SOPHOS

El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio

Resultados de un estudio independiente realizado a 3000 responsables de TI/ciberseguridad de 14 países durante enero y febrero de 2023.

Monográficos de Sophos. Abril 2023

Metodología del estudio

Para analizar el impacto empresarial real de la ciberseguridad en 2023, Sophos encargó una encuesta independiente a 3000 responsables de TI/ciberseguridad de 14 países. Todos los encuestados pertenecían a empresas de entre 100 y 5000 empleados. La investigación fue llevada a cabo en enero y febrero de 2023 por Vanson Bourne.

3000
encuestados

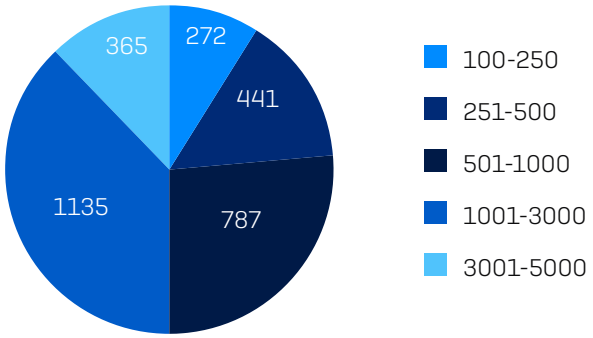
100-5.000
empleados

14
países

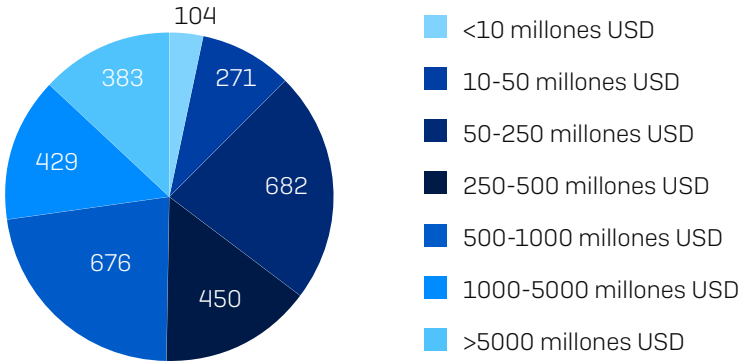
<10 MUSD->5000 MUSD
Ingresos anuales

Ene/feb 23
investigación realizada

Encuestados por tamaño de la organización (número de empleados)



Encuestados por tamaño de la organización (ingresos anuales)



Encuestados por país

PAÍS	NÚMERO DE ENCUESTADOS	PAÍS	NÚMERO DE ENCUESTADOS
Estados Unidos	500	Reino Unido	200
Alemania	300	Sudáfrica	200
India	300	Francia	150
Japón	300	España	150
Australia	200	Austria	100
Brasil	200	Singapur	100
Italia	200	Suiza	100

Resumen ejecutivo

Situación: los adversarios aceleran y los encargados de la seguridad no pueden seguir el ritmo

El estudio reveló que la realidad actual es un sistema de ciberseguridad de dos velocidades, en el que adversarios y responsables de la seguridad se mueven a ritmos diferentes. A través de la automatización, los modelos de ciberdelincuencia «como servicio», la adaptación y la suplantación sigilosa, los adversarios están acelerando, y ya son capaces de ejecutar una amplia gama de ataques sofisticados a escala. Teniendo en cuenta que el 94 % de las organizaciones sufrieron algún tipo de ciberataque en el último año, todas las empresas (independientemente de su tamaño o ingresos) deben dar por sentado que serán víctimas en 2023.

Los responsables de la seguridad son incapaces de seguir el ritmo, frenados por la escasez de expertos, un volumen abrumador de alertas y demasiado tiempo dedicado a la respuesta a incidentes. La mayoría de las organizaciones tienen dificultades para poner en práctica la detección y respuesta a amenazas, y el 93 % considera que la ejecución de las tareas esenciales de las operaciones de seguridad es un reto.

La investigación de las alertas de seguridad es un problema muy extendido. De media, algo menos de la mitad (48 %) de todas las alertas se investigan para determinar si son indicios de actividad maliciosa, y a la mayoría de las organizaciones les cuesta identificar (71 %) y priorizar (71 %) qué alertas o eventos investigar. Para las alertas que lo requieren, el proceso completo de detección, investigación y respuesta tarda una media de nueve horas en las organizaciones con entre 100 y 3000 empleados, duración que se dispara a 15 horas para las que tienen entre 3001 y 5000 empleados.

Desde el punto de vista operativo, los encargados de la seguridad no confían en sus procesos, y los errores de configuración de las herramientas de seguridad constituyen el principal riesgo para la seguridad percibido de cara a 2023. Más de la mitad (52 %) de los profesionales de TI afirman que las ciberamenazas son demasiado avanzadas para que su organización las gestione por sí sola, porcentaje que se eleva al 64 % entre las pequeñas empresas (100-250 empleados).

Impacto empresarial: la situación tiene consecuencias financieras, operativas y de dotación de recursos

Este sistema de dos velocidades tiene un impacto considerable en la organización en general. Las repercusiones financieras directas de un ciberincidente son enormes y bien conocidas, y es que el coste medio de remediar un ataque de ransomware para una pyme asciende a 1,4 millones USD[1]. Sin embargo, estos costes de limpieza de incidentes son solo una parte de la historia.

La capacidad de cumplimiento del programa de TI se ve reducida, y el 55 % de los encuestados afirma que lidiar con las ciberamenazas ha repercutido negativamente en el trabajo del equipo de TI en otros proyectos. La naturaleza urgente e impredecible de la ciberseguridad también se interpone en el camino de los esfuerzos centrados en el negocio: el 64 % desearía que el equipo de TI dedicara más tiempo a cuestiones estratégicas y menos a apagar fuegos.

El tiempo que se invierte en detectar, investigar y remediar las alertas de seguridad también tiene un impacto financiero considerable en términos de costes de recursos.

La situación también supone una gran carga para los empleados. El 57 % de los profesionales de TI afirma que la preocupación de que la organización sufra un ciberataque a veces les quita el sueño, porcentaje que se eleva al 65 % entre los que trabajan en organizaciones con entre 3001 y 5000 empleados. Dados los elevados costes de contratación, formación y retención del personal en este ámbito, estas repercusiones crean retos y costes adicionales para la empresa.

1 El estado del ransomware 2022, Sophos

Recomendación: impulse el volante de inercia de los encargados de la seguridad para que adelanten a los adversarios

Permitir que los responsables de la seguridad adelanten a los atacantes en la carrera de la ciberseguridad de 2023 requiere un enfoque integral a la vez que sencillo. En primer lugar, las organizaciones deben establecer un proceso de respuesta a incidentes que pueda ampliarse, lo que se consigue minimizando la superficie de ataque y el volumen de alertas que requieren atención, y optimizando el tiempo de respuesta sacando partido de servicios especializados.

A continuación, deben implantar defensas adaptativas que se ajusten automáticamente a la situación. Esto les permite frenar a los adversarios y ganar tiempo para que los encargados de la seguridad respondan.

