Enterprise Strategy Group | Getting to the bigger truth.™

Modernización de SOC y el rol de XDR

Jon Oltsik, analista principal sénior, socio de ESG
Dave Gruber, analista principal

JUNIO DE 2022

Objetivos de la investigación

Las operaciones de seguridad exigen una escala masiva para recopilar, procesar, analizar y actuar sobre cantidades masivas de datos. El primer XDR estaba anclado a dos fuentes de datos principales: terminales y redes. Si bien esto significó una mejora en las herramientas de EDR y NDR desconectadas, la detección y respuesta de amenazas en las organizaciones empresariales exige una apertura más amplia, incluidas las cargas de trabajo en la nube, las fuentes de inteligencia de amenazas, las aplicaciones de SaaS y la visibilidad de la administración de identidades y accesos. Al mismo tiempo, para modernizar los centros de operaciones de seguridad y mantenerse al día con el volumen de alertas de seguridad, las grandes organizaciones necesitan análisis avanzados para automatizar las tareas de analistas de nivel 1, como la evaluación de alertas, la correlación de alertas con IoC y la preparación de incidentes para las investigaciones.

Con el fin de obtener información sobre estas tendencias, ESG encuestó a 376 profesionales de TI y ciberseguridad de organizaciones en América del Norte (EE. UU. y Canadá) responsables personalmente de evaluar, comprar y utilizar productos y servicios de seguridad de respuesta y detección de amenazas.

ESTE ESTUDIO BUSCÓ:

Examinar las personas, los procesos y la tecnología que respaldan la modernización de las operaciones de seguridad.

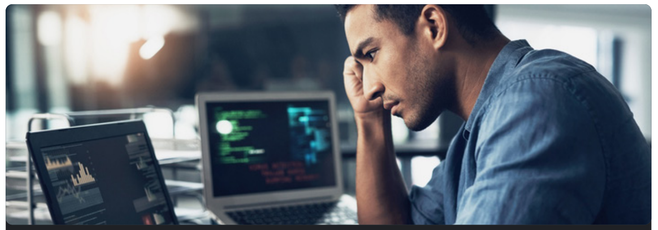
Identificar los puntos de valor clave, las métricas necesarias para respaldar esos puntos de valor y lo que se espera de los productos y servicios administrados para la modernización de XDR y SOC.

Determinar la percepción actual y el rol de XDR como componente de los esfuerzos de modernización de las operaciones de seguridad.

Explorar las estrategias utilizadas para automatizar la evaluación, acelerar las investigaciones y ayudar a las organizaciones a encontrar amenazas desconocidas.

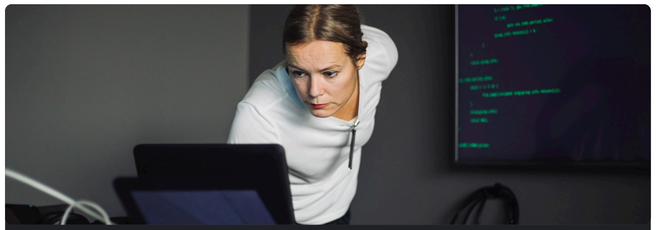
HALLAZGOS CLAVE

HAGA CLIC PARA SEGUIR



Las operaciones de seguridad siguen siendo un desafío.

La creciente dificultad se debe a la mayor superficie de ataque, el peligroso panorama de amenazas y el aumento en el uso de la computación en la nube.



Los profesionales de seguridad quieren más datos y mejores reglas de detección.

Pese a la gran cantidad de datos de seguridad en uso, se desea más, al igual que mejores reglas de detección.

Las inversiones en automatización de procesos de SecOps están demostrando ser valiosas.

Si bien las estrategias de implementación varían, las inversiones en automatización están dando sus frutos para la mayoría.

El marco MITRE ATT&CK está resultando valioso para la mayoría.

Sin embargo, muchos aún están descubriendo cómo y dónde aplicarlo para obtener valor.

El impulso de XDR sigue en auge.

Si bien existe confusión sobre lo que es XDR, la inversión para favorecer la detección avanzada de amenazas es significativa.

MDR es una tendencia dominante y se está expandiendo.

Si bien los casos de uso varían, los servicios de MDR están siendo ampliamente aceptados en organizaciones de todos los tamaños y niveles.

Volver al contenido

Las operaciones de seguridad siguen siendo un reto

Las operaciones de **seguridad** se han vuelto más difíciles en la mayoría de las organizaciones en los últimos años. Específicamente, más de la mitad (52 %) de los encuestados cree que el entorno de operaciones de seguridad de su organización se ha vuelto más difícil de administrar en los últimos dos años. Esto se debe a factores como el panorama de amenazas cada vez más peligroso, una creciente superficie de ataque, el volumen y la complejidad de las alertas de seguridad, y la proliferación de la nube pública. Dado que estos desafíos solo se acelerarán en el futuro, muchos CISO se dan cuenta de que las estrategias de SOC actuales son inadecuadas. Para hacer frente al creciente volumen de amenazas y la escala y la expansión de TI, las organizaciones tienen varias iniciativas centradas en la modernización de los SOC.

52 %

de las organizaciones cree que las operaciones de seguridad son más difíciles hoy que hace dos años.

Las operaciones de seguridad son más difíciles hoy que hace dos años porque:

el panorama de amenazas está creciendo y cambiando rápidamente;

41 %

la superficie de ataque se ha expandido;

40 %

la superficie de ataque cambia y evoluciona continuamente;

39 %

el volumen y la complejidad de las alertas de seguridad han aumentado;

37 %

ha aumentado el uso de servicios de nube pública.

34 %

“Las organizaciones tienen varias iniciativas **centradas en la modernización de los SOC.”**

Volver al contenido

Las operaciones de seguridad se ven afectadas por la escasez global de habilidades

Además de los desafíos generales de las operaciones de seguridad, vale la pena señalar que el 81 % de las organizaciones está de acuerdo en que las operaciones de seguridad se han visto afectadas por la escasez global de habilidades en ciberseguridad. Por lo general, esto conduce a un aumento de la carga de trabajo del personal existente, así como a la deserción y el agotamiento del personal. Los profesionales de seguridad señalan varias áreas en las que el personal y las habilidades son especialmente insuficientes, incluidos los arquitectos de seguridad, los ingenieros de seguridad, los analistas de nivel 3 y los analistas de evaluación/priorización de vulnerabilidades.

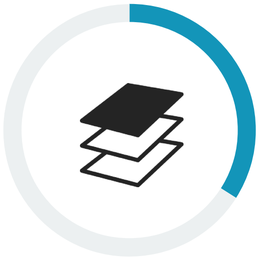
81 %

de las organizaciones coincide en que sus operaciones de seguridad **se han visto afectadas por la escasez de habilidades en ciberseguridad.**

La mayoría de las áreas de operaciones de seguridad cuentan con poco personal.

