Informe sobre el estado de las tecnologías SOAR, 2020

Cuarta encuesta anual sobre la respuesta a incidentes

Contenido

Resumen ejecutivo

Le presentamos la cuarta entrega de nuestra serie anual de informes sobre el estado de las tecnologías SOAR. Como en años anteriores, hemos encuestado a cientos de profesionales de la seguridad que ocupan diversos cargos en grandes organizaciones de varios sectores. Les preguntamos su opinión sobre el estado de la respuesta a incidentes (IR, por sus siglas en inglés) y sobre el encaje actual y futuro de las tecnologías de orquestación, automatización y respuesta (SOAR, por sus siglas en inglés) en sus estrategias y operaciones de seguridad.

Del informe se desprenden las siguientes conclusiones clave:

- **El entorno de ciberamenazas al que se enfrentan los analistas de seguridad es cada vez más adverso**. Los ataques son variados y voluminosos, hasta el punto de que el 63 % de las organizaciones han tenido que repeler ataques presuntamente ejecutados por actores estatales.
- **El proceso de respuesta a incidentes sobrepasa a cualquiera**. Los analistas tienen que estar atentos a una media de 6,8 canales de inteligencia sobre amenazas y gestionar a mano un número excesivo de alertas. Los procesos de respuesta a incidentes tienen su origen en multitud de sistemas diferentes, con un flujo de trabajo que cruza muchas barreras organizacionales.
- **La COVID-19 lo ha empeorado todo**. La pandemia está agravando los retos de la respuesta a incidentes, con nuevas amenazas que combatir y consecuencias negativas en la colaboración entre los miembros del equipo del centro de operaciones de seguridad (SOC, por sus siglas en inglés). El 40 % de los encuestados consideran que la pandemia está estrangulando aún más la disponibilidad de los recursos.
- **Los analistas saben muy bien lo que necesitan para mejorar la respuesta a incidentes**. Quieren:
  - » Más automatización para acelerar el proceso de respuesta a incidentes y reducir el número de operaciones manuales. Para el 65 % de los encuestados, la automatización de la respuesta a incidentes será una prioridad a lo largo de los próximos 12 meses.
  - » Que las herramientas del SOC se integren con sistemas de terceros para que puedan conectarse fácilmente con otros departamentos y procesos de respuesta a incidentes. El 30 % de los encuestados afirman querer una plataforma común que permita responder como un equipo transversal.
  - » Acceso a más libros de estrategias —ya sean de terceros o de una comunidad que comparta este tipo de recursos— para aprovechar los conocimientos y la experiencia de otros equipos. Al 78 % de los encuestados les gustaría que existiera un marco de trabajo común y una comunidad para compartir libros de estrategias e integraciones.
  - » Inteligencia sobre amenazas integrada con las herramientas de SecOps para reducir la cantidad de canales de inteligencia sobre amenazas que tienen que supervisar para anticiparse a las amenazas más graves. El 52 % de los encuestados consideran que los flujos de trabajo de las operaciones de seguridad serían más eficientes si la inteligencia sobre amenazas estuviera mejor integrada.
- **Hay que poner fin al exceso de alertas de una vez por todas**. Los equipos SOC reclaman una herramienta que reduzca el volumen de alertas o agilice su gestión.
- **Las tecnologías SOAR ofrecen una solución a muchos de estos problemas.** Están ayudando a los equipos SOC a ahorrar tiempo, agilizar la clasificación de alertas y acortar los procesos de respuesta a incidentes.
  - » El proceso de detección y respuesta del 45 % por ciento de los equipos SOC implica el uso de alguna tecnología SOAR. También se utiliza para valorar la prioridad de las vulnerabilidades (37 %), comprobar si se cumple la normativa (30 %) y llevar a cabo auditorías de seguridad (30 %).
  - » Los equipos SOC creen que, en el futuro, las tecnologías SOAR también se usarán para la gestión del Internet de las Cosas (23 % de los encuestados), los flujos de trabajo de equipo rojo (17 %) y la seguridad en la nube (38 %).
  - » El 43 % de los encuestados afirman que tienen previsto aumentar el gasto en herramientas SOAR en 2020; el 24 % implementará alguna tecnología SOAR en los próximos 12 meses.
  - » El 47 % de los encuestados han intensificado el uso de las tecnologías SOAR a raíz de la pandemia de COVID-19.

Introducción

Este informe presenta los resultados de una encuesta anual dirigida a profesionales de la seguridad. Estudia las tendencias en la respuesta a incidentes (IR) y el potencial de la tecnología de orquestación, automatización y respuesta de seguridad (SOAR) en dicho proceso. Los encuestados ocupan diversos cargos en los equipos de seguridad de grandes organizaciones de varios sectores.

Los centros de operaciones de seguridad y los analistas que los integran necesitan ayuda. Como se observa en la figura 1, el equipo SOC está sometido a una tensión permanente para mitigar una amplia variedad de ataques. El 86 % de los encuestados afirmaban haber tenido que lidiar con algún ataque de *phishing* durante los últimos 12 meses. El 63 % tuvo que detectar y neutralizar rápidamente ataques de malware. Los ataques a contraseñas, de denegación de servicio (DoS, por sus siglas en inglés) y ransomware son incidentes activos a los que tuvieron que enfrentarse el 51, el 39 y el 37 % de los encuestados, respectivamente.

De hecho, tal y como Gartner compartía en su informe de 2020, *Top Security and Risk Management Trends* (*Tendencias principales en seguridad y gestión de riesgos*, disponible en inglés), «los ataques son cada vez más veloces y creativos. Los delincuentes seguirán aprovechando todas las herramientas, tácticas y técnicas que tengan a su alcance para dirigir sus ataques a un público cada vez más diversificado con objetivos cada vez más variados. Todo esto reduce aún más la capacidad de anticipar y prevenir los fallos de seguridad».[1]

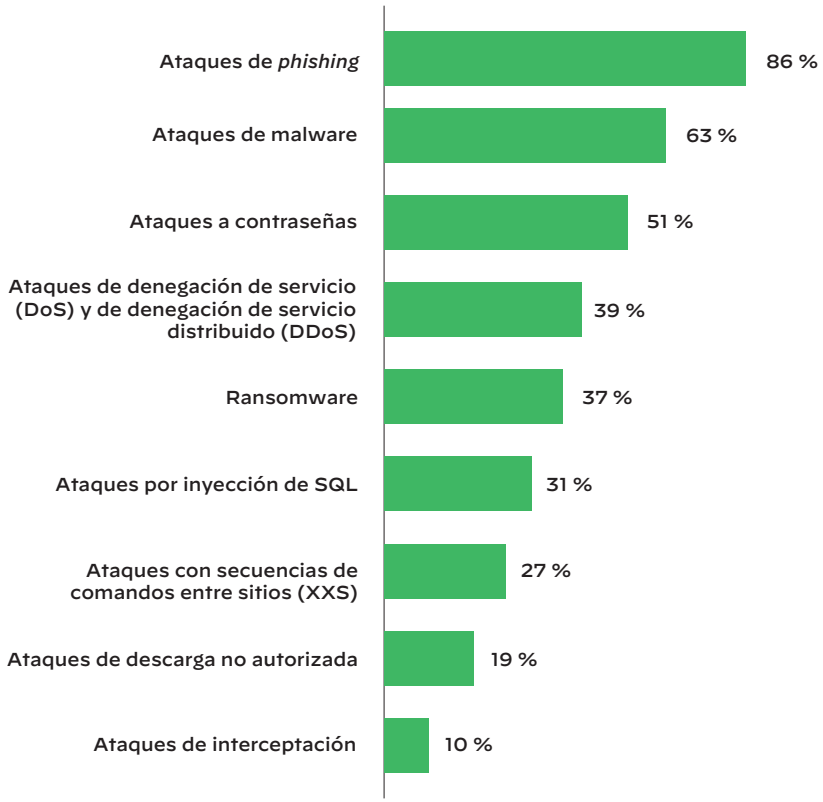

Figura 1: Ataques sufridos por las organizaciones de los encuestados a lo largo de los últimos 12 meses

Un abultado 63 % de las organizaciones que participaron en la encuesta afirmaban haber sido víctimas de ciberataques presuntamente ejecutados por actores estatales durante los 12 meses anteriores. Estos peligrosísimos atacantes emplearon, entre otras tácticas, *phishing*, denegación de servicio distribuido (DDoS, por sus siglas en inglés), ransomware e inyección de SQL. Por último, esta situación se ve agravada por la pandemia de COVID-19 (información ampliada en el apartado «El impacto de la COVID-19 en la respuesta a incidentes»).

Descripción general de las tecnologías SOAR

SOAR es una categoría de tecnología de operaciones de seguridad que permite a los equipos SOC gestionar el proceso de respuesta a incidentes de una forma más eficiente y eficaz. Las soluciones SOAR nacieron como un intento de automatizar los flujos de trabajo de respuesta a incidentes, que eran —y, en gran medida, siguen siéndolo— fundamentalmente manuales. La tecnología también se desarrolló para ayudar a los analistas de los SOC a orquestar los procesos de respuesta a incidentes que tenían lugar entre distintos sistemas, como las soluciones de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés), las plataformas de gestión de casos y otras herramientas similares.

Además de para agilizar y optimizar la respuesta a incidentes, las soluciones SOAR están diseñadas para llevar a cabo investigaciones forenses de incidentes detalladas y útiles. La tecnología proporciona al equipo SOC un conjunto de funciones básicas:

- La **orquestación** engarza las funciones de cada sistema con el fin de alcanzar los objetivos del flujo de trabajo de respuesta a incidentes. Gracias a la orquestación, que suele emplear interfaces de programación de aplicaciones (API, por sus siglas en inglés) basadas en estándares, la solución SOAR envía correos electrónicos de notificación, busca amenazas y crea incidencias de servicio, entre otras funciones, aunque cada una resida en un sistema distinto.
- La **automatización** consiste en configurar los equipos para que ejecuten tareas que antes se hacían de forma manual. En el contexto de las tecnologías SOAR, la automatización suele considerarse, más que un sustituto del talento humano, una forma de mejorarlo. La automatización suprime una gran parte del trabajo repetitivo y aburrido que tanto desgaste profesional genera en los analistas de los SOC, y agiliza el proceso de respuesta a incidentes y su investigación.
- Los **libros de estrategias** son secuencias de acciones predefinidas que el equipo SOC puede implementar en la solución SOAR en respuesta a una amenaza dada. Por ejemplo, si el equipo detecta una amenaza de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés) y dispone de un libro de estrategias con el que mitigarla, puede ejecutarlo en lugar de inventarse una respuesta desde cero. El resultado es siempre un proceso de respuesta a incidentes más rápido y eficiente.
- Las **herramientas de elaboración de informes y visualización de datos** de las soluciones SOAR brindan al equipo SOC una forma intuitiva y eficiente de identificar, correlacionar, clasificar y documentar las fases de desarrollo de los incidentes, así como las etapas del proceso de respuesta a incidentes y sus resultados.

