DEBATES ciberseguridad TIC

Detección y respuesta sin descanso: cuando el reto no es solo ver, sino decidir a tiempo

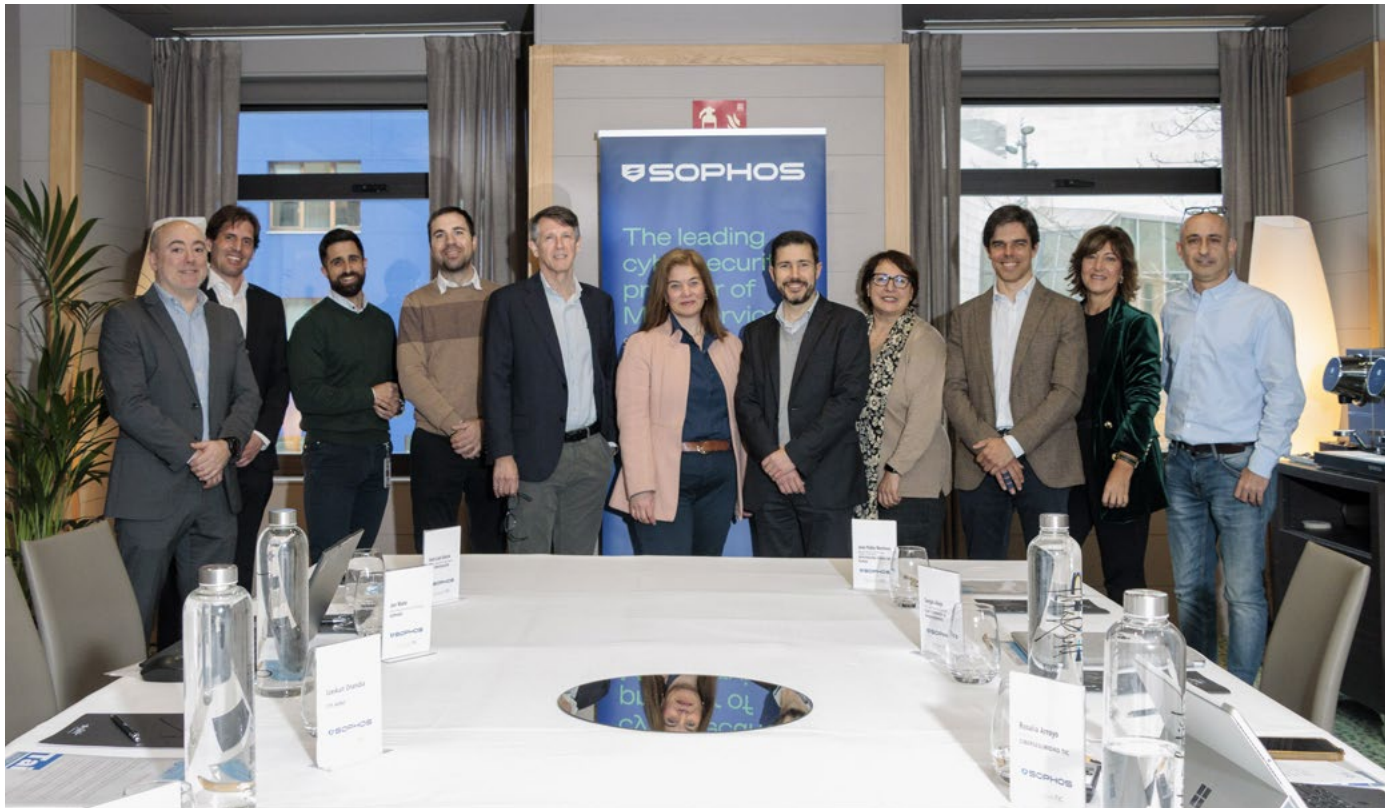
SOPHOS

IR A PÁGINA SIGUIENTE

Detección y respuesta sin descanso: cuando el reto no es solo ver, sino decidir a tiempo

La detección y respuesta ante incidentes se ha convertido en uno de los grandes puntos de fricción de la ciberseguridad actual. En un momento en el que las organizaciones acumulan más herramientas, más superficie de ataque y más presión regulatoria, el problema ya no es únicamente identificar una amenaza, sino saber interpretarla, priorizarla y actuar con rapidez sin poner en riesgo el negocio.