Arquitecto de seguridad
37 %

Ingenieros de seguridad
35 %



Analistas de nivel 3*
34 %

Analistas de evaluación/ priorización de vulnerabilidades
33 %

** Es decir, similar a los analistas de nivel 2, pero con más experiencia y centrados en problemas difíciles o críticos.*

Volver al contenido

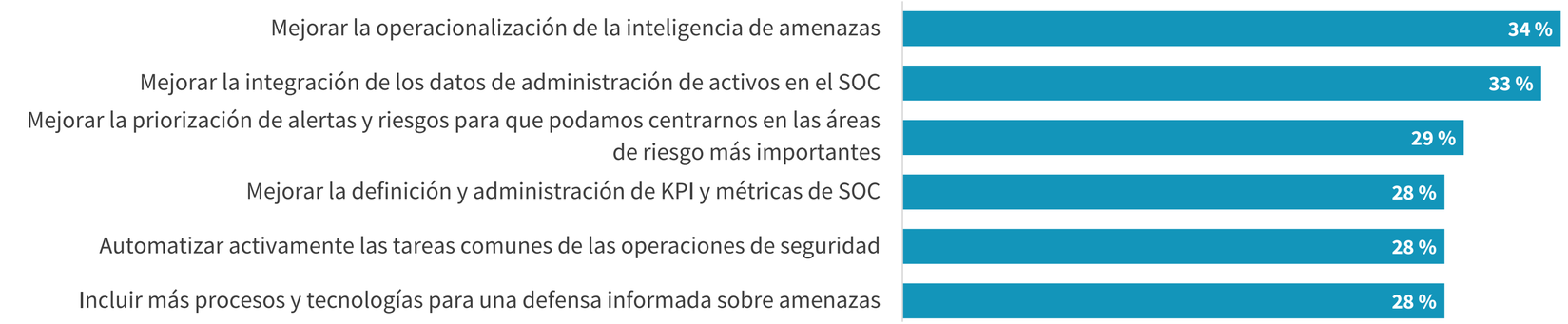
Prioridades de modernización del SOC a corto plazo

¿Cómo planean las organizaciones lidiar con entornos de operaciones de seguridad cada vez más difíciles, incluidos niveles de personal insuficientes? La modernización de los SOC es una iniciativa clave del programa; cabe señalar que el 88 % de las organizaciones aumentaron el gasto en operaciones de seguridad este año. A corto plazo, los equipos de SOC planean centrar sus esfuerzos en áreas como mejorar la operatividad de la inteligencia de amenazas, mejorar la integración de datos de administración de activos en el SOC, mejorar la priorización de riesgos y alertas, mejorar la definición y administración de los KPI de SOC, y automatizar tareas comunes de operaciones de seguridad.

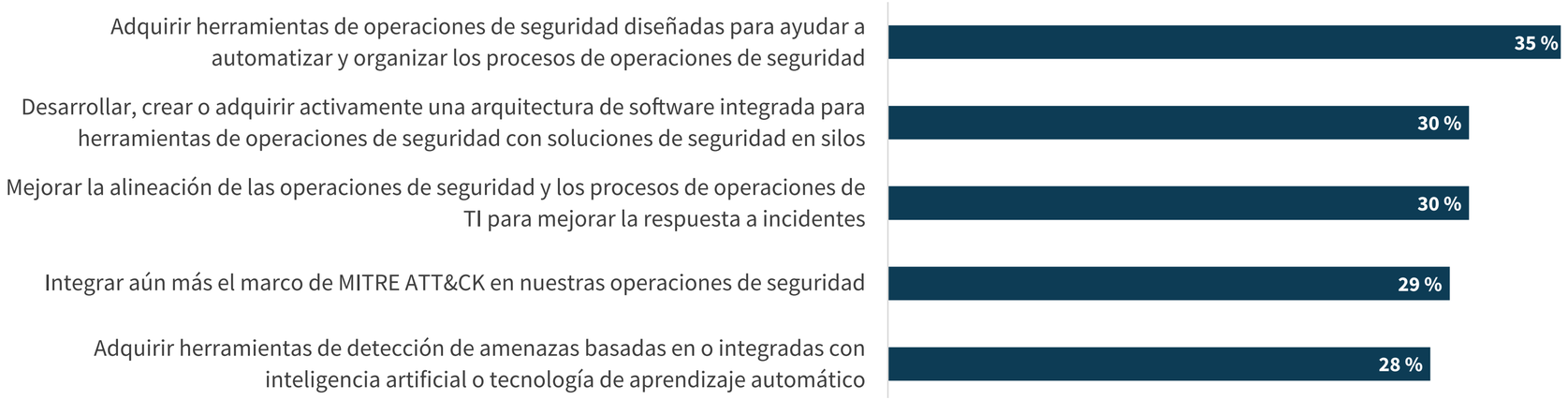
Más adelante, las organizaciones realizarán otras acciones en favor de la modernización de los SOC, como compra de herramientas de automatización del proceso de seguridad, desarrollo o creación de operaciones de seguridad integradas y arquitectura de plataforma de análisis (SOAPA), mejorar la alineación de las operaciones de seguridad y de TI, integrar aún más el marco MITRE ATT&CK en las operaciones de seguridad, y comprar herramientas de análisis avanzado para la detección de amenazas.

Estos avances llevarán tiempo y pueden requerir soporte de servicios de seguridad. Sin embargo, deben verse como paradas en un viaje hacia la modernización de los SOC. El objetivo es crear un SOC que pueda ofrecer la escala, el rendimiento, la inteligencia, la automatización y la capacidad de administración para prevenir, detectar y responder a las amenazas, administrar el riesgo y respaldar la misión de la organización.

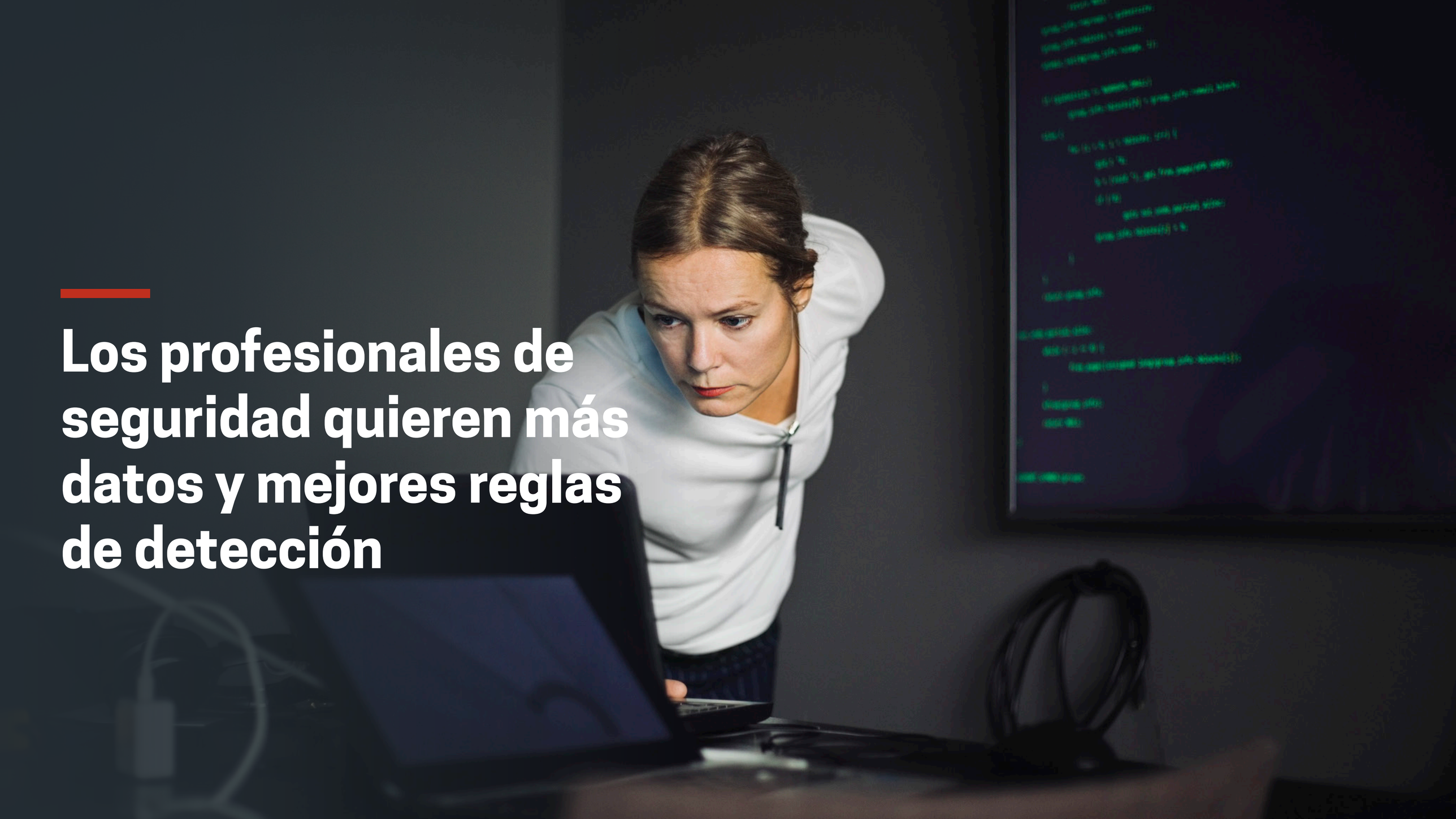
Objetivos centrados en el SOC previstos para los próximos 12 meses.



