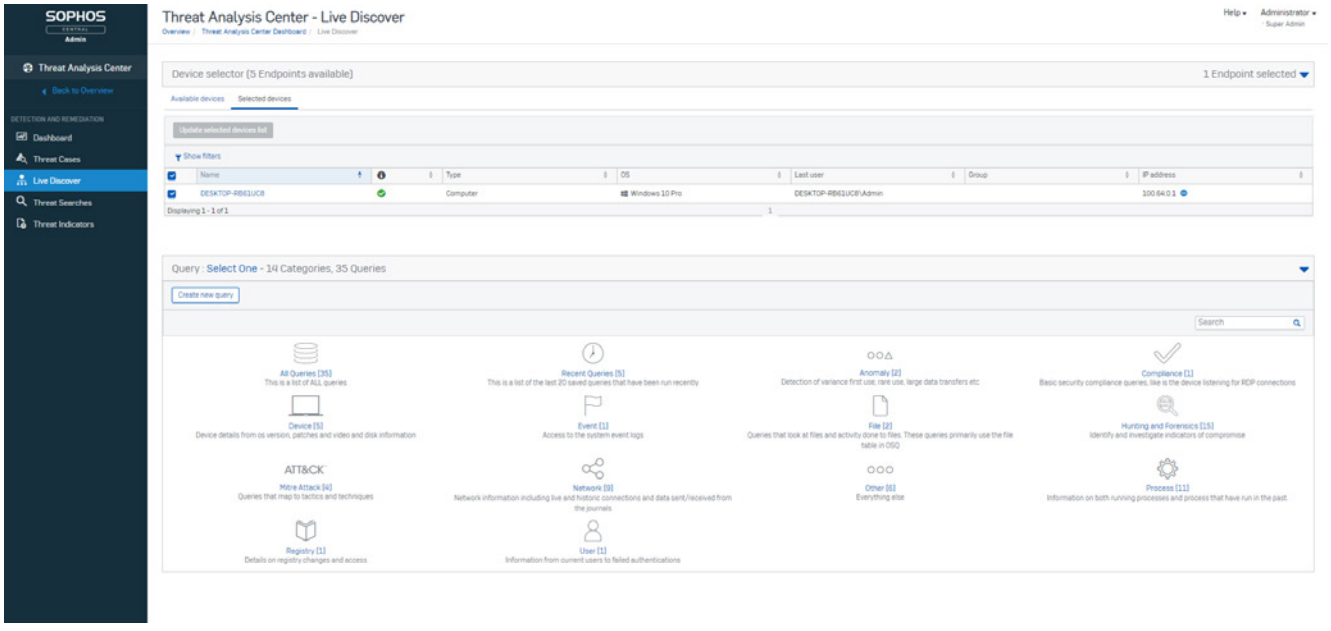


Figura 1: Sophos Intercept X with EDR permite a los usuarios formular preguntas detalladas en toda su infraestructura

Detecte ataques que han pasado desapercibidos

Cuando se trata de ciberseguridad, incluso las herramientas más avanzadas pueden ser derrotadas con tiempo y recursos suficientes, lo que complica entender realmente cuándo se producen los ataques. Las empresas a menudo dependen únicamente de la prevención para mantenerse protegidas, y aunque la prevención es fundamental, la EDR ofrece otra capa de funciones de detección para poder dar con incidentes que han pasado desapercibidos.

Las empresas pueden utilizar la EDR para detectar ataques mediante la búsqueda de indicadores de peligro (IOC). Es una manera rápida y directa de dar caza a ataques que pueden haberse pasado por alto. Las búsquedas de amenazas se inician a menudo tras una notificación de información sobre amenazas de terceros: por ejemplo, una agencia gubernamental (como US-CERT, CERT-UK o CERT Australia) puede informar a una empresa de que hay actividad sospechosa en su red. La notificación puede ir acompañada de una lista de IOC, que puede utilizarse como punto de partida para determinar qué está sucediendo.

