SOPHOS
Cybersecurity delivered.

# Introducción a la búsqueda de amenazas

**Guía práctica sobre cómo prepararse para buscar y neutralizar ciberamenazas esquivas**

Los ciberataques están evolucionando. Los adversarios están recurriendo cada vez más a métodos sofisticados y altamente evasivos para organizar y ejecutar sus ataques. Por lo tanto, la práctica de buscar y neutralizar actividad maliciosa se ha convertido en algo fundamental en la lucha contra estas amenazas avanzadas, aunque no es sencillo.

En este monográfico proporcionamos una guía que le permita iniciarse en la búsqueda de amenazas y un resumen de las herramientas y los marcos utilizados por los equipos de seguridad para mantenerse un paso por delante de las ciberamenazas más recientes y responder con rapidez a cualquier ataque potencial. También le daremos los cinco pasos que cualquier profesional de TI debe seguir en su preparación para la búsqueda de amenazas.

*Monográficos de Sophos. Agosto de 2022*

# El estado de las ciberamenazas en 2022

## Los ataques han experimentado un aumento en cuanto a su volumen, complejidad e impacto

El desafío que la ciberseguridad representa para las organizaciones no deja de crecer. Durante el último año, el 57 % de las organizaciones experimentó un aumento del volumen de los ciberataques, el 59 % vio aumentar la complejidad de los ataques y el 53 % afirmó que había aumentado su impacto. Casi tres de cada cuatro organizaciones (72 %) apreciaron un aumento en por lo menos una de estas áreas.

Una tendencia creciente es el aumento de los ataques a la cadena de suministro, como el incidente de SolarWinds revelado en marzo de 2021. Los atacantes insertaron instrucciones modificadas en el código fuente de su solución Orion, usada para administrar redes complejas de forma remota. Esta puerta trasera permitió a los adversarios acceder a las redes de los clientes de SolarWinds, incluidas varias agencias gubernamentales.

## El ransomware es una amenaza real para todas las organizaciones

El año pasado se vieron afectadas por el ransomware el 66 % de las organizaciones encuestadas, mientras que en 2020 fueron el 37 %. Esto representa un incremento del 78 % en el transcurso de un año, lo que demuestra que los adversarios se han vuelto considerablemente más capaces de ejecutar ataques a escala.

## El uso creciente de herramientas legítimas en los ciberataques

Los adversarios se aprovechan cada vez más de las copias ilegales o piratas de software comercial legítimo y de las herramientas gratuitas de código abierto. Normalmente, estas herramientas están diseñadas para simular ciberataques con el fin de mejorar la seguridad, aunque pueden ser explotadas por los criminales para justo lo contrario.

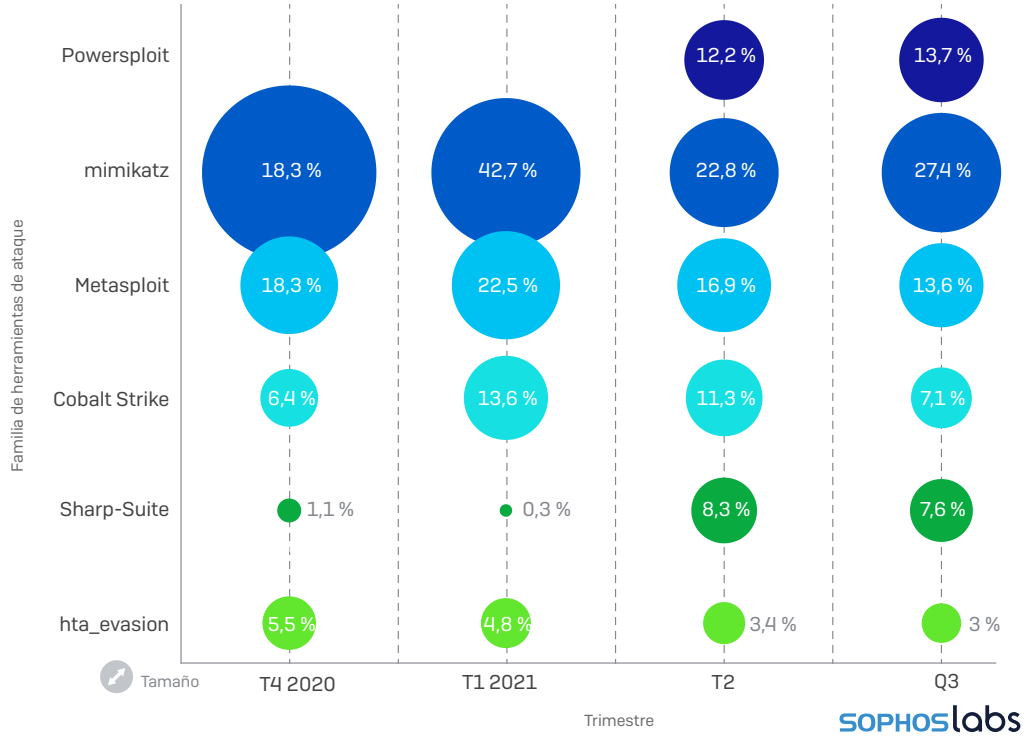
Herramientas como Mimikatz (usadas tanto por técnicos de pruebas de penetración como autores de malware), aunque no sean productos comerciales en el sentido estricto, se usaron de forma generalizada y aparecieron en prácticamente todos los incidentes manuales que Sophos investigó el año pasado.