Rosalía Arroyo



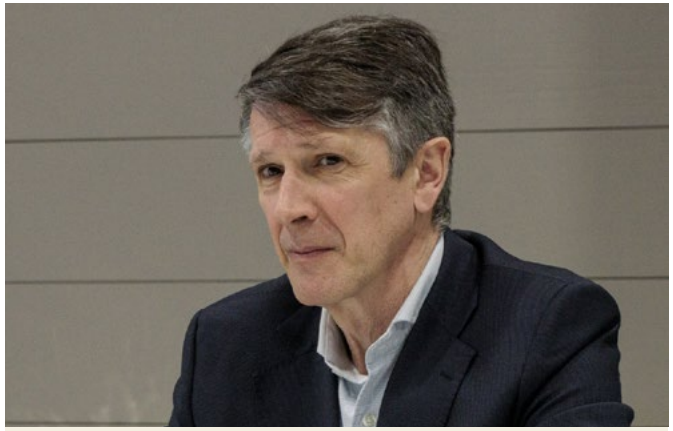
Ese fue el punto de partida del almuerzo celebrado en Bilbao por Ciberseguridad TIC con el patrocinio de Sophos, centrado en el papel de los servicios de detección y respuesta gestionada (MDR). A lo largo de la conversación, responsables de IT y ciberseguridad de organizaciones industriales, sanitarias y del ámbito público compartieron una preocupación común: la dificultad de mantener visibilidad, contexto y capacidad de respuesta en entornos cada vez más complejos. A partir de ahí, el debate fue dibujando un mapa muy realista de las tensiones

que atraviesan hoy los equipos de seguridad: la falta de recursos, el exceso de alertas, la dependencia del conocimiento interno, la presión del 24/7 y la necesidad de apoyarse en terceros sin perder el control.

La conversación arrancó con una preocupación compartida por todos los asistentes: cómo gestionar la detección y respuesta ante incidentes en entornos cada vez más complejos, con más superficie de ataque, más dependencia tecnológica y recursos internos que casi nunca crecen al mismo ritmo que las amenazas.

Desde Betapack, José Luis Corona, IT manager de la compañía, describió un entorno exigente, marcado por la convivencia entre IT y OT en una planta muy automatizada. “La visibilidad la tenemos”, explicaba, apuntando a que, en su caso, el reto no está tanto en la visibilidad como en la operativa diaria, todavía muy apoyada en una sola persona. Esta situación, admitía, puede introducir cierta dependencia y añade complejidad a la hora de trasladar necesidades de recursos a la dirección.

José Díaz Alegre, responsable de ciberseguridad de BilbaoPort, puso el foco en un elemento clave: el contexto. Tras años trabajando con servicios de SOC, señalaba que su principal preocupación no es la cantidad de alertas, sino la capacidad de interpretarlas correctamente. “Puedes tener muchísimos eventos… pero si no hay contexto, la respuesta no va a ser buena”, advertía. Este reto se complica cuando ese conocimiento debe trasladarse a un proveedor externo. “Transmitirles esa parte de contexto es complicado”, reconocía, especialmente en entornos de contratación pública donde los servicios son limitados en el tiempo. Por eso, defendía reforzar el conocimiento y el criterio interno, porque “los fabricantes cambian, pero mis necesidades de ciberseguridad van a seguir ahí”.



