Telefónica Tech

El SOC del Futuro: Cómo la IA y la automatización están redefiniendo la ciberseguridad

paloalto NETWORKS

FROST & SULLIVAN

Índice

01

Principales desafíos en la evolución hacia el SOC del futuro

Al diseñar las estrategias de ciberseguridad de las empresas y gobiernos, los responsables de ciberseguridad se enfrentan a un panorama increíblemente complejo, en constante cambio y evolución. La ciberseguridad sigue consolidándose como una prioridad global, impulsada por el **crecimiento de la superficie de ataque**, resultado de la adopción de nuevas tecnologías como la inteligencia artificial generativa (*GenAI*) y la migración a nubes públicas, según el estudio de *Morgan Stanley, Cybersecurity 2025 Outlook*. A pesar del uso de herramientas como la inteligencia artificial (IA), *machine learning* (ML) y *GenAI* por parte de los actores maliciosos, más del 90% de los SOC (*Security Operations Center* o Centro de Operaciones de Seguridad en español) siguen dependiendo de procesos manuales, de acuerdo con datos del informe *Incident Response 2024* publicado por Unit 42, el equipo encargado de la investigación de amenazas y ciberinteligencia en Palo Alto Networks.

Aunque el número de ataques de *ransomware* está moderándose, **los costes totales de las brechas de seguridad siguen aumentando**. Según el Informe sobre el Estado de la Seguridad 2024 H2, publicado por Telefónica Tech, en el segundo semestre de 2024 se detectaron más de 333 millones de eventos de ciberseguridad. Además, el informe *Incident Response 2024* revela un dato preocupante: el 4,1 % de los ataques de *malware* en 2023 tuvieron como objetivo la destrucción de datos, cinco veces superior al año anterior.

La profunda transformación digital de empresas y gobiernos, reflejada en altos índices de trabajo remoto, adopción de la nube o implementación del Internet de las Cosas (IoT), tiene un impacto directo para los responsables de ciberseguridad: **un ecosistema cada vez más híbrido, más complejo y difícil de proteger.** De acuerdo con el *2024 State of the Cloud Report* publicado por Flexera, el 89% de las organizaciones están utilizando infraestructura multi-nube, y el 73% está utilizando infraestructura de nube híbrida.

+90%

de los SOCs siguen dependiendo de procesos manuales

Fuente: Incident Response 2024 (Unit 42)

+333 millones

de eventos de ciberseguridad fueron detectados en el segundo trimestre de 2024

Fuente: Informe sobre el Estado de la Seguridad 2024 H2 (Telefónica Tech)

Otro factor agravante es la escasez global de talento en ciberseguridad, que limita y condiciona la búsqueda de analistas. Según el *2024 ISC2 Cybersecurity Workforce Study,* de ISC2, hay cerca de 4,8 millones de puestos sin cubrir en ciberseguridad. **Esto representa un crecimiento de 19,1% en la brecha de talento respecto al año anterior.** La demanda desmesurada de profesionales dificulta su contratación y retención. Como resultado, para los responsables de ciberseguridad es muy complicado gestionar y ejecutar una estrategia de seguridad compleja, que haga un uso efectivo de soluciones sofisticadas capaces de responder a la constante batería de ataques.

Adicionalmente, existen **múltiples normativas y regulaciones de seguridad establecidas por distintos gobiernos para incrementar la resiliencia de las organizaciones**, como GDPR (*General Data Protection Regulation*) en Europa, ENS (Esquema Nacional de Seguridad), CRA (*Cyber Resilience Act* de la Unión Europea), la directiva NIS2 (*European Network and Information Security Directive*), y las regulaciones dictadas por la *US National Security Strategy*. El cumplimiento de dichas normas obliga a los encargados de la ciberseguridad a mantener registros exhaustivos de su información y reportar incidentes, aumentando la necesidad de herramientas de seguridad que provean visibilidad sobre el ecosistema.

Para hacer frente a ataques cada vez más sofisticados, los líderes de ciberseguridad requieren capacidades avanzadas de prevención, detección y respuesta. Para ello, deben aprovechar las mismas herramientas que sus atacantes, impulsando su seguridad mediante el uso de IA, algoritmos de ML y *copilots* de *GenAI* que potencien la eficiencia de los analistas, reduzcan el volumen de alertas, minimicen los tiempos de respuesta y mejoren la capacidad de reacción ante las amenazas modernas. Además, sus estrategias de seguridad deben alinearse con un objetivo empresarial clave: garantizar la protección manteniendo los costes bajo control. En este escenario, contar con un SOC moderno y con tecnología avanzada es la solución.

02

Transformación en la ciberdefensa: Superando las amenazas para *mejorar la visibilidad*

El primer requisito de una estrategia efectiva de ciberseguridad es tener una visibilidad total del ecosistema. Sin embargo, los factores previamente mencionados hacen que esto sea un desafío significativo para las organizaciones que operan en entornos híbridos y multinube. Estas infraestructuras amplían la superficie de ataque, incrementan la exposición a amenazas y añaden complejidad en la gestión del tráfico de datos.

Desafíos principales de ciberseguridad para las organizaciones en todo el mundo

Figura 1. Fuente: *Voice of the Enterprise Security Customer de* ***Frost & Sullivan.***

88%

menos de tiempo de investigación gracias al uso de EDR, que agrupa alertas y analiza causas raíz.

