SOC 2026: cuando detectar ya no es suficiente

ciberseguridadTIC

SOC 2026: cuando detectar ya no es suficiente

La explosión del cloud, la identidad, la inteligencia artificial y la automatización está obligando a replantear el papel del centro de operaciones de seguridad. CISO, proveedores de servicios y fabricantes coinciden en que el gran reto ya no consiste en generar más alertas, sino en comprender mejor el riesgo y responder con mayor rapidez.

¿Está preparado el SOC para una nueva generación de amenazas?

Durante años, la evolución de la ciberseguridad estuvo marcada por una carrera constante por mejorar la capacidad de detección. Cada nueva tecnología incorporaba una nueva fuente de información: primero fueron los firewalls, después los SIEM, llegaron los EDR y XDR, el cloud multiplicó los eventos que monitorizar y, más recientemente, la inteligencia artificial ha añadido una nueva capa de datos, automatización y capacidades de análisis.

El resultado es que las organizaciones nunca habían tenido tanta información sobre lo que ocurre en sus entornos. Sin embargo, dispo-

ner de más datos no ha simplificado necesariamente el trabajo de los equipos de seguridad. Al contrario. La proliferación de identidades, servicios cloud, aplicaciones SaaS, dispositivos conectados, terceros con acceso a la infraestructura y agentes de inteligencia artificial ha ampliado la superficie de exposición hasta un punto en el que el principal desafío ya no consiste en descubrir amenazas, sino en entender cuáles son realmente relevantes.

En ese contexto, el SOC está viviendo probablemente la transformación más profunda desde su aparición. Su misión ya no se limita a monitorizar eventos o coordinar la respuesta ante incidentes. Cada vez se le exige una mayor capacidad para interpretar el contexto, priorizar riesgos, automatizar procesos y facilitar decisiones que reduzcan el impacto de los incidentes sobre el negocio.

Para conocer cómo está evolucionando realmente este modelo operativo, Ciberseguridad TIC ha recogido la visión de responsables de seguridad de grandes organizaciones, proveedores de servicios y fabricantes especializados; todos coinciden en una idea: el futuro del SOC dependerá menos de su capacidad para generar alertas y mucho más de su capacidad para convertir la información en decisiones.

> “Hemos ganado visibilidad, pero también una complejidad operativa que obliga a mejorar la correlación y acelerar la respuesta”
>
> **Alejandro Velilla Alonso,** CTO, **Embou MasOrange**

¿Qué preocupa realmente a quienes dirigen la seguridad?

Escuchar a quienes conviven diariamente con la operación de un SOC deja una sensación clara: el problema ya no consiste únicamente en mejorar la capacidad de detección. La preocupación se ha desplazado hacia cuestiones mucho más profundas, como la capacidad para responder con rapidez, gestionar una superficie de ataque cada vez más amplia y adaptar los modelos tradicionales de operación a un escenario radicalmente distinto al de hace solo unos años.

Alejandro Velilla Alonso, CTO de Embou MasOrange, considera que los SOC han mejorado notablemente su capacidad para gestionar incidentes conocidos, aunque reconoce que todavía existen limitaciones cuando se trata de amenazas más sofisticadas o movimientos laterales dentro de la red. A ello se suma una dificultad añadida: trasladar esa capacidad de detección a procesos de contención y recuperación realmente ágiles, especialmente

en organizaciones de gran tamaño. Si tuviera que priorizar una mejora inmediata, no duda en señalar la reducción del ruido operativo: “Ahora mismo hay demasiado ruido, lo que impacta directamente en la capacidad de detectar amenazas reales y actuar en consecuencia”, explica, convencido de que una mejor correlación de eventos tendría un efecto inmediato sobre toda la operación.

En CESCE la reflexión se sitúa en un plano diferente. Para Enrique Cervantes Mora, director de Seguridad e Infraestructura Tecnológica de la compañía, el error consiste en pensar que la respuesta a un incidente depende exclusivamente del SOC. Tiene claro que “puede ser el primer paso, pero la respuesta siempre debe ser un resultado de la colaboración completa de todas las áreas de una compañía. Empezando por el Comité”. Desde su punto de vista, la eficacia de un SOC no depende únicamente de las herramientas o de la capacidad de detección, sino también del grado de coordinación entre los equipos técnicos, los responsables

> “Hoy necesitamos mirar en lugares donde antes ni siquiera buscábamos, porque la superficie de ataque ha cambiado por completo”
>
> **Enrique Cervantes Mora,** director de Seguridad e Infraestructura Tecnológica,**CESCE**

de negocio y los procedimientos de continuidad. “Necesitamos todas esas nuevas herramientas y mirar en sitios en los que no mirábamos antes”, señala, apuntando a las cadenas de suministro como uno de los ámbitos donde sigue siendo más difícil mantener una visibilidad completa.