Acciones previstas para mejorar las operaciones de seguridad en los próximos 12 a 18 meses.



Volver al contenido



Los profesionales de seguridad quieren más datos y mejores reglas de detección

A pesar del cambio a XDR, los datos de terminales siguen siendo los más valiosos

Ocho de cada diez organizaciones recopilan, procesan y analizan datos de operaciones de seguridad de más de diez fuentes de datos. Los profesionales de la seguridad creen que las fuentes más importantes son los datos de seguridad de los terminales, las fuentes de inteligencia de amenazas, los registros de dispositivos de seguridad, los datos de administración de la postura en la nube y los registros de flujo de la red. Si bien esto parece una gran cantidad de datos, los encuestados realmente quieren utilizar más datos para las operaciones de seguridad, lo que impulsa la necesidad de repositorios de datos back-end escalables, de alto rendimiento y basados en la nube.

80 %

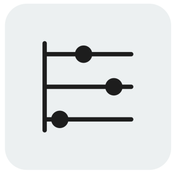
de las organizaciones utilizan más de 10 fuentes de datos como parte de las operaciones de seguridad.

> “Los encuestados realmente desean utilizar **más datos para las operaciones de seguridad.**”

Fuentes de datos más importantes para las operaciones de seguridad.

24 %
Datos de seguridad del terminal

21 %
La inteligencia de amenazas Fuentes

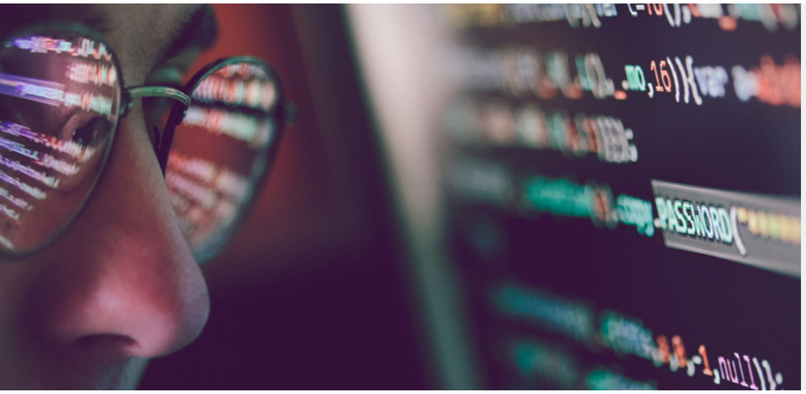


20 %
Registrar datos de dispositivos de seguridad

20 %
Sistemas de administración de la postura de seguridad en la nube

18 %
Datos de NetFlow o IPFIX o registros de flujo de VPC

Volver al contenido

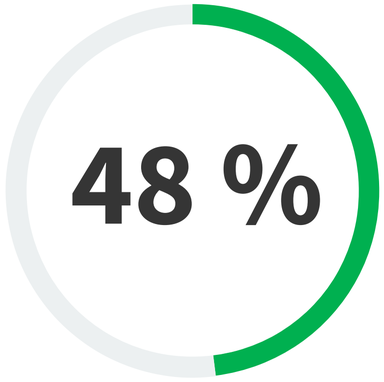


La mayoría de las organizaciones desarrollan sus propias reglas de detección personalizadas

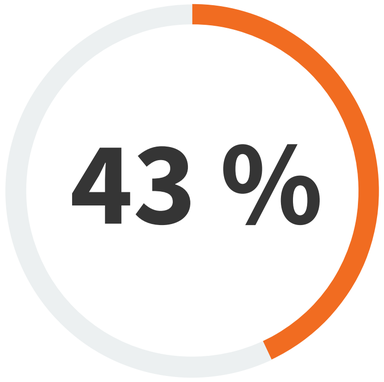
Si bien los proveedores proporcionan volúmenes crecientes de contenido listo para usar para la detección de amenazas, el 91 % de las organizaciones complementa estos esfuerzos con su propia ingeniería de detección. De hecho, los equipos de SOC recopilan, procesan y analizan una variedad de telemetría de seguridad para ayudarlos a determinar las debilidades de detección donde se necesitan reglas personalizadas. Los equipos de seguridad personalizan los conjuntos de reglas del proveedor para satisfacer sus necesidades y desarrollan reglas personalizadas para detectar amenazas dirigidas a su sector u organización. Para respaldar esta tendencia, los proveedores deben facilitar la cooperación de la red de los usuarios al tiempo que adoptan estándares abiertos, como Sigma y YARA, con el soporte establecido de la industria.

Alcance de las reglas personalizadas de detección de amenazas.

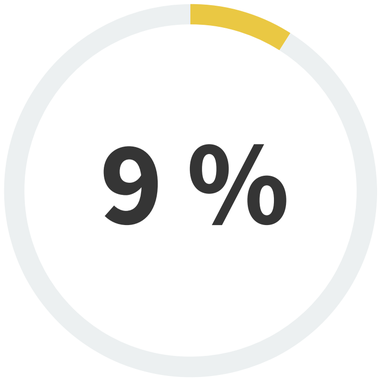
Mi organización desarrolla una cantidad significativa de reglas personalizadas para complementar las reglas de detección proporcionadas por los proveedores.



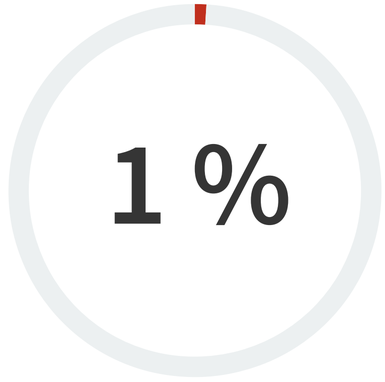
Mi organización desarrolla algunas reglas personalizadas para complementar las reglas de detección proporcionadas por los proveedores



Mi organización puede desarrollar una pequeña cantidad de reglas de detección personalizadas, pero se basa principalmente en las proporcionadas por los proveedores