Fuente: Palo Alto Networks

El primer paso para lograr visibilidad en la mayoría de las organizaciones es desplegar soluciones de EDR (*endpoint detection and response*) que permiten detectar, investigar y responder a amenazas que han superado el perímetro y alcanzado los *endpoints*. Según Palo Alto Networks, el uso de EDR puede reducir el tiempo de investigación en un 88% al agrupar alertas y analizar causas raíz. Sin embargo, un EDR no funciona de manera aislada, sino que se complementa con *firewalls*, seguridad en la nube e identidad y gestión de accesos (IAM), entre otras soluciones, para cubrir todos los vectores de ataque. El desafío surge cuando estas herramientas operan en silos independientes, sin compartir información entre sí.

La única solución efectiva es romper estos silos mediante un enfoque de plataforma, donde todas las soluciones de seguridad estén integradas y trabajen de manera coordinada, mejorando la detección y respuesta ante amenazas de forma eficiente.

03

Viaje sin fronteras: Eliminando los silos de seguridad para obtener *una visión integral*

Los profesionales de ciberseguridad están en alerta constante debido al alto volumen de notificaciones que reciben sobre posibles amenazas en el entorno que deben proteger.

Cada día, los sistemas de seguridad generan miles de alertas sobre posibles amenazas, aunque muchas de ellas terminan siendo falsos positivos. Según el informe *Incident Response 2024*, el 75% de las alertas son casos confirmados, el 15% son falsos positivos y el 10% restante suponen casos casi incidentes.

Por ello, **la denominada "fatiga de alertas" (*alert fatigue*) se ha convertido en uno de los mayores desafíos para los SOCs.** El principal problema es que investigar cada alerta en profundidad resulta inviable. Incluso al centrarse solo en las de mayor prioridad, la carga de trabajo sigue siendo abrumadora. Lo urgente no deja tiempo para lo importante: desarrollar y hacer madurar la estrategia de ciberseguridad de la organización a gran escala.

Por si esto fuera poco, las amenazas más sofisticadas tienen diferentes maneras de evitar los controles de seguridad, enmascarar su comportamiento y evitar generar alertas. Los ataques internos, los ataques dirigidos y el *malware* evasivo no muestran suficientes indicadores de riesgo, sino que se basan en comportamiento, por lo que las soluciones tradicionales de seguridad no pueden detectarlos.

Adicionalmente, **la cantidad de vulnerabilidades de día cero (zero-day vulnerabilities) ha mostrado una tendencia creciente en los últimos años**, y la forma en que estos ataques aprovechan vulnerabilidades críticas para infiltrarse en las redes de un sistema puede pasar desapercibida para la mayoría de las soluciones de seguridad. De acuerdo con el 2023 *Unit 42 Network Threat Trends Research Report*, entre 2021 y 2023, la explotación de vulnerabilidades para ataques aumentó en un 55%.

Cantidad de vulnerabilidades del día cero descubiertas

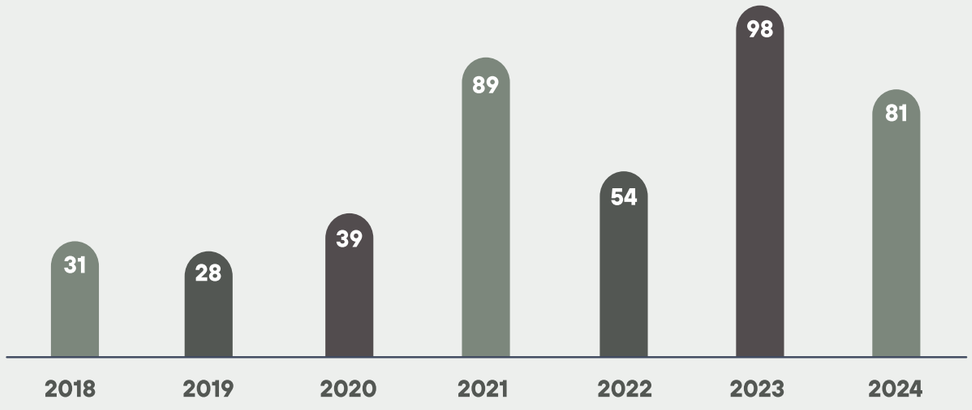


Figura 2. Fuente: *Base de datos de **Zero-Day.cz***

Según el *Incident Response 2024* publicado por *Unit 42* de Palo Alto Networks, en 2023 la principal vía de acceso utilizada por los atacantes fue la explotación de vulnerabilidades en *software* expuesto a internet, superando al *phishing* como método más común. Este cambio refleja una **tendencia hacia la automatización y el escalado masivo de ataques mediante la identificación de sistemas vulnerables en línea.** Además, las credenciales previamente comprometidas experimentaron un notable incremento como vector de ataque, quintuplicándose en los últimos dos años y destacando la importancia de prácticas sólidas de gestión de contraseñas y autenticación.

Dentro de los incidentes más destacados del segundo semestre de 2024, analizados en el *Informe sobre el Estado de la Ciberseguridad H2 2024* de Telefónica Tech, se registraron ataques que paralizaron negocios durante días y provocaron pérdidas millonarias en sectores clave como el tecnológico, financiero, automotriz y de gestión de datos.