Por último, también necesitan instaurar un círculo virtuoso que combine tecnología y experiencia humana para reforzar las defensas, lo que hará aumentar la velocidad, la eficacia y el impacto. Esto permitirá impulsar el volante de inercia de los responsables de la seguridad y hacerles avanzar.

Para que este enfoque tenga éxito, es fundamental recurrir a especialistas externos. La buena noticia es que las organizaciones ya aplican un enfoque mixto a la prestación de ciberseguridad, pues el 94 % de las empresas colaboran con especialistas externos de alguna manera para ampliar sus operaciones. A medida que los adversarios intensifican sus esfuerzos, resulta cada vez más imprescindible contar con expertos en operaciones de seguridad.

Principales conclusiones

El **94 %** de las organizaciones sufrieron algún tipo de ciberataque en el último año

La **exfiltración de datos** es la principal preocupación en materia de seguridad para 2023

El **93 %** considera que ejecutar operaciones de seguridad esenciales es un reto

El **48 %** de las alertas de seguridad se investigan

15 horas es el tiempo medio para detectar, investigar y responder a una alerta en organizaciones de 3001-5000 empleados

Los **errores de configuración de las herramientas de seguridad** son el principal riesgo de seguridad percibido en 2023

El **52 %** afirma que las ciberamenazas son ahora demasiado avanzadas para que su organización se ocupe de ellas por su cuenta

El **55 %** afirma que lidiar con las ciberamenazas ha repercutido negativamente en el trabajo del equipo de TI en otros proyectos

El **64 %** desearía que el equipo de TI dedicara más tiempo a cuestiones estratégicas y menos a apagar fuegos

Al **57 %** de los profesionales de TI les quita el sueño el temor a que la organización sufra un ciberataque

Ciberamenazas 2023: la realidad desde la primera línea

Principales preocupaciones en materia de ciberseguridad para 2023

Al 99 % de los profesionales de TI les preocupan las ciberamenazas que afectarán a su organización en 2023. La exfiltración de datos (robo por parte de un atacante externo) encabeza la lista de amenazas que más preocupan a los profesionales de TI, seguida de cerca por el phishing (incluido el spear phishing). El ransomware ocupa el tercer puesto.

Es importante recordar que estas tres amenazas suelen estar relacionadas: un correo electrónico de phishing es a menudo el inicio de un ataque que culmina con la exfiltración de datos y el ransomware.

CIBERAMENAZA	PORCENTAJE DE ENCUESTADOS QUE AFIRMAN QUE ES UNA DE SUS PRINCIPALES PREOCUPACIONES
Exfiltración de datos (robo por parte de un atacante externo)	41 %
Phishing (incluido el spear phishing)	40 %
Ransomware	35 %
Ciberextorsión	33 %
Ataques de denegación de servicio (DDoS)	32 %
Estafa por correo electrónico corporativo comprometido (BEC)	31 %
Adversarios activos (ataques que incluyen hacking manual realizado por humanos)	30 %
Malware para móviles	30 %
Criptomineros	22 %
Wipers	16 %
Otros	0 %
No me preocupa que una ciberamenaza afecte a mi organización en 2023	1 %
No lo saben	0 %

Con vistas a 2023, ¿qué ciberamenazas le preocupan más que puedan afectar a su organización? (n=3000)

Los adversarios ejecutan innumerables ataques a escala

Las preocupaciones de los profesionales de TI coinciden mucho con la realidad de lo que está ocurriendo en primera línea, ya que el 94 % de las organizaciones sufrieron al menos un ciberataque en el último año. Aunque el ransomware fue el ataque más citado, los adversarios ejecutan una amplia gama de ataques a escala. Esta amplitud y alcance de los ataques crea un reto considerable y cada vez mayor para los encargados de la seguridad.

Detrás de estas cifras está la creciente profesionalización de la economía de la ciberdelincuencia, incluido el aumento del modelo «como servicio», que incluye el «acceso como servicio», el «phishing como servicio» y las «estafas como servicio». Esta evolución de las operaciones de ciberdelincuencia ha facilitado la entrada a los atacantes en potencia. [Para obtener más información, consulte el Informe de Sophos sobre amenazas 2023].

Selección de ciberataques no relacionados con ransomware ocurridos y porcentaje de organizaciones que los notificaron

27 %	**27 %**	**26 %**
Correo electrónico malicioso	Phishing (incluido el spear phishing)	Exfiltración de datos (por un atacante)
24 %	**24 %**	**21 %**
Ciberextorsión	Estafa por correo electrónico corporativo comprometido	Malware para móviles
18 %	**24 %**	**14 %**
Criptomineros	Denegación de servicio (DDoS)	Wipers

Los ataques de adversarios activos ya son habituales

23 %
de las organizaciones sufrieron un ataque por parte de un adversario activo en el último año

30 %
afirma que los adversarios activos son una de sus principales preocupaciones en materia de ciberseguridad para 2023

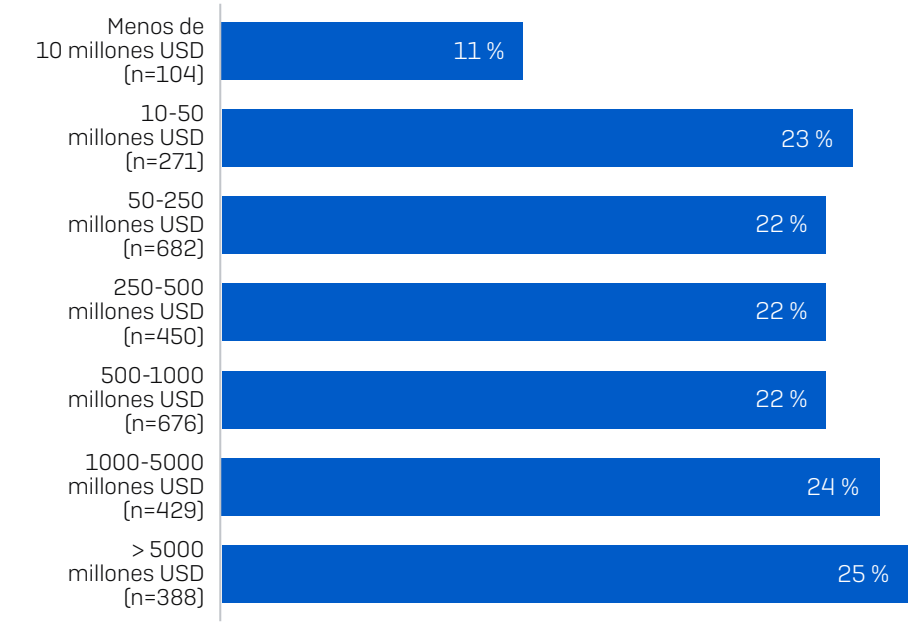
Los adversarios activos son ciberdelincuentes que adaptan sus técnicas, tácticas y procedimientos (TTP) sobre la marcha mediante acciones manuales en tiempo real en respuesta a las medidas adoptadas por las tecnologías y los encargados de la seguridad, y como táctica para eludir la detección. Estos ataques, que a menudo dan lugar a devastadores incidentes de ransomware y filtración de datos, se encuentran entre los más difíciles de detener.

El 23 % de los encuestados declararon que su organización sufrió un ataque perpetrado por un adversario activo en el último año. El índice de ataques fue constante independientemente del tamaño de la organización, variando solo en dos puntos porcentuales en todos los segmentos de tamaño de la organización.