La función Indicadores de amenazas de Intercept X proporciona la lista de los principales eventos sospechosos a fin de que los analistas sepan exactamente qué deben investigar. Al aprovechar las funciones de Machine Learning de SophosLabs, se presenta una lista de los eventos más sospechosos, clasificados por su puntuación de peligro. Esto facilita a los analistas priorizar sus cargas de trabajo y centrarse en los eventos más importantes.

Al saber dónde tiene que empezar, el analista puede rastrear todas las instancias de ese elemento sospechoso en toda la infraestructura y tomar medidas rápidamente para limpiarlo. Asimismo, puede servirse de potentes consultas SQL para buscar otros indicadores de peligro, como procesos que modifican claves del registro o procesos que intentan conectarse a puertos no estándar.

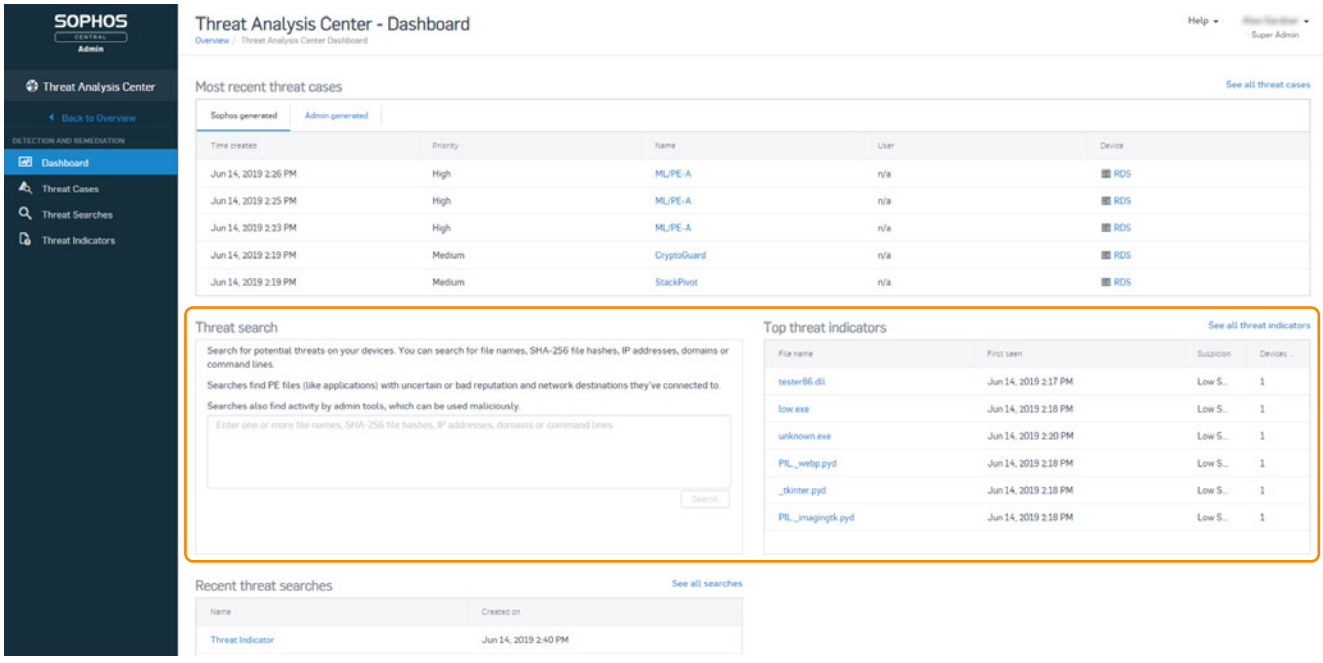


Figura 2: Sophos Intercept X with EDR ofrece la posibilidad de buscar indicadores de peligro en toda la red. También se sirve del Machine Learning para determinar los principales eventos sospechosos que deben investigarse.

Gracias a la capacidad de formular preguntas detalladas, la orientación para saber dónde empezar y la información sobre amenazas gestionada, los administradores no tienen que renunciar a ninguna ventaja y se benefician de la facilidad de uso de Sophos EDR sin sacrificar potencia ni granularidad.