> “El valor del MDR está en quitar esa dependencia del 24/7 interno, porque si al final todo sigue pasando por la misma persona, el problema no cambia”

José Luis Corona,
IT Manager, **Betapack**

Andoni Jiménez, de ZIV Aplicaciones y Tecnología, reforzó esa idea desde el ángulo del ruido operativo. En su experiencia, el problema no es la falta de alertas, sino su ambigüedad: “muchas veces tienes que analizar si la alerta corresponde a una actividad real del negocio o si se trata de un incidente que requiere actuación”. Esa incertidumbre obliga a invertir tiempo y esfuerzo en discriminar qué merece realmente atención. Como él mismo apuntaba, “no es un proceso lineal, es una iteración”. Al final, todo remite al equilibrio entre protección, agilidad y apetito de riesgo. “Si tienes demasiados avisos, ¿cuál crees que es el bueno?”, se preguntaba, poniendo sobre la mesa el riesgo de normalizar el ruido.

El problema ya no es solo detectar un ataque, sino interpretarlo con contexto y decidir a tiempo, porque el volumen de alertas y la complejidad del entorno hacen que no todo sea evidente

Desde una perspectiva distinta, Sergio Alejo, de CAF Turnkey and Engineering, trasladó el problema al terreno de los grandes proyectos industriales. En su caso, la principal dificultad no está tanto en operar un SOC como en definirlo correctamente. “No existen los requisitos para construirlo”, recordaba, refiriéndose a proyectos donde el cliente exige un SOC 24/7 pero no concreta qué debe hacer ni cómo debe funcionar. Sin esa definición, explicaba, solo quedan dos opciones: quedarse corto o irse a máximos. Ambas igual de malas. Para evitarlo, CAF está optando por adelantarse y definir sus propios casos de uso. No tanto por exigencia del cliente como por necesidad interna: “lo hacemos por nuestro propio bien”, aunque eso implique asumir el riesgo de “mojarse” en decisiones que otros prefieren no concretar.

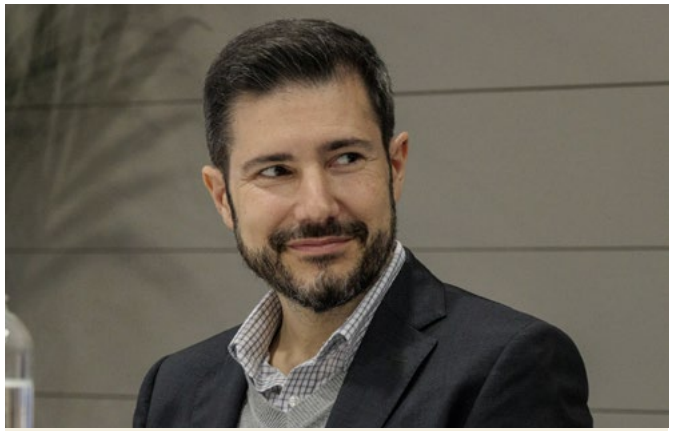
La intervención de Juan Pablo Martínez, Jefe de Servicio de Estrategia Digital e Informática de la Diputación Foral de Álava, desplazó el debate hacia la gobernanza. Al frente de un equipo muy pequeño —“estamos tres personas, tres técnicos”—, con apoyo técnico de una sociedad pública, contaba que están inmersos en la adecuación al ENS, NIS2 y la normativa de protección de datos. En ese proceso, una de las lecciones más claras ha sido que la ciberseguridad “no tiene mucha visibilidad en los consejos de gobierno, consejos de administración”, reconocía. Para corregirlo, han adoptado un enfoque intensivo y sistemático: presentar cada mes ante el Consejo de Administración de la Sociedad Pública una diapositiva con “todos los ataques y todos los intentos de ataque que hemos tenido durante el mes”. Además, están combinando formación, simulacros y pedagogía interna, también con perfiles políticos, convencidos de que la concienciación no puede quedarse solo en el área técnica. Sus dos grandes preocupaciones están muy claras: por un lado, “los

“Para nosotros, el MDR tiene que incluir capacidad real de actuación; si al final mi equipo sigue pendiente del teléfono, no resuelve el problema”

Iratxe Ijalbe,
Directora de Sistemas de Información y Seguridad, **Mutualia**

posibles ataques un viernes a la tarde", cuando la capacidad de reacción baja; por otro, esos "patrones camuflados" que permiten que alguien "poco a poco te vaya filtrando información" sin que el incidente aflore de inmediato.