Curiosamente, en el caso de las organizaciones con unos ingresos anuales inferiores a 10 millones USD, el índice de ataques de adversarios activos se redujo a tan solo el 11 %, lo que puede indicar que los ciberdelincuentes se centran deliberadamente en blancos con mayor poder adquisitivo. La detección de adversarios activos requiere un alto nivel de destreza y es probable que el índice real de incidentes sea superior.

Teniendo en cuenta el potencial de devastación de estos ataques, el 30 % de los encuestados señaló que los adversarios activos son una de sus principales preocupaciones en materia de ciberseguridad para 2023.

Organizaciones que han sufrido un ataque de adversarios activos, según los ingresos

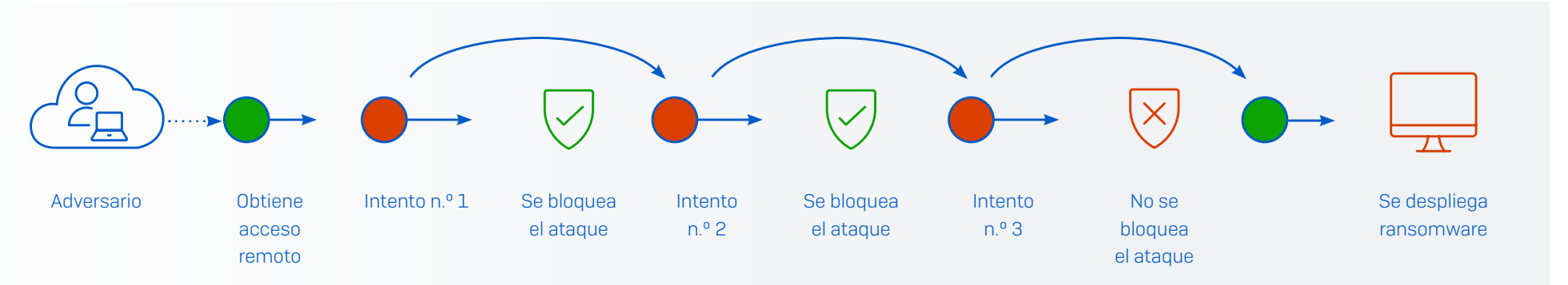


¿Ha sufrido algún ciberataque en el último año? Sí – Adversarios activos (ataques que incluyen hacking manual realizado por humanos)

Entender a los adversarios activos

Para hacerse una idea del reto al que se enfrentan los encargados de la seguridad, es esencial comprender que no basta con bloquear a los adversarios activos para neutralizarlos. Estos hábiles y persistentes ciberdelincuentes despliegan múltiples técnicas, tácticas y procedimientos (TTP) para lograr sus objetivos, entre los que se incluyen:

- Explotar deficiencias de seguridad para penetrar en las organizaciones y moverse lateralmente una vez dentro de la red, incluyendo credenciales robadas, vulnerabilidades sin parchear y errores de configuración de las herramientas de seguridad.
- Utilizar herramientas de TI legítimas usadas por los responsables de la seguridad para evitar que se activen las detecciones.
- Modificar sus ataques en tiempo real en respuesta a los controles de seguridad, recurriendo continuamente a nuevas técnicas hasta encontrar la forma de lograr sus objetivos.



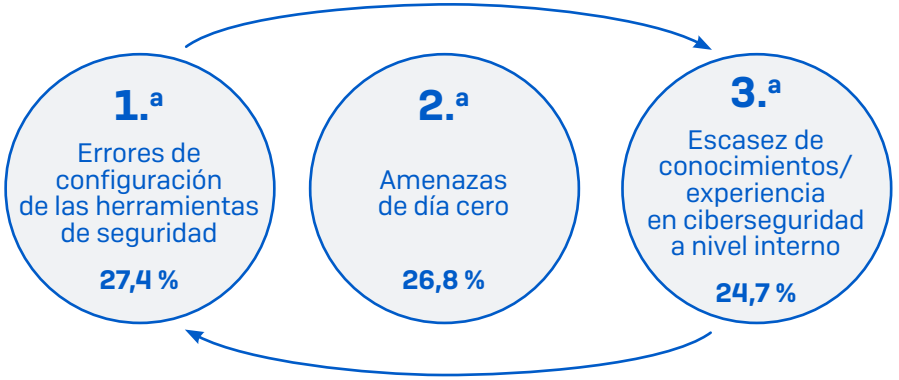
Ciberseguridad 2023: el estado de los encargados de la seguridad

Principales preocupaciones en materia de ciberriesgos

Los errores de configuración de los controles de seguridad (por ejemplo, de una solución para endpoints o firewalls) son el riesgo de seguridad percibido que más se menciona, y un 27,4 % de los encuestados lo incluyen entre los tres mayores ciberriesgos. Este primer puesto ilustra los retos a los que se enfrentan los equipos de TI a la hora de garantizar que sus controles de seguridad permanezcan correctamente configurados y desplegados en todo momento, y la facilidad con la que los adversarios aprovechan cualquier brecha en las defensas de una organización.

Los ataques de día cero, es decir, los que explotan una vulnerabilidad de seguridad o un defecto de software desconocidos hasta el momento, ocupan el segundo lugar, con un 26,8 %. La escasez de conocimientos y experiencia en ciberseguridad a nivel interno ocupa el tercer lugar de la lista, y el 25 % de los encuestados lo considera uno de los tres principales riesgos para la seguridad.

Existe una relación directa entre la escasez de competencias y los errores de configuración de las herramientas de seguridad: al carecer de tiempo, conocimientos y experiencia para configurar correctamente los controles, se crean lagunas en las defensas.



RIESGO DE CIBERSEGURIDAD	PORCENTAJE COMO UNA DE LAS TRES PRINCIPALES PREOCUPACIONES
Errores de configuración de los controles de seguridad (p. ej., de una solución para endpoints o firewalls)	27 %
Amenazas de día cero (amenazas que se aprovechan de una técnica de ataque desconocida hasta el momento)	27 %
Escasez de conocimientos y experiencia en ciberseguridad a nivel interno	25 %
Robo de datos de acceso y credenciales	24 %
Dispositivos desprotegidos (incluidos los desconocidos)	24 %
Escasez de herramientas de ciberseguridad	23 %
Vulnerabilidades sin parchear	22 %
Permitir el acceso a usuarios remotos	20 %
Redes inalámbricas no seguras	20 %
Usuarios internos (accidentalmente)	18 %
Partners/cadena de suministro	18 %
Herramientas de acceso remoto	18 %
Usuarios internos (deliberadamente)	17 %
Dispositivos IoT	17 %
Otros	0 %
Ninguno supone un riesgo de ciberseguridad para mi organización	0 %
No lo saben	0 %

¿Cuáles considera que son los tres principales riesgos para la ciberseguridad en su organización? Combinación de las respuestas clasificadas como primera, segunda y tercera (n=3000)

Diferentes enfoques a la investigación de alertas

Las organizaciones investigan el **48 % de sus alertas de seguridad** para determinar si son indicios de actividad maliciosa

Uno de los retos a los que se enfrentan los responsables de la seguridad es determinar qué alertas investigar y cómo aprovechar al máximo sus limitados recursos.