Un ataque puede pasar desapercibido si se analiza de forma aislada desde distintas soluciones de seguridad, como un EDR, un *firewall* o una *Cloud Workload Protection Platform* (CWPP). **Cada una de estas herramientas podría no detectar un comportamiento sospechoso por sí sola, pero al correlacionar eventos y analizar el contexto de manera conjunta, es posible identificar que forman parte de un mismo ataque**. Este fenómeno se asemeja al experimento en el que un grupo de personas con los ojos vendados toca diferentes partes de un elefante como su trompa, orejas, colmillos, cola y patas. Individualmente, cada persona percibe sólo una fracción de la realidad, lo que dificulta entender lo que tienen delante. Sólo al compartir información y conectar piezas sueltas se obtiene una visión completa. Del mismo modo, **una ciberseguridad eficaz requiere un enfoque unificado, donde todas las soluciones trabajen en conjunto para detectar y mitigar amenazas de manera más precisa y eficiente.**

Un caso de alto impacto

En febrero de 2024, una empresa del sector sanitario en Estados Unidos, cuya plataforma conecta pagadores, proveedores y pacientes, fue víctima de un ciberataque de gran impacto. Dado su papel clave en el funcionamiento del sistema de salud del país, el ataque dejó al sector paralizado durante días y provocó pérdidas millonarias a la compañía. Se estima que la brecha pudo haber expuesto los datos de 1 de cada 3 ciudadanos del país. A día de hoy, las consecuencias siguen presentes: clientes que enfrentan problemas con la plataforma, proveedores con pérdidas económicas y otros efectos colaterales. La causa del incidente fue un servidor sin autenticación multifactor, lo que permitió el acceso no autorizado a los sistemas de la empresa. Este caso refuerza la importancia de contar con visibilidad total del ecosistema y aplicar análisis de comportamiento para prevenir y mitigar ataques de esta magnitud.

x5

el incremento de credenciales previamente comprometidas como vector de ataque en los últimos **2 años**

Fuente: *2024 Unit 42 Incident Response*

Entre

2021 y 2023

la explotación de vulnerabilidades para ataques aumentó en un **55%**

Fuente: *2023 Unit 42 Network Threat Trends Research Report*

Las plataformas de *extended detection and response* (XDR, Detección y Respuesta Extendidas) están basadas en el principio de que el **todo es mayor que la suma de sus partes**, y por tanto buscan unificar la seguridad y destruir los silos, incrementando la ciberresilencia mediante la sinergia y la comunicación entre los controles de seguridad.

XDR presenta **tres pilares clave: el primero es la detección y respuesta a las amenazas en todo el ecosistema.** Para lograrlo, las soluciones líderes de XDR recopilan telemetría de diversos controles de seguridad, incluyendo *endpoint*, redes, nube, identidades, *email,* móviles, IoT, OT, entre otros. Después, analizan y correlacionan estos datos, apoyándose en *machine learning* (ML) e inteligencia artificial (IA), descartando falsos positivos, reduciendo de manera significativa el volumen de alertas que saturan el SOC y analizando el comportamiento de las entidades del ecosistema. Además, agregan alertas e incidentes en procesos que cuentan la historia completa del ataque y proporcionan contexto esencial para los analistas.

Todo este proceso permite a los responsables de ciberseguridad tener una visibilidad casi ilimitada sobre su ecosistema, eliminando las barreras que imponen los entornos híbridos y multi-nube. La correlación y el uso de IA y ML para trabajar con los datos reduce el ruido y maximiza el valor de los analistas de ciberseguridad, permitiendo que se enfoquen en las alertas realmente importantes. Además, la solución detecta amenazas astutas que son más que la suma de sus partes, o que no presentan indicadores de riesgo tradicionales. **XDR es una plataforma unificada**, que centraliza múltiples fuentes de seguridad de una organización, reduciendo la complejidad y ofreciendo una respuesta eficaz frente amenazas avanzadas.

> *"Palo Alto Networks reportó que la implementación de XDR como pieza principal en un SOC puede lograr hasta una reducción del **80%** en el volumen alertas, además de **una mejora del 93%** en el tiempo de detección y **un 90%** en el tiempo de respuesta."*

04

Una ruta multidimensional: Extendiendo la cobertura a datos de terceros para incrementar la *resiliencia y flexibilidad*

La integración total del portafolio de seguridad de un proveedor mediante una solución de XDR es algo que puede proveer a las organizaciones de múltiples beneficios en términos de resiliencia, visibilidad, interoperabilidad y facilidad de despliegue. Pero para la mayoría de los responsables de ciberseguridad, esto es un imposible. Según Frost & Sullivan, más de 7 de cada 10 compañías trabajan con 5 proveedores de ciberseguridad o más.

Cantidad de compañías de seguridad con las que trabajan las organizaciones a lo largo del mundo

Figura 3. Fuente: *Voice of the Enterprise Security Customer de* ***Frost & Sullivan.***

Esto se debe a múltiples factores, desde la falta de presupuesto que obliga a las organizaciones a intentar hacer valer al máximo sus inversiones de seguridad, pasando por la preferencia personal y el interés en tener la mejor solución de su tipo, hasta las relaciones interempresariales y los contratos de múltiples años que hacen imposible cambiar de proveedor en cualquier momento. A pesar de la flexibilidad que otorga el trabajar con múltiples compañías de ciberseguridad, y según el estudio *Cybersecurity 2025 Outlook* de Morgan Stanley, existe una tendencia a la consolidación de proveedores.