1. Peter Firstbrook, Neil MacDonald, Lawrence Orans, Mario de Boer, Katell Thielemann, Bart Willemsen, Akif Khan y Michael Kranawetter, *Top Security and Risk Management Trends* (ID G00466211) (disponible en inglés), Gartner, 27 de febrero de 2020, https://www.gartner.com/en/documents/3981492/top-security-and-risk-management-trends.

Respuesta a incidentes: una coreografía de personas, procesos, herramientas y datos

Cada organización encuestada aborda el flujo de trabajo de respuesta a incidentes a su manera. Pero, por norma general, el proceso consta de cuatro elementos:

- **Procesamiento y contextualización de los incidentes:** proceso por el cual el SOC recaba información detallada sobre un incidente de seguridad y lo contextualiza para entender mejor qué está pasando. Por ejemplo, si un ataque se puede atribuir a una CVE determinada, el proceso de contextualización podría añadir detalles sobre la CVE, los sistemas a los que afecta, cómo se puede mitigar, etcétera.
- **Gestión de casos:** cada incidente se convierte (o debería convertirse) en un caso para que lo gestionen el SOC y otros equipos de la organización, como el de operaciones informáticas, el de operaciones de red, el jurídico o el de recursos humanos.
- **Investigación de incidentes:** los analistas de seguridad investigan un incidente para determinar cuál es la mejor manera de responder a ataques similares en el futuro y protegerse de ellos. La investigación requiere, además de conocimientos y experiencia, sistemas capaces de ofrecer detalles acerca de la causa del incidente.
- **Respuesta y aplicación de políticas:** esta fase de la respuesta a incidentes se refiere a la implementación de los pasos de mitigación decididos durante el proceso de investigación.

Estos elementos se solapan y refuerzan entre sí. La contextualización viene a completar las conclusiones extraídas durante la fase de investigación, que a su vez guían la respuesta. Las herramientas y prácticas de gestión de casos dan orden al flujo de trabajo y mantienen informadas a las partes interesadas, al menos en teoría.

El impacto de la COVID-19 en la respuesta a incidentes

El 60 % de los encuestados afirmaban que la COVID-19 estaba engendrando nuevos modelos de trabajo para los empleados y los miembros del equipo SOC, como el teletrabajo. El 42 % consideraba que la pandemia ha intensificado la necesidad de colaboración virtual, aunque para el 40 % ha menguado aún más los recursos. Tal vez por este motivo, el 24 % reconocía que la COVID-19 está acrecentando la necesidad de automatización, mientras que el 23 % mencionaba la adopción de nuevos servicios en la nube como una de las consecuencias de la pandemia.

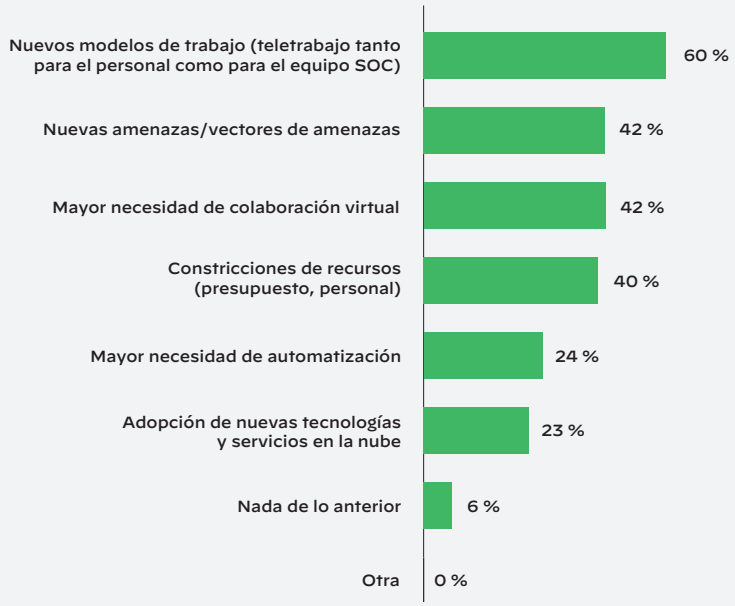

Figura 2: Resultados de la encuesta: efectos de la COVID-19 en el SOC y los analistas de seguridad

La estrategia y las prácticas de seguridad también se vieron afectadas y, según el 42 % de los encuestados, la COVID-19 ha producido nuevas amenazas y vectores de amenazas. En términos de adopción de las tecnologías SOAR, la COVID-19 ha suscitado una interesante división de opiniones. Para el 47 % de los encuestados en cuyas organizaciones se utiliza las tecnologías SOAR en mayor o menor grado, la pandemia llevará a un incremento del uso de estas herramientas y acelerará su adopción. El mismo porcentaje opinaba lo contrario: el 47 % consideraba que la COVID-19 reduciría el uso de las tecnologías SOAR y retrasaría su implementación.

Conclusiones clave de la encuesta de 2020 sobre las tecnologías SOAR

La encuesta de 2020 sobre las tecnologías SOAR ha corroborado algunas de las conclusiones extraídas en encuestas anteriores. Los equipos SOC continúan lidiando con altos niveles de alertas. Esta situación se ve agravada por el déficit de profesionales cualificados, tal y como pone de manifiesto el informe de 2020 publicado por Gartner *Top Security and Risk Management Trends* (*Tendencias principales en seguridad y gestión de riesgos*, disponible en inglés), según el cual «el déficit de formación en seguridad irá a más, acrecentado por la complejidad cada vez mayor de los sistemas informáticos y la gran velocidad a la que cambian las herramientas de seguridad para proteger esta infraestructura tan volátil».[2]

Para responder a todas estas exigencias, los equipos SOC quieren más automatización. La encuesta revelaba un interés claro por la integración de sistemas de terceros. Los equipos SOC también parecen interesados en disponer de acceso a más libros de estrategias y algunos de ellos expresaban el deseo de cooperar con mercados de terceros y comunidades de intercambio de recursos. La gente busca soluciones y siente curiosidad por saber qué hace el de al lado para combatir las amenazas a las que se enfrentan.

La respuesta a incidentes, hoy: un flujo de trabajo cada vez más complejo y exigente

Cada organización aborda la respuesta a incidentes a su manera y utiliza su propia constelación de herramientas. La encuesta revelaba que el proceso de respuesta a incidentes arranca desde distintas interfaces, dependiendo de la organización. Como muestra la figura 3, más de la mitad de los flujos de trabajo de respuesta a incidentes comienzan en la solución SIEM, mientras que el 33 % lo hace en plataformas de gestión de incidencias como ServiceNow® y Zendesk®. De ellos, tan solo el 6 y el 2 % se originan en las herramientas de gestión de casos y las soluciones SOAR, respectivamente.

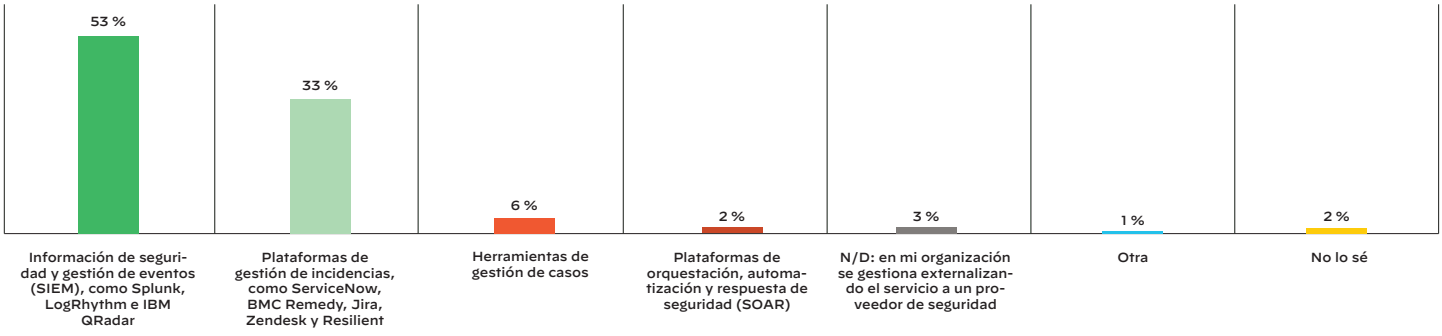

Figura 3: «¿Qué interfaz utiliza principalmente para iniciar sus flujos de trabajo de respuesta a incidentes?»

Según revela la figura 4, buena parte del proceso de respuesta a incidentes descansa sobre los hombros de proveedores externos y procesos manuales. El 22 % de los flujos de trabajo de respuesta a incidentes utilizan proveedores de servicios de seguridad gestionados y servicios gestionados de detección y respuesta (MSSP y MDR, respectivamente, por sus siglas en inglés). Dado que parte del trabajo lo realizan entidades externas, tiene sentido que el flujo de trabajo de respuesta a incidentes suela llevar aparejados procesos manuales. A menos que el servicio MSSP o MDR esté integrado con herramientas automatizadas del flujo de trabajo de respuesta a incidentes, su uso tendrá que ser manual al menos en parte.

El 38 % de los procesos de investigación de incidentes son manuales, mientras que el porcentaje es del 35 % entre los procesos de respuesta y aplicación de políticas. En el contexto de los resultados que se muestran en la figura 3, esta dependencia de los procesos manuales tiene todo el sentido: si el 53 % de los flujos de trabajo de respuesta a incidentes se originan en soluciones SIEM, cuyas funciones en esta área no suelen estar automatizadas, los miembros de los equipos SOC necesitan echar mano de otras herramientas.

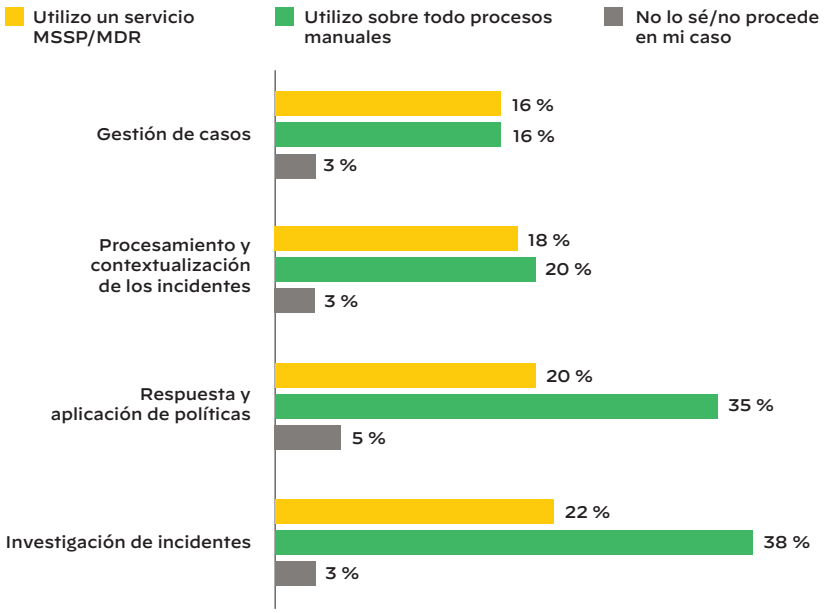

Figura 4: «¿Qué soluciones utiliza en cada paso del proceso de respuesta a incidentes?»