De media, algo menos de la mitad (48 %) de todas las alertas de seguridad se investigan para identificar si son indicios de actividad maliciosa, porcentaje que se eleva al 54 % en las organizaciones con entre 3001 y 5000 empleados. Sin embargo, los enfoques difieren mucho: el 16 % de las organizaciones investiga más de tres cuartas partes de sus alertas (incluido el 5 % que afirma investigar todas las alertas), mientras que el 18 % investiga una cuarta parte o menos.

Desde una perspectiva sectorial, el gobierno central y federal investiga el porcentaje más bajo de alertas (39 %) (n=89), mientras que los sectores de la energía, el petróleo/gas y los servicios públicos son los que más alertas investigan (55 %) (n=69).

Coste en tiempo de la detección, investigación y respuesta

La mediana de tiempo para detectar, investigar y responder a una alerta es de nueve horas para las organizaciones con 100-3000 empleados, y asciende a 15 horas para las organizaciones con 3001-5000 empleados, lo que probablemente refleja una mayor complejidad de sus entornos operativos.

La encuesta reveló variaciones considerables según el sector: las organizaciones de los sectores de fabricación y producción (15 horas) y energía, petróleo/gas y servicios públicos (18 horas) tardaron más del doble que las de TI, tecnología y telecomunicaciones (6,75 horas).

Es importante señalar que la mayoría de las alertas no llegarán a la fase de respuesta. La mayoría de los ataques serán bloqueados de forma proactiva por las tecnologías de seguridad, mientras que una parte de las alertas se clasificará y someterá a investigación. Las acciones de respuesta también variarán considerablemente según la naturaleza del evento que requiera remediación, desde eliminar un correo electrónico de phishing de la bandeja de entrada de los usuarios hasta reconstruir todo un clúster de servidores.

Mediana de tiempo para detectar, investigar y responder a una alerta

ACTIVIDAD	100-3000 EMPLEADOS (n=2.460)	3.001-5000 EMPLEADOS (n=350)	TI, TECNOLOGÍA Y TELECOMUNICACIONES (n=98)	FABRICACIÓN Y PRODUCCIÓN (n=331)	ENERGÍA, PETRÓLEO/GAS Y SERVICIOS PÚBLICOS (n=66)
Detección	3 horas	3 horas	1,5 horas	3 horas	6 horas
Investigación	3 horas	6 horas	2,25 horas	6 horas	6 horas
Respuesta	3 horas	6 horas	3 horas	6 horas	6 horas
Total	**9 horas**	**15 horas**	**6,75 horas**	**15 horas**	**18 horas**

¿Cuánto tarda su organización en detectar, investigar y, en caso necesario, remediar un posible incidente? (n=2812 encuestados que investigan las alertas a nivel interno)

Las organizaciones carecen de competencias esenciales en operaciones de seguridad

Como ya hemos visto, los profesionales de TI consideran que la escasez de conocimientos/experiencia en ciberseguridad a nivel interno es uno de sus mayores riesgos de seguridad para 2023. Si profundizamos en esta cuestión, la encuesta revela que a la mayoría de las organizaciones les cuesta realizar a diario las tareas básicas de las operaciones de seguridad, y el 93 % califica de «difícil» al menos una de las siguientes actividades:

- Distinguir las señales del ruido (difícil para el 71 %)
- Priorizar qué señales/alertas investigar (difícil para el 71 %)
- Obtener datos suficientes para determinar si una señal es maliciosa o benigna (difícil para el 71 %)
- Remediar alertas o incidentes maliciosos a tiempo (difícil para el 71 %)
- Identificar la causa raíz del incidente (difícil para el 75 %)
- Llevar un registro preciso de las investigaciones (difícil para el 68 %)

Identificar la causa raíz del incidente es el problema más generalizado, y un 75 % de los encuestados afirman que les resulta difícil.

Las organizaciones con los ingresos anuales más bajos (menos de 10 millones USD) son las que más tienden a considerar problemáticas las tareas de las operaciones de seguridad, seguidas de las que tienen mayores ingresos (más de 5000 millones USD). Ambos extremos del espectro se enfrentarán a obstáculos diferentes, y es probable que la complejidad organizativa y de los sistemas desempeñe un papel más importante en las organizaciones más grandes.

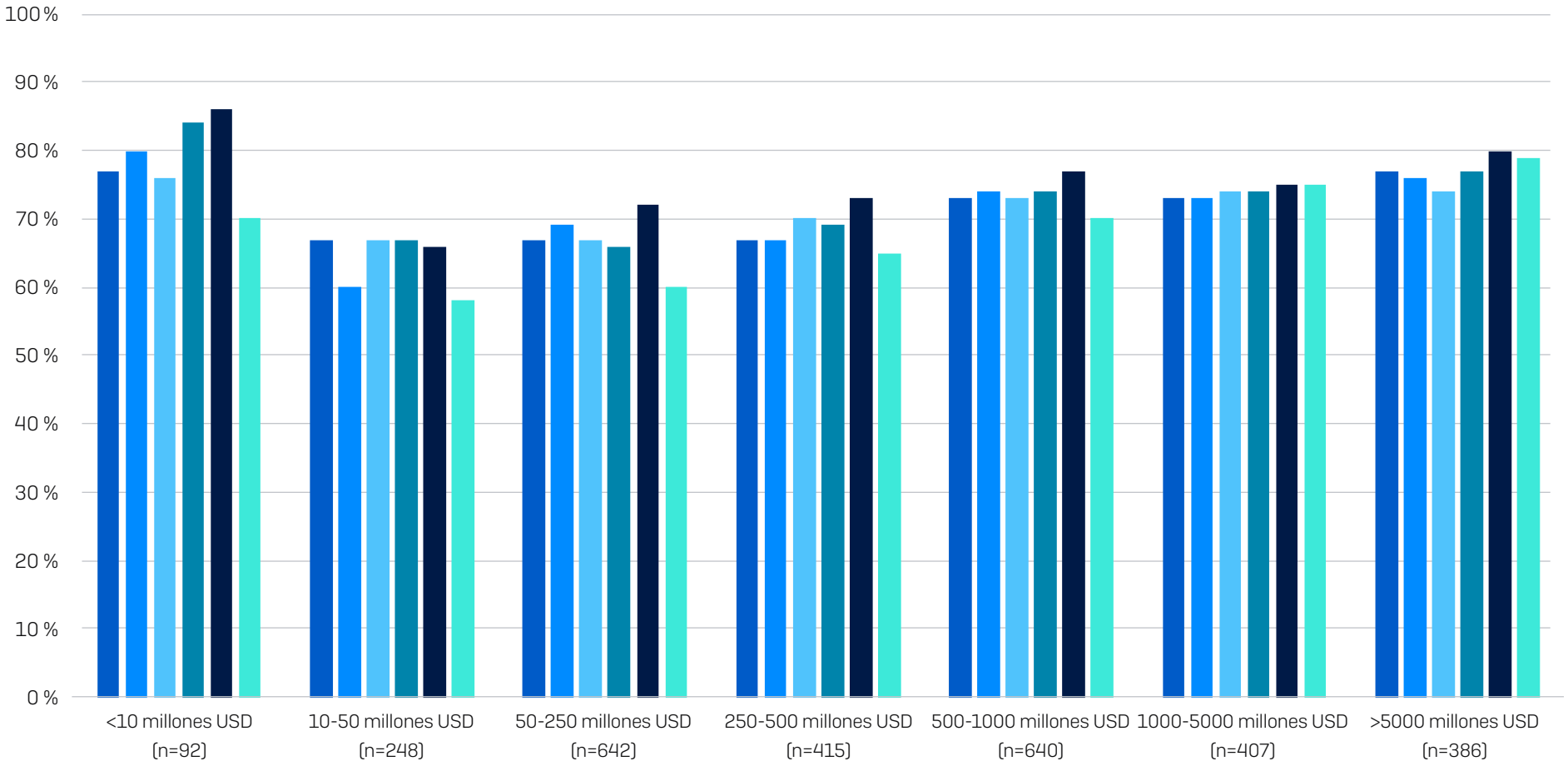
Esta escasez de competencias crea un efecto dominó: investigar las alertas lleva más tiempo, lo que, a su vez, reduce la capacidad del equipo y aumenta la exposición al riesgo.