Desde IMQ Prevención, Juan Luis García, director de sistemas de información, aportó una visión muy ligada al valor y la sensibilidad del dato. Su organización maneja información médica y de prevención de riesgos laborales, por lo que cualquier incidente puede tener un impacto elevado. Aunque cuentan con ISO 27001 y avanzan hacia el ENS, destacaba la importancia del apoyo de proveedores externos: "nos apoyamos en los proveedores y en la sabiduría", ya que combinan el conocimiento interno con una visión más amplia de ataques y protocolos. Su principal preocupación no es tanto la autoría del incidente como su alcance: "determinar y acotar bien qué sistemas se han visto involucrados". Si la organización se queda solo con "la punta del iceberg", la respuesta puede ser incompleta. Por eso insistía en una detección "fina", capaz de aclarar "qué es exactamente lo que se ha visto afectado, ya sea información



"Un MDR solo aporta valor si incorpora contexto; puedes tener muchos eventos, pero sin ese conocimiento la respuesta no va a ser buena"

José Díaz Alegre,
responsable de ciberseguridad, **Bilbao Port**

comprometida o sistemas bloqueados" antes de actuar.

Izaskun Onandia, Director Security & Information Compliance de ITP Aero, situó como principal inquietud la evolución del ataque impulsado por inteligencia artificial. En una compañía global con seguridad unificada, explicaba que este modelo centralizado es "para bien y para mal": aporta coherencia, pero también concentra la responsabilidad, que abarca seguridad física, del dato y gobernanza de la IA. "Me preocupa la inteligencia artificial", señalaba, en referencia a su uso por parte de los atacantes. Le inquieta especialmente la velocidad y capacidad de adaptación: "la propia inteligencia artificial es capaz de mutar y que el ataque mute". Incluso con múltiples herramientas, considera que no siempre están preparadas para ese nivel de sofisticación y que la última barrera sigue siendo humana.

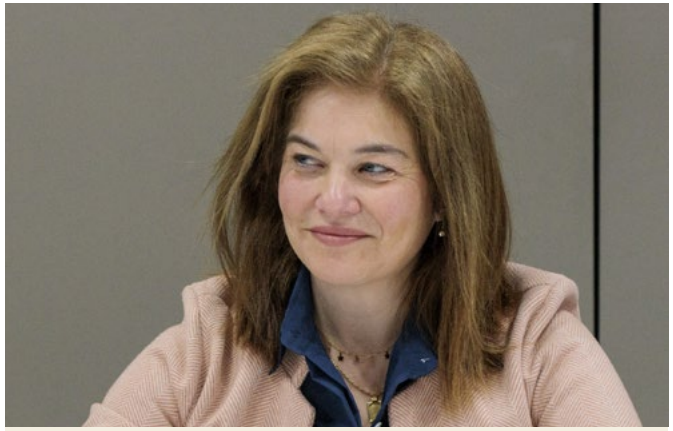
Aun así, describía una estructura consolidada, con SIEM propio y un SOC parcialmente externalizado. Aunque el equipo no es grande, la centralización les permite detectar patrones y anticiparse mejor, especialmente en un entorno expuesto. También defendía integrar la gobernanza de la IA dentro de la ciberseguridad, porque limitar el problema al dato personal "se queda corto".

Esta preocupación fue recogida por varios asis-

tentes. Desde Betapack, José Luis Corona explicaba cómo han optado por reforzar el control sobre el uso de aplicaciones conectadas a IA, combinando medidas técnicas con un modelo de gobernanza que permite identificar qué herramientas utilizan estos servicios y qué prácticas son aceptables. La conclusión es que el riesgo ya no se limita a herramientas concretas, sino que se extiende a "un montón de aplicaciones que conectan con sistemas de inteligencia artificial", a lo que se suma "lo de la agentica".