2. *Top Security and Risk Management Trends* (disponible en inglés), Gartner, 27 de febrero de 2020.

La respuesta a incidentes plantea obstáculos a los responsables de la seguridad en términos de velocidad y capacidad

Los encuestados compartieron detalles acerca de sus procesos de respuesta a incidentes que sugerían la existencia de obstáculos relativos a la velocidad y la capacidad. Como se puede observar en la figura 5, menos de la mitad de los encuestados tiene acceso a paneles personalizados. Solo el 40 % dispone de herramientas de elaboración de informes en tiempo real y programados, mientras que tan solo el 15 % disfruta de recomendaciones basadas en el aprendizaje automático para mejorar las operaciones de seguridad. Estos datos delatan un entorno de operaciones de seguridad lento e ineficiente. Si los miembros del equipo SOC dependen de paneles estandarizados incapaces de reflejar la función específica de un analista, y carecen de información inmediata, el trabajo se demora. A su vez, los resultados resultarán menos valiosos. El aprendizaje automático puede resultar de ayuda, pero tal y como muestran los datos, solo está disponible en 1 de cada 6 SOC.

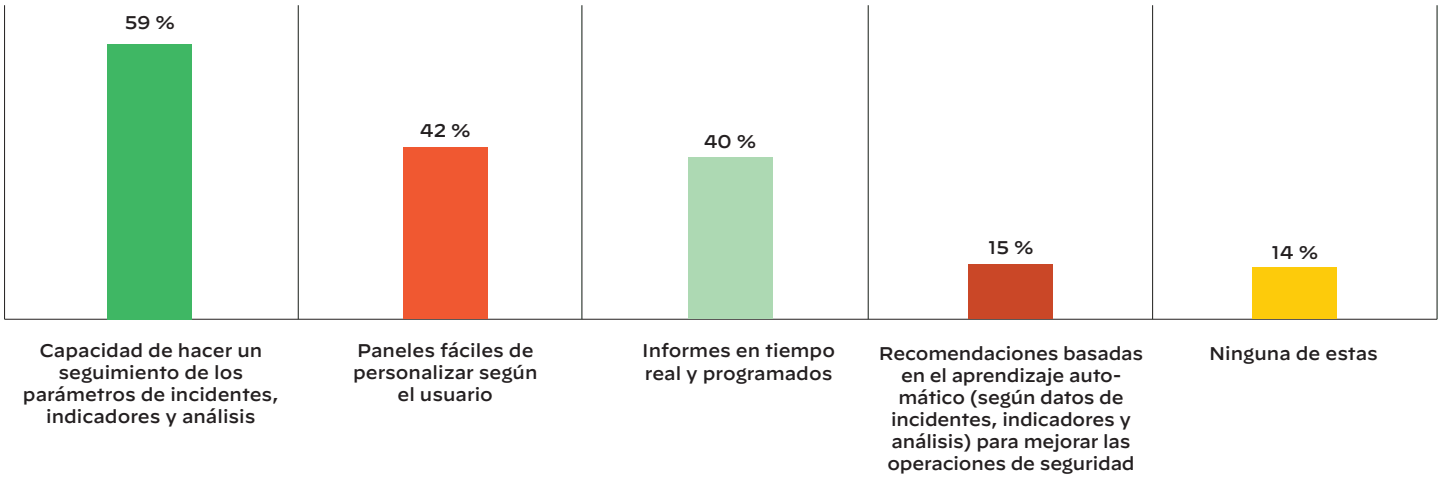

Figura 5: «¿Qué recursos utiliza para hacer un seguimiento de la respuesta a incidentes y del rendimiento de los analistas? (Seleccione todas las respuestas que correspondan)».

La respuesta a incidentes debe ser menos manual, con procesos y libros de estrategias automatizados

La encuesta revela una necesidad de mayor automatización en la respuesta a incidentes. Los encuestados indicaron que el 44,7 % de sus procesos de respuesta a incidentes estaban automatizados; puede parecer un porcentaje alto, pero es del todo insuficiente. Aunque 4 de cada 10 procesos de respuesta a incidentes automatizados es mejor que ninguno, la prevalencia de los procesos manuales sigue siendo un impedimento que malogra la eficacia y la eficiencia de esta importante función. De hecho, el 93 % de los equipos de operaciones de seguridad consideran que el año que viene será prioritario aumentar la automatización en sus procesos de respuesta a incidentes.

Los incidentes se procesan y contextualizan mediante métodos solo parcialmente automatizados

Las fases de procesamiento y contextualización de los procesos de respuesta a incidentes solo están automatizadas en parte. Como se aprecia en la figura 6, la mitad del procesamiento de los datos está automatizado en varias fuentes. El nivel de automatización prácticamente es el mismo (46 %) en la priorización de alertas y en la correlación de alertas e indicadores entre productos. Dado el estrés y la sobrecarga de trabajo a los que suelen estar sometidos los miembros de los equipos SOC, no parece que tener automatizada solo la mitad del trabajo de procesamiento sea ningún logro. En el caso de la contextualización, la cifra es significativamente inferior: solo el 28 % de los encuestados dicen disponer de procesos de contextualización automatizados. Un 30 % afirma hacerlo de forma manual.

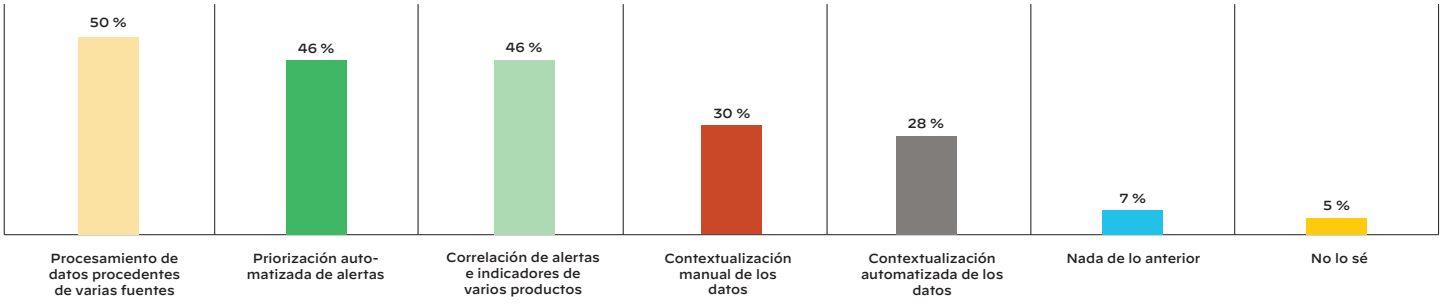

Figura 6: «¿Qué recursos utiliza para procesar y contextualizar los incidentes? (Seleccione todas las respuestas que correspondan)».

Implementación del proceso de respuesta a incidentes: una combinación de flujos de trabajo automatizados y manuales

En la implementación del proceso de respuesta a incidentes también hay un poco de todo. La figura 7 muestra que el 53 % de los procesos están formados por una mezcla de libros de estrategias, runbooks y procesos manuales y automatizados. Solo el 18 % de los libros de estrategias y runbooks están automatizados del todo. Curiosamente, solo el 6 % de los procesos prescinde de libros de estrategias. Los libros de estrategias son el método principal que están utilizando los SOC para gestionar la implementación del proceso de respuesta a incidentes —proceso al que le falta automatización—.

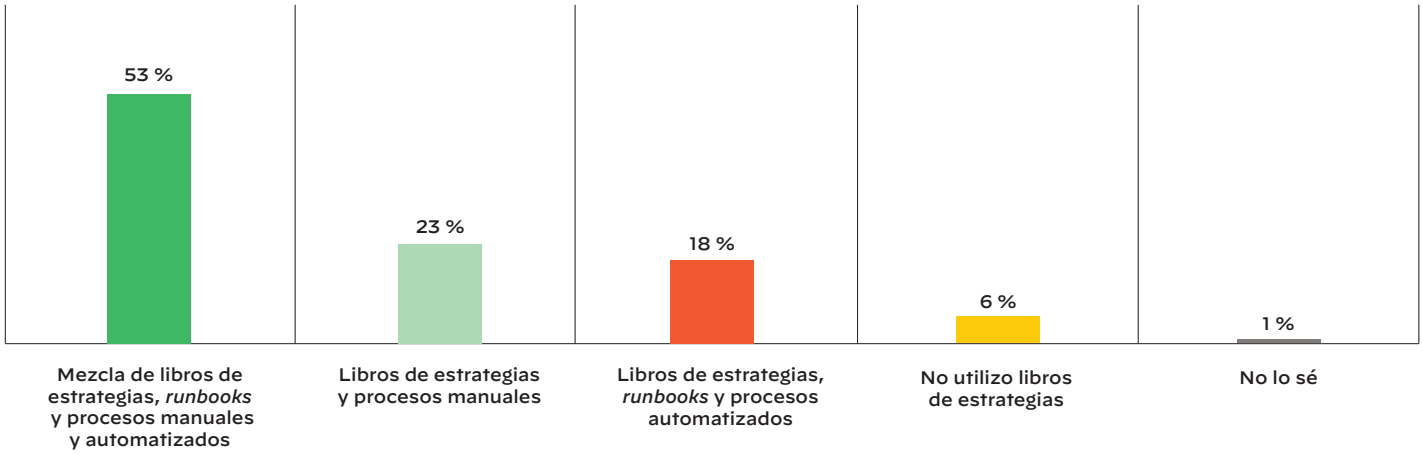

Figura 7: «¿Cuál de estas opciones describe mejor la implementación del proceso de respuesta a incidentes de su organización?»

Los flujos de trabajo de investigación y posteriores a un incidente tienen una automatización limitada

La fase de investigación del proceso de respuesta a incidentes tiene cierta automatización, pero sigue estando limitada. Aunque el 37 % de la ejecución telemática de las herramientas de seguridad está automatizada, el 49 % sigue siendo manual. En particular, solo el 18 % de los flujos de trabajo de respuesta a incidentes documentan las labores de investigación automáticamente. Esto sugiere que más del 80 % de la documentación de las actividades de investigación se realiza de forma manual o —en la mayoría de los casos— directamente no se realiza.