93 %
consideran que las operaciones de seguridad son un reto

75 %
les cuesta identificar la causa del incidente

71 %
tienen dificultades para determinar qué alertas deben investigarse

Organizaciones a las que les resultan «difíciles» las tareas de operaciones de seguridad, por ingresos



Encuestados cuya organización considera «muy difíciles» o «algo difíciles» las tareas de operaciones de seguridad cuando investigan alertas sospechosas (n=2812 encuestados que investigan alertas de seguridad de forma interna)

- Distinguir las señales del ruido, es decir, saber qué señales o alertas hay que investigar
- Priorizar qué señales/alertas investigar
- Obtener datos suficientes para determinar si una señal es maliciosa o benigna
- Identificar la causa raíz del incidente, es decir, cómo entró el adversario en la organización
- Remediar alertas o incidentes maliciosos a tiempo
- Llevar un registro preciso de las investigaciones

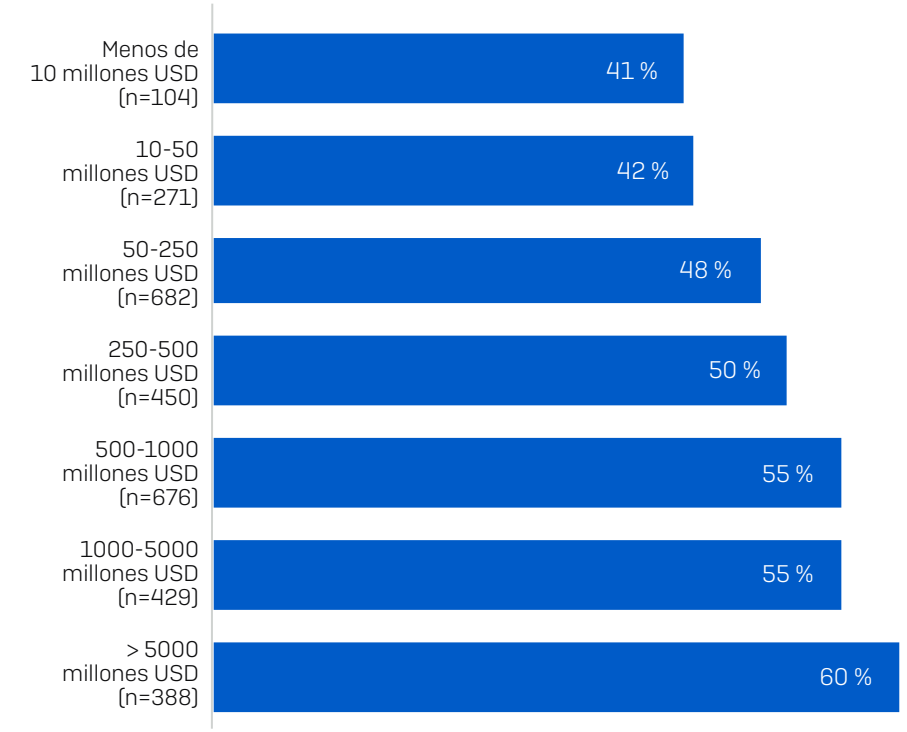
Los adversarios han aventajado a los responsables de la seguridad

52 %
afirma que las ciberamenazas son ahora demasiado avanzadas para que su organización se ocupe de ellas por sí sola

Más de la mitad (52 %) de los profesionales de TI afirman que las ciberamenazas son demasiado avanzadas para que su organización las gestione por sí sola, porcentaje que se eleva al 64 % entre las pequeñas empresas (100-250 empleados).

A medida que aumentan los ingresos de las organizaciones, también lo hace la probabilidad de que los equipos internos no puedan seguir el ritmo. Esto probablemente refleje la mayor complejidad del entorno de ciberseguridad interna en las organizaciones con mayores ingresos, así como una mayor propensión a contratar servicios de seguridad especializados. También puede reflejar una mayor comprensión del entorno de amenazas y de los retos que plantea la defensa frente a las amenazas avanzadas.

Las ciberamenazas son ahora demasiado avanzadas para que la organización se ocupe de ellas por sí sola



¿Hasta qué punto está o no de acuerdo con la afirmación: las ciberamenazas son demasiado avanzadas para que nuestra organización las gestione por sí sola? Muy de acuerdo, un poco de acuerdo (números base en el gráfico)

El impacto en el negocio

Impacto en el cumplimiento del programa de TI

64 %
desearía que el equipo de TI dedicara más tiempo a cuestiones estratégicas y menos a apagar fuegos