Junto a los retos asociados a la complejidad operativa o la coordinación entre equipos, Manuel Barrios Paredes Paredes, Global Chief Information Security Officer de SGS, incorpora un nuevo elemento al debate: el cambio de paradigma que supone la irrupción de atacantes automatizados impulsados por IA. Explica que muchos SOC continúan diseñándose con una premisa que empieza a quedarse obsoleta: asumir que el atacante es humano, y que durante muchos años se calibraron tiempos de detección, *playbooks* y SLAs “asumiendo que el atacante era humano, que dormía, que cometía errores por fatiga... Ese modelo mental está quedando obsoleto”. Frente a unos equipos que trabajan por turnos, los ataques automatizados impulsados por inteligencia artificial pueden operar de forma continua, aprender del entorno y modificar su comportamiento sin intervención humana.

Ese cambio de paradigma tiene consecuencias

directas sobre la operación diaria. Aunque reconoce que las organizaciones disponen hoy de más telemetría, más conectores y una capacidad de observación muy superior a la de hace unos años, lanza una advertencia que resume buena parte del debate actual: “Acumular señal no es lo mismo que tener inteligencia accionable”. En su opinión, los puntos ciegos más preocupantes ya no son únicamente el movimiento lateral, el Shadow IT o las identidades con exceso de privilegios. Empiezan a surgir otros relacionados con agentes internos de inteligencia artificial, identidades no humanas, ataques de *prompt injection* o nuevos mecanismos de exfiltración que escapan a muchos de los controles tradicionales.

La consecuencia es que también cambia la forma de entender las prioridades del SOC. Barrios volvería a elegir la reducción del volumen de alertas como principal objetivo, pero introduce un matiz que resulta especialmente revelador: no se trata simplemente de generar menos avisos, sino de replantear qué debe considerarse realmente una alerta. Los modelos actuales, explica, fueron diseñados para detectar comportamientos anómalos de usuarios humanos y no siempre son capaces de identificar desviaciones producidas por agentes automatizados. El reto pasa por incorporar nuevas reglas de correlación, modelos específicos para supervisar agentes de IA y una automatización defensiva capaz de responder con la misma velocidad con la que evolucionan los ataques.

> “Acumular señal no es lo mismo que tener inteligencia accionable”
>
> **Manuel Barrios Paredes,**
> Global Chief Information Security Officer, **SGS**

En conjunto, las tres visiones dibujan un escenario mucho más amplio que el de la simple evolución tecnológica del SOC. Hablan de organizaciones que deben responder más rápido, coordinar mejor sus procesos, gestionar una complejidad creciente y prepararse para amenazas que ya no se comportan como las de hace apenas unos años. Y esa percepción es, precisamente, la que más tarde confirman tanto los operadores de SOC como los propios fabricantes.

¿Qué está ocurriendo en los SOC que operan para múltiples organizaciones?

Si los responsables de seguridad describen los retos desde la perspectiva de una única organización, quienes gestionan SOC para decenas o cientos de clientes disponen de una visión mucho más amplia sobre el grado de madurez del mercado. Y una de las primeras conclusiones es que todavía conviven realidades muy diferentes.

"La ausencia de contexto sigue siendo una de las principales causas de los falsos positivos"

Carlos Fernández,
responsable Global de xMDR, **Prosegur Cybersecurity**

Carlos Fernández, responsable global de xMDR en Prosegur Cybersecurity, distingue claramente entre las grandes organizaciones, que han invertido en equipos especializados y capacidades avanzadas de detección y respuesta, y un amplio tejido empresarial que continúa apoyándose en proveedores externos para gestionar su seguridad. Pero incluso dentro de estos servicios gestionados, observa diferencias importantes: "mayormente seguimos viendo operaciones que trabajan en modo reactivo, con pocas tecnologías y un gran número de falsos positivos debido a la ausencia de contexto".