Además, los miembros de los equipos SOC suelen estar demasiado ocupados para documentar lo que van haciendo. Sin embargo, esta información resulta muy útil para las labores de análisis y las mejoras que suceden a un incidente con vistas a mejorar futuras respuestas. Esta falta de automatización representa una oportunidad perdida para aprender de la respuesta a incidentes y mejorar el proceso. Ante la misma pregunta acerca de los flujos de trabajo posteriores a un incidente, solo el 23 % de los encuestados contestaron que las revisiones quedaban registradas de forma automática.

La automatización será una prioridad en la respuesta a incidentes

En lo que se refiere a la automatización de los procesos de respuesta a incidentes, las prioridades y planes de futuro expresados por los participantes en la encuesta son reveladores. Tal y como muestra la figura 8, para el 65 % de los encuestados la automatización de la respuesta a incidentes será una prioridad a lo largo de los próximos 12 meses. Algo menos, el 58 %, quiere automatizar ante todo la priorización de amenazas, mientras que el 46 % se centra en la elaboración de informes y la visibilidad entre equipos. Son una minoría los encuestados para quienes la automatización no es ninguna prioridad y, en el caso particular de la respuesta a incidentes, solo sostenía esta opinión el 2 %.

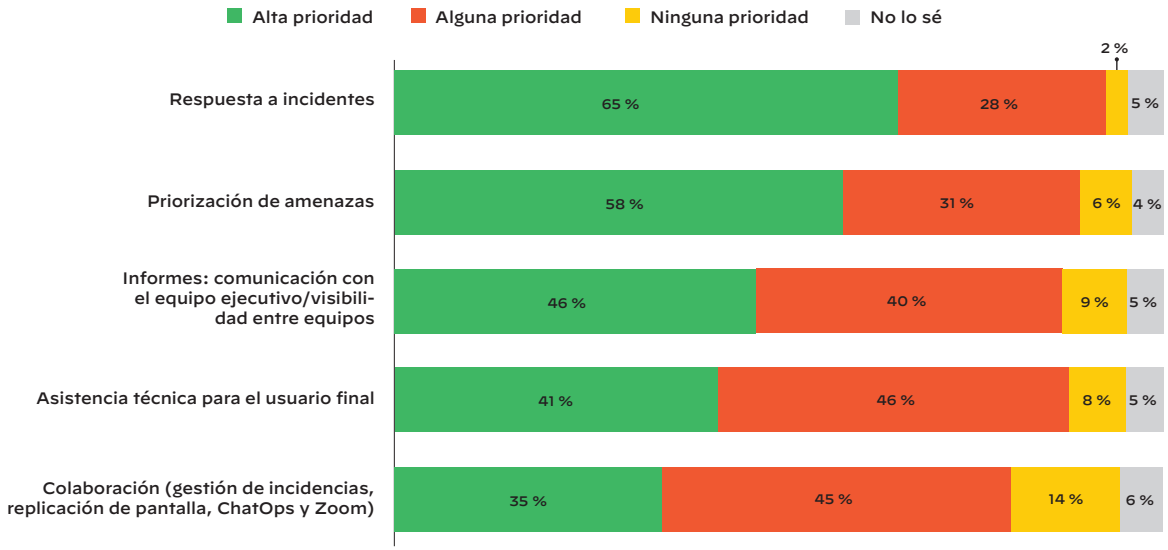

Figura 8: «Durante los próximos 12 meses, ¿con qué prioridad piensa aumentar la automatización de estos procesos de operaciones de seguridad?»

La inteligencia sobre amenazas debería integrarse con los flujos de trabajo de respuesta a incidentes para facilitar su gestión

En un entorno global de amenazas cada vez más diverso y voluminoso, los equipos SOC necesitan disponer de la inteligencia sobre amenazas más actualizada. El 81 % de los encuestados consideran que la inteligencia sobre amenazas es crucial para sus procesos de respuesta a incidentes. Ahora las empresas se suscriben a 6,8 canales de amenazas por término medio para mantenerse informadas de las amenazas. Sin embargo, si todos estos datos no se gestionan de una forma coherente e integrada, es fácil perder la pista a amenazas que podrían ser graves. De hecho, según el 62 % de los encuestados, el uso de inteligencia sobre amenazas es un proceso que consume mucho tiempo.

Por tanto, la integración con la inteligencia sobre amenazas se presenta como uno de los factores más demandados a la hora de invertir en una herramienta de seguridad nueva. Tal y como refleja la figura 9, el 50 % de los encuestados dijeron que los flujos de trabajo de sus operaciones de seguridad serían mucho más eficientes si la inteligencia sobre amenazas estuviera mejor integrada. Teniendo en cuenta que el 46 % respondió que sus flujos de trabajo de respuesta a incidentes serían «algo» más eficientes, un nada desdeñable 96 % se muestra a favor de la integración de la inteligencia sobre amenazas.

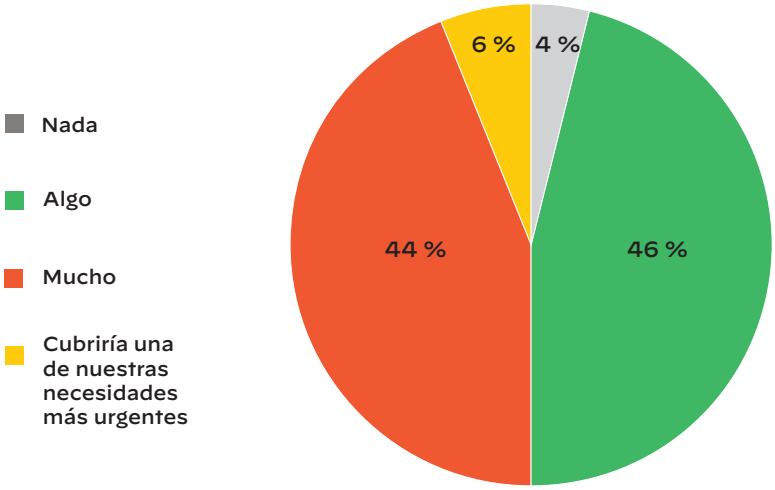

Figura 9: «¿Hasta qué punto cree que los flujos de trabajo de sus operaciones de seguridad serían más eficientes si la inteligencia sobre amenazas estuviera mejor integrada?»

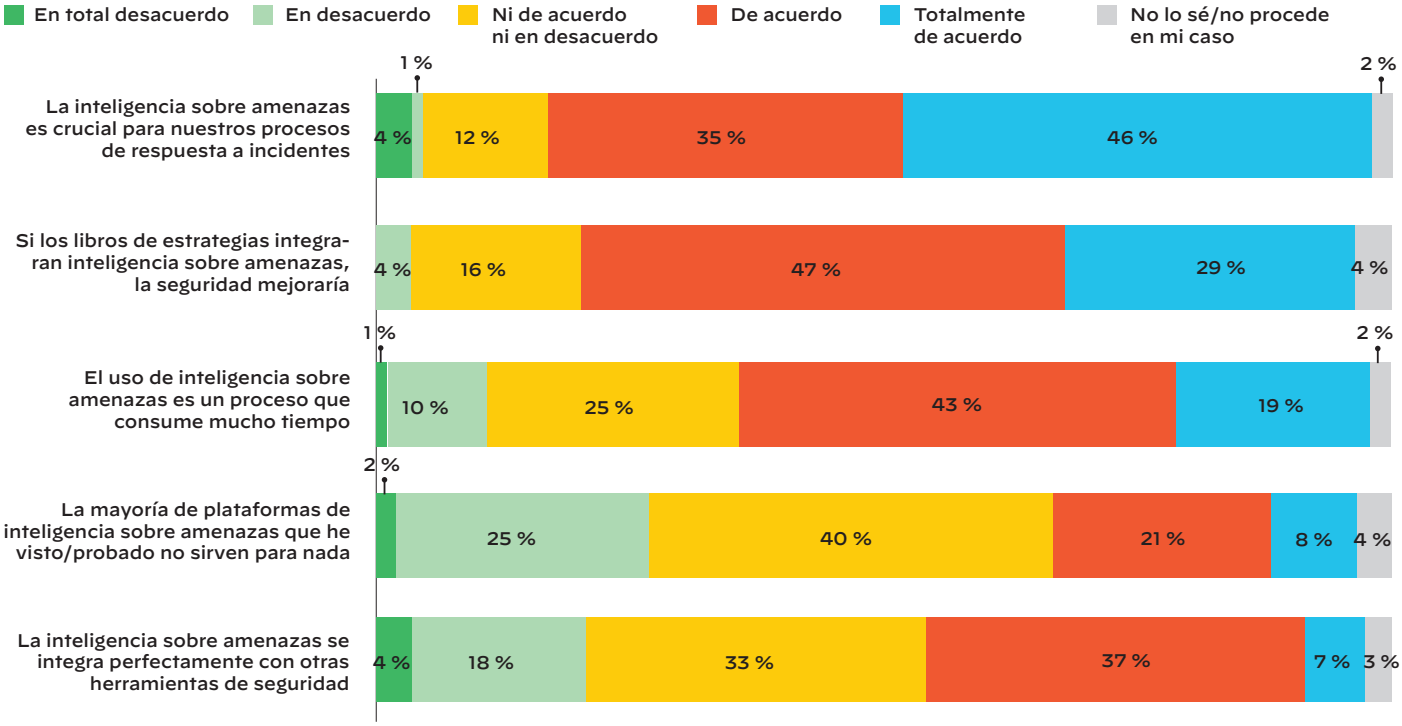

Figura 10: «Valore su grado de acuerdo con estas afirmaciones relativas a la inteligencia sobre amenazas».

Dicho esto, la tasa de integración real es relativamente baja: solo el 43 % de los encuestados manifiesta estar de acuerdo con la siguiente afirmación: «La inteligencia sobre amenazas se integra perfectamente con otras herramientas de seguridad». Además, tan solo el 28 % de los procesos de investigación de incidentes están conectados a las fuentes de inteligencia sobre amenazas.

La explicación para la divergencia entre el deseo de integrar la inteligencia sobre amenazas y la tasa real de integración se desprende de ciertos datos de la encuesta. Un problema es que hay demasiados tipos de personas involucradas en la gestión de la inteligencia sobre amenazas, simple y llanamente. Tal y como indica la figura 11, intervienen el equipo de operaciones de seguridad, el de seguridad empresarial, el de operaciones informáticas y los que se ocupan en concreto de la inteligencia sobre amenazas, entre otros. Un factor adicional podría ser la calidad percibida de las plataformas de inteligencia sobre amenazas. El 29 % de los encuestados están de acuerdo con la siguiente afirmación: «La mayoría de plataformas de inteligencia sobre amenazas que he visto/probado no sirven para nada».

Según revela la figura 12, el proceso de inteligencia sobre amenazas de por sí utiliza del orden de 12 sistemas distintos o más. Los empleados descritos en la figura 11 están realizando trabajo relacionado con la inteligencia sobre amenazas en sistemas SIEM, herramientas de análisis del tráfico de red, soluciones de vigilancia de intrusiones, etcétera. Hay demasiada gente intentando gestionar la inteligencia sobre amenazas en demasiadas plataformas con muy poca integración: una fórmula frustrante, qué duda cabe.