También fueron notablemente predominantes (gracias a que su código fuente se filtró en 2020) las copias piratas de Cobalt Strike (un software de simulación de adversarios), que no solo se utilizaron en ataques de ransomware, sino que también se distribuyeron como carga inicial de otro malware.

[1] *El estado del ransomware 2022 - Sophos*
[2] *El estado del ransomware 2022 - Sophos*

**Incidencia de las principales herramientas de ataque**

*Por equipos individuales, las herramientas de ataque más frecuentes observadas en 2020-2021*




*Informe de amenazas 2022 de Sophos*

La función Beacon de Cobalt Strike, que proporciona una puerta trasera capaz de acceder a equipos Windows, ha hecho que el software se haya convertido en la herramienta favorita de los ciberdelincuentes. Así, la mayoría de casos de ransomware que hemos visto durante el último año implicaron el uso de cargas Beacon de Cobalt Strike.

*Consulte el último Informe de amenazas de Sophos para obtener una visión más detallada del estado de las ciberamenazas en la actualidad.*

## Las prácticas de ciberseguridad proactivas son indispensables

Ataques a la cadena de suministro. Exploits de software. Herramientas legítimas. El hilo conductor es la naturaleza de estos métodos. Están dirigidos por humanos. Son selectivos y sofisticados. Son evasivos e indetectables con medios tradicionales.

Las organizaciones tienen que adoptar enfoques de ciberseguridad más proactivos para mantenerse un paso por delante de los delincuentes. Responder a adversarios humanos requiere un enfoque dirigido por humanos.

De ahí la búsqueda de amenazas.

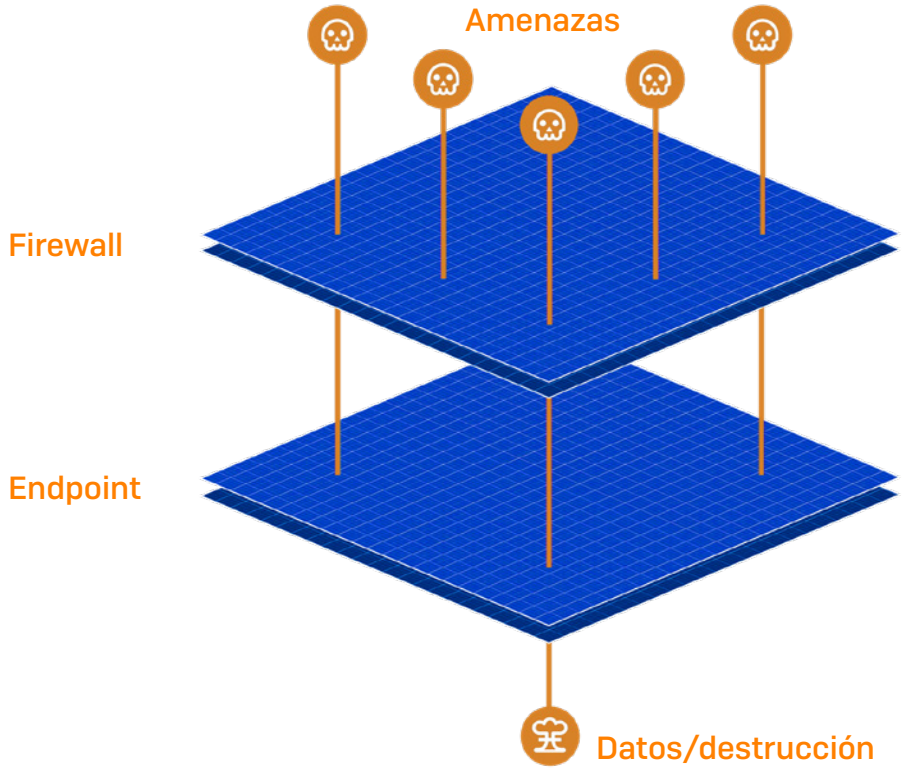
## ¿Qué es la búsqueda de amenazas?

La búsqueda de amenazas es el proceso iterativo y proactivo de realizar búsquedas en la telemetría de los endpoints y la red para identificar actividad maliciosa, que se realiza partiendo del supuesto de que los adversarios ya han superado las defensas. La definimos como iterativa porque la práctica requiere adaptarse constantemente para asegurar que siga siendo un método efectivo para buscar y neutralizar las ciberamenazas actuales que evolucionan de igual forma.

Durante una búsqueda de amenazas, los equipos analizan las herramientas, las técnicas y los procedimientos (TTP, por sus siglas en inglés) utilizados por los adversarios para determinar la fase del ataque y acumular información. Una vez establecido esto, tomarán la acción apropiada para neutralizar la amenaza en caso necesario.

## ¿Por qué necesitamos realizar una búsqueda de amenazas?

Las razones son múltiples, aunque la razón principal es una sola verdad: al contrario de lo que se afirma en innumerables ocasiones, la tecnología por sí sola no puede detener el 100 % de las amenazas. A pesar de las múltiples capas de defensa, algunas amenazas siguen colándose y comprometiendo los entornos informáticos.