La evolución, sin embargo, ya está en marcha. Para Francisco Valencia, director general de Secure&IT, las organizaciones avanzan de forma decidida hacia modelos cada vez más automatizados. Los EDR, los *playbooks* o las plataformas SOAR llevan años reduciendo tareas manuales y, con la incorporación de la inteligencia artificial, esa automatización está ganando velocidad. "Especialmente con el uso de la inteligencia artificial, esos *playbooks* y esa capacidad de respuesta son mucho más automáticos y mucho más rápidos", afirma.

Cómo ha evolucionado el SOC

Ayer	Hoy	Mañana
Perímetro	Identidad + cloud + datos	Agentes IA + identidades no humanas
SIEM	Plataformas integradas	IA agéntica
Detectar	Priorizar	Anticipar
Alertas	Contexto	Decisiones
Analista	Analista + IA	Automatización supervisada
Tecnología	Riesgo	Negocio

Ambos coinciden también en que el crecimiento del cloud, la identidad y la protección del dato ha incrementado la complejidad de la operación, aunque analizan sus consecuencias desde perspectivas diferentes. Carlos Fernández considera que la proliferación de nuevas tecnologías ha provocado una creciente fragmentación tanto tecnológica como organizativa, impulsando la demanda de plataformas capaces de reunir información procedente de múltiples fabricantes y ofrecer una visión unificada del riesgo.

Francisco Valencia, por su parte, introduce un matiz interesante. A su juicio, la inteligencia artificial no sólo está aumentando la capacidad de análisis, sino que también está ayudando a simplificar la operación y mejorar la visibilidad. Sin embargo, identifica un nuevo punto ciego que apenas empezamos a comprender: el uso que las propias personas hacen de la IA y la dificultad para interpretar cómo toman decisiones los modelos. En su opinión, “el punto ciego clave es la explicabilidad que tiene la IA y el uso que nuestros propios agentes o usuarios hacen de ella”, señala.

> “El objetivo no es tener menos alertas, sino que las alertas sean realmente relevantes”
>
> **Francisco Valencia,**
> Director general de **Secure&IT**

Las diferencias también aparecen cuando se les pregunta por las prioridades del SOC. Mientras muchas organizaciones sitúan la reducción del ruido entre sus principales objetivos, Carlos Fernández considera que el verdadero reto no consiste en eliminar alertas, sino en ser capaces de contextualizarlas. Asegurando que la eliminación de alertas “no deja de ser la creación de puntos ciegos”, añade que la combinación de múltiples fuentes de información y el apoyo de la IA permiten aumentar la precisión de la detección, reducir los falsos positivos y acelerar la respuesta sin renunciar a la visibilidad.

Francisco Valencia comparte esa idea desde otro enfoque. Más que recibir menos avisos, considera que el objetivo debe ser que las alertas “sean reales”. Detectar mejor, responder antes y reducir el ruido forman parte, en su opinión, de un mismo proceso, donde la IA y la automatización ya están ayudando a mejorar la eficacia de los SOC.

En conjunto, las respuestas reflejan una evolución que va mucho más allá de la incorporación de nuevas tecnologías. Los SOC están automatizando procesos, integrando información procedente de múltiples fuentes y utilizando la inteligencia artificial para acelerar la investigación

y la respuesta. Sin embargo, la madurez sigue siendo desigual y el gran reto continúa siendo el mismo: transformar un volumen creciente de datos en decisiones rápidas, contextualizadas y útiles para el analista.

Un SOC todavía en construcción

Después de escuchar a responsables de seguridad y operadores de SOC, surge una pregunta inevitable: ¿está respondiendo la tecnología a los nuevos desafíos que plantea la operación de seguridad? La respuesta de los fabricantes es afirmativa, aunque todos coinciden en un matiz importante: el problema ya no consiste únicamente en incorporar nuevas herramientas, sino en conseguir que todas ellas trabajen de forma coordinada y aporten el contexto necesario para tomar mejores decisiones.

Aunque el mercado lleva años hablando de automatización, inteligencia artificial o plataformas unificadas, pocos consideran que el proceso haya terminado. Para Miguel Carrero, vicepresidente global de Partner Ecosystem Growth y Cuentas Estratégicas de WatchGuard Technologies, el SOC sigue siendo, en gran medida, un "work in progress". En su opinión, muchas organizaciones han dejado atrás un modelo puramente reactivo, pero todavía conviven con silos tecnológicos, procesos excesivamente manuales y un volumen de alertas difícil de gestionar.