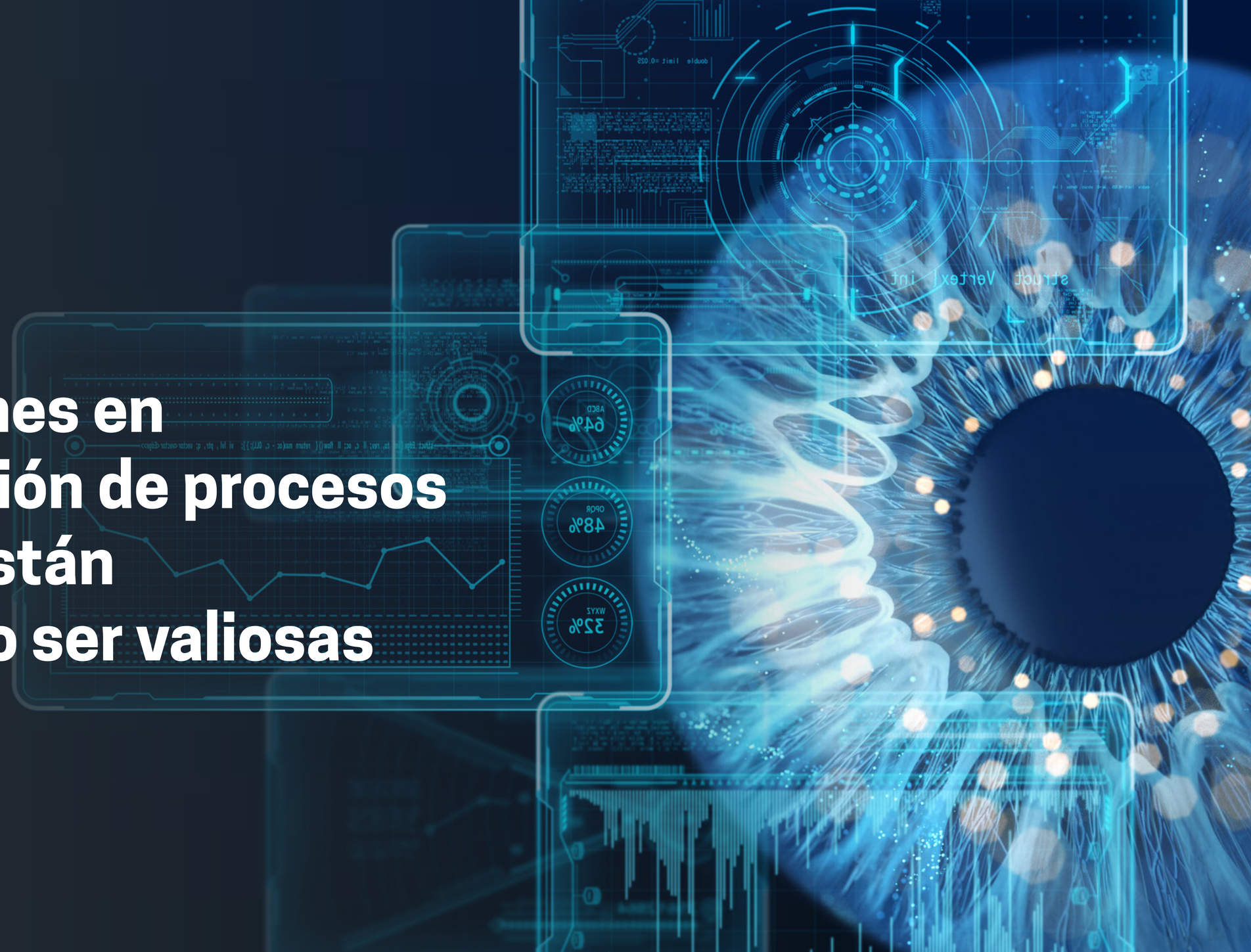


Mi organización no desarrolla ninguna regla de detección personalizada y se basa completamente en las proporcionadas por los proveedores



Volver al contenido

Las inversiones en automatización de procesos de SecOps están demostrando ser valiosas



Muchas organizaciones se han beneficiado de la automatización de los procesos de seguridad, pero los desafíos persisten

La automatización de procesos de seguridad es popular, como lo demuestra el 90 % de las organizaciones que actualmente automatizan los procesos de operaciones de seguridad, y el 46 % describe sus esfuerzos de automatización como extensos. Quienes participan en la automatización de procesos de seguridad informan beneficios como una mejor detección de amenazas mediante cuadernos de estrategias, MTTR y priorización de incidentes, así como la capacidad de aislar más rápidamente los recursos infectados. Dados los desafíos de las operaciones de seguridad, como la creciente superficie de ataque, las tormentas de alertas y el panorama de amenazas peligrosas, la automatización de los procesos de seguridad continuará y probablemente se fusionará con la automatización de los procesos de TI para ofrecer eficiencias en toda la TI y la seguridad.

Si bien la automatización de procesos de seguridad sigue siendo popular y beneficiosa, conlleva algunos desafíos. Casi dos de cada cinco (39 %) organizaciones afirman que su equipo de operaciones de seguridad no tiene las habilidades de programación adecuadas para desarrollar runbooks o flujos de trabajo en herramientas SOAR, mientras que el 21 % afirma que sus procesos de operaciones de seguridad son inmaduros y necesitan una nueva ingeniería antes de poder automatizarse. En estos casos, las organizaciones necesitan más para evaluar los flujos de trabajo de los procesos, y buscan cuellos de botella antes de pasar a la automatización. Aquellos con habilidades de programación limitadas deben investigar las opciones de SOAR de código bajo o sin código, o utilizar la funcionalidad de automatización de procesos integrada en otras herramientas de operaciones.

Beneficios más comúnmente obtenidos de la automatización de procesos de operaciones de seguridad.

Mejor detección de amenazas con cuadernos de estrategias

51 %

Mejor tiempo promedio de respuesta

49 %

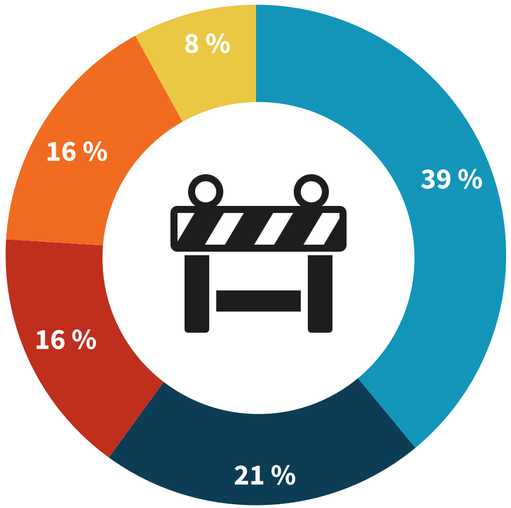
Priorización mejorada de incidentes

44 %

Recursos infectados aislados con mayor rapidez

44 %

Los mayores impedimentos para la automatización de procesos de operaciones de seguridad.



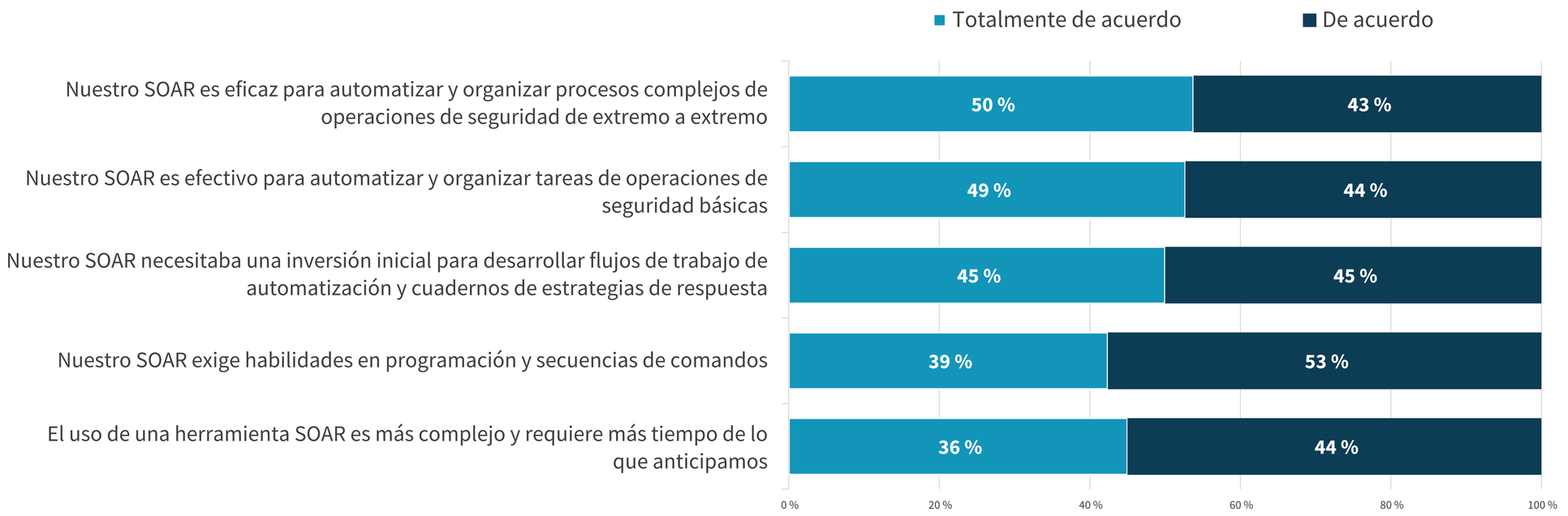
- Habilidades de desarrollo de software: nuestro equipo de operaciones de seguridad no tiene las habilidades de programación para desarrollar runbooks o flujos de trabajo.
- Falta de madurez de los procesos: nuestros procesos de operaciones de seguridad son relativamente inmaduros, por lo que realmente tendríamos que rediseñarlos antes de proceder con la automatización de procesos.
- Tiempo: el equipo de seguridad no tiene tiempo suficiente para trabajar en la automatización de procesos.
- Herramientas: nuestra organización no tiene tecnologías, como SOAR, necesarias para la automatización del proceso de seguridad.
- Sin impedimentos.