Como ya hemos mencionado más arriba, los adversarios modernos están recurriendo cada vez más a enfoques adaptativos y evasivos que son, literalmente, «manuales directos», en lugar de los ataques automatizados y a gran escala de antaño.

Esto se refleja en lo que ven nuestros equipos de respuesta a amenazas, que informan de un aumento significativo del número de adversarios humanos que controlan y dirigen los ataques. Esto implica que los equipos de seguridad no solo se ven obligados a buscar lo desconocido para mantenerse por delante, sino que también tienen que adoptar la actitud de que ya se ha producido una intrusión.

## La mentalidad de la búsqueda de amenazas

Los cazadores de amenazas experimentados frecuentemente asumen que una amenaza potencial ya ha eludido sus defensas, independientemente de en qué punto de la cadena de ataque se encuentre. Adoptan esta mentalidad porque les obliga a hacer dos cosas.

### Limitar el tiempo de permanencia del adversario

Adoptar esta mentalidad obliga a los equipos a limitar el tiempo de permanencia del adversario. Cuanto más tiempo esté un hacker en su red, más tiempo tendrá para ejecutar sus viles actividades. Por lo tanto, cuanto menos tiempo demos a un adversario dentro de una red, menor es el daño que puede hacer. Los equipos de seguridad se ven obligados a buscar las amenazas antes de que sus impactos se hagan sentir asumiendo que las defensas ya han sido superadas.

### Reducir el tiempo de detección

Adoptar esta mentalidad también obliga a los equipos a reducir el tiempo medio de detección. Posiblemente disponga de múltiples capas de defensa, y la amenaza evasiva puede activar su defensa más adelante en su cadena de ataque. El problema es que, llegado a este punto, ya es demasiado tarde: el daño está hecho, ya que la amenaza ha llegado demasiado lejos. Buscar la amenaza nos permite identificar debilidades en nuestra seguridad y ocuparnos de ellas seguidamente, lo que en definitiva reduce el tiempo de detección de amenazas iguales o similares en el futuro.

## ¿Quién se dedica a la búsqueda de amenazas?

### Perfil de un cazador de amenazas

Antes de profundizar en el tema de quién debe encargarse de la búsqueda de amenazas, es esencial comprender el rol de un cazador de amenazas. La búsqueda de amenazas es una operación altamente compleja. Las personas que trabajan en este ámbito deben poseer unos conocimientos específicos a la vez que muy especializados. Dicho esto, el perfil típico de un cazador de amenazas debe caracterizarse por lo siguiente:

- **Creatividad y curiosidad**: buscar amenazas puede ser como buscar una aguja en un pajar. Los cazadores de amenazas a menudo pueden pasar días buscando amenazas, utilizando numerosos métodos para sacarlas a la luz.
- **Experiencia en ciberseguridad**: la búsqueda de amenazas es una de las operaciones más avanzadas dentro de la ciberseguridad. Por lo tanto, es obligatorio disponer de experiencia previa en el campo y conocimientos básicos.
- **Conocimiento del panorama de amenazas**: comprender las tendencias más recientes de las amenazas es imprescindible a la hora de buscar y neutralizar entidades desconocidas.
- **Mentalidad de adversario**: la capacidad de pensar como un hacker es fundamental para combatir los métodos dirigidos por humanos de hoy en día.
- **Capacidad de redacción técnica**: los cazadores de amenazas deben mantener un registro de todos sus descubrimientos como parte del proceso de investigación. Por lo tanto, la capacidad de comunicar una información tan compleja es crucial para proseguir la búsqueda hasta su conclusión.
- **Conocimiento de sistemas operativos (SO) y redes**: un conocimiento avanzado de ambos es esencial.
- **Experiencia en codificación/scripting**: necesaria para ayudar a los cazadores de amenazas a crear programas, automatizar tareas, analizar registros y realizar tareas de análisis de datos para apoyar y hacer avanzar sus investigaciones.

Desafortunadamente, a esta particular combinación de competencias se suma una notable escasez de conocimientos en el sector de TI, ya que el 54 % de los administradores de TI creen que, incluso con todas las herramientas necesarias a su disposición, los ciberataques actuales son demasiado avanzados para que sus equipos de TI puedan encargarse de ellos por sí solos. Dicho esto, en los casos en que se dispone de personal adecuado para este rol, en general observamos que la búsqueda de amenazas es realizada por uno de dos equipos distintos.

### Centro de operaciones de seguridad (SOC) interno

Cuando las organizaciones deciden realizar la búsqueda de amenazas ellas mismas, el personal correspondiente forma parte del SOC. Un SOC es una función interna centralizada de la organización centrada en la supervisión, la detección, la investigación y la respuesta a las ciberamenazas, a la vez que mejora la posición de seguridad general de la organización matriz. Es el equipo de la organización al que acudir para cuestiones de ciberseguridad.

### Proveedores de operaciones de seguridad externos

Muchas organizaciones están subcontratando cada vez más sus operaciones de seguridad a proveedores externos. Esto puede deberse a la falta de capacidad interna (en el último año, los equipos de TI experimentaron un aumento del 69 % en la carga de trabajo en materia de ciberseguridad), la falta de conocimientos o la preferencia por expertos externos para esta crítica tarea 24/7.