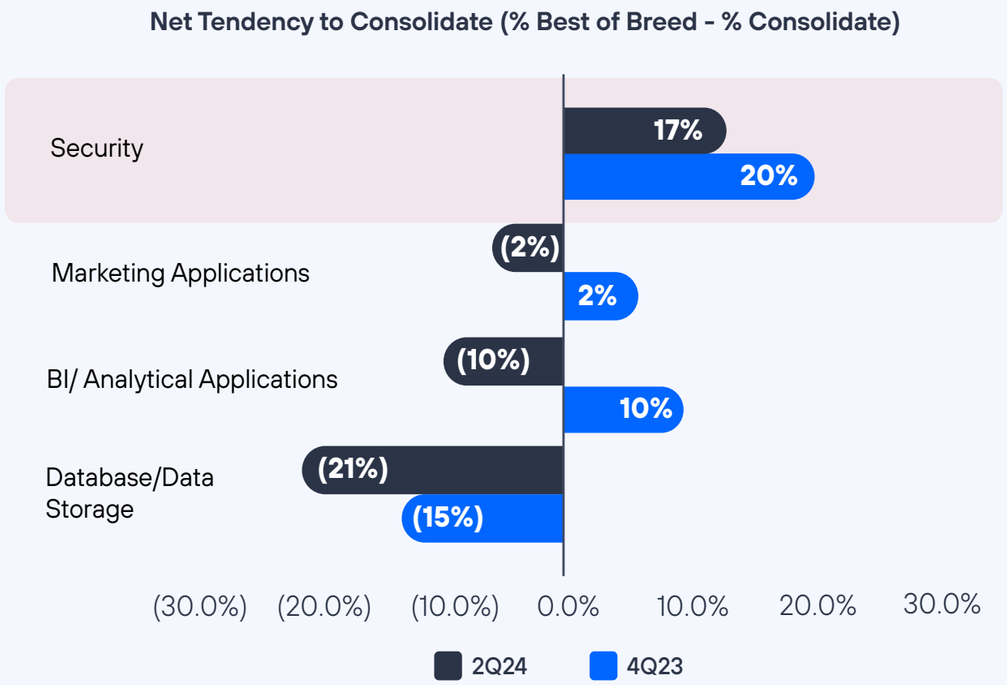


Figura 4. Fuente: *Datos del grupo AlphaWise de Morgan Stanley.*

Integrar soluciones de terceros es doblemente esencial para las compañías en sectores críticos que hacen uso de tecnología industrial, como lo son las áreas de salud, manufactura, servicios públicos, petróleo y gas, minería y entidades gubernamentales. En muchos casos ocurre que la tecnología que usan estas organizaciones para sus tareas no permite el despliegue de una solución de EDR o similar que pueda proporcionar visibilidad en la misma. Adicionalmente, los elementos de OT suelen tener vulnerabilidades que pueden ser aprovechadas por los actores maliciosos para infiltrarse en el sistema y moverse lateralmente. De acuerdo con datos de *Palo Alto Networks*, casi el 70% de las compañías industriales han recibido un ciberataque específicamente orientado a OT en 2024, y el 25% de las empresas han tenido que poner en pausa sus operaciones debido a un incidente de seguridad.

70%

de las compañías industriales han recibido un ciberataque específicamente orientado a OT en 2024

Fuente: Palo Alto Networks

25%

de las empresas han tenido que poner en pausa sus operaciones debido a un incidente de seguridad.

Fuente: Palo Alto Networks

Entre abril y agosto de 2024, dos investigadores del *Dutch Institute for Vulnerability Disclosure* (DIVD), *Wietse Boonstra y Hidde Smit*, descubrieron seis vulnerabilidades en el dispositivo *Enphase IQ Gateway,* un componente esencial de paneles solares fabricado y distribuido por la empresa *Enphase* que sirve para transformar la corriente continua producida por los paneles en corriente alterna. Las primeras tres de estas vulnerabilidades habilitaban a un atacante a conectarse y tomar el control completo del dispositivo y de cualquier otro conectado al mismo, siempre que estuvieran ambos sobre una red pública. De acuerdo con *Enphase*, que colaboró con los investigadores para la divulgación de estas vulnerabilidades, hay cerca de cuatro millones de sus sistemas desplegados en más de 150 países. Un ataque a este tipo de infraestructura puede generar consecuencias catastróficas tanto dentro de una organización como para terceros, causando daños significativos, sanciones, mayores regulaciones y una serie de impactos negativos. Por ello, **es fundamental mantener la visibilidad y controles sobre estos dispositivos, ya que resultan imprescindibles para mitigar un ataque en caso de que se explote una vulnerabilidad previamente desconocida.**

En cualquier caso, la necesidad de integración de tecnología, logs y datos de terceras partes no deberían ser un límite para una solución de XDR. **El segundo pilar de la plataforma es la integración de soluciones de ciberseguridad de terceros.** Es decir, una plataforma de XDR no debería obligar a sus usuarios a realizar una práctica de *rip and replace* de sus controles de seguridad como EDR, *firewall o cloud*. Por el contrario, por diseño, debe proveer soporte directo a todas las organizaciones que busquen unificar la gestión de múltiples soluciones ofrecidas por una gran variedad de proveedores de seguridad.

Este proceso se puede lograr de diversas formas, incluyendo:

- **La integración directa y *out-of-the-box*** de ciertas soluciones de ciberseguridad dentro de la misma plataforma de XDR, proporcionando funcionalidad inmediata con las soluciones de seguridad líderes en el mercado.
- El uso de **APIs públicas** que permiten a terceros conectarse directamente, sumado a la creación y distribución de **kits de desarrollo de *software* (SDKs)** para que los usuarios puedan crear ellos mismos sus integraciones. Esto permite a las empresas con menor madurez y presupuesto integrar cualquier control de seguridad, aprovechando sus inversiones existentes.
- La integración a través de una solución de ***security information and event management (SIEM),*** que puede ser propia o de terceros, y permite recolectar datos en tiempo real de múltiples fuentes, incluidos los registros de todo el entorno de TI.