Volver al contenido

Las herramientas SOAR pueden generar resultados con las inversiones y expectativas adecuadas

Más de una cuarta parte (29 %) de las organizaciones utilizan algún tipo de herramienta de organización, automatización y respuesta de seguridad (SOAR) para la automatización de procesos. El uso de SOAR puede ser beneficioso: el 93 % de los profesionales de seguridad está de acuerdo en que su SOAR es eficaz para automatizar los complejos procesos de operaciones de seguridad de extremo a extremo y para automatizar u organizar las tareas básicas de las operaciones de seguridad. Sin embargo, SOAR no es gratis. El éxito depende de una planificación inicial, inversiones y las habilidades adecuadas. Por ejemplo, el 90 % de los profesionales de seguridad afirma que SOAR necesitaba una inversión inicial para crear flujos de trabajo de automatización y estrategias de respuesta, el 92 % coincide en que SOAR exige habilidades de programación y secuencias de comandos, y el 80 % coincide en que usar una herramienta SOAR es más complejo y requiere más tiempo de lo previsto. En función de estos datos, las organizaciones deben reconocer que SOAR debe verse como un proyecto, no como una panacea. Los beneficios de SOAR solo se pueden lograr con el nivel adecuado de planificación, capacitación y administración de proyectos.

Sentimiento respecto de las herramientas de organización, automatización y respuesta de seguridad (SOAR)



“El uso de SOAR puede ser beneficioso.”

Volver al contenido

El marco MITRE ATT&CK está demostrando ser valioso para la mayoría

La mayoría de las organizaciones utiliza y ve el valor en el marco de MITRE ATT&CK para las operaciones de seguridad

El marco de trabajo MITRE ATT&CK ha ganado popularidad hasta el punto de que casi nueve de cada diez organizaciones lo usan en cierta medida hoy en día. Cuando los administradores de SOC miran hacia el futuro, ven un uso mucho más elevado de MITRE. De hecho, el 97 % de los profesionales de seguridad cree que MITRE ATT&CK (y los proyectos derivados) serán fundamentales, muy importantes o importantes para la estrategia de operaciones de seguridad de su organización.

Uso del marco MITRE ATT&CK para operaciones de seguridad.

¿Las organizaciones utilizan el marco de trabajo MITRE ATT&CK para las operaciones de seguridad?

Importancia del marco de trabajo MITRE ATT&CK para las operaciones de seguridad.

97 %

de los profesionales de seguridad creen que MITRE ATT&CK (y los proyectos derivados) serán fundamentales, muy importantes o importantes para la estrategia de operaciones de seguridad de su organización.

Volver al contenido

Aumentan los casos de uso de MITRE ATT&CK

MITRE ATT&CK también se ha convertido en una pieza clave en una variedad de procesos de operaciones de seguridad. De las organizaciones que adoptan el marco de MITRE ATT&CK, el 38 % lo usa para ayudarlos a aplicar la inteligencia de amenazas en su evaluación de alertas o el proceso de investigación, el 37 % lo usa como lineamiento para la ingeniería de seguridad, el 35 % usa MITRE para comprender mejor las tácticas, las técnicas y procedimientos de los adversarios cibernéticos, y el 34 % utiliza el marco para lograr comprender el alcance total de los ataques con mayor rapidez.

De esta manera, las organizaciones operativizan MITRE ATT & CK en la prevención, detección y respuesta de amenazas.

Maneras en las que las organizaciones utilizan el marco de trabajo de MITRE ATT&CK.

Para ayudarnos a aplicar mejor la inteligencia de amenazas en nuestros procesos de evaluación o investigación de alertas.

38 %

Como lineamiento para la ingeniería de seguridad.

37 %

Para comprender mejor las tácticas, las técnicas y los procedimientos de los adversarios cibernéticos.

35 %

Para ayudar a las organizaciones a comprender con mayor rapidez el alcance total de los ataques.

34 %

Para asegurarnos de estar recopilando los datos correctos de las fuentes de datos correctas.

33 %

> “MITRE ATT&CK también se ha convertido en **fundamental en una variedad de procesos de operaciones de seguridad.”**