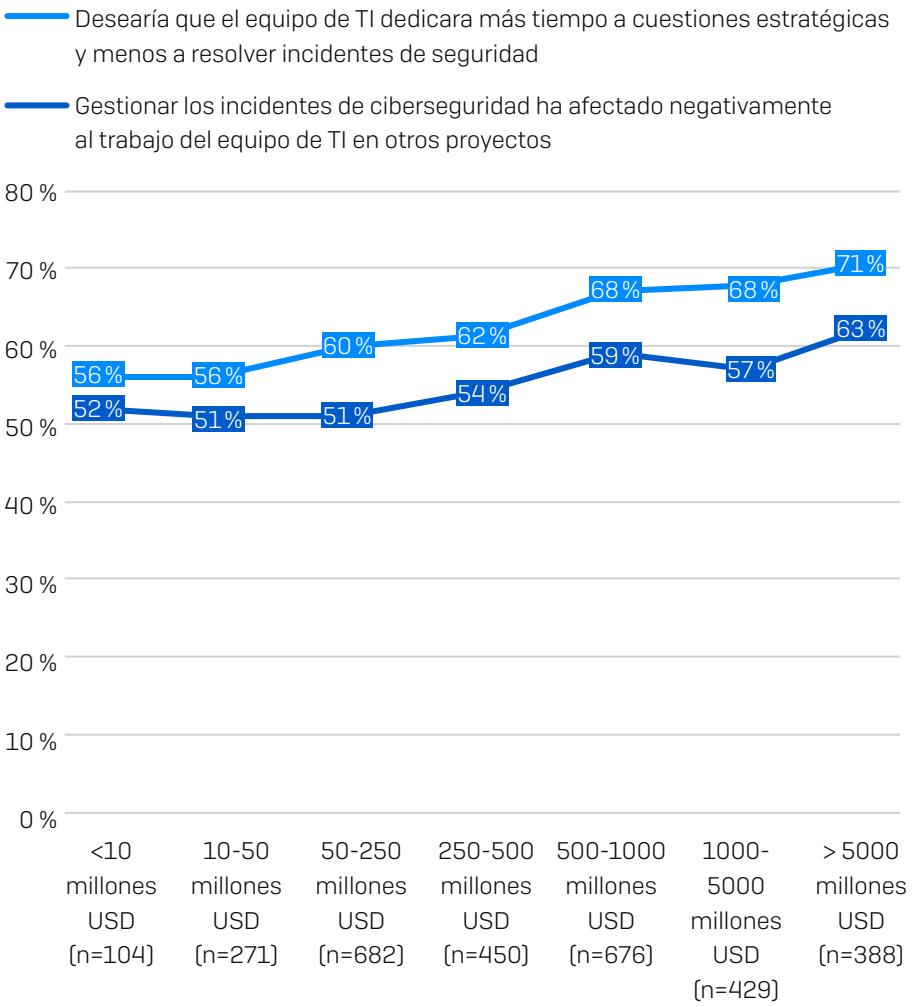
55 %
afirma que lidiar con las ciberamenazas ha repercutido negativamente en el trabajo del equipo de TI en otros proyectos

Para el 60 % de las organizaciones, la ciberseguridad y las funciones de TI en general están estrechamente vinculadas: El 52 % tiene un equipo de ciberseguridad dentro de su equipo de TI, mientras que para el 8 %, el equipo de TI gestiona su ciberseguridad. El 40 % restante tiene equipos independientes de ciberseguridad y TI. El tiempo y el esfuerzo que exige la ciberseguridad tienen consecuencias considerables para la organización de TI.

Más de la mitad (55 %) de las organizaciones afirman que lidiar con las ciberamenazas ha repercutido negativamente en el trabajo del equipo de TI en otros proyectos, siendo las organizaciones con mayores ingresos las que han registrado el mayor impacto.

La naturaleza urgente e impredecible de la ciberseguridad también se interpone en el camino de los esfuerzos centrados en el negocio: De media, el 64 % desearía que el equipo de TI dedicara más tiempo a cuestiones estratégicas y menos a apagar fuegos. De nuevo, conforme aumentan los ingresos, también lo hace el impacto en el cumplimiento del programa de TI en general.

La ciberseguridad afecta negativamente al cumplimiento del programa de TI



Hasta qué punto está o no de acuerdo con la afirmación: Gestionar los incidentes de ciberseguridad ha afectado negativamente al trabajo del equipo de TI en otros proyectos, Desearía que el equipo de TI dedicara más tiempo a cuestiones estratégicas y menos a resolver incidentes de seguridad (números base en el gráfico)

Impacto financiero

El complejo entorno de la ciberseguridad tiene múltiples repercusiones financieras para una organización. Las facturas de remediación más elevadas se producen en caso de ciberincidente grave. Según el informe El estado del ransomware 2022 de Sophos, la factura media de remediación de ransomware asciende a 1,4 millones USD.

Sin embargo, el impacto financiero de lidiar con ciberataques no se limita a los costes de limpieza. Teniendo en cuenta que el salario medio de un especialista en seguridad TI en Estados Unidos es de casi 100 000 dólares anuales[2], el coste por hora en recursos de cada investigación de alertas de seguridad es considerable. Aunque los salarios variarán en función de las condiciones locales, el impacto financiero del largo proceso de investigación de incidentes es notable.

2 Basado en el salario medio de los especialistas en seguridad TI a fecha de marzo de 2023, https://www.indeed.com/career/it-security-specialist/salaries

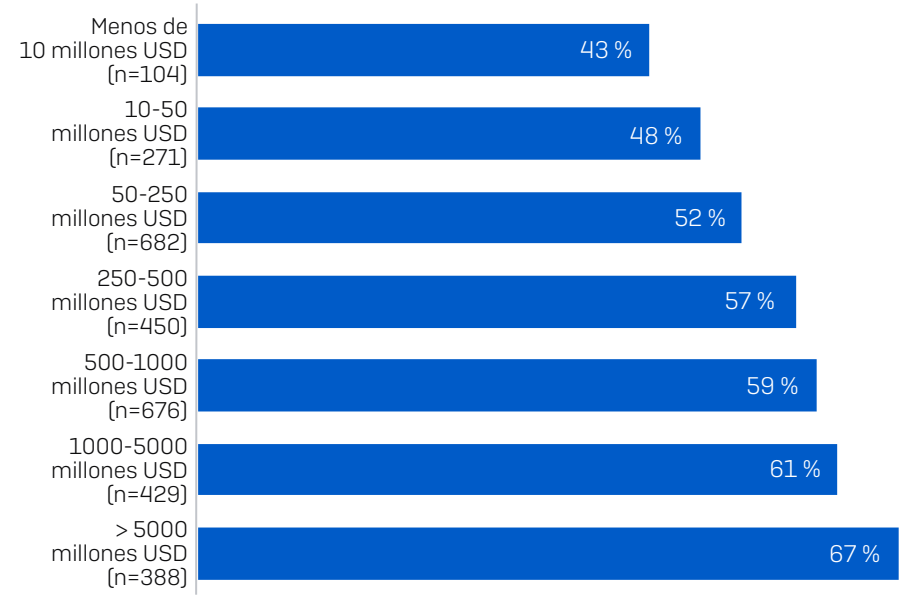
Impacto en el equipo

El 57 % de los encuestados afirma que la preocupación de que la organización sufra un ciberataque a veces les quita el sueño. Dados los elevados costes de contratación y retención de personal en este ámbito, se trata de un motivo de preocupación tanto desde el punto de vista del bienestar como económico. También sugiere que los encargados de la seguridad no confían plenamente en sus herramientas.

El desgaste profesional es uno de los principales problemas en el campo de la ciberseguridad. El exceso de alertas y de tareas supone un estrés considerable para los empleados. Los equipos sobrecargados son más propensos a pasar por alto señales importantes, lo que añade más presión. Con el tiempo, la gente acaba quemándose.

La predisposición a que las preocupaciones por la ciberseguridad quiten el sueño a la plantilla aumenta progresivamente a medida que crecen los ingresos de la organización, desde un 43 % en las organizaciones con ingresos anuales inferiores a 10 millones USD hasta un 67 % en las organizaciones que facturan 5000 millones USD o más.

Porcentaje de encuestados que afirma que temer que la organización sufra un ciberataque les quita el sueño



Hasta qué punto está o no de acuerdo con la afirmación: La preocupación por que la organización sufra un ciberataque a veces me quita el sueño (números base en el gráfico)

Recomendaciones

Para hacer frente a la situación se requiere un sencillo enfoque de tres pasos: implantar un proceso de respuesta a incidentes más escalable que acelere el tiempo de respuesta, potenciar las defensas adaptativas para frenar a los adversarios, y crear un círculo virtuoso que mejore la protección y reduzca los costes.