### Proveedores de detección y respuesta gestionadas (MDR)

La detección y respuesta gestionadas como un servicio completamente gestionado permite a las organizaciones contar con un equipo dedicado de analistas de seguridad encargado de la búsqueda de amenazas latentes 24/7/365. De hecho, «el 51 % utiliza un proveedor de servicios de detección y respuesta gestionadas (MDR) para ayudar a integrar los datos de telemetría para la detección y respuesta a las amenazas», según una investigación de ESG.

Los proveedores de MDR presentan una serie de ventajas con respecto a un programa de operaciones de seguridad exclusivamente interno. La más significativa de todas ellas suele ser la experiencia.

El equipo de Sophos MDR cuenta con miles de horas de experiencia y ha visto y resuelto todo aquello con que puedan atacar los adversarios. También puede aprender de los ataques a una organización y aplicarlo a sus demás clientes. Otro beneficio es la escala: el equipo de Sophos MDR puede proporcionar soporte 24/7 con tres equipos globales.

### Proveedores de servicios de seguridad gestionados (MSSP)

Los MSSP se utilizan para gestionar parte o la totalidad de las operaciones de seguridad TI de una organización, permitiendo a los equipos internos centrarse más en las tareas diarias. Los MSSP ofrecen capacidades de búsqueda de amenazas como parte de un servicio gestionado. Esto también puede incluir servicios de MDR como se ha detallado ya más arriba.

## Instrumentos para la búsqueda de amenazas

### Detección y respuesta para endpoints/ampliadas (EDR/XDR)

Para identificar e investigar actividades potencialmente maliciosas, los cazadores de amenazas necesitan datos y herramientas de investigación. Para ello, usan la EDR y la XDR. Permiten a los cazadores ver rápidamente las detecciones sospechosas e investigarlas a fondo.

Como sugiere su nombre, la EDR proporciona datos desde la solución para endpoints. En cambio, la XDR consolida las señales de todo el entorno de TI, incluyendo el firewall, los dispositivos móviles, el correo electrónico y las soluciones de seguridad en la nube. Dado que los adversarios aprovechan cualquier oportunidad de ataque, cuanto más amplía sea su red de señales, mejor será su detección temprana.

Uno de los mayores desafíos prácticosde las soluciones de EDR/XDR es el ruido: los cazadores de amenazas reciben tantas señales que puede ser difícil separar el grano de la paja. Por eso es esencial combinar su solución de EDR/XDR con una protección de endpoints potente que detenga más amenazas desde un principio, para que los responsables de la seguridad puedan centrarse en menos detecciones más precisas.

# Anatomía de la detección y respuesta a amenazas

La búsqueda de amenazas es un componente de una operación más amplia: la detección y respuesta a amenazas. En Sophos aplicamos un marco de detección y respuesta a amenazas a nuestras búsquedas. Este está compuesto por cinco componentes clave.


## 1. Prevención

Disponer de tecnologías de prevención robustas y configuradas correctamente (como una solución de protección de endpoints) evita que los atacantes puedan entrar en su red. Más importante aún, también reduce el número de alertas de seguridad generadas a diario o incluso cada hora. Con menos alertas con las que lidiar, el equipo de seguridad puede detectar mejor y centrarse en las señales importantes, en este caso, los adversarios evasivos humanos.

## 2. Recopilación de eventos, alertas y detecciones de seguridad

Los datos son el combustible necesario para la búsqueda y el análisis de amenazas. Es díficil que los equipos de operaciones de seguridad identifiquen con precisión los posibles indicadores de ataque si el tipo, el volumen o la calidad de las señales no son los adecuados. A su vez, la falta de contexto de los datos complica la decisión de condena del analista. Sin metadatos significativos asociados a la señal, el analista tendrá dificultades para determinar si las señales son maliciosas o benignas.

## 3. Priorización de las señales que importan

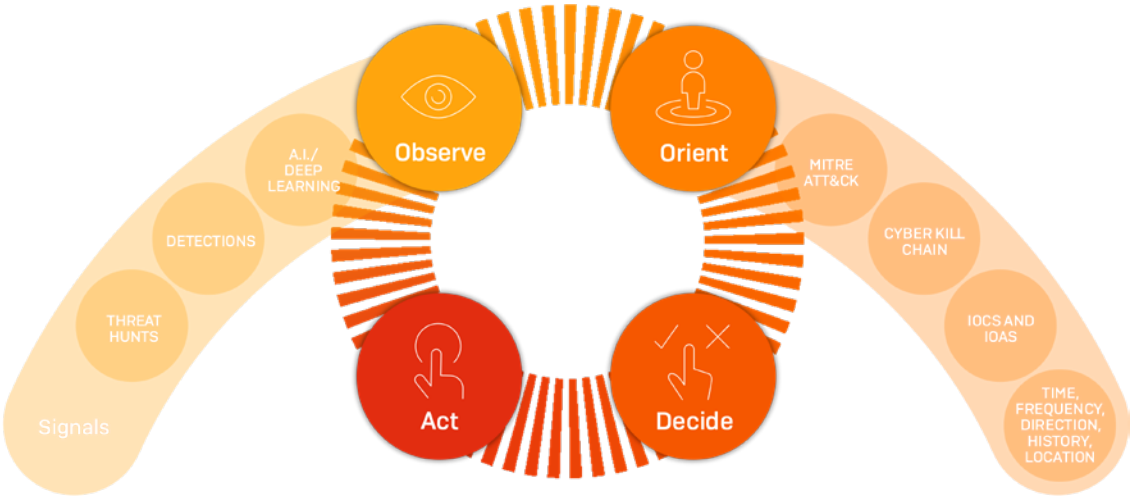
Para evitar verse desbordado por los datos y no ver los elementos merecedores de una investigación más a fondo, debe ser capaz de identificar las alertas que son importantes. Esto es más difícil de lo que parece. Cuanto más pueda mejorar la relación señal-ruido utilizando una combinación de contexto que solo los productores de eventos pueden proporcionar, junto con la inteligencia automatizada y artificial, mejor. Incluso con automatización, no es un proceso sencillo.