Responda a incidentes potenciales con mayor rapidez

Una vez que se detectan los incidentes, los equipos de TI y de seguridad suelen afanarse por remediarlos lo más rápido posible para reducir el riesgo de que los ataques se propaguen y limitar cualquier daño potencial. Naturalmente, la pregunta más pertinente es cómo deshacerse de cada amenaza. De media, los equipos de seguridad y de TI dedican más de tres horas a tratar de remediar cada incidente. La EDR puede agilizar este proceso significativamente.

El primer paso que podría dar un analista durante el proceso de respuesta a incidentes sería detener la propagación de un ataque. Intercept X with EDR aísla los endpoints y servidores a demanda, lo cual es un paso clave para evitar que una amenaza se extienda por todo el entorno. Los analistas a menudo hacen esto antes de investigar, ganando tiempo mientras determinan el mejor modo de proceder.

El proceso de investigación puede ser lento y complicado. Por supuesto, esto supone que se lleva a cabo una investigación. Tradicionalmente, la respuesta a los incidentes depende en gran medida de analistas humanos altamente cualificados. La mayoría de las herramientas de EDR también dependen en gran parte de los analistas para saber qué preguntas hacer y cómo interpretar las respuestas. Sin embargo, con Intercept X with EDR, los equipos de seguridad de todos los niveles de cualificación pueden responder rápidamente a los incidentes de seguridad gracias a las investigaciones guiadas que ofrecen sugerencias de los pasos que se deben dar, representaciones visuales claras de los ataques y experiencia integrada.

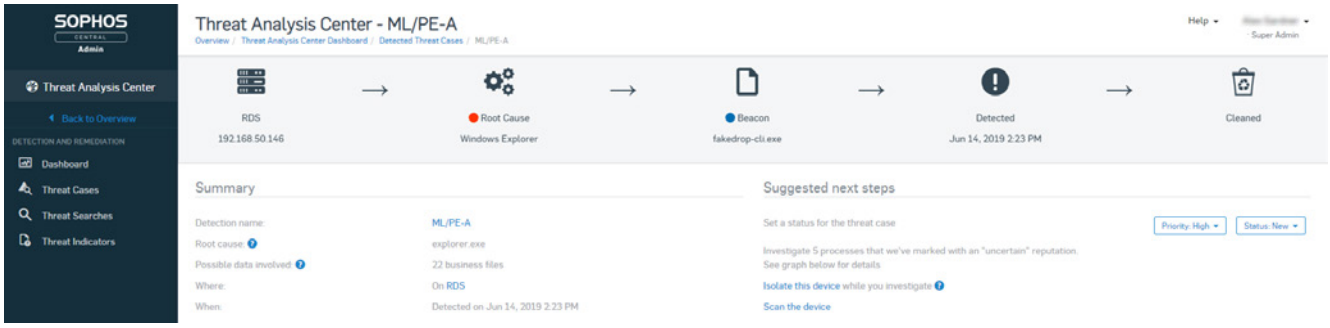
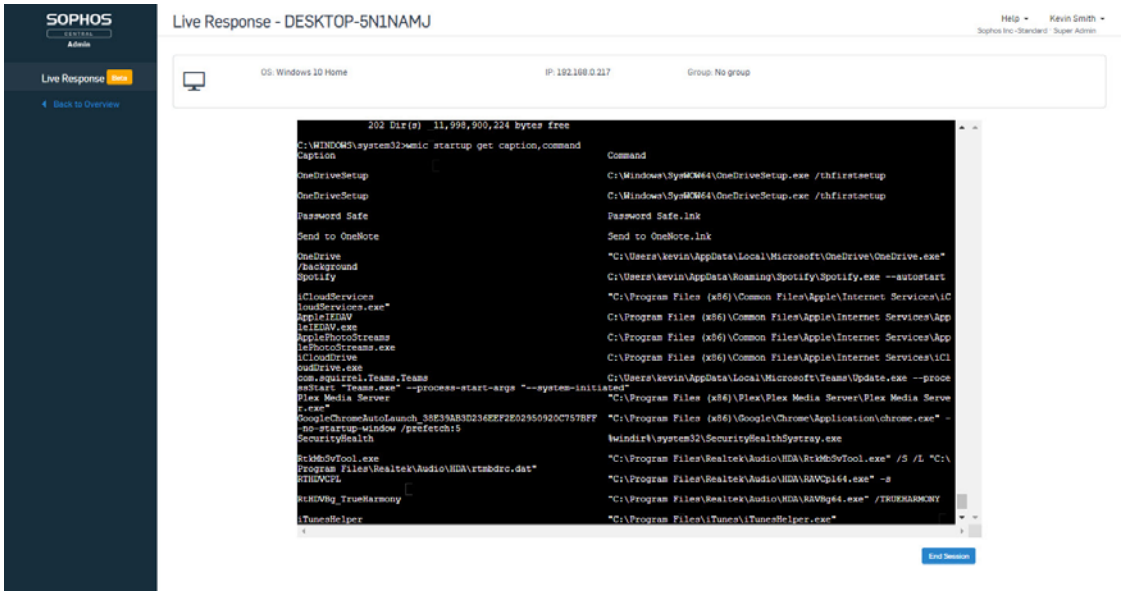