> "La madurez de un SOC no se mide por la cantidad de IA que incorpora, sino por la fricción operativa que consigue eliminar"

Miguel Carrero, Vicepresidente global de Partner Ecosystem Growth y Cuentas Estratégicas, **WatchGuard Technologies**

A su juicio, uno de los errores más habituales consiste en evolucionar de forma desequilibrada. Explica que, si una organización invierte mucho en detección, pero no tiene capacidad de respuesta "o automatiza sin una buena base de protección, o no prioriza según la criticidad del activo y el riesgo real para el negocio, la efectividad de la seguridad y el retorno de la inversión se resienten". Por eso defiende que la operación moderna debe centrarse "menos en identificar o ver más alertas y más en entender qué importa, qué riesgo implica y qué acción debe ejecutarse primero".

Una percepción muy similar comparte Ignacio Franzoni, director de ingeniería de soluciones de Netskope. También él considera que las organizaciones atraviesan un periodo de transición entre modelos tradicionales y operaciones mucho más orientadas al riesgo. "La diferencia estriba en pasar de gestionar alertas a comprender la exposición, el contexto y el impac-

“La IA sólo aporta valor cuando existe una arquitectura capaz de convertir la información en contexto”

Ignacio Franzoni,
director de Ingeniería de Soluciones, **Netskope**

to potencial”, resume, añadiendo que la IA está acelerando esa evolución y advirtiendo que aún existen obstáculos importantes relacionados con la calidad de los datos, la integración entre herramientas y, sobre todo, la confianza necesaria para delegar determinadas decisiones en modelos automatizados.

La diferencia estriba en pasar de gestionar alertas a comprender la exposición, el contexto y el impacto potencial

La inteligencia artificial acelera el cambio

Si hay una tecnología que aparece de forma transversal en todas las respuestas es la inteligencia artificial. Sin embargo, ninguno de los fabricantes la presenta como una solución capaz de resolver por sí sola los problemas del SOC.

Miguel Carrero distingue incluso tres niveles de aplicación. El primero busca mejorar la productividad de los analistas mediante asistentes capaces de resumir investigaciones o documentar incidentes. El segundo incorpora capacidades más avanzadas para correlacionar información, automatizar investigaciones y reducir los tiempos de detección y respuesta. El tercero, sin embargo, obliga a mirar la IA desde otra perspectiva: como una nueva superficie de ataque. Los ciberdelincuentes también están utilizando inteligencia artificial para automatizar campañas, perfeccionar la ingeniería social o acelerar sus operaciones, mientras fenómenos como el Shadow AI plantean nuevos retos de gobernanza dentro de las organizaciones. “La IA no arregla un SOC desordenado; lo puede amplificar”, advierte.

Desde Silverfort, Javier Gómez Berruezo,Regional Sales Manager Iberia de la compañía, coi ncide en que el verdadero freno no está en la tecnología. Al describir la situación de muchos equipos de operaciones, desbordados por miles de registros y alertas que apenas les dejan margen para evolucionar afirma que “es difícil construir el futuro cuando el presente te

consume". En ese contexto, considera que la IA ya está demostrando su utilidad para correlacionar señales y ayudar en la priorización, pero recuerda que "la IA no hace magia con malos datos". Sin información contextualizada y de calidad, explica, cualquier automatización termina generando más frustración que eficiencia.

Ignacio Franzoni comparte esa idea. A su juicio, la IA sólo aporta verdadero valor cuando se utiliza para enriquecer el contexto, explicar el riesgo y asistir a los analistas en la toma de decisiones. En su opinión "la IA no sustituye a una buena estrategia de seguridad, sino que la potencia cuando hay buen contexto, buenas políticas y una arquitectura bien integrada".

Del exceso de información al contexto

Si existe un concepto que aparece una y otra vez en todas las respuestas es el de contexto. Los fabricantes coinciden en que las organizaciones nunca habían dispuesto de tanta información sobre lo que ocurre en sus infraestructuras.

"El reto ya no es ver más, sino entender mejor cada interacción"

Pablo Chapinal,
Regional Director Iberia, **Zscaler**

Sin embargo, esa capacidad de observación no siempre se traduce en una mejor comprensión del riesgo.