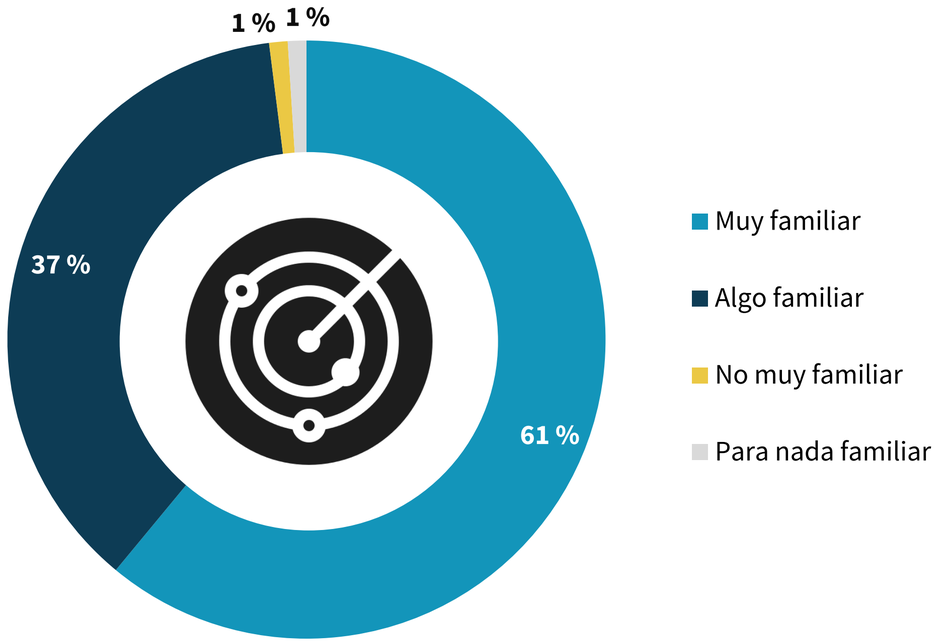
Volver al contenido

El impulso de XDR continúa en aumento

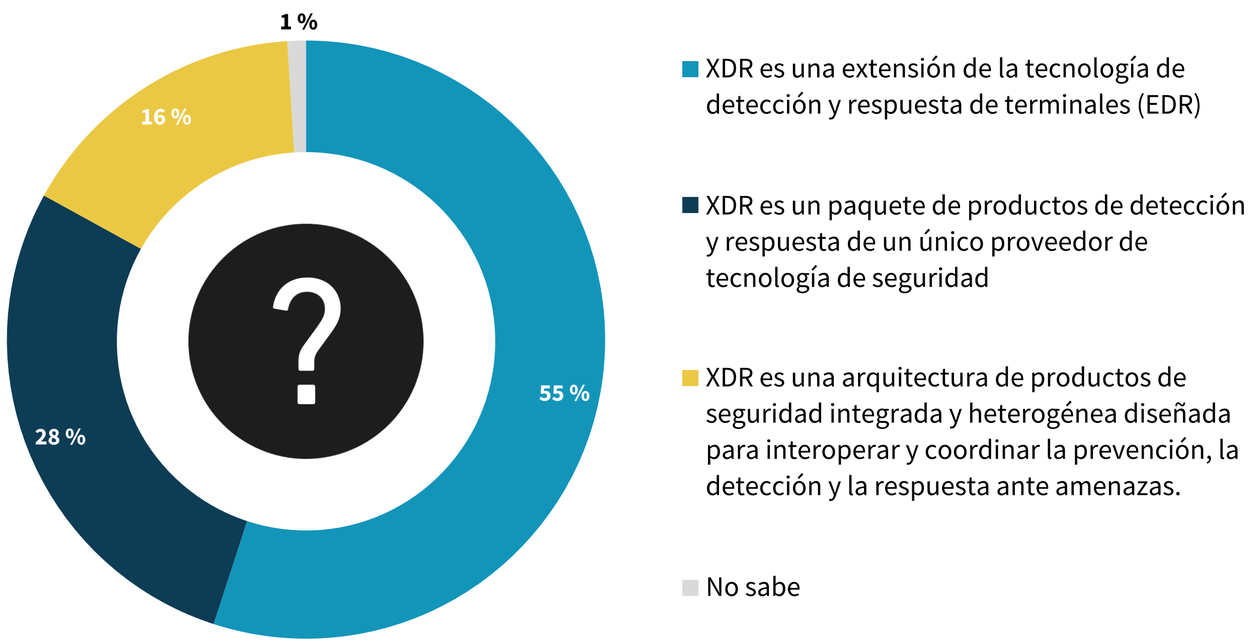
El conocimiento de XDR continúa desarrollándose, aunque la mayoría ve las tecnologías de SOC que complementan o consolidan XDR

Si bien XDR ha obtenido mayor atención por parte de la industria, sigue siendo un concepto amorfo con diferentes componentes y definiciones. Esto se refleja en el hecho de que el 61 % de los profesionales de seguridad afirman estar muy familiarizados con la tecnología XDR. Si bien esto es una mejora con respecto a la investigación de ESG de 2020 (cuando solo el 24 % de los profesionales de seguridad estaban muy familiarizados con XDR), el 39 % aún está algo familiarizado, no está muy familiarizado o no está en absoluto familiarizado con XDR. Los usuarios también están confundidos sobre qué es XDR. Si bien el 55 % de los encuestados afirma que XDR es una extensión de EDR, el 44 % cree que XDR es un producto de detección y respuesta de un solo proveedor de tecnología de seguridad, o una arquitectura de productos de seguridad integrada y heterogénea diseñada para interoperar y coordinar la prevención, detección y respuesta. Es seguro decir que XDR sigue siendo un trabajo en progreso.

Familiaridad con la tecnología XDR.



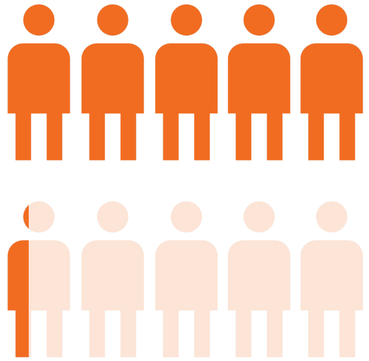
Definiciones organizativas de la tecnología XDR.



Volver al contenido

La mayoría ve las tecnologías de SOC que complementan o consolidan XDR

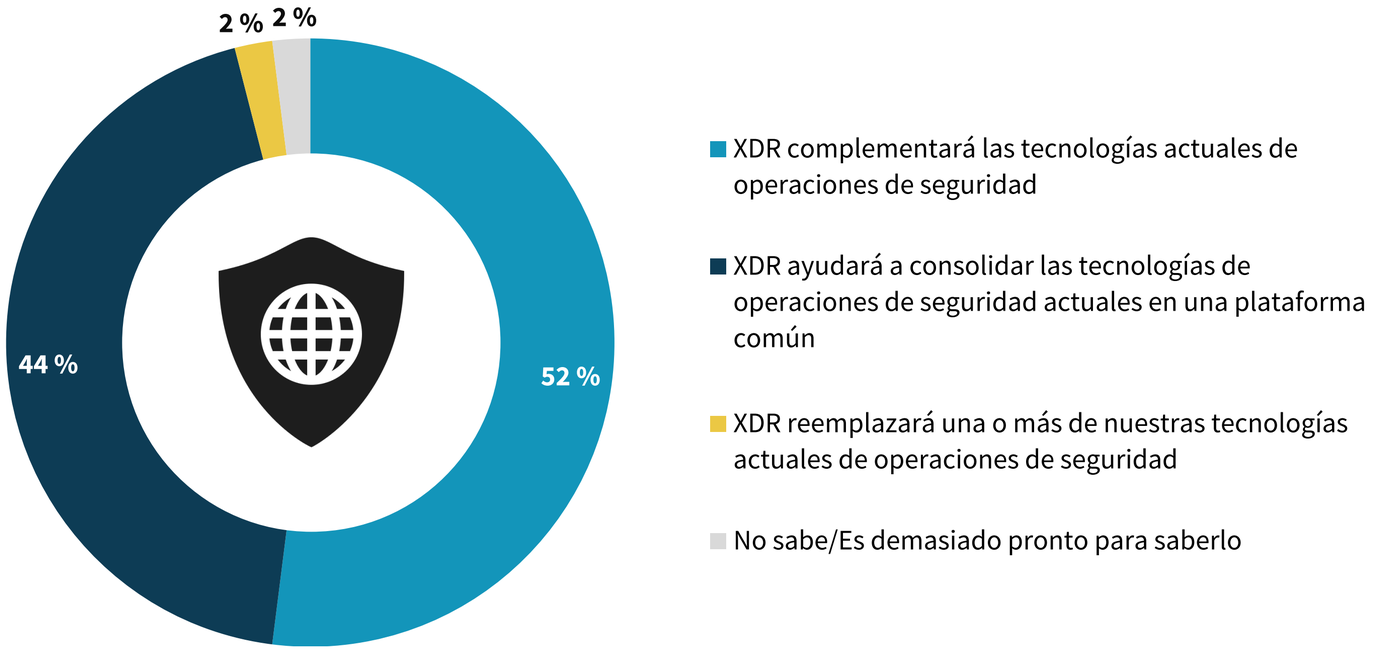
En ese sentido, en este momento, XDR no se considera un reemplazo potencial para las tecnologías SOC como SIEM, SOAR y TIP. Por el contrario, más de la mitad (52 %) de los profesionales de seguridad creen que XDR complementará las tecnologías de operaciones de seguridad existentes, mientras que el 44 % considera que XDR consolida las tecnologías de operaciones de seguridad actuales en una plataforma común. Solo el 2 % cree que XDR reemplazará cualquier tecnología de operaciones de seguridad actual.



MÁS DE LA MITAD

de los profesionales de la seguridad creen que **XDR complementará las tecnologías de operaciones de seguridad existentes.**

Impacto esperado de XDR en los entornos de operaciones de seguridad.