Hay que reducir el número de alertas que revisan los equipos de SecOps

Los analistas de los SOC tienen demasiadas alertas que procesar. Es abrumador. El exceso de alertas, también conocido como mal de alertas, es un fenómeno demasiado real que puede desgastar a los empleados y aumentar la rotación de personal. También está el riesgo de pasar por alto una amenaza grave en mitad del ruido. Y, para rematar, está la COVID-19. La encuesta revelaba que el 47 % de las empresas han experimentado un aumento de alertas desde el inicio de la pandemia. Las empresas que han sufrido un incremento en las alertas debido a la COVID-19 vieron crecer el volumen de alertas un 34,2 % por término medio.

Las tecnologías de SecOps deben integrarse fácilmente con las soluciones de terceros

Los flujos de trabajo de respuesta a incidentes pueden iniciarse en una gran variedad de sitios, como demuestra la figura 13. A partir de ahí, el proceso de respuesta a incidentes puede saltar de solución en solución y de un departamento a otro. De este modo, la integración entre las herramientas de respuesta a incidentes y las soluciones de terceros puede ayudar a los equipos SOC a ser más productivos y diseñar una estrategia de respuesta a los incidentes más eficaz. Esta idea se ve refrendada por los resultados de la encuesta, según los cuales el 30 % de los participantes afirmaban querer una plataforma común para poder responder desde diferentes equipos; mientras que tan solo el 32 % de ellos cuentan con una plataforma común para investigación transversal.

Para entender la magnitud del problema, hay que tener en cuenta que los equipos SOC utilizan distintas herramientas en cada una de las cuatro grandes fases del flujo de trabajo de respuesta a incidentes. Como se ve en la figura 13, dominan los sistemas SIEM, con el 69 % de los procesos de procesamiento y contextualización de los incidentes, y poco menos de la mitad de los pasos de gestión de casos e investigación de incidentes. Las plataformas SOAR se utilizan en el 20 % de los procesos de respuesta y aplicación de políticas, así como en el 22 % de las investigaciones de incidentes. Las plataformas de inteligencia sobre amenazas (TIP, por sus siglas en inglés), que representan menos del 20 % de los procesos que se desarrollan en estas cuatro etapas, son menos habituales.

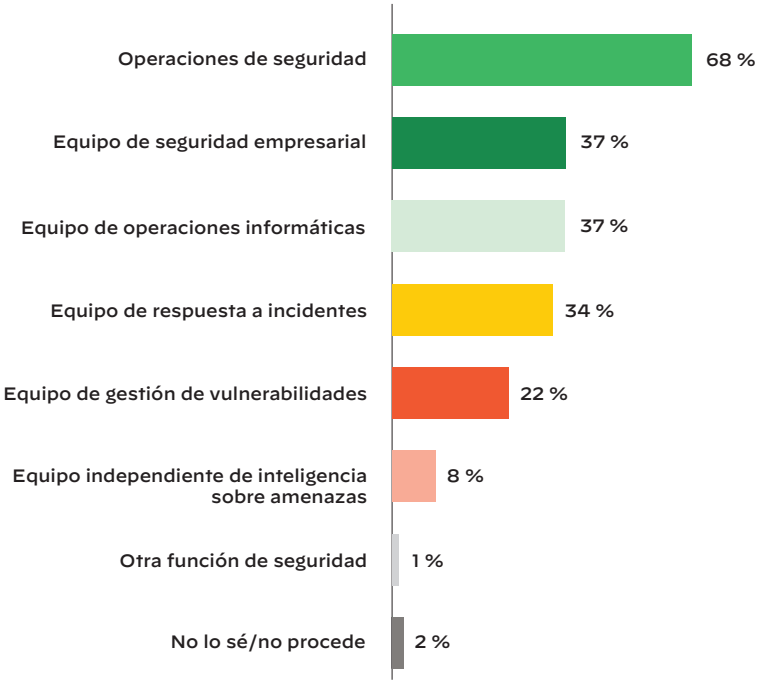

Figura 11: «¿Qué miembros de su organización están involucrados en la gestión de la inteligencia sobre amenazas?»

Figura 12: «¿Qué tipos de herramientas de gestión o funciones utiliza para agregar, analizar o presentar la inteligencia sobre amenazas? (Seleccione todas las respuestas que correspondan)».

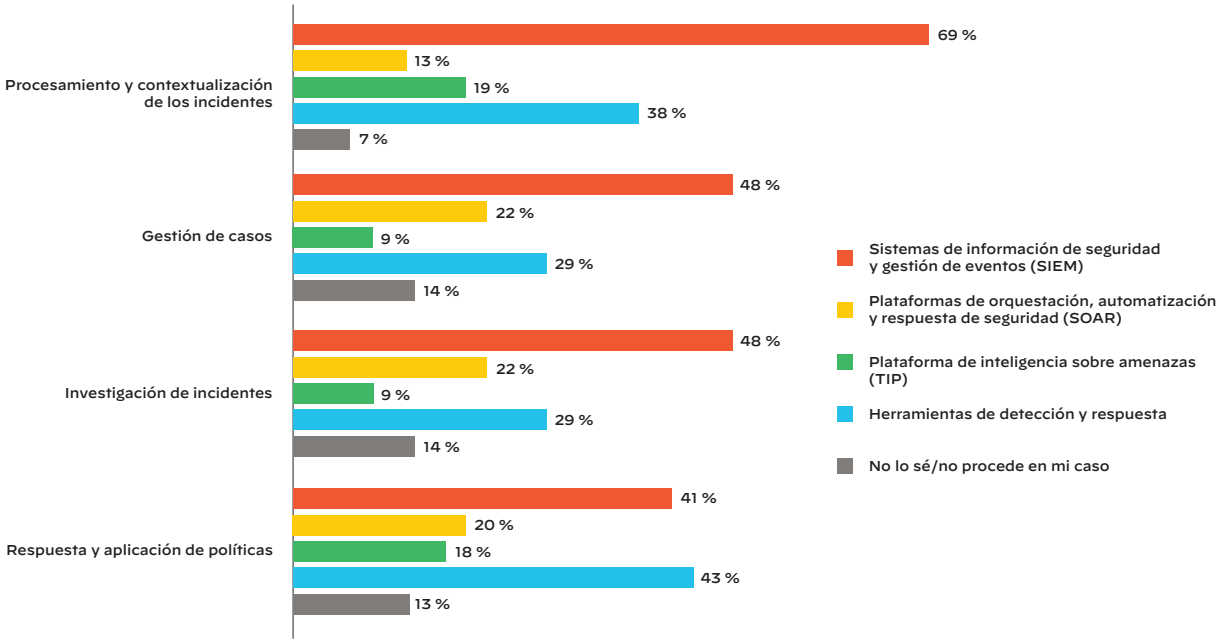

Figura 13: «¿Qué soluciones utiliza en cada paso del proceso de respuesta a incidentes? (Seleccione todas las respuestas que correspondan)».

Al mismo tiempo, el flujo de trabajo de respuesta a incidentes está repartido entre muchos departamentos corporativos distintos, aunque la integración entre los sistemas de cada uno es limitada. Tal y como muestra la figura 14, la mayor parte de la integración se produce entre las soluciones de respuesta a incidentes y las del equipo informático, con el 23 % de los sistemas y procesos descritos como «perfectamente integrados». Con el equipo del centro de operaciones de red (NOC, por sus siglas en inglés) solo estaban perfectamente integrados el 16 % del tiempo. Con el de recursos humanos, el 50 % de los sistemas y procesos estaban separados. La prevalencia de separación entre los equipos de respuesta a incidentes y el jurídico y de cumplimiento normativo era del 48 y el 30 %, respectivamente.

La respuesta «Compartimos algunos sistemas y procesos» se daba el 51 % del tiempo entre los equipos de respuesta a incidentes y el de cumplimiento normativo, el 56 % con el equipo informático y el 52 % con el equipo NOC. Algunos sistemas y procesos se comparten con otros grupos menos de la mitad del tiempo. La integración más baja (solo el 7 %) se daba entre el equipo de respuesta a incidentes y el jurídico. Esto puede ser reflejo del uso de sistemas especializados por parte del departamento jurídico para gestionar los casos. Aunque no todos los incidentes de seguridad sean del interés del departamento jurídico, hay una alta probabilidad de que la falta de integración se traduzca en una pérdida de tiempo y en gastos innecesarios, ya que la gente que trabaja para los equipos de respuesta a incidentes y jurídico tiene que coordinar sus flujos de trabajo a mano.

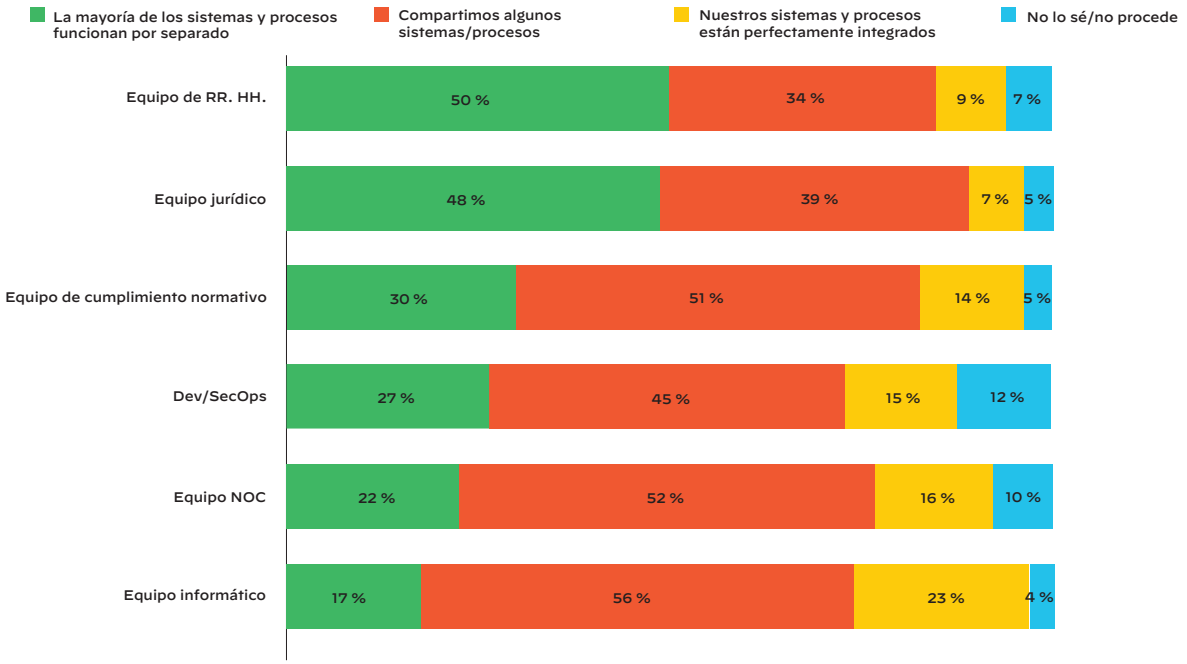

Figura 14: «¿Hasta qué punto comparte herramientas, procesos, sistemas y flujos de datos con estos equipos?»