En esa línea, Andoni Jiménez planteó un enfoque centrado en el control del dato, basado en políticas de clasificación y herramientas de etiquetado para evitar fugas de información. Eso sí, advertía de que alcanzar ese nivel de madurez "requiere de un proceso de meses de trabajo" y una alta implicación del usuario.

La intervención de Iratxe Ijalbe, de Mutualia, fue probablemente una de las más crudas y completas del bloque. "Me preocupan muchas cosas", arrancó. Su organización maneja dato médico, cuenta con ISO 27001 desde hace siete años y ENS medio desde hace cuatro, además de auditorías continuas y ejercicios de ethical



"El MDR puede ser una pieza importante, pero tiene que estar preparado para escenarios donde los ataques evolucionan con inteligencia artificial"

Izaskun Onandia, Director Security & Information Compliance, **ITP Aero**

hacking. A su juicio, la normativa ayuda a consolidar medidas y a interiorizar procedimientos. Pero su principal preocupación no es el ataque visible, sino el que pasa desapercibido durante meses. "Me preocupa que haya un bicho que se detecte tarde", confesaba, pensando en intrusiones que "llevaba meses ahí metido y nadie se ha enterado". A partir de ahí, explicaba, se desencadena todo lo demás: backups comprometidos, dudas sobre la inmutabilidad de las copias, recuperación incierta, filtración de información e impacto reputacional. "Me preocupa todo eso", resumía.

A esta presión se suma la económica. Mantener la ciberseguridad, con todas sus capas, se ha convertido en "un shock" presupuestario, a lo que se añade la creciente complejidad del ciberseguro, cada vez más caro y difícil de contratar.

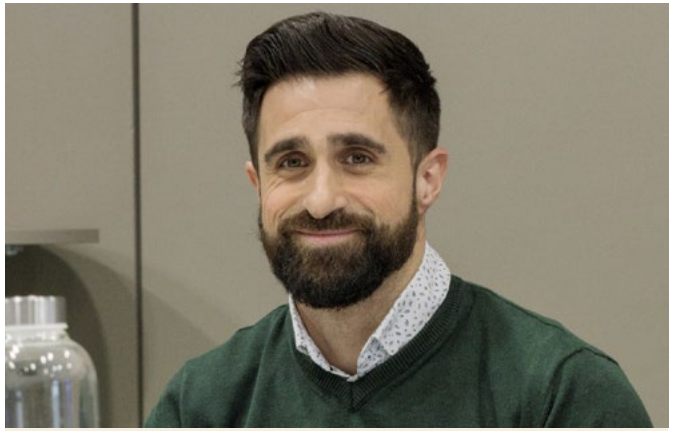
La respuesta

Cuando llegó el turno de Sophos, la conversación giró desde las preocupaciones de los clientes hacia la forma en que el fabricante interpreta ese escenario. Jon Nieto, senior account manager de la compañía, recogió varias de las ideas que habían ido apareciendo, empezando por una que consideró central: el contexto. "Es un tema crítico", defendía, y precisamente por eso insistía en que la respuesta no puede construirse solo desde la herramien-

ta, sino escuchando a quien conoce el entorno. “Sois los que conocéis realmente vuestro día a día, vuestro entorno y cómo evoluciona”, decía, subrayando que una parte clave del trabajo del proveedor consiste en entender esa realidad y adaptarse a ella.

Nieto enmarcó además la evolución de Sophos en ese cambio de demanda. Recordó que muchos clientes les identificaban históricamente con productos concretos —endpoint, firewall y otras capas—, pero admitió que eso ya no basta. “Hay unas partes ahí que se quedan fuera de la pura tecnología”, reconocía, porque el problema ya no es solo disponer de herramientas, sino cubrir también la parte de personas, operación y servicio. En ese terreno siguen siendo claves la concienciación, la formación y el apoyo de la dirección, algo que las normativas ayudan a impulsar.