A modo de analogía, podemos pensar en la frase «arriba escudos». Detener a los adversarios avanzados y persistentes exige que las organizaciones optimicen la eficacia de sus defensas («escudos»), incluidas las tecnologías sensibles al contexto que pueden elevar el nivel de protección en función de la situación. Y, lo que es más importante, también deben aprovechar el tiempo que les conceden sus defensas para aplicar los conocimientos humanos para resolver la causa raíz.

Unos escudos resistentes son esenciales

La calidad de las tecnologías de ciberseguridad es primordial, y los controles de seguridad deben:

- **Optimizar la prevención**, detectando y deteniendo automáticamente el mayor número posible de amenazas en una fase temprana de la cadena de ataque. De este modo, se reduce el riesgo para la organización al tiempo que se libera a los encargados de la seguridad para que se centren en menos incidentes.
- **Reducir la exposición** al facilitar el despliegue correcto y óptimo de las inversiones en seguridad y evitar los problemas relacionados con errores de configuración.
- **Desestabilizar a los adversarios**. Las tecnologías que detectan e interrumpen automáticamente la actividad de los adversarios frenan a los atacantes y dan tiempo a los responsables de la seguridad para neutralizar el incidente.

Optimizar la prevención

Detenga los ataques lo antes posible para minimizar su impacto

Reducir la exposición

Minimice las oportunidades de que los adversarios exploten las lagunas o puntos débiles de la seguridad

Desestabilizar a los atacantes

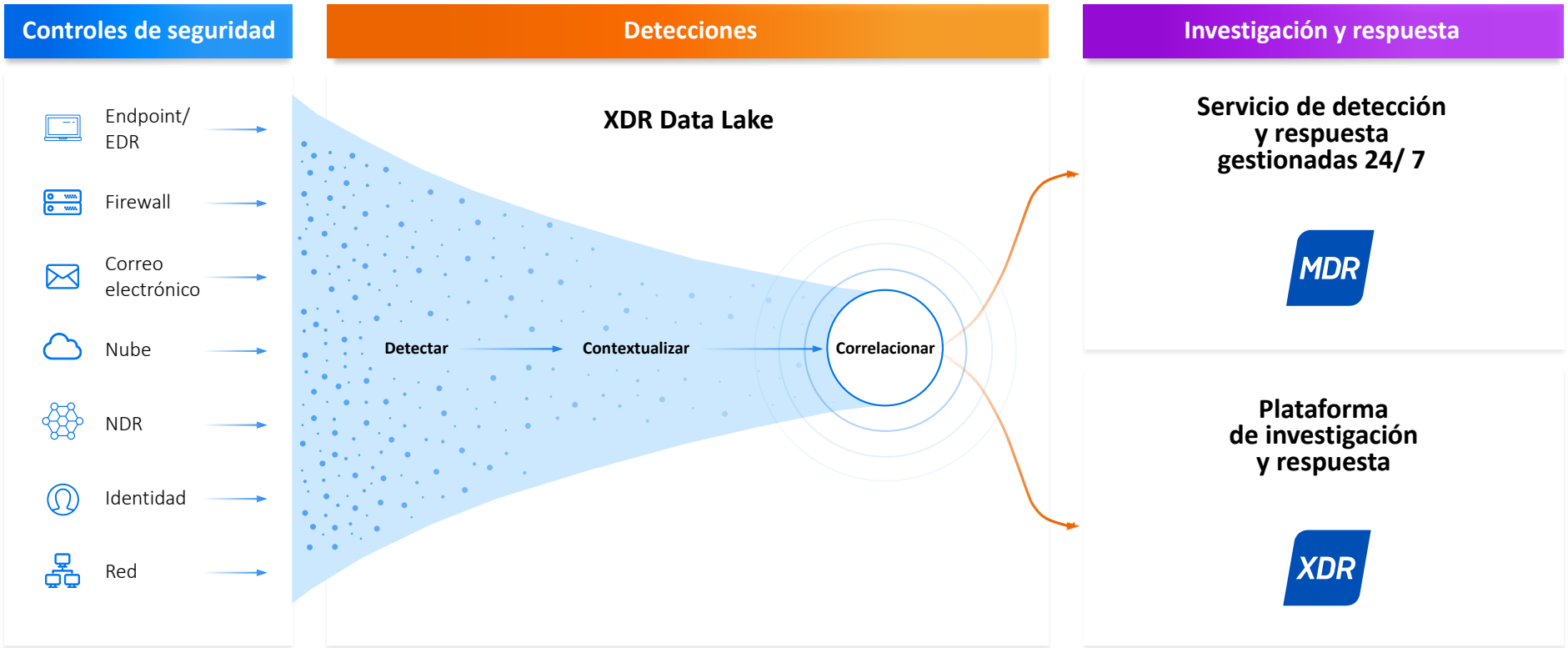
Gane tiempo para que los responsables de la seguridad respondan en caso de un ataque avanzado perpetrado por humanos

Aborde la causa raíz con personas y tecnología

Los escudos permiten a los responsables de la seguridad ganar un tiempo valioso para investigar y responder a los ataques. Sin embargo, no garantizan una prevención del 100 %, por lo que es esencial una remediación rápida, bien informada y bien ejecutada de la causa raíz.

Como ha demostrado la investigación, los adversarios no siguen un único camino. Sacar partido de la telemetría de todo el entorno de seguridad, utilizando los controles de seguridad que las organizaciones ya tienen, permite detectar las amenazas y responder a ellas con mayor rapidez, al tiempo que aumenta el retorno de las inversiones existentes.

Encontrar actividad maliciosa entre las alertas benignas suele ser como buscar una aguja en un pajar, o incluso en una pila de agujas. Procesar las señales a través de una plataforma de detección y respuesta ampliadas (XDR) que añade información contextual y conecta las alertas relacionadas permite a los responsables de la seguridad internos centrarse rápidamente en lo importante. El equipo interno puede llevar a cabo la investigación y la respuesta a través de una plataforma XDR. Otra posibilidad es que las organizaciones subcontraten las tareas de detección, investigación y respuesta a un servicio especializado de detección y respuesta gestionadas (MDR).



Acelere el volante de inercia de los responsables de la seguridad

Una vez que un volante de inercia empieza a girar a alta velocidad, no dejará de hacerlo. Cuanta mayor sea la fuerza que lo impulse, más rápido irá. Las organizaciones pueden impulsar su volante de inercia de ciberseguridad combinando tecnologías de seguridad y experiencia humana. Los controles de seguridad exhaustivos reducen el volumen de alertas que deben atender los responsables de la seguridad, lo que les permite centrarse en neutralizar los ataques y mejorar su postura de seguridad. A su vez, esto incrementa la eficacia de sus controles de seguridad, creando así un círculo virtuoso.

La mayoría de las organizaciones tiene previsto adoptar los controles y servicios de seguridad necesarios

La encuesta reveló que la mayoría de las organizaciones tiene previsto añadir soluciones de detección y respuesta a amenazas a su pila de seguridad en los próximos 12 meses. Más de tres cuartas partes (78 %) tienen previsto añadir herramientas de detección y respuesta para endpoints (EDR) y/o de detección y respuesta ampliadas (XDR) en el próximo año.