Los mercados de terceros y las comunidades de intercambio de recursos suscitan gran interés

El campo de la ciberseguridad cuenta con una larga tradición de personas y organizaciones con vocación de aprender todo lo posible de la comunidad para mejorar su seguridad. Es posible que los orígenes de este patrón estén en las raíces de código abierto de buena parte de la tecnología de seguridad e informática, así como un pasado compartido por los profesionales del cumplimiento normativo legal y del ejército, desde donde se promueve el intercambio de inteligencia. Aunque las realidades del trabajo no siempre responden a este ideal, hay un claro deseo de compartir la inteligencia y las prácticas recomendadas con el resto de la comunidad.

Los resultados de la encuesta avalan esta opinión, pues el 78 % de los participantes preferirían que existiera un marco de trabajo común y una comunidad para compartir libros de estrategias e integraciones. Solo el 42 % consideraba que creaba los mejores libros de estrategias. Además de la comunidad, los encuestados se mostraban partidarios de los mercados de terceros: el 52 % decía estar dispuesto a comprar tecnologías valiosas de integración con herramientas de terceros. La figura 15 recoge en toda su profundidad el interés por los marcos de trabajo comunes, las comunidades de intercambio de recursos y los mercados de terceros.

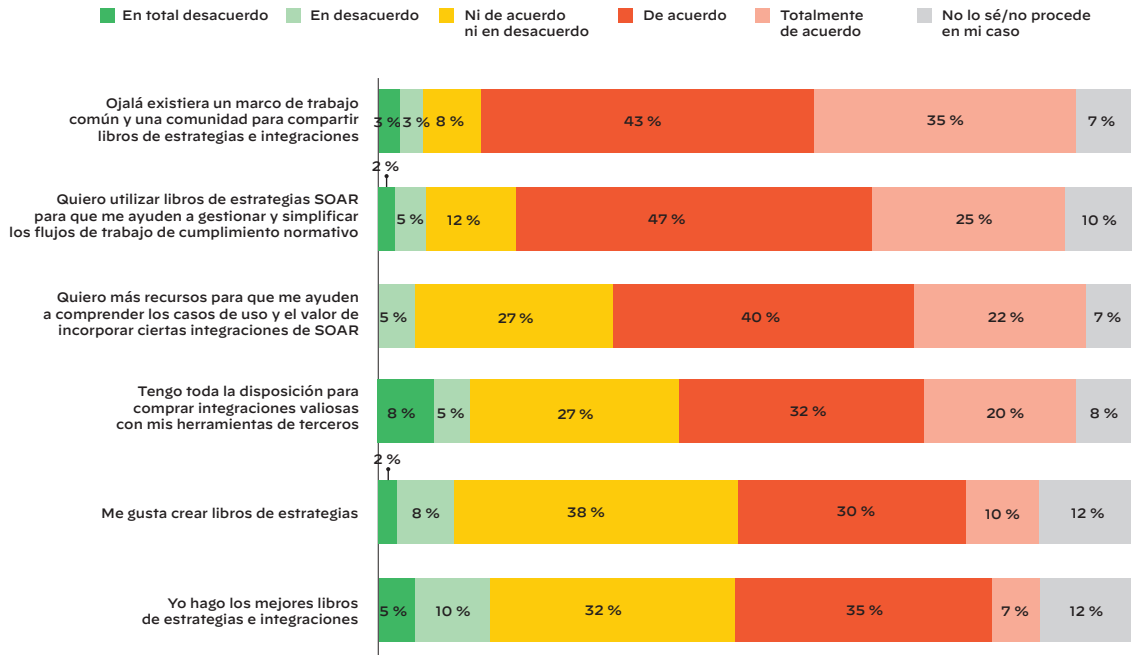

Figura 15: «¿Hasta qué punto comparte herramientas, procesos, sistemas y flujos de datos con estos equipos?»*

¿A quién pertenecen los libros de estrategias en que confían los profesionales de la seguridad? Con un 53 %, la figura 16 demuestra que los libros de estrategias en los que más confían los encuestados son los certificados por los proveedores de soluciones SOAR. A continuación, se decantan por los libros de estrategias desarrollados por ellos mismos (47 %), los creados por el proveedor de SOAR (44 %) y los creados por algún MSSP o algún otro socio de seguridad (35 %).

Curiosamente, aunque cerca de 8 de cada 10 encuestados querían una comunidad con la que compartir recursos, solo el 20 % confiaría más en un libro de estrategias creado por los miembros de la comunidad. En realidad, esta aparente contradicción no lo es tanto si se tiene en cuenta que el 53 % prefiere los libros de estrategias certificados por algún proveedor. Los resultados reflejan, por tanto, que la certificación es importante.

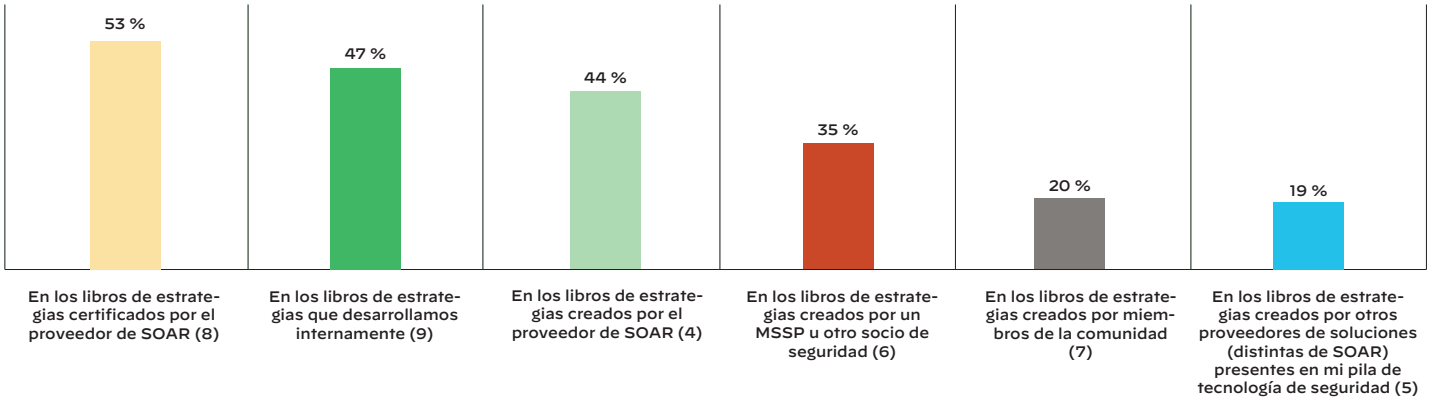

Figura 16: «¿En cuáles de estas fuentes de libros de estrategias de SOAR confía más? (Seleccione todas las respuestas que correspondan)».

* Debido al redondeo, es posible que los totales superen el 100 %.

El estado de las tecnologías SOAR

Las tecnologías SOAR ofrecen respuestas a muchos de los retos que ponen en evidencia los resultados de la encuesta, como la falta de automatización, la necesidad de reducir el mal de alertas, etcétera. La encuesta demuestra un gran interés en las herramientas SOAR, quizá debido al tipo de problemas que resuelven. La proporción de encuestados que ya utilizan alguna solución SOAR o están interesados en implementar la tecnología en los próximos 12 meses es sorprendentemente alta. Las tecnologías SOAR desempeñan un papel cada vez más activo en la respuesta a incidentes y en el entorno de las SecOps en general, y todo apunta a que el año que viene seguirá creciendo.

Los casos de uso de las tecnologías SOAR cada vez son más variados

Los equipos SOC están aprovechando las tecnologías SOAR en diversos casos de uso. Como se aprecia en la figura 17, los encuestados están utilizando las tecnologías SOAR, sobre todo, para detectar las amenazas y darles respuesta (45 %), priorizar las vulnerabilidades (37 %), comprobar si se cumple la normativa (30 %) y llevar a cabo auditorías de seguridad (30 %).

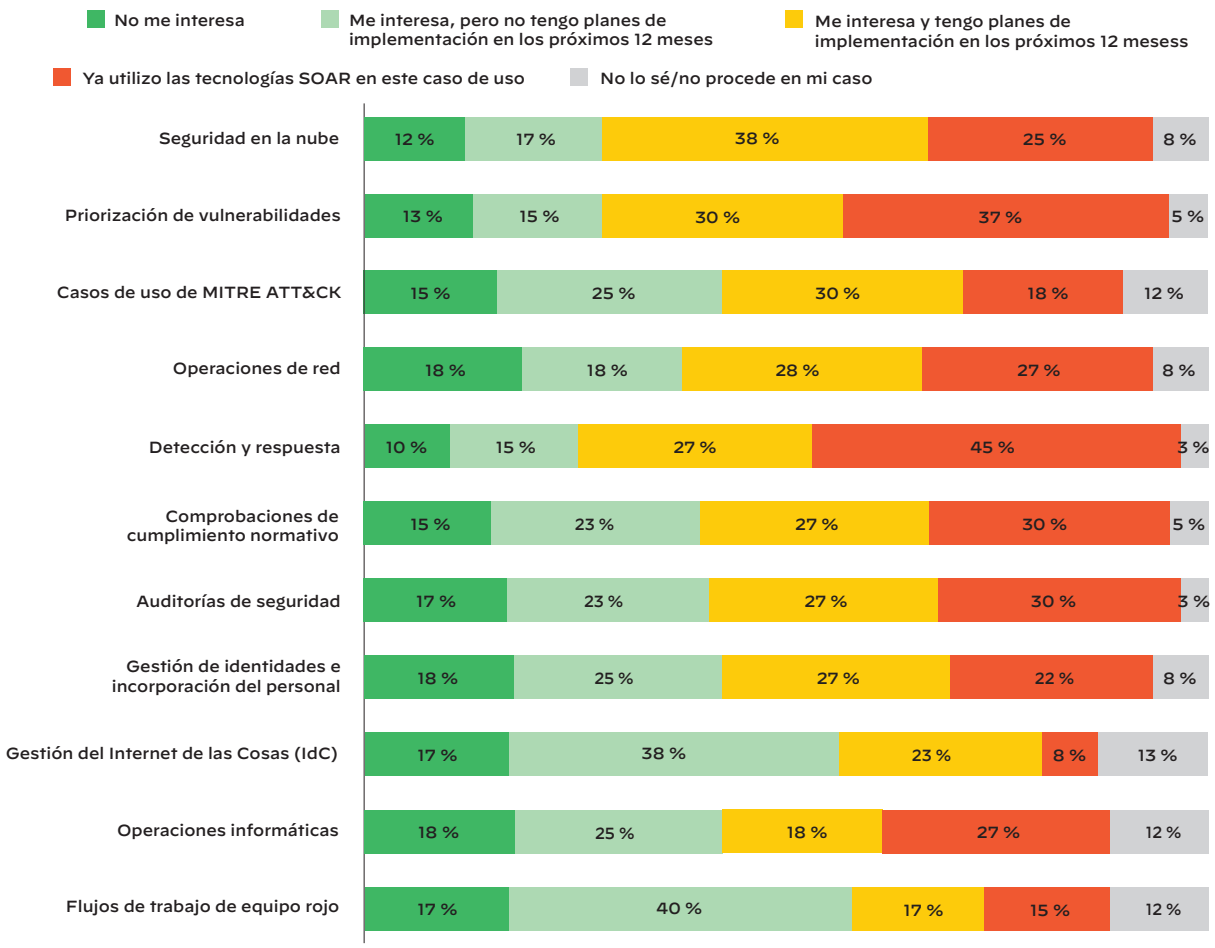

Figura 17: «¿Qué intención tiene de ampliar el uso de las tecnologías SOAR para estos casos?»