El análisis basado en el comportamiento y las identidades que ofrece XDR se alinea con una de las grandes tendencias de la industria: **pasar de un enfoque reactivo a uno proactivo**. **Los datos sobre la identidad, así como soluciones como identity and access management (IAM) o identity threat detection and response (ITDR), son esenciales para poder dar una respuesta más rápida a los incidentes.** Debido a la popularidad de técnicas como el *phishing, el man-in-the-middle*, las brechas de datos y otros tipos de incidentes que resultan en credenciales robadas, estos ataques son cada vez más comunes. Según el reporte de IBM *X-Force Threat Intelligence Index 2024*, los ataques que se aprovechan de credenciales comprometidas han aumentado un 71% en el último año. De acuerdo con el informe *Incident Response 2024* de Unit 42 de Palo Alto Networks, el tiempo medio entre compromiso y exfiltración de datos se redujo a dos días en 2023, comparado con nueve días en años anteriores. En el 45% de los casos, los atacantes exfiltran datos en menos de un día, lo que subraya la necesidad de una respuesta rápida. Un ejemplo en relación al Black Basta *ransomware*, **supuso atacar a 10.000 endpoints en menos de 14 horas** desde el acceso inicial hasta la ejecución de *ransomware*.

> *El tiempo medio entre compromiso y exfiltración de datos se redujo a dos días en 2023*
>
> Fuente: *Informe Incident Response 2024 de Unit 42*

Al combinar la información del entorno de identidad con el análisis de comportamiento, es posible prevenir estos ataques revocando de inmediato los permisos de usuarios sospechosos. Esto puede detener de manera efectiva incidentes de seguridad que, de otro modo, serían extremadamente difíciles o incluso imposibles de detectar. Según el informe *Incident Response 2024*, un despliegue parcial o incompleto de soluciones como EDR/XDR es una causa común de éxito de los atacantes.

Para multiplicar la capacidad proactiva de un SOC, **las soluciones de XDR y SIEM deben ser capaces de integrar fuentes, datos y plataformas de *cyber threat intelligence* (CTI).** Según datos de Frost & Sullivan, el 51% de las organizaciones a nivel mundial ya cuentan con una solución de CTI, por lo que poder integrar las soluciones de terceros es esencial para este paso. El informe *Incident Response 2024 publicado por Unit 42 de Palo Alto Networks* reveló que el 20% de los incidentes son identificados por terceros (*partners* o externos). Además, en todo el mundo, y particularmente en Europa, existen iniciativas como los *information sharing and analysis centers* (ISACs), que ofrecen verdaderos tesoros en términos de información sobre amenazas, libremente compartida. **Contar con la mayor amplitud de ciber inteligencia posible permite a las organizaciones estar un paso por delante de los actores maliciosos y las amenazas**, ya que incrementa la capacidad de predicción frente a los ataques modernos y presenta oportunidades para modificar la postura de seguridad, así como para preparar detecciones, configuraciones y acciones automatizadas antes de que el ataque ocurra.

Gracias a esta integración total, los analistas de un SOC moderno tendrán toda la información a su disposición para resolver los incidentes de seguridad de la mejor manera posible, encontrando la causa raíz de cada intrusión y mitigando efectivamente el daño de estos ataques**. Sin embargo, el volumen de alertas sigue siendo excesivo, especialmente cuando la visibilidad aumenta de manera exponencial. Por ello, es fundamental un componente clave para potenciar aún más a los analistas: la automatización.**

↑71%

de ataques que se aprovechan de credenciales comprometidas en el último año

Fuente: *Informe X-Force Threat Intelligence Index 2024 IBM*

45%

de los casos, los atacantes exfiltran datos en menos de un día

Fuente: Informe Incident Response 2024 de Unit 42

20%

de los incidentes son identificados por terceros (partners o externos)

Fuente: Informe Incident Response 2024 de Unit 42

05
Evolución Inteligente: *SOCs impulsados por la IA*

El tercer pilar de XDR es la automatización de las tareas y procesos para aliviar la carga de los analistas. Para que un SOC funcione eficazmente en el contexto actual, caracterizado por amenazas numerosas y sofisticadas, así como por la escasez de talento, es esencial aprovechar al máximo las distintas formas de automatización.

El CISO de una empresa de más de mil empleados del sector servicios, entrevistado por Frost & Sullivan, declaró que **las capacidades de automatización de la plataforma de XDR le permitían multiplicar por 4 el valor de su equipo de ciberseguridad**, reduciendo la carga laboral de los analistas y eliminando la necesidad de contratar personal adicional tras la expansión regional de la organización.

Por otra parte, la integración de la IA y los *large language models* (LLMs, modelos de lenguaje grandes) está revolucionando los SOCs, ofreciendo soluciones innovadoras para automatizar la gestión de alertas, enriquecer el análisis de amenazas, reducir costes y optimizar los tiempos de respuesta. Según el informe de Ciberseguridad 2025 de Morgan Stanley, se estima que entre el 20% y el 40% de las tareas de analistas de seguridad pueden ser automatizadas con IA generativa, incluyendo procesos como la monitorización de los registros, el análisis de alertas y la gestión de parches.

20%-40%

de las tareas de analistas de seguridad pueden ser automatizadas con IA generativa

Fuente: Informe de Ciberseguridad 2025 de Morgan Stanley

La integración de la IA dentro de un SOC permite resolver los desafíos actuales a los que se enfrentan las organizaciones y ofrecer una respuesta a la presión constante para reducir el tiempo de detección (MTTD) y el tiempo de respuesta (MTTR) a las amenazas. Según el informe Incident Response 2024 publicado por Unit 42, la IA es capaz de reducir el tiempo medio de detección a 10 segundos y el tiempo medio de respuesta a 1 minuto, mejorando la eficiencia y rapidez en la gestión de incidentes.