Volver al contenido

Los usuarios desean que XDR aborde los desafíos comunes de detección y respuesta de amenazas

Independientemente de cómo se defina XDR, los profesionales de seguridad están interesados en usar XDR para ayudarlos a abordar varios desafíos de detección y respuesta de amenazas. XDR parece una opción atractiva, ya que las herramientas actuales tienen dificultades para detectar e investigar amenazas avanzadas, requieren habilidades especializadas y no son eficaces para correlacionar las alertas. En resumen, los CISO quieren herramientas XDR que puedan mejorar la eficacia de la seguridad, especialmente en lo que respecta a la detección avanzada de amenazas. Además, quieren que XDR optimice las operaciones de seguridad y aumente la productividad del personal.

Los profesionales de la seguridad parecen tener en mente varios casos de uso comunes de XDR. Por ejemplo, el 26 % de los profesionales de seguridad desea que XDR contribuya a priorizar las alertas basadas en el riesgo, el 26 % busca una detección mejorada de amenazas avanzadas, el 25 % desea investigaciones de amenazas o análisis forenses más eficientes, el 25 % desea una incorporación en capas a las herramientas de detección de amenazas existentes y el 25 % considera que XDR podría mejorar la detección de amenazas para reforzar los controles de seguridad y evitar futuros ataques similares. Claramente, los usuarios desean que XDR cubra las brechas dentro de la pila de seguridad y, al mismo tiempo, mejore la eficacia de la detección y la respuesta ante amenazas.

Los cinco desafíos más comunes que impulsan el interés de XDR.

51 %

Las herramientas actuales tienen dificultades para detectar e investigar amenazas avanzadas

38 %

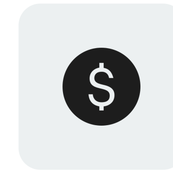
Las herramientas actuales requieren demasiadas habilidades especializadas

36 %

Las herramientas actuales no son eficaces para correlacionar alertas

35 %

Brechas específicas en las capacidades de detección y respuesta en la nube



32 %

El enfoque actual de las herramientas es demasiado costoso

Cinco casos de uso de XDR de máxima prioridad.

26 %

Una solución XDR que podría ayudar a priorizar las alertas basadas en el riesgo

26 %

Detección mejorada de amenazas avanzadas

25 %

Análisis forenses o investigaciones de amenazas más eficientes

25 %

Adición en capas a las herramientas de detección de amenazas existentes, con el objetivo de identificar amenazas avanzadas o más complejas

25 %

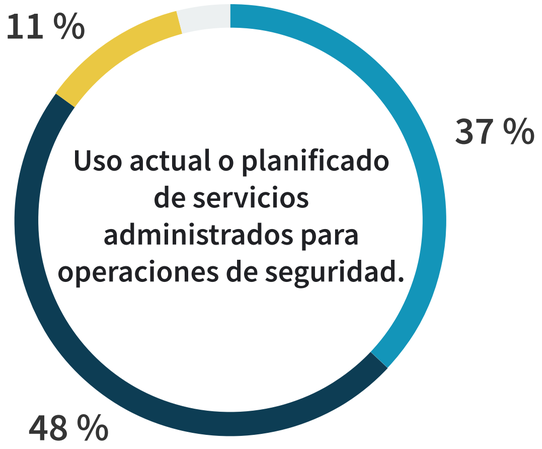
Uso de la detección de amenazas mejorada para reforzar los controles de seguridad y prevenir futuros ataques similares

Volver al contenido

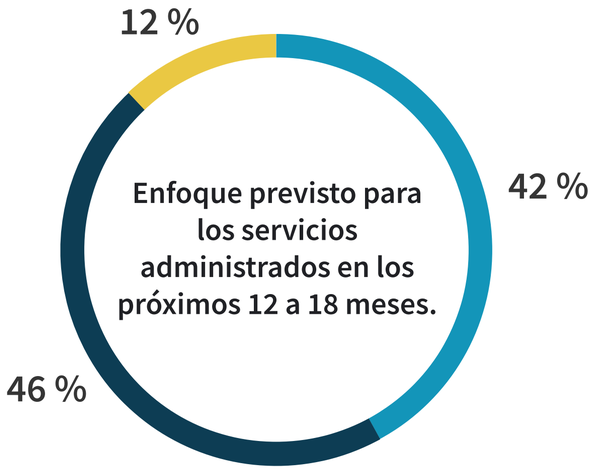
MDR es convencional y se está expandiendo

El uso de MDR es generalizado... y va en aumento

Independientemente de las definiciones de tecnología o las estrategias de implementación, los datos de ESG demuestran una verdad casi universal: las organizaciones necesitan ayuda de los proveedores de servicios para las operaciones de seguridad. El 85 % de las organizaciones utiliza servicios administrados para una parte o la mayoría de sus operaciones de seguridad en la actualidad. Y de los que utilizan servicios de seguridad administrados, el 88 % aumentará el uso de servicios administrados para las operaciones de seguridad en el futuro.



- Utilizamos servicios administrados para la mayoría de nuestras operaciones de seguridad
- Utilizamos servicios administrados para una parte de nuestras operaciones de seguridad
- Utilizamos servicios administrados para operaciones de seguridad con capacidad limitada



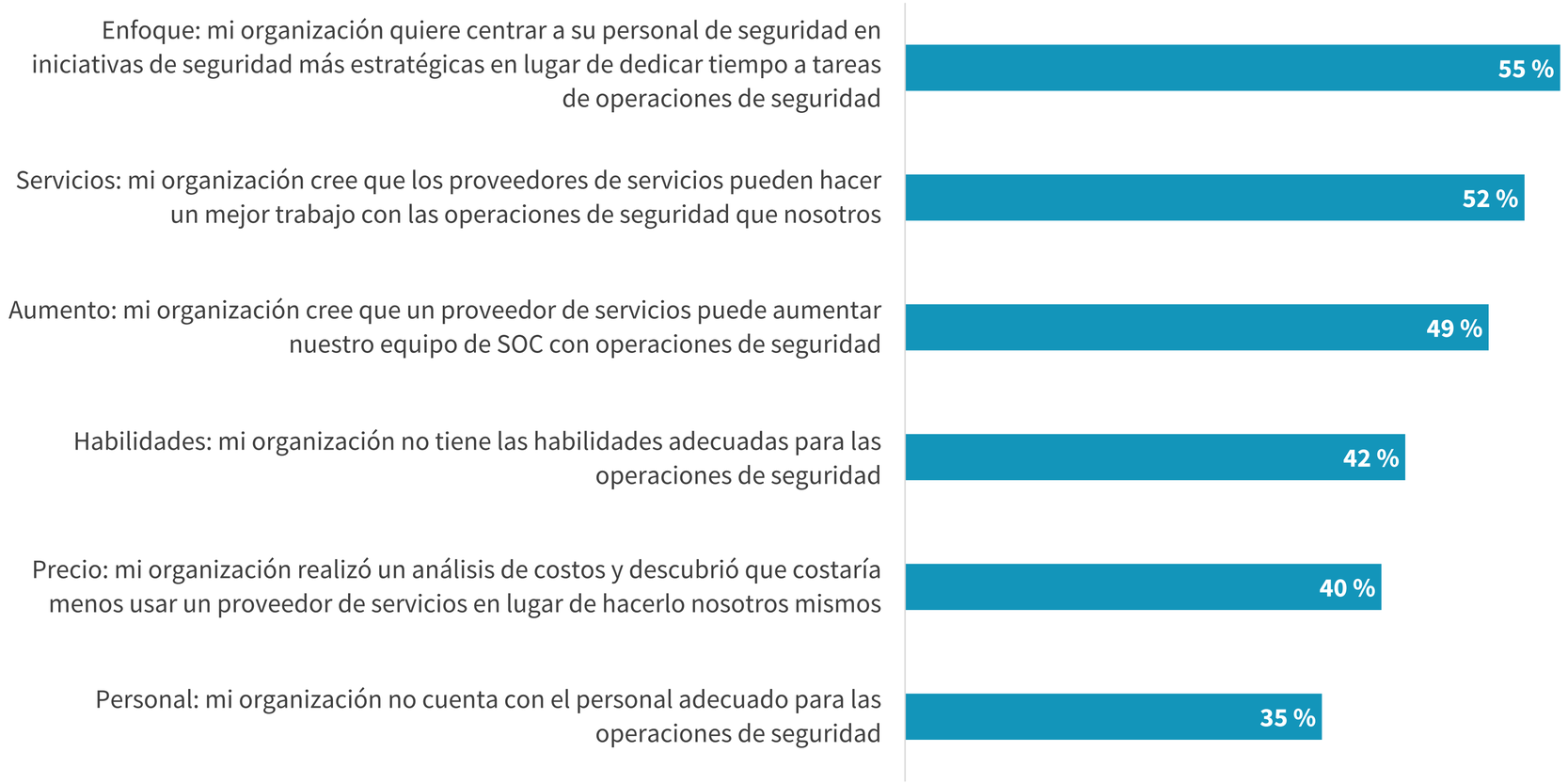
- Aumentaremos significativamente nuestro uso de servicios administrados para operaciones de seguridad
- Aumentaremos ligeramente nuestro uso de servicios administrados para operaciones de seguridad
- Mantendremos nuestro uso actual de los servicios administrados para las operaciones de seguridad