## 4. Investigación

Una vez tenga aisladas las señales clave, es el momento de añadir un elemento de juicio y evaluar sus descubrimientos según los marcos y modelos de la industria para crear un umbral de confianza que permita determinar si se trata de un comportamiento malicioso o benigno.

### Marco de investigación OODA

Los analistas de seguridad experimentados suelen utilizar un marco para guiar sus investigaciones. Por ejemplo, el equipo de Sophos MDR utiliza una metodología de investigación conocida como el ciclo OODA, que permite llevar a cabo la secuencia de acciones mencionada anteriormente para comprobar y confirmar la validez de todos los resultados obtenidos:




El ciclo OODA es un concepto militar que permite a nuestro equipo seguir un ciclo de razonamiento para comprender completamente un evento y sus condicionantes. El equipo puede entonces basarse en estos conocimientos y emplear la toma de decisiones y la intuición humanas para concluir si hay actividad maliciosa en el entorno de un cliente y, en función de ello, decidir cómo actuar.

Al aplicar el marco OODA, los analistas de seguridad de Sophos a menudo realizarán los siguientes pasos:

- **Observar**: ¿qué vemos en esta detección?
  - Observación de las posibles conexiones externas e internas relacionadas con la detección.
  - Determinación de dónde se está produciendo la detección y si hay usuarios finales asociados a ella.
- **Orientar**: ¿qué sabemos sobre está detección?
  - Recopilación de datos basados en evidencias.
  - Comprensión de los TTP comunes o específicos de este ataque o atacante. Uno de los recursos utilizados para identificar los TTP es el marco de MITRE ATT&CK, que trataremos más adelante en este informe.
  - Recopilación de información de indicadores de ataque (IOA) e indicadores de peligro (IOC).
- **Decidir**: ¿es esta detección maliciosa, sospechosa o benigna? ¿Es necesario actuar?
- **Actuar**: basándose en los pasos anteriores, ¿qué medida se debe tomar?
  - Mitigar - neutralizar – repetir el ciclo – mejorar.

## 5. Acción

Esta es una fase importantísima. Una vez que ha determinado que tiene en frente una amenaza, debe hacer dos cosas, y ambas son igualmente importantes.

La primera es mitigar el problema inmediato, mientras que la segunda es recordar que probablemente solo está resolviendo un síntoma del ataque y que todavía necesita buscar y neutralizar la causa raíz. La primera se debe hacer sin menoscabar su capacidad para hacer la segunda.

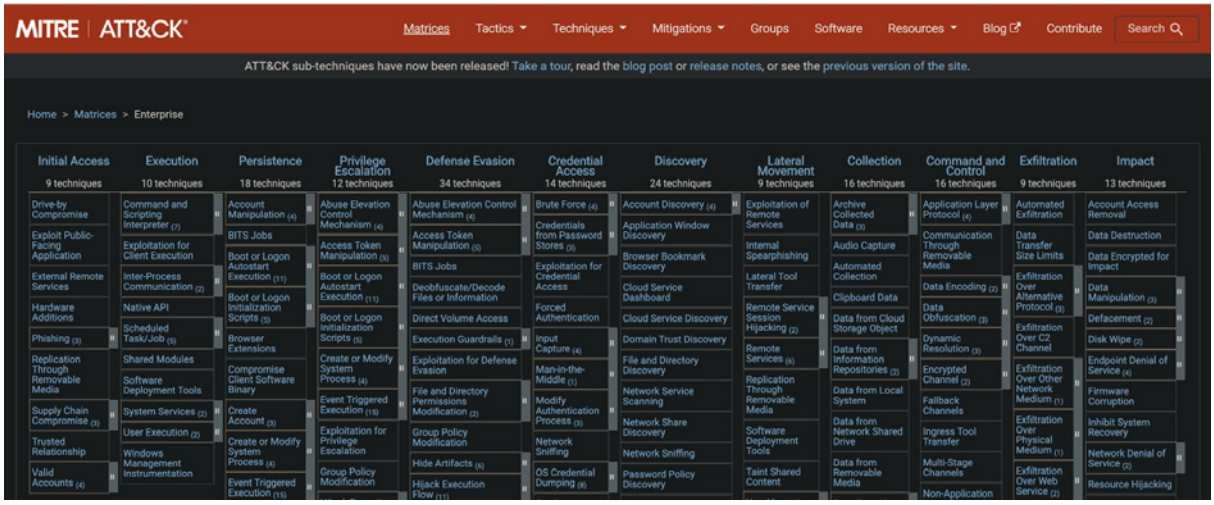
Algunas veces será suficiente con poner en cuarentena un equipo o desconectarlo de la red, mientras que en otros casos, el equipo de seguridad deberá profundizar más en la red para erradicar por completo todo rastro del atacante.