Figura 3: la respuesta guiada a incidentes ofrece sugerencias sobre los siguientes pasos que dar y el aislamiento de los endpoints a demanda para resolver los incidentes de forma rápida y segura.

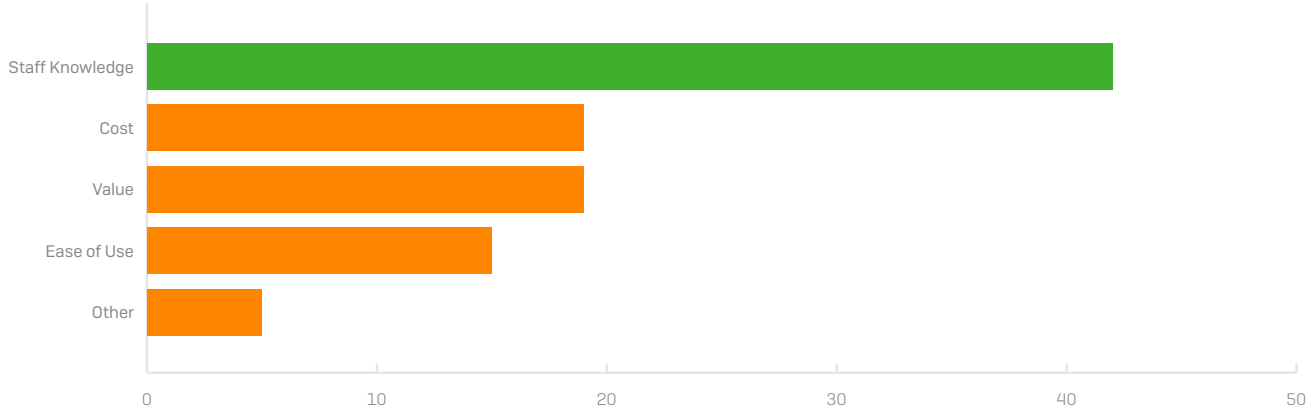
Sophos EDR también ofrece la capacidad de acceder de forma remota a los dispositivos a través de una interfaz de línea de comandos. Es ideal para una respuesta rápida, incluso si el empleado no se encuentra en la oficina. Tras acceder al dispositivo, el administrador puede realizar más investigaciones desplegando herramientas forenses, instalar y desinstalar software, finalizar procesos y reiniciar el dispositivo.



Figuras 4: los botones de acción de Intercept X with EDR ofrecen múltiples opciones de remediación, siendo «limpiar y bloquear» la más común.