> *"La IA permite reducir el tiempo medio de detección a **10 segundos** y el tiempo medio de respuesta a **1 minuto**"*

Fuente: *Informe Incident Response 2024 de Unit 42*

La transformación con IA y LLMs representa una solución innovadora para optimizar la seguridad en los SOCs. La automatización de la gestión de alertas reduce la carga de trabajo repetitiva, mientras que el enriquecimiento de los datos de amenazas mejora la calidad de la información para una detección más precisa. Los LLMs pueden resumir y analizar las múltiples fuentes de ciberinteligencia, complementándose con la correlación automatizada de datos del ecosistema para mejorar la eficacia operativa del SOC y proporcionar respuestas más rápidas y eficientes a los incidentes.

El ecosistema del mercado SOC enfrenta desafíos tanto de demanda como de oferta. Las soluciones de ***security orchestration automation and response (SOAR)*** de próxima generación, que integran LLMs, **están mejorando la facilidad de uso y ofreciendo una combinación de automatización y análisis avanzado.**

La arquitectura del SOC del futuro se basa en tres capas fundamentales:

1. **Ingesta y procesamiento de datos:** recopila información de múltiples fuentes como *endpoints*, redes, identidad, *email* y nube, procesándola y combinándola con inteligencia de amenazas.
2. **Almacenamiento y detección:** utiliza SIEM, XDR y plataformas en la nube para almacenar y analizar datos, permitiendo una detección avanzada de amenazas.
3. **Respuesta y automatización con IA:** incorpora SOAR y análisis avanzado basado en IA, combinando inteligencia artificial con intervención humana para agilizar la respuesta ante incidentes y optimizar la ciberseguridad operativa.

Los principales proveedores, como Palo Alto Networks, **han evolucionado sus soluciones EDR/XDR tradicionales hacia plataformas con *copilots* de seguridad habilitados por IA.** Estas herramientas no solo permiten correlacionar alertas y priorizar investigaciones automáticamente, sino que también generan informes detallados y análisis de código para identificar amenazas en tiempo real.

Un ejemplo destacado es **Cortex XSIAM de Palo Alto Networks,** que combina inteligencia avanzada en *endpoints* con capacidades de orquestación y respuesta automatizada, aprovechando grandes volúmenes de telemetría. Esta plataforma ayuda a los analistas de seguridad a optimizar su trabajo, reducir los tiempos de respuesta y tomar decisiones informadas, respaldadas por análisis avanzados y modelos de IA de última generación.

06

Del futuro al presente: La evolución del SOC con *Telefónica Tech y Palo Alto Networks*

Ante la creciente complejidad del panorama de amenazas y los desafíos que enfrentan los responsables de ciberseguridad, Telefónica Tech y Palo Alto Networks han unido fuerzas para construir el SOC del futuro, basado en visibilidad, ciberinteligencia, inteligencia artificial, proactividad y experiencia.

Como partner tecnológico en esta asociación, Palo Alto Networks aporta su portafolio de soluciones, con Cortex XSIAM como la base del SOC moderno. Esta plataforma unificada integra capacidades de XDR (con EDR integrado), SOAR y SIEM, simplificando significativamente la gestión del SOC y ofreciendo:

Visibilidad, detección y respuesta en todo el ecosistema: Es capaz de ingerir y correlacionar datos de múltiples controles de seguridad de Palo Alto Networks, incluyendo EDR, firewalls, Prisma Access, Prisma Cloud y Zero Trust Network Access, entre otros. Esto le permite identificar y responder a incidentes en cualquier punto del ecosistema.

Integración de soluciones de terceros: Las capacidades SIEM de la plataforma permiten recopilar y procesar datos y logs de terceros. Su integración con más de 750 herramientas de seguridad amplía la visibilidad en infraestructuras complejas, incluidos dispositivos OT e IoT, proporcionando flexibilidad y seguridad holística.

Automatización y uso de IA: La plataforma correlaciona, normaliza y categoriza la información de los controles de seguridad para reducir los falsos positivos. Mediante IA y modelos de ML identifica incidentes de seguridad reales y, con su capacidad de SOAR, automatiza la respuesta, agilizando la mitigación de amenazas de manera eficiente. Su IA evoluciona continuamente al entrenarse con datos de miles de ecosistemas de clientes, lo que permite generar recomendaciones de automatización y eficientizar aún más la labor del SOC.

Además, emplea análisis de comportamiento para identificar actores maliciosos. La solución establece primero una línea base del comportamiento del usuario, creando un perfil que recoge patrones y actividades típicas a partir de *logs*, autenticación y actividad en *endpoints*, redes y entornos en la nube. Al comparar este estándar de comportamiento con la actividad del usuario en todo momento, es capaz de **detectar desviaciones que puedan indicar conductas maliciosas,** respondiendo a ataques como exfiltraciones de datos, movimientos laterales y el uso de credenciales comprometidas. Este enfoque proactivo refuerza la **resiliencia del SOC**, permitiendo la prevención temprana y evitando el alto coste de gestionar incidentes de seguridad complejos.