Aunque los índices de adopción de las tecnologías SOAR son inferiores en otros casos de uso incluidos en la encuesta, resulta evidente que las tecnologías se están utilizando. Los equipos de seguridad utilizan las tecnologías SOAR en flujos de trabajo de equipo rojo (15 %), operaciones informáticas (27 %), operaciones de red (27 %) y casos de uso de MITRE ATT&CK® (18 %). Todos estos hallazgos sugieren que los equipos de seguridad están interesados en las tecnologías SOAR, aunque el proceso de implementación avance con lentitud.

Las tecnologías SOAR están cada vez más presentes

Parece que las tecnologías SOAR están ganando terreno en el SOC; según los resultados de la encuesta, algo menos de la mitad de los encuestados (46 %) ya la utilizan o tienen previsto adoptarla en los próximos 12 meses. Sin embargo, el uso de las tecnologías SOAR a largo plazo es relativamente limitado: tan solo el 7 % de los encuestados indicaron que las habían utilizado durante más de dos años. La figura 18 muestra la lista desglosada completa de datos de uso de las tecnologías SOAR. Cabe mencionar que el 41 % sabe de la existencia de las tecnologías SOAR, pero no tiene pensado implementarlas en los próximos 12 meses, y el 12 % nunca ha oído hablar de ellas. Este último dato, sin embargo, puede deberse a que la categoría hasta hace relativamente poco recibía el nombre de «SAO», no de «SOAR».

La respuesta a incidentes y las operaciones de seguridad mejoran con las tecnologías SOAR

Varias áreas de la respuesta a incidentes y las operaciones de seguridad están cosechando los frutos de las tecnologías SOAR, quizá gracias a su capacidad de automatizar las operaciones de seguridad. Como apunta Gartner, «las tecnologías SOAR emergentes prometen llevar la automatización, coherencia y eficiencia a las operaciones de seguridad más allá de lo que es posible hoy con las soluciones SIEM».[3]

Entre los participantes en la encuesta que han utilizado las tecnologías SOAR durante al menos dos años, el 54 % reconocían que SOAR les ha ahorrado tiempo a la hora de responder a los incidentes. Otras mejoras son la agilización del proceso de mitigación (51 %), la reducción del tiempo medio de respuesta a incidentes de inicio a fin (47 %) y la aceleración del proceso de clasificación de alertas (44 %). Un 37 % sostenía que SOAR le ayudó a abreviar el proceso de respuesta a incidentes.

La figura 19 ofrece información sobre cómo han mejorado las tecnologías SOAR el rendimiento del SOC para este grupo; a saber:

- Los procesos están mejor definidos (79 %).
- La comunicación entre el equipo de operaciones de seguridad y el resto de departamentos ha mejorado (53 %).
- Los equipos SOC pueden reducir o incluso eliminar pasos innecesarios del flujo de trabajo (47 %).
- La estructura del equipo se ha homogeneizado gracias a la nivelación al alza de las habilidades de los analistas (42 %).
- Permite responder a casos de uso de seguridad más complejos (42 %).
- La estructura del equipo se ha homogeneizado gracias a la automatización de los procesos (37 %).

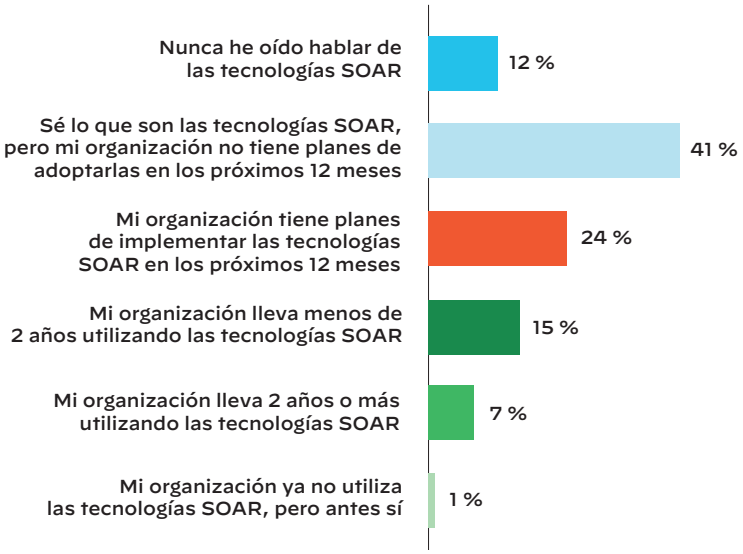

Figura 18: «¿Cuál de estas opciones describe mejor el uso que hace de las herramientas SOAR, el interés que le suscitan y su familiaridad con ellas?»

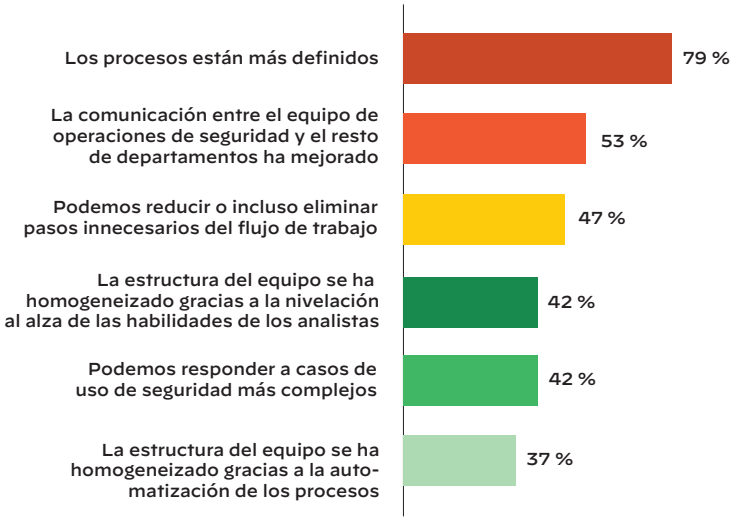

Figura 19: «¿Cómo ha cambiado sus flujos de trabajo la implementación de las tecnologías SOAR? (Seleccione todas las respuestas que correspondan)». Nota: N = 19

Estos resultados sugieren que las tecnologías SOAR ofrecen una solución viable a algunos de los retos a los que se enfrentan actualmente los equipos SOC. La mejora de la comunicación con los equipos externos ayuda a resolver el problema señalado en la figura 14 sobre la dificultad de los SOC para tratar con los departamentos jurídico, de recursos humanos e informático, entre otros. Gracias a que se tarda menos tiempo en gestionar y resolver incidentes, las tecnologías SOAR contribuyen a aliviar el estrés derivado del altísimo volumen de alertas que se generan y de la necesidad de seguir demasiados canales de amenazas. Como la clasificación es más rápida y los equipos SOC son más productivos, estos se pueden concentrar en incidentes más complejos en lugar de perder el tiempo en alertas de baja prioridad.

3. *Top Security and Risk Management Trends* (disponible en inglés), Gartner, 27 de febrero de 2020.

Hay interés e intención de comprar

¿Qué planes de futuro tienen los responsables de la seguridad con respecto a las tecnologías SOAR? El 43 % de los encuestados —incluidos tanto los que ya tienen alguna solución SOAR como los que no— afirman que el año que viene tienen previsto invertir más en herramientas SOAR.

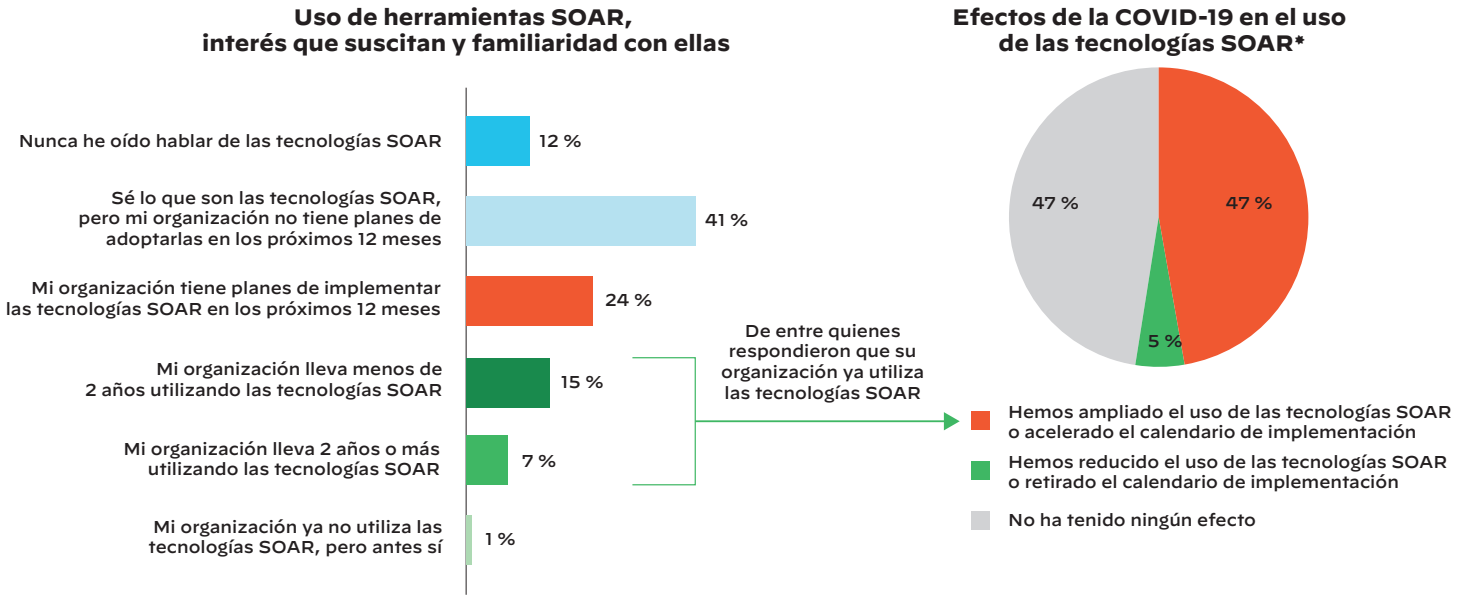

Figura 20: «¿Cómo ha influido la pandemia de COVID-19 en el uso (ya sea planificado o implementado) de las tecnologías SOAR por parte de su organización?»
Nota: N = 19

IdC, MITRE y equipos rojos: una apuesta clara por las tecnologías SOAR

En sus planes para los próximos años, los usuarios de las tecnologías SOAR tienen en mente cargas de trabajo específicas. La tabla 1 desglosa el resumen de las respuestas dadas a la pregunta: «¿Qué intención tiene de ampliar el uso de las tecnologías SOAR para estos casos?». De entre las organizaciones que ya utilizan SOAR, el 38 % tiene previsto ampliar su uso a la gestión del Internet de las Cosas (IdC) en los próximos 12 meses, mientras que el 23 % está interesado en ese caso de uso pero sin planes de implementarlo en los próximos 12 meses. Cuando se combina con las organizaciones que ya utilizan SOAR para gestionar el IdC, un asombroso 69 % de las empresas que utilizan las tecnologías las contemplan como un elemento más de su estrategia de gestión del IdC.