Añada experiencia, no personal

Por un amplio margen, las empresas que desean añadir funciones de detección y respuesta para endpoints citan los «conocimientos del personal» como el principal impedimento para adoptar la EDR. Esto no debería ser una gran sorpresa, ya que la carencia de talento para encontrar profesionales cualificados en ciberseguridad se ha debatido ampliamente durante varios años. Esta barrera es especialmente pronunciada en las empresas más pequeñas.



Principales razones por las que las empresas no han implementado la EDR

Figura 5: los conocimientos del personal fueron citados como la razón principal por la que las empresas no han adoptado una solución de detección y respuesta para endpoints (EDR) (Fuente: Estudio de Sapio en colaboración con Sophos, octubre de 2018)

Para combatir la falta de conocimientos del personal, Intercept X with EDR replica las capacidades asociadas a los analistas tan difíciles de encontrar. Aprovecha el Machine Learning para integrar una visión profunda de la seguridad y se optimiza con la información sobre amenazas que mantiene SophosLabs, de modo que pueda añadir experiencia sin tener que añadir personal. Las capacidades de detección y respuesta inteligentes para endpoints ayudan a subsanar las carencias causadas por la falta de conocimientos del personal, reproduciendo las funciones de varios tipos de analistas:

- Analistas de seguridad: Estos son los analistas de primera línea a los que se ha encomendado la tarea de detectar los incidentes y determinar qué alertas deben abordarse de inmediato. Preferiblemente, también son capaces de detectar de forma proactiva cualquier ataque que pueda haber pasado desapercibido. Intercept X with EDR detecta y prioriza automáticamente las posibles amenazas. Mediante el Machine Learning, se identifican los eventos sospechosos y se les da una puntuación de peligro. Los eventos con las puntuaciones más altas son los más importantes de forma inmediata. Los analistas pueden ver rápidamente dónde centrar su atención y empezar a investigar.
- Analistas de malware: Las empresas pueden confiar en expertos en malware especializados en ingeniería inversa de archivos sospechosos para analizarlos. Este enfoque no solo lleva mucho tiempo y es difícil de lograr, sino que supone un nivel de sofisticación de ciberseguridad que no tienen la mayoría de las empresas. Los analistas de malware son necesarios para decidir si un archivo que no ha sido bloqueado es realmente malicioso. También pueden analizar los archivos que han sido clasificados como maliciosos pero en realidad pueden ser falsos positivos. Intercept X with EDR ofrece un mejor enfoque para el análisis de malware al servirse del Machine Learning. Utilizando el mejor motor de detección de malware para endpoints de la industria, el malware se analiza automáticamente con extremo detalle, desglosando los atributos de los archivos y los componentes de código y comparándolos con millones de archivos. Los analistas pueden ver fácilmente qué atributos y segmentos de código son similares a los archivos "buenos conocidos" y "malos conocidos" para determinar si un archivo debe bloquearse o permitirse.
- Analistas de información sobre amenazas: Las investigaciones pueden basarse en información sobre amenazas de terceros (a menudo con un coste adicional) para añadir perspectiva y contexto a las amenazas. Se necesitan analistas que interpreten e integren estos datos para garantizar que añadan valor. La información sobre amenazas puede

utilizarse como punto de partida para las investigaciones, como medio para preguntar a la comunidad de seguridad qué piensa de un archivo sospechoso o para determinar si un ataque se dirige contra la empresa. Intercept X with EDR proporciona a los administradores de TI y de seguridad la capacidad de recopilar más información accediendo a la información sobre amenazas a demanda mantenida por SophosLabs. Para mantener una visibilidad completa sobre el panorama de amenazas, SophosLabs realiza el seguimiento, la deconstrucción y el análisis de 400 000 ataques de malware únicos y desconocidos cada día en una búsqueda constante de las técnicas de ataque más recientes y eficaces. Esta información sobre amenazas se recopila, agrega y resume para facilitar el análisis, de modo que los equipos que no cuentan con analistas de información de amenazas especializados ni acceso a servicios de información de amenazas costosos y difíciles de entender pueden beneficiarse de uno de los mejores equipos de investigación de ciberseguridad y ciencia de datos del mundo.