A partir de ahí, vinculó esa transformación con la presión creciente sobre los recursos. Cada vez hay “más capas”, los presupuestos suben y “parece que hace falta más para todo”, resumía. La propuesta de Sophos pasa por ayudar en la operación diaria de la ciberseguridad, aportando no solo tecnología, sino también servicio y capacidad de respuesta. Ahí destacó dos elementos: por un lado, la visión global que les da operar con clientes de distintos sectores y geografías —“vemos lo que ocurre en otros lados del mundo”— y, por otro, la necesidad de adaptar el servicio a realidades muy diferentes, desde IT hasta OT o producción, definiendo con cada cliente “si en caso de un ataque podemos actuar directamente sobre este tipo de entornos, sí o no”. La compra de Secureworks, añadía, refuerza precisamente esa evolución hacia los servicios de operación y detección y respuesta.



> “Si ya tienes un SOC, el MDR tiene que aportar algo más, porque el presupuesto es limitado y hay que justificar muy bien cada capa adicional”
>
> **Andoni Jiménez,**
> head of **IT ZIV Aplicaciones y Tecnología**

La intervención de Álvaro Fernández, sales manager de Sophos, llevó después ese discurso a un plano más concreto. Lo primero que hizo fue cuestionar la ambigüedad del término SOC. A su juicio, “un SOC puede ser muchas cosas”, porque bajo esa etiqueta conviven servicios muy distintos: desde soporte operativo o gestión de reglas hasta capacidades más amplias de detección y respuesta. Por eso sospechaba que muchos de los asistentes no estaban trabajando todavía con un MDR “como tal”, sino con servicios de SOC más o menos extendidos.

Su planteamiento del MDR fue el de un servicio flexible, no reservado a organizaciones muy maduras. Para algunos clientes, explicaba, es “su todo”, su primera barrera real porque no tienen

"El reto no es solo tener un MDR, sino definir bien qué debe hacer y cómo encaja en el modelo operativo, algo que muchas veces no está claro"

Sergio Alejo, OT Cybersecurity Manager, **CAF Turnkey and Engineeringz**

equipo interno de ciberseguridad. Para otros es "una línea más", complementaria al SOC tradicional. En ambos casos, defendía que un MDR bien desplegado puede abordar muchas de las preocupaciones expresadas en la mesa porque

Cada vez preocupa más el ataque que no se ve: amenazas que permanecen meses dentro de la organización, avanzando poco a poco sin levantar señales claras

no se limita a avisar, sino que actúa según lo pactado. "Va a poder tomar acción o te va a poder mandar un correo, una llamada... lo que se acuerde", explicaba, incluyendo incluso la posibilidad de actuar si no hay respuesta en un plazo definido: "tomamos nosotros la acción".

Eso provocó una reacción inmediata de José Díaz Alegre, que verbalizó una diferencia fundamental entre avisar y responder. Ya había visto modelos donde el proveedor solo notificaba al cliente, y fue tajante: "yo te pido que me respondas ante mi seguridad, quiero que puedas actuar, no que simplemente me recomiendes". A partir de ahí, Álvaro Fernández detalló las dos modalidades de respuesta que manejan: una más centrada en la contención, y otra más avanzada de respuesta ante incidentes, con determinadas acciones ejecutables directamente y otras que requieren apoyo del cliente o del partner.

Esa explicación conectó enseguida con la intervención de Iratxe Ijalbe, que volvió a llevar el debate al terreno práctico. Para ella, esa capacidad de actuación "tiene que estar incluido", porque una de las razones de acudir a este tipo de servicios es precisamente evitar que el equipo interno siga viviendo en guardia permanente. Si el resultado final es que su gente tenga que seguir pendiente del teléfono, el problema no se resuelve. "Al final tengo a la gente atendiendo también el teléfono", concluía. De ahí que, en su opinión, un servicio útil de verdad tenga que ser gestionado de verdad.