Investigar y responder a las ciberamenazas avanzadas es una competencia especializada, y proporcionar cobertura 24/7 requiere un mínimo de cinco o seis personas. La escasez de competencias/experiencia en ciberseguridad a nivel interno figura como uno de los tres principales ciberriesgos percibidos para 2023, por lo que muchas organizaciones buscan el apoyo de expertos externos: el 44 % de las organizaciones tiene previsto empezar a trabajar con un proveedor de detección y respuesta gestionadas (MDR) en los próximos 12 meses.

Porcentaje de organizaciones que tienen previsto adoptar soluciones de detección y respuesta en los próximos 12 meses

78 %	**44 %**
EDR/ XDR	MDR

Sophos puede ayudar

Sophos ofrece los servicios y tecnologías que permiten a las organizaciones impulsar el volante de inercia de los responsables de la seguridad y adelantarse a los adversarios. Protegemos a más de 550 000 organizaciones contra las amenazas más avanzadas, y Sophos MDR es el servicio MDR en el que más confía el mundo.

Empiece con los escudos más resistentes

Nuestras soluciones para endpoints/EDR, redes, firewalls, el correo electrónico y la nube frenan a los atacantes y conceden a los responsables de la seguridad el tiempo y la información que necesitan para responder:

- **Optimice la prevención:** Sophos bloquea automáticamente el 99,98 % de las amenazas desde el primer momento, minimizando el riesgo y permitiendo a los encargados de la seguridad centrarse en menos incidentes que requieran intervención humana.
- **Reduzca la exposición:** la configuración de protección óptima se despliega automáticamente desde el primer día, con lo que se eliminan las carencias de seguridad. Las comprobaciones integradas del estado de seguridad de las cuentas detectan los problemas de configuración y de falta de software que pueden provocar infecciones evitables.
- **Desestabilice a los adversarios:** la protección contra adversarios activos adaptativa pone en marcha inmediatamente las defensas reforzadas cuando se detecta una intrusión manual directa en un endpoint, lo que frena a los atacantes y hace ganar tiempo a los responsables de la seguridad para responder.

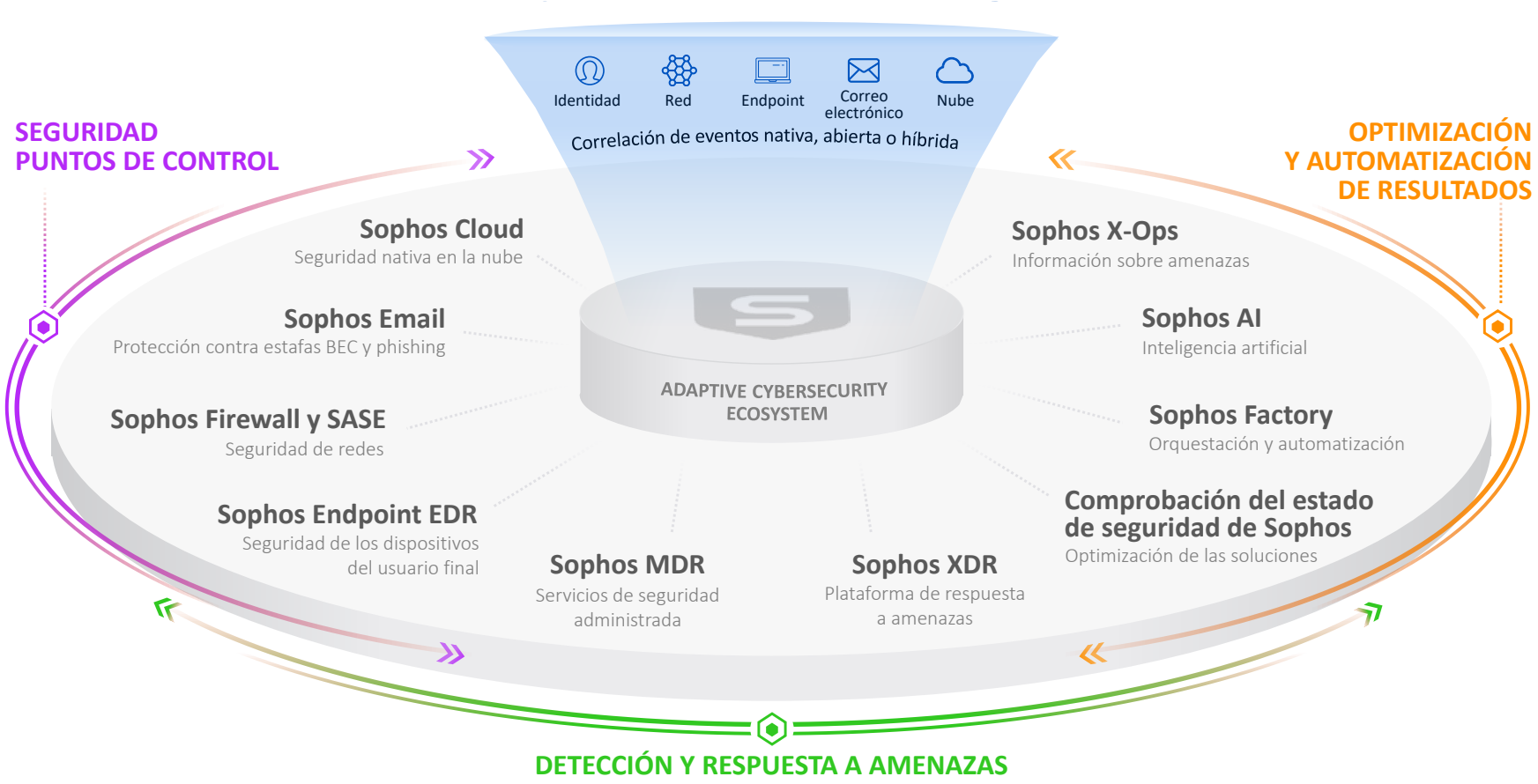
Optimice la detección, investigación y respuesta

Cuanto más vean los encargados de la seguridad, más rápido podrán actuar. En Sophos, utilizamos detecciones de todo el entorno de seguridad, integrando la telemetría tanto de Sophos como de controles de seguridad de terceros para acelerar la detección y la respuesta, y aumentar el retorno de las inversiones en seguridad existentes.

El servicio Sophos MDR cuenta con más de 500 expertos que buscan, investigan y responden a adversarios activos y otros ataques en su nombre 24/7/365. Sophos MDR, con un tiempo medio de respuesta a las amenazas de tan solo 38 minutos, es mucho más rápido que la media de los equipos internos. Las organizaciones también pueden utilizar la plataforma Sophos XDR, que incluye todas las funciones EDR necesarias para investigar y responder a los ataques directamente o trabajar en colaboración con el equipo de Sophos MDR.

Independientemente de dónde se encuentre su organización hoy y dónde quiera estar en el futuro, Sophos puede ayudarle a impulsar el volante de inercia de los responsables de la seguridad y adelantarse a los adversarios avanzados de hoy en día. Para más información, visite es.sophos.com o póngase en contacto con un asesor de seguridad.

Logre resultados óptimos en ciberseguridad con Sophos



2023-03-29 (WP-NP)

SOPHOS