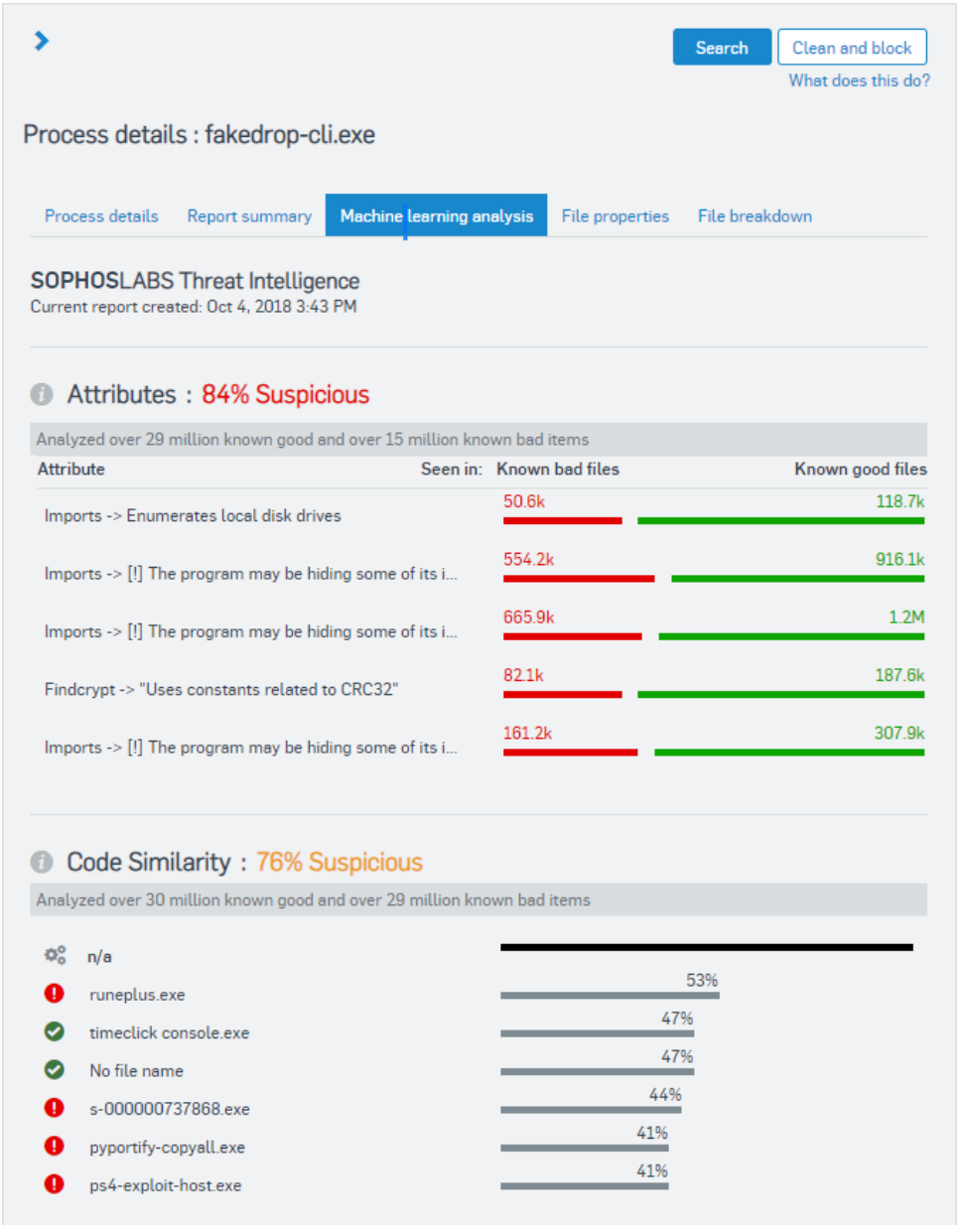


Figura 6: el análisis de Machine Learning muestra los atributos, la similitud de código y el análisis de la ruta de los archivos para ofrecer un análisis potente pero sencillo.