¿Qué le pides a un servicio MDR?

A partir de ahí, la pregunta sobre qué le pedirían a un MDR hizo que la conversación bajara aún más a la realidad operativa. José Luis Corona lo resumía con una formulación muy directa:

espera que el servicio haga “lo que tú quieres o lo que has decidido en tus escenarios que tienes que hacer”, sin obligar al cliente a intervenir permanentemente. En una empresa industrial, eso exige algo más que monitorización: exige conocer la infraestructura, haber pactado los escenarios de antemano y entender el impacto de cada decisión en el negocio.

Andoni Jiménez recogía esa idea, pero la llevaba a una duda práctica: dónde está la frontera entre un SOC gestionado y un MDR. Si ya tiene un SOC con capacidad de operación y playbooks definidos, añadir otra capa como el MDR puede ser útil, pero hay que justificarlo bien. “El presupuesto es limitado”, recordaba. Aun así, veía el MDR como una forma de “vitaminar” lo que ya existe, siempre que haya una coordinación clara y se entienda quién actúa como primera línea.

Sergio Alejo llevó esa misma duda a un plano aún más técnico. Desde la perspectiva de quien diseña estas soluciones en proyectos complejos, su preocupación no era solo el coste, sino la sencillez de gestión. Si ya dispone de un SOC con capacidades de detección y respuesta,

> “El MDR puede reforzar capacidades, pero no sustituye la necesidad de concienciación y apoyo desde los niveles de decisión”
>
> **Juan Pablo Martínez,** Jefe de Servicio de Estrategia Digital e Informática, **Diputación Foral de Álava**

cuestionaba qué aporta realmente dividir esas funciones entre dos actores. “¿Qué me aporta a mí meter a dos actores para la misma funcionalidad?”, planteaba, apuntando al incremento de complejidad y al reparto de responsabilidades.

Álvaro Fernández devolvió la discusión al terreno de los resultados. A su juicio, la clave está en qué KPI tiene hoy la organización y qué necesita mejorar. Si el SOC ya responde adecuadamente, quizá no sea necesario añadir más capas. Pero si se requiere investigar alertas “en cuestión de minutos” o ejecutar acciones sobre equipos y usuarios, el MDR puede cubrir “un caso de uso que no tenéis ahora mismo”.

En ese intercambio también se abordó el alcance del MDR dentro de los modelos actuales de operación. Álvaro Fernández subrayó que “al final el MDR es el servicio”, explicando que integra ingesta de telemetría, normalización, correlación, casos de uso y respuesta. Jon reforzó esta idea al señalar que “el servicio es completo, es detección y respuesta”, especialmente orientado a aquellas áreas más difíciles de cubrir con recursos internos.

A partir de ahí, Sergio Alejo reformuló su planteamiento: más que una tecnología adicional, lo que valoraba era el expertise en el diseño de la solución, es decir, la capacidad de revisar el inventario de activos y definir “qué y cómo incluye el MDR” en función del contexto y la industria.

José Díaz Alegre volvió entonces sobre otro de los grandes problemas del mercado: que sigue sin estar claro qué es exactamente un SOC. Después de "12 años" trabajando con este tipo de servicios y haber visto pasar "más de 32 proveedores", reconocía que cada uno se lo había vendido de una forma distinta: "hay gente que te lo vende como MDR, otro como SOC". Por eso seguía con interés la nueva certificación CCN-STIC 896, que podría ayudar a acotar mejor qué capacidades mínimas debe tener un SOC.