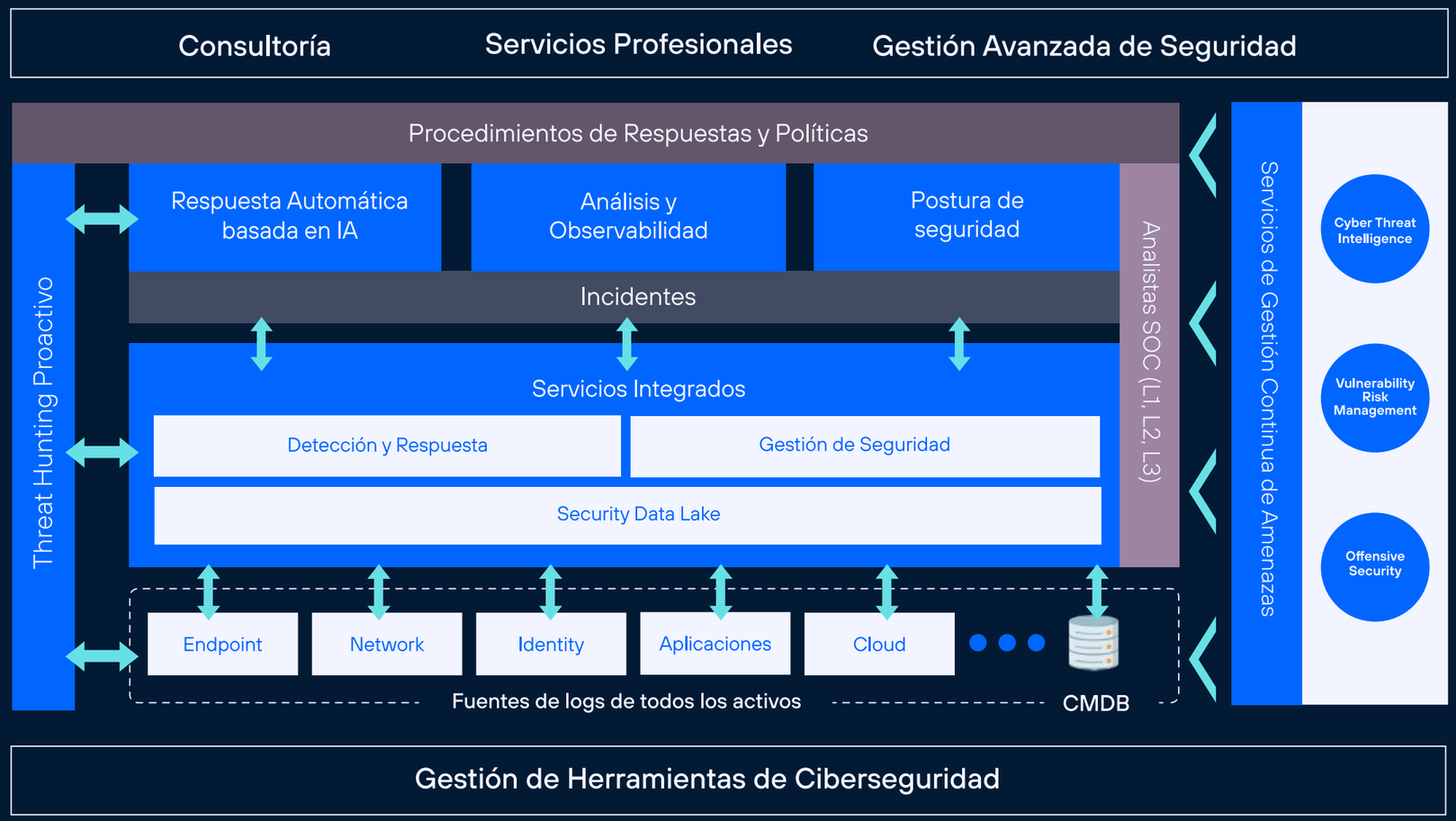
Telefónica Tech, por su parte, cuenta con NextDefense SOC, el primer centro de operaciones de seguridad diseñado para aprovechar al máximo la tecnología de Palo Alto Networks, incluyendo Cortex XSIAM, Prisma Cloud y Prisma SASE.

- NextDefense actúa como el eslabón clave en la gestión de ciberseguridad, ofreciendo una variedad de servicios que **potencian el valor de la tecnología de Palo Alto Networks**. Entre sus capacidades destacan la monitorización y gestión continua, la integración de fuentes de datos y ciberinteligencia de terceros, la detección y respuesta en múltiples entornos, *threat hunting*, así como servicios profesionales y de consultoría especializados.

- La efectividad de un SOC del futuro depende de una mejora continua basada en mediciones, pruebas y la implementación de nuevas estrategias de ciberseguridad. Telefónica Tech ofrece un **abanico completo de servicios que permiten identificar puntos débiles en la postura de seguridad de una organización**, permitiendo hacer una gestión integral del ecosistema, vulnerabilidades, riesgos y exposiciones, al tiempo que optimiza la visibilidad del entorno. Como uno de los mayores proveedores de servicios en Europa, aporta su amplio conocimiento en seguridad aplicado a diversas industrias y sectores. Además, su experiencia en la resolución de decenas de miles de incidentes para numerosos clientes **proporciona una valiosa capa de información para la toma de decisiones dentro del SOC.**

- Telefónica Tech impulsa la **modernización del SOC mediante la aceleración de la adopción de IA y la automatización.** Ofrece actualizaciones continuas de playbooks adaptadas a cada industria y basadas en las mejores prácticas de sus clientes. Sus servicios de evaluación de postura de seguridad ayudan a los responsables de ciberseguridad a definir estrategias de automatización alineadas con el riesgo, la criticidad, las vulnerabilidades y las prioridades del negocio, facilitando una evolución estructurada y efectiva del SOC.

NextDefense SOC de Telefónica Tech



El enfoque de Telefónica Tech en la gestión del SOC del futuro facilita la transformación a los responsables de seguridad, combinando seguridad gestionada, consultoría y servicios profesionales. Apoyándose en la tecnología de Palo Alto Networks y una estrategia conjunta, Telefónica Tech aborda los desafíos más críticos de la ciberseguridad, proporcionando una protección holística capaz de mitigar las amenazas más sofisticadas.