Por ejemplo, el que haya bloqueado y eliminado el malware de su sistema con éxito y haya dejado de ver la alerta que le puso sobre la pista no significa que se haya expulsado al atacante de su entorno.

Los cazadores de amenazas profesionales que ven miles de ataques saben cuándo y dónde es necesario profundizar. También buscan qué más están haciendo los atacantes, qué han hecho o pueden estar planificando hacer en la red, y también lo neutralizan.

## Clasificación de amenazas: el marco de MITRE ATT&CK

Un recurso frecuentemente utilizado por los cazadores de amenazas es el marco de MITRE ATT&CK. Si se ha dedicado alguna vez a la ciberseguridad, seguramente haya oído hablar de ella. Entre otros muchos marcos, MITRE es una base de conocimiento accesible globalmente que contiene TTP de adversarios definidos a partir de observaciones del mundo real. Se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicos. Permite a los cazadores de amenazas asignar los comportamientos de los ataques a una gran cantidad de TTP identificados previamente. Esto, a su vez, permite a los cazadores establecer en qué punto del ciclo de vida se encuentra el ataque en curso. El marco es crítico para la fase «Orientar» del marco OODA.




*Puede acceder a información más detallada sobre el marco MITRE ATT&CK aquí.*

# Métodos de búsqueda de amenazas

En esta sección vamos a ver algunos de los métodos de búsqueda de amenazas más comunes. En Sophos, solemos iniciar las búsquedas de dos formas distintas.

## Búsquedas de amenazas a partir de pistas

En nuestra organización, cualquier detección que requiera una investigación más profunda es revisada por un analista de amenazas humano capaz de aplicar el contexto empresarial y el razonamiento humano a cualquier situación. Observará el comportamiento, considerará el contexto empresarial establecido previamente, formulará una hipótesis y actuará en consecuencia. La hipótesis puede ser involucrarse de forma activa en el incidente potencial o realizar trabajos de investigación adicionales para afianzar sus conocimientos sobre el problema en cuestión.

Para completar el ciclo, el analista esperará y hará una evaluación para ver los resultados de la hipótesis y las comprobaciones. Si es necesario investigar más, puede repetir este ciclo hasta tomar una decisión. Si el evento evoluciona y se convierte en un incidente activo, el analista pasa al modo de respuesta completa para combatir activamente la amenaza.

## Búsquedas de amenazas sin pistas

Mientras que las búsquedas de amenazas a partir de pistas requieren que uno de nuestros sensores detecte o genere una «señal» de interés, las búsquedas sin pistas son mucho más orgánicas. Aunque sigamos utilizando nuestros algoritmos de inteligencia artificial para procesar la enorme cantidad de datos que recibimos, las búsquedas de amenazas sin pistas están casi siempre dirigidas por analistas de amenazas humanos.

En lugar de depender de esa señal sistemática inicial que nos avisa de que algo necesita ser investigado, ejecutamos de forma proactiva consultas en los entornos de un cliente o varios clientes a la vez. Esto puede ocurrir por varias razones, entre otras:

- Un cliente del mismo sector vertical ha sido atacado de una forma particular, y queremos ser cautos y asegurarnos de que los mismos atacantes no están intentando atacar a ninguno de nuestros otros clientes.
- SophosLabs ha informado al equipo de MDR de un ataque importante dirigido a clientes pertenecientes al mismo sector vertical o con propiedades similares.
- Ha tenido lugar un acontecimiento significativo en el ámbito de la seguridad y queremos cerciorarnos de si hay clientes nuestros afectados.