Managed Threat Response (MTR)

¿Necesita ayuda para gestionar la EDR? Sophos MTR fusiona la tecnología y el análisis de expertos para mejorar la búsqueda y la detección de amenazas, ofrecer una investigación más a fondo de las alertas y facilitar acciones concretas para responder a las amenazas.

Comprenda cómo ha ocurrido un ataque y cómo evitar que vuelva a ocurrir

Los analistas de seguridad tienen pesadillas recurrentes en las que han sufrido un ataque: un ejecutivo grita: «¿Cómo ha ocurrido esto?» y todo lo que pueden hacer es encogerse de hombros. Identificar y eliminar los archivos maliciosos resuelve el problema inmediato, pero no aclara cómo ha llegado allí en primer lugar ni qué ha hecho el atacante antes de que se bloqueara el ataque.

Los casos de amenazas, incluidos en Intercept X with EDR, destacan todos los eventos que han conducido a una detección, lo que facilita entender qué archivos, procesos y claves de registro ha tocado el malware para determinar el impacto de un ataque. Proporciona una representación visual de toda la cadena de ataque, lo que garantiza un informe seguro sobre cómo ha comenzado el ataque y hacia dónde se ha dirigido el atacante. Y lo que es más importante, al comprender la causa raíz de un ataque, es mucho más probable que el equipo de TI impida que vuelva a ocurrir.

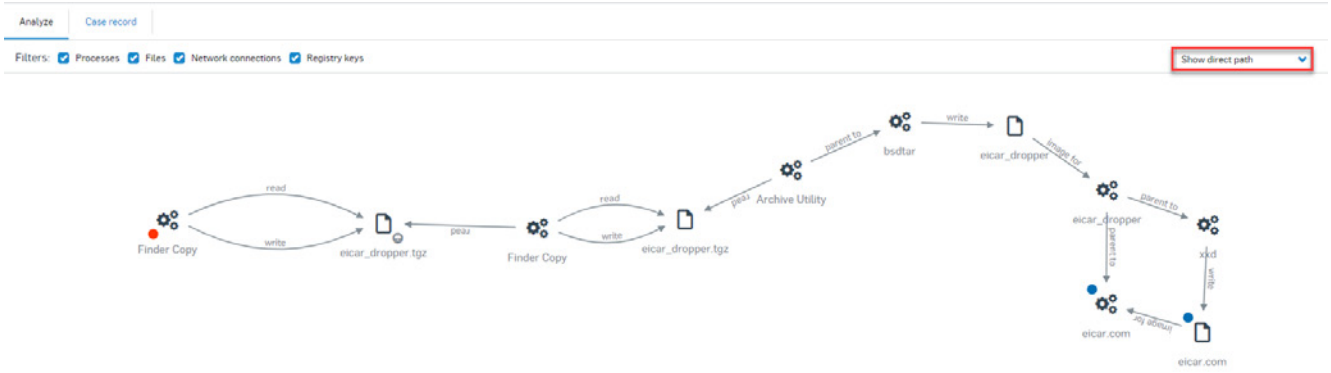


Figura 7: los casos de amenazas proporcionan una representación visual e interactiva de la cadena de ataque.

Visibilidad en toda la infraestructura para sus endpoints y servidores

Sophos ofrece EDR para Intercept X e Intercept X for Server, lo que le brinda una visibilidad sin precedentes en toda su infraestructura. Y esto además de una protección líder en el sector que detiene las amenazas más recientes como el ransomware, bloquea técnicas de explotación y frena a los hackers.

Obtenga más información e inicie una prueba gratuita en es.sophos.com/interceptx

Pruébelo gratis hoy mismo

Regístrese para conseguir una evaluación gratuita de 30 días en es.sophos.com/interceptx

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

2020-05-27 (MP)

SOPHOS