07

Conclusión: Transformando el SOC hacia una unidad *moderna, resiliente y proactiva*

A lo largo de este recorrido, hemos analizado los pasos que debe seguir un responsable de ciberseguridad para impulsar la evolución del SOC en una organización.

Los responsables de seguridad deben establecer, en primer lugar, visibilidad con soluciones como **EDR**. Luego, expandirla en todo el ecosistema, incorporando fuentes de datos externas a través del despliegue de **XDR** y soluciones como **SIEM.** El proceso entero debe estar impulsado por herramientas donde la **IA**, algoritmos de **ML** y asistentes de **GenAI** minimicen los procesos manuales, agilicen la respuesta a amenazas y disminuyan el tiempo de detección y respuesta. Finalmente, el SOC moderno debe apoyarse en la inclusión de **datos de identidades, el análisis de comportamiento** de usuarios y dispositivos y en la **ciberinteligencia** para reforzar la prevención de amenazas.

Para evolucionar su SOC, los responsables de seguridad deben apoyarse en dos tipos de socios: **socios tecnológicos**, que provean las soluciones avanzadas como base de la arquitectura del SOC, y **proveedores de servicios de seguridad,** que impulsen la transformación mediante buenas prácticas, evaluaciones, procesos optimizados y conocimiento estratégico, aportando la experiencia necesaria para adaptar el SOC a un entorno de amenazas en constante evolución.

La propuesta conjunta de Telefónica Tech y Palo Alto Networks ofrece a los responsables de ciberseguridad un camino para revolucionar el SOC con la ayuda de la IA.

Telefónica Tech, a través de NextDefense, lidera la evolución del SOC del futuro, ofreciendo una seguridad avanzada y proactiva que permite a las organizaciones fortalecer su resiliencia ante un panorama de amenazas en constante evolución. Como parte esencial de esta propuesta, Cortex XSIAM de Palo Alto Networks amplía la visibilidad en todo el ecosistema al ingerir, enriquecer y correlacionar datos de múltiples controles de seguridad, garantizando un enfoque holístico. Gracias a la integración de inteligencia artificial y *machine learning* (ML), reduce falsos positivos, automatiza la resolución de incidentes y optimiza los tiempos de respuesta, minimizando la carga operativa y los costes de seguridad.

NextDefense es el único SOC que integra completamente esta tecnología, combinándola con la experiencia y el conocimiento de sus analistas para identificar superficies de riesgo, detectar amenazas avanzadas y responder con rapidez y precisión. A través de servicios como *threat hunting*, gestión de vulnerabilidades y ciberinteligencia, Telefónica Tech cierra el círculo de retroalimentación continua que impulsa una seguridad más robusta y predictiva. Finalmente, mediante evaluaciones de postura de seguridad, ayuda a los responsables de ciberseguridad a definir su estrategia de automatización e inteligencia artificial de acuerdo con sus riesgos específicos.

Con alianzas estratégicas y tecnología de vanguardia, el SOC moderno de Telefónica Tech se posiciona como la solución definitiva para afrontar amenazas sofisticadas, adaptarse a la complejidad del ecosistema digital y superar la escasez de talento especializado.

Acerca de Telefónica Tech:

Telefónica Tech es un integrador de tecnología global, líder en transformación digital. La compañía cuenta con una amplia oferta de servicios y soluciones tecnológicas integradas de Ciberseguridad, Cloud, IoT, Big Data o Inteligencia Artificial. En todas estas verticales, contamos tanto con nuestras propias tecnologías como también con los mejores ecosistemas de partners estratégicos y así nos lo reconocen tanto los analistas de la industria como nuestros clientes. Y todo ello es posible también gracias a nuestros hubs en España, UK, Alemania, Brasil e Hispam llegamos a más de 5,5 millones de clientes en más de 175 países.

Acerca de Palo Alto:

Palo Alto Networks es reconocida por analistas de la industria y miles de clientes como un líder global en ciberseguridad. Con plataformas de vanguardia, inteligencia de amenazas de primer nivel y profesionales altamente capacitados en seguridad, Palo Alto Networks ayuda a las empresas de todo el mundo a protegerse en un entorno en constante cambio. Cada día, el SOC de Palo Alto Networks, que utiliza Cortex XSIAM®, procesa 75 terabytes de datos, detecta un promedio de 133 incidentes, resuelve el 100% de ellos de forma automatizada y alcanza un MTTR (Tiempo Medio de Resolución) de 1 minuto.Cortex XSIAM ha sido reconocido como líder y destacado en el GigaOm Radar 2023 para Centros de Operaciones de Seguridad Autónomos.

Acerca de Frost & Sullivan:

Frost & Sullivan, la empresa especializada en crecimiento estratégico, ayuda a sus clientes a acelerar su crecimiento y alcanzar posiciones de excelencia en crecimiento, innovación y liderazgo. Su servicio Growth Pipeline as a Service proporciona al CEO y a su equipo de crecimiento estrategias transformadoras y modelos de mejores prácticas para impulsar la generación, evaluación e implementación de iniciativas de crecimiento de alto impacto. Frost & Sullivan cuenta con más de 60 años de experiencia colaborando con empresas del Global 1000, negocios emergentes y la comunidad de inversión, operando desde más de 40 oficinas en seis continentes.

Si tienes alguna duda y quieres saber más sobre cómo podemos ayudarte, por favor:

→ **CONTÁCTANOS**

Telefónica Tech

paloalto NETWORKS

FROST & SULLIVAN