Parece que la probabilidad de utilizarlas en los futuros flujos de trabajo de equipo rojo, seguridad en la nube y casos de uso de MITRE ATT&CK® también es bastante elevada; el 57, 55 y 55 % de las organizaciones, respectivamente, ya utilizan las tecnologías SOAR para estos propósitos o manifiestan interés en hacerlo. Hasta los casos de uso que mostraban niveles de interés más bajos —como la priorización de vulnerabilidades, las operaciones informáticas y la detección y respuesta— lo tenían aun así en un 45, 43 y 42 %, respectivamente, en el momento de responder a la encuesta y en el futuro.

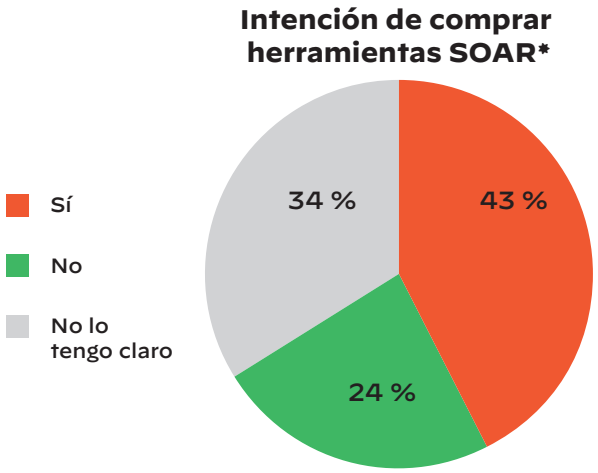

Figura 21: «¿Está su organización planeando aumentar el gasto en herramientas SOAR en 2020?»

* Debido al redondeo, es posible que los totales superen el 100 %.

Tabla 1: Respuestas a la pregunta: «¿Qué intención tiene de ampliar el uso de las tecnologías SOAR para estos casos?»		
	Con interés y planes de implementarlas en los próximos 12 meses	Ya utilizo las tecnologías SOAR en este caso de uso
Gestión del IdC	38 %	8 %
Flujos de trabajo de equipo rojo	40 %	15 %
Seguridad en la nube	17 %	25 %
Casos de uso de MITRE ATT&CK	25 %	18 %
Gestión de identidades e incorporación del personal	25 %	22 %
Comprobaciones de cumplimiento normativo	23 %	30 %
Auditorías de seguridad	23 %	30 %
Operaciones de red	18 %	27 %
Priorización de vulnerabilidades	15 %	37 %
Operaciones informáticas	25 %	27 %
Detección y respuesta	15 %	45 %
Promedios	24 %	26 %

Cómo puede ayudar Cortex XSOAR

Cortex™ XSOAR de Palo Alto Networks ofrece una única plataforma que orquesta las acciones que se llevan a cabo en toda la pila de productos de seguridad con el fin de lograr una respuesta a incidentes más rápida y escalable. Optimiza los procesos de respuesta a incidentes conectando herramientas dispares y automatizando las tareas manuales y repetitivas que no requieren intervención humana. Cortex XSOAR es la primera solución de operaciones de seguridad del sector que integra de forma nativa en una sola plataforma todas las funciones de colaboración y gestión de incidentes, orquestación y automatización de la seguridad, e inteligencia sobre amenazas.

Según los participantes en esta encuesta, y como se aprecia en la tabla 2, Cortex XSOAR ayuda a resolver los retos relacionados con la respuesta a incidentes.

Tabla 2: Cómo responde Cortex XSOAR a los retos derivados de la respuesta a incidentes		
Reto/deseo	Solución necesaria	Lo que ofrece Cortex XSOAR
Demasiados procesos de respuesta a incidentes manuales	Más automatización para acelerar el proceso de respuesta a incidentes y reducir el número de operaciones manuales.	Automatización de acciones repetitivas coordinando los procesos en toda la pila de productos de seguridad con libros de estrategias.
Falta de integración con productos de terceros	Integración de las herramientas del SOC con sistemas de terceros para que puedan conectarse fácilmente con otros departamentos y procesos de respuesta a incidentes.	Más de 450 integraciones de productos de terceros para coordinar y automatizar las operaciones de seguridad.
Compartir libros de estrategias creados por la comunidad/otros compañeros de profesión	Acceso a más libros de estrategias —ya sean de terceros o de una comunidad que comparta este tipo de recursos— para aprovechar los conocimientos y la experiencia de otros equipos.	Más de 15 000 compañeros que comparten prácticas recomendadas en una comunidad abierta de investigación forense digital y respuesta a incidentes (DFIR, por sus siglas en inglés).
Demasiados canales de amenazas que supervisar	Inteligencia sobre amenazas integrada con las herramientas de SecOps para reducir la cantidad de canales de inteligencia sobre amenazas que tienen que supervisar para anticiparse a las amenazas más graves.	Gestión de la inteligencia sobre amenazas que permite al SOC hacerse con el control de cualquier fuente de inteligencia sobre amenazas al unificar la agregación, la puntuación y el uso compartido de información con la automatización probada basada en libros de estrategias.
Demasiadas alertas que gestionar de forma eficaz o eficiente	Reducción de alertas.	Reducción de hasta un 95 % en el volumen de alertas que requieren revisión.

Conclusión

Este cuarto informe anual sobre el estado de las tecnologías SOAR da cuenta de lo rápido que cambia la ciberseguridad. Las amenazas son más graves, ya que además los SOC tienen que enfrentarse a ataques sumamente sofisticados diseñados por actores estatales. En estas circunstancias, aunque las operaciones de seguridad han mejorado en ciertos aspectos, la respuesta a incidentes sigue siendo para los analistas un proceso abrumador: hay que gestionar demasiadas alertas y supervisar demasiados canales de amenazas; los procesos manuales siguen siendo excesivos, lo que ralentiza las respuestas e impide atender las alertas realmente importantes.

Los analistas de seguridad saben perfectamente lo que hay que hacer para mejorar la situación. Quieren una mayor automatización de los procesos de respuesta a incidentes y menos alertas que gestionar. Las herramientas del SOC tienen que integrarse con los sistemas de otros fabricantes. Disponer de un catálogo más amplio de libros de estrategias, sobre todo que hayan recibido la certificación de algún proveedor, contribuye a que el SOC funcione de manera más efectiva. La inteligencia sobre amenazas tiene que integrarse perfectamente con las herramientas de SecOps.

Las tecnologías SOAR ofrecen una solución a muchos de estos problemas. Plataformas como Cortex XSOAR ayudan a los equipos SOC a ahorrar tiempo, agilizar la clasificación de alertas y acortar los procesos de respuesta a incidentes. Tal y como revelan los resultados de la encuesta, los equipos de los SOC están planificando usar las tecnologías SOAR el año que viene de formas innovadoras. Pese a que la COVID-19 ha añadido aún más presión a los miembros del SOC, es un buen momento para mejorar la eficacia y la productividad de estos centros con las tecnologías SOAR.

Apéndice: Datos demográficos de la encuesta

Los encuestados se seleccionaron en la comunidad Virtual Intelligence Briefings, formada por más de 150 000 profesionales de la seguridad. La figura 22 muestra de qué tamaño son las organizaciones representadas y en qué proporción respondieron a la encuesta. Todos los participantes desempeñan funciones relacionadas con la seguridad y el cumplimiento de la normativa.

La encuesta descalificó a aquellas personas que:

- trabajaban en organizaciones de menos de 1000 empleados o tenían externalizados todos los servicios de seguridad;
- no estaban seguras de si los servicios de seguridad de su organización estaban externalizados total o parcialmente;
- no ejercían un cargo relacionado con la seguridad o el área de seguridad estaba por debajo de ellas en la cadena de gestión.

En la encuesta están representados los siguientes sectores: servicios financieros (17 %), tecnología o servicios tecnológicos (15 %), salud (13 %) y comercio minorista, y otros en menores proporciones. Ningún sector tiene más de un 20 % de encuestados. En cuanto a las funciones desempeñadas por los participantes, el 24 % son ingenieros o analistas de seguridad. El 17 % son responsables de supervisar una función de ciberseguridad y el 14 % son arquitectos de seguridad.

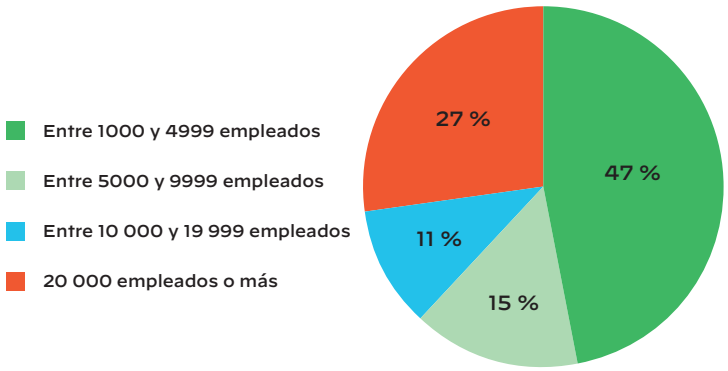

Figura 22: Perfil demográfico de las organizaciones a las que pertenecen los encuestados

paloalto NETWORKS
Oval Tower, De Entrée 99 - 197
1101 HE Ámsterdam
Países Bajos
Tel.: +31 20 888 1883
www.paloaltonetworks.es