# Estudio de caso: La caza de ransomware que sacó a la luz un troyano bancario histórico

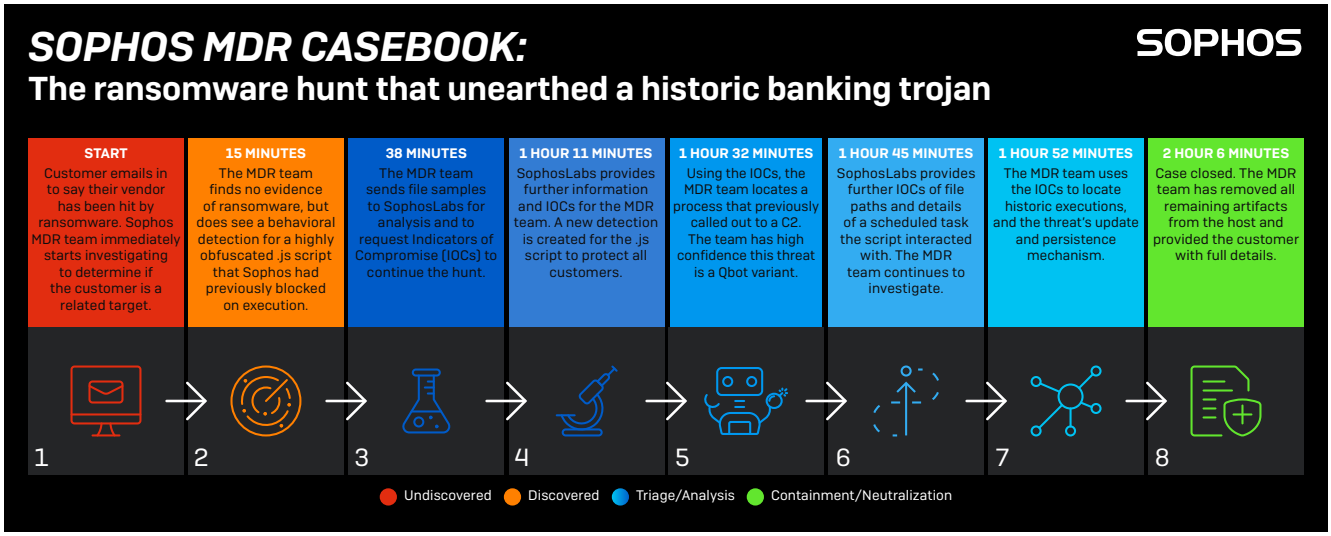
Ahora que ya hemos descrito los entresijos de la búsqueda de amenazas, veamos a continuación una búsqueda de amenazas en acción. Tal y como lo investigó el equipo de Sophos MDR, este caso es un gran ejemplo de cómo una búsqueda de amenazas puede descubrir lo inesperado. En este caso, un cliente nos contactó para decirnos que un proveedor con el que trabajaba había sufrido un ataque de ransomware, y que le preocupaba estar infectado también.

El equipo de Sophos MDR comenzó la investigación inmediatamente, trabajando con nuestros expertos en SophosLabs. Determinaron rápidamente que no había ninguna evidencia de ransomware. Llegados a este punto, algunos equipos habrían cerrado el caso y pasado a otra tarea. Sin embargo, el equipo de Sophos MDR siguió investigando y descubrió un troyano bancario histórico.

El cliente se quedó tranquilo sabiendo que no había sido afectado por ningún ransomware y que un malware bancario histórico había sido eliminado completamente, un resultado que no se habría producido sin esta intervención experta.

Y como muestra este caso, aunque el ransomware es a menudo la amenaza prioritaria, es esencial también estar alerta ante los ataques que prefieren mantenerse ocultos en la sombra.

En dos horas y seis minutos todo el incidente había sido investigado y limpiado.




*Para profundizar en este caso, lea el artículo aquí.*

# Preparación para la búsqueda de amenazas: cinco pasos para garantizar un resultado satisfactorio

A estas alturas, seguramente ya tenga una buena noción de todo lo que tiene que ver con la búsqueda de amenazas. Sin embargo, antes de que pueda comenzar, es esencial asegurarse de que su organización está perfectamente preparada para realizarla de forma efectiva.

## 1. Comprender la madurez de sus operaciones de ciberseguridad actuales

Antes de poder comenzar a comprender a los posibles adversarios, es necesario entender el estado de sus operaciones de ciberseguridad actuales. Referenciar sus procesos a un modelo de madurez de ciberseguridad (como el CMMC) es una excelente forma de determinar lo bien preparado (o no) que está para comenzar a buscar amenazas. También es buena idea auditar su posición de seguridad para establecer su nivel de susceptibilidad a las amenazas.

## 2. Decidir cómo realizar la búsqueda de amenazas

Una vez haya establecido su cibermadurez, puede decidir si la búsqueda de amenazas es algo que quiere hacer internamente, externalizar completamente o una combinación de ambas alternativas.

## 3. Identificar carencias tecnológicas

Revise sus herramientas existentes e identifique qué más necesita para llevar a cabo una búsqueda de amenazas efectiva. ¿Qué eficacia tiene su tecnología de prevención? ¿Ofrece o admite las capacidades de búsqueda de amenazas que aportan la EDR/XDR?

## 4. Identificar carencias de conocimientos

Buscar amenazas es algo complejo que requiere conocimientos especializados. Si no tiene la experiencia necesaria a nivel interno, busque cursos de formación que ayuden a desarrollar las competencias necesarias. Considere también trabajar con un proveedor externo para complementar su equipo.

## 5. Desarrollar e implementar un plan de respuesta a incidentes

Antes de comenzar con la búsqueda de amenazas, es esencial disponer de una respuesta a incidentes completa para asegurar que cualquier respuesta pueda ser evaluada y controlada.  Contar con un plan de respuesta bien preparado y bien entendido que todas las partes clave puedan ejecutar de forma inmediata reduce enormemente el impacto de un ataque en una empresa.

Un buen plan de respuesta a incidentes debe definir protocolos de preparación, detección y generación de informes, clasificación y análisis, contención y neutralización, y actividades posteriores al incidente. Consulte nuestra guía de respuesta a incidentes para obtener consejos sobre cómo crear un plan eficaz de respuesta a incidentes.