Volver al contenido

MDR ayuda a las organizaciones a centrar los esfuerzos de seguridad y abordar las habilidades y la escasez de personal

¿Por qué las organizaciones necesitan servicios administrados para las operaciones de seguridad? Más de la mitad (55 %) quiere servicios de seguridad para poder centrar al personal de seguridad en iniciativas de seguridad estratégicas. Otros creen que los proveedores de servicios administrados pueden lograr cosas que su organización simplemente no puede; el 52 % cree que los proveedores de servicios pueden proporcionar mejores operaciones de seguridad que su organización, el 49 % afirma que un proveedor de servicios administrados puede aumentar su equipo de SOC y el 42 % admite que su organización no tiene las habilidades adecuadas para las operaciones de seguridad.

Motivos principales detrás del uso o los planes de servicios administrados para las operaciones de seguridad.



Volver al contenido

cisco SECURE

Una cosa está clara, XDR desempeñará un papel fundamental en la modernización del SOC. Definir cómo ayudará a su equipo de seguridad y con qué partners trabajar a medida que desarrolla su enfoque XDR determinará su nivel de éxito. No se dedique simplemente a recopilar más datos. Busque una solución que pueda ayudar a convertirlos en datos mejores y procesables con contexto. La automatización puede ayudar a abordar las brechas de habilidades, lo que reduce el tiempo necesario para detectar, investigar y resolver incidentes para que la responsabilidad pueda trasladarse a analistas menos experimentados. Lo que permite a las organizaciones reasignar el tiempo de los analistas de seguridad sénior para madurar sus operaciones de seguridad. Nunca subestime la importancia de un partner de confianza.

Desde la seguridad de la red hasta el terminal y del correo electrónico a la nube, el portafolio de Cisco Secure conecta las detecciones con las respuestas seguras con funcionalidades integradas en cada punto de control para lograr el XDR más amplio del sector. Nuestro enfoque XDR transforma su infraestructura de una serie de soluciones inconexas en un ecosistema totalmente integrado, lo que evita que las amenazas desvíen la atención de los equipos de seguridad abrumados. Y como pueden atestiguar más de 300 000 clientes en todo el mundo, Cisco ofrece la experiencia en la que los CISO pueden confiar. Tengamos una conversación hoy.

MÁS INFORMACIÓN

ACERCA DE ESG

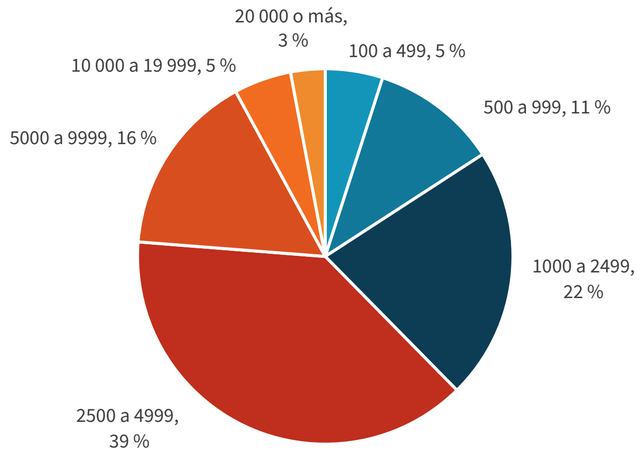
Enterprise Strategy Group es una empresa integrada de análisis, investigación y estrategia de tecnología que ofrece inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad tecnológica global.

Metodología de investigación

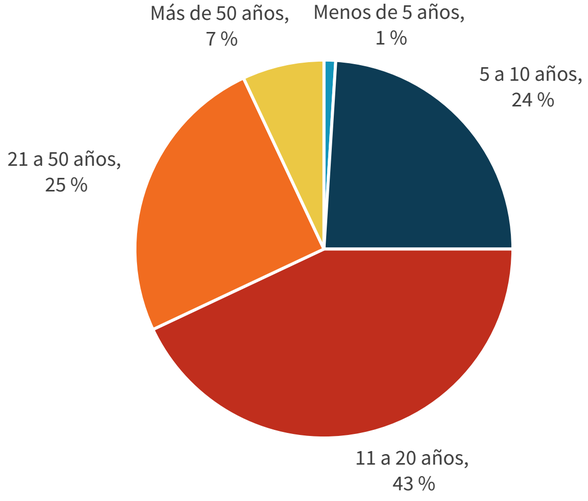
Para recopilar datos para este informe, ESG realizó una encuesta integral en línea a profesionales de TI y ciberseguridad de organizaciones del sector público y privado en América del Norte entre el 4 de abril de 2022 y el 15 de abril de 2022. Para requisito para calificar para esta encuesta, los encuestados debían ser profesionales de TI o ciberseguridad responsables de evaluar, comprar y utilizar productos y servicios de seguridad de respuesta y detección de amenazas. Todos los encuestados recibieron un incentivo para completar la encuesta en forma de premios en efectivo o equivalentes de efectivo.

Después de filtrar a los encuestados no calificados, eliminar las respuestas duplicadas y filtrar las respuestas completadas restantes (según una serie de criterios) para la integridad de los datos, nos quedamos con una muestra total final de 376 profesionales de TI y ciberseguridad.

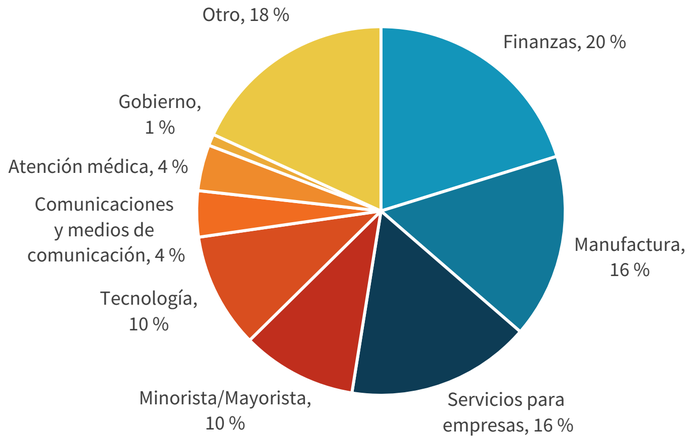
ENCUESTADOS POR CANTIDAD DE EMPLEADOS



ENCUESTADOS POR EDAD DE LA EMPRESA



ENCUESTADOS POR SECTOR



Volver al contenido

Enterprise Strategy Group es una empresa integrada de análisis, investigación y estrategia de tecnología que ofrece inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad tecnológica global.