"Las organizaciones tienen más datos que nunca, pero no necesariamente más visibilidad útil", afirma Ignacio Franzoni, señalando que la incorporación de nuevas capas asociadas al cloud, la identidad, las aplicaciones SaaS, la protección del dato o la IA generativa ha multiplicado las fuentes de telemetría, pero también la dificultad para integrarlas en una visión coherente del riesgo.

Pablo Chapinal, Regional Director Iberia de Zscaler, coincide plenamente con este diagnóstico. A su juicio, las organizaciones han ganado capacidad para analizar el contexto de acceso, la identidad, el uso de aplicaciones cloud, el movimiento de los datos o el comportamiento de los usuarios. Sin embargo, recuerda que esa ventaja desaparece cuando cada tecnología funciona de manera aislada. "El reto ya no es únicamente ver más, sino entender mejor cada interacción: quién accede, desde dónde, a qué aplicación, con qué nivel de riesgo y qué datos están implicados", explica. Por ello considera que el objetivo del SOC debe ser transformar miles de señales dispersas en información accionable que permita responder antes y con mayor precisión.

> “Hoy tenemos más datos que nunca y, paradójicamente, menos claridad que antes”

Javier Gómez Berruezo,
Regional Sales Manager Iberia, **Silverfort**

El próximo desafío: identidades que ya no son personas

Otro de los cambios que empiezan a dibujar el futuro del SOC tiene que ver con la identidad. Pero no tanto con la gestión de usuarios tradicionales como con la aparición de nuevos actores digitales que operan dentro de las organizaciones.

Javier Gómez Berruezo considera que uno de los principales puntos ciegos actuales ya no está en las personas, sino en las identidades no humanas. Advierte que las cuentas de servicio, automatizaciones, integraciones entre sistemas, “y ahora también agentes de IA, se mueven por la infraestructura con privilegios elevados sin que nadie los supervise de verdad”. El resultado, añade, es una paradoja cada vez más habitual: “Tienes más datos que nunca y menos claridad que antes”.

Su reflexión conecta directamente con la preocupación expresada anteriormente por Manuel Barrios sobre la necesidad de desarrollar nuevos modelos de supervisión para agentes de inteligencia artificial capaces de actuar de forma autónoma. Ambos coinciden en que una parte importante de la próxima evolución del SOC pasará por aprender a gobernar estas nuevas identidades y comprender su comportamiento antes de que se conviertan en un nuevo punto ciego para las organizaciones.

Qué preocupa hoy a cada actor

CxO	MSSP	Fabricantes
Reducir el ruido	Automatizar	Contextualizar
Responder antes	Correlacionar	Aplicar IA
Proteger el negocio	Integrar plataformas	Unificar la operación

El SOC ya no se mide por las alertas que genera, sino por las decisiones que ayuda a tomar

Hace apenas unos años, la madurez de un SOC se asociaba principalmente a indicadores como el número de eventos monitorizados, la capacidad de detección o el tiempo necesario para responder a un incidente. Hoy esos parámetros siguen siendo importantes, pero ya no bastan para medir la eficacia de una operación de seguridad. Las conversaciones mantenidas con responsables de seguridad, proveedores especializados y fabricantes apuntan a un cambio de enfoque mucho más profundo. El verdadero reto ya no consiste en incorporar nuevas herramientas o generar más alertas, sino en comprender mejor el riesgo, reducir el ruido operativo y ayudar a la organización a tomar decisiones con mayor rapidez.

La inteligencia artificial será una pieza clave en esa evolución. Automatizará tareas, acelerará las investigaciones y ayudará a correlacionar información procedente de múltiples fuentes. Sin embargo, todos los participantes coinciden en una idea: cuanto más automatizada sea la operación, más importante será el criterio humano para interpretar el contexto, valorar el impacto sobre el negocio y decidir cuál es la respuesta más adecuada.

Porque la gran transformación del SOC va mucho más allá de la tecnología. Está dejando de ser un centro de monitorización para convertirse en una capacidad estratégica que conecta operaciones, riesgo y negocio. Al final, su éxito ya no dependerá de cuántas alertas sea capaz de procesar, sino de su capacidad para ofrecer el contexto necesario que permita a las organizaciones tomar la decisión correcta en el momento adecuado.