*No se pierda la Sophos Threat Hunting Academy para ver más consejos prácticos sobre cómo preparar y realizar la búsqueda de amenazas.*

# Cómo puede ayudar Sophos

Como ya hemos mencionado, la búsqueda de amenazas efectiva es increíblemente compleja y requiere tecnologías next-gen en combinación con una extensa experiencia humana. Afortunadamente, Sophos puede apoyarle en sus objetivos de búsqueda de amenazas, independientemente de su madurez de ciberseguridad.

## Impedir que las amenazas penetren en su red: Sophos Intercept X Endpoint

Los cazadores de amenazas solo pueden desempeñar sus funciones de forma eficiente si no se les inunda de alertas de seguridad. Una forma de lograrlo es introduciendo las mejores tecnologías de prevención para que los responsables de la seguridad puedan centrarse en menos detecciones más precisas y agilizar los procesos de investigación y respuesta posteriores. La solución es Sophos Intercept X Endpoint.

Sophos Intercept X es la solución de seguridad para endpoints líder de la industria que reduce la superficie expuesta a ataques y evita que estos se produzcan. Combinando tecnologías antiexploits, antiransomware y de control e IA con Deep Learning, detiene las amenazas antes de que impacten en sus sistemas. Intercept X utiliza un completo enfoque de defensa exhaustiva para la protección de endpoints en lugar de depender de una técnica de seguridad principal.

Las capacidades de prevención de Sophos Intercept X Endpoint Protection bloquean el 99,98 % de las amenazas (puntuación media de AV-TEST de enero-noviembre 2021). Los encargados de la defensa pueden entonces centrarse mejor en las señales sospechosas que requieren intervención humana.

Puede obtener más información o realizar una evaluación de Intercept X Endpoint aquí.

## Realizar búsquedas de amenazas usted mismo: Sophos XDR

Diseñado para analistas de seguridad que trabajan en equipos SOC dedicados y administradores de TI encargados de la seguridad y otras cuestiones de TI, Sophos XDR permite a su equipo detectar, investigar y responder a incidentes en endpoints, servidores, firewall, cargas de trabajo en la nube, correo electrónico, dispositivos móviles y más.

Acceda inmediatamente a la información que le interesa: elija entre una biblioteca de plantillas ya escritas y personalizables que cubren muchos escenarios distintos de búsqueda de amenazas y operaciones de TI, o bien escriba las suyas propias. Tiene acceso a los datos de los dispositivos en tiempo real, hasta 90 días de datos en el disco, 30 días de datos almacenados en el repositorio en la nube de Sophos Data Lake y una lista generada automáticamente de elementos sospechosos para que sepa exactamente por dónde empezar.

Si desea probar Sophos XDR para realizar sus propias búsquedas de amenazas, Sophos le ofrece las herramientas necesarias para la búsqueda de amenazas avanzadas y la higiene de las operaciones de seguridad. Puede iniciar una prueba directamente desde el producto (si tiene una cuenta de Sophos Central) o realizar una evaluación de Sophos Intercept X, que incluye XDR.

## Búsqueda de amenazas como servicio completamente gestionado o como apoyo de su equipo: Sophos MDR

Sophos MDR es una solución MDR polifacética, completa y galardonada que aplica la experiencia y los conocimientos del equipo de analistas de seguridad de Sophos y su extenso abanico de capacidades a su red y entornos en la nube. En efecto, Sophos se convierte en una ampliación de sus operaciones de seguridad, añadiendo sus enormes capacidades a las de su equipo.

El equipo de Sophos MDR de cazadores de amenazas y expertos en respuesta se dedican a:

- Buscar y validar de forma proactiva posibles amenazas e incidentes.
- Utilizar toda la información disponible para determinar el alcance y la gravedad de las amenazas.
- Aplicar el contexto empresarial adecuado para las amenazas reales.
- Iniciar acciones para interrumpir, contener y neutralizar amenazas de forma remota.
- Brindar asesoramiento práctico para abordar la causa raíz de los incidentes recurrentes.

Incluso si su organización tiene un centro de operaciones de seguridad maduro, es posible que quiera que un segundo par de ojos supervise su entorno para asegurarse de que nada se cuela entre las rendijas. Sophos MDR aúna la búsqueda de amenazas y la protección de endpoints, a la vez que proporciona supervisión y experiencia cada día. Su red y sus recursos en la nube son una prioridad máxima para los analistas de red y los cazadores de amenazas de Sophos que monitorizan y remedian y neutralizan activamente las amenazas en su nombre.

Con un buen servicio de MDR, usted y su organización pueden disfrutar de la tranquilidad de saber que hay un equipo de expertos cualificados que supervisan constantemente su empresa, buscan amenazas, investigan actividades sospechosas y responden a posibles incidentes. Con el panorama de las amenazas de ciberseguridad en permanente evolución, trabajar con un equipo cuyo único objetivo es la ciberseguridad aporta tranquilidad.

Hable con su representante de Sophos o solicite una llamada para obtener más información sobre cómo Sophos MDR puede ayudar a su organización. Mientras tanto, póngase al día con las investigaciones y los libros de casos de MDR más recientes.

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

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



22-08-08 WP-ES (PC)