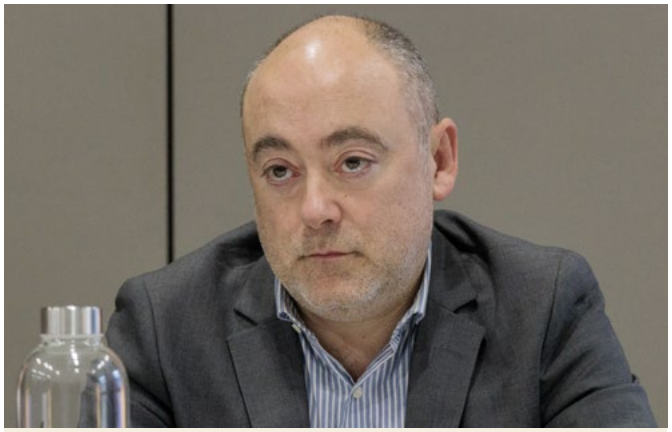
En este último tramo, la conversación se volvió todavía más pragmática. Sergio Alejo insistía en que, incluso entendiendo bien lo que es un MDR, no todo puede ni debe automatizarse. En entornos industriales, decía, cortar una instalación no es una decisión trivial: "un horno que está tal, lo cortas igual... ¿qué ocurre?". Y añadía un matiz fundamental: aunque el servicio actúe, el cliente va a estar implicado sí o sí.

José Luis Corona reforzaba esa idea recordando que estos servicios funcionan sobre protocolos de escalado muy definidos y que la clave es tener claro qué pasa cuando pasa algo, especialmente cuando "el tiempo es crítico".

> La inteligencia artificial está cambiando el escenario de ataque, porque permite campañas más rápidas, más adaptativas y capaces de evolucionar

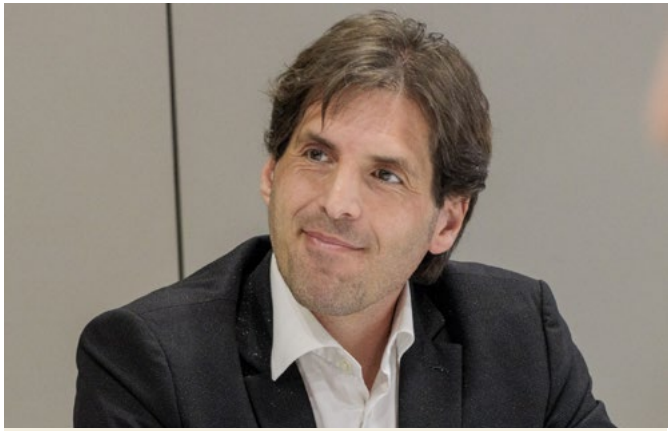
Desde Sophos, Álvaro Fernández insistía en el valor preventivo del modelo: monitorizar proactivamente permite detectar antes y contener mejor, evitando llegar al lunes con el incidente ya desplegado. Pero, como subrayó enseguida Izaskun Onandia, eso solo funciona si "el que te está atendiendo... tiene el contexto claro".

Álvaro Fernández recogió esa idea para insistir en que el MDR combina herramienta y servicio, y que el contexto se construye con el cliente. Además, explicó cómo el servicio ha ido incorporando nuevas capas, como el análisis continuo de vulnerabilidades o la monitorización de identidades comprometidas. Aun así, quiso dejar claro que "no quiero decir que sea MDR la panacea", sino una base sólida, adaptable según el grado de madurez de cada organización.



> "Nos apoyamos en proveedores para complementar nuestro conocimiento, y ahí el MDR tiene sentido si realmente ayuda a acotar bien el alcance de un incidente."
>
> **Juan Luis García,**
> director de Sistemas de Información, **IMQ Prevención**

Andoni Jiménez coincidía en ese punto: puede servir tanto para reforzar entornos maduros



> “Nuestro enfoque con MDR es combinar servicio y conocimiento global para adaptarlo a realidades muy distintas, desde IT hasta entornos industriales”

Jon Nieto,
Senior Executive Account Manager, **Sophos**

como para ofrecer una primera capa de protección en organizaciones más pequeñas.

Más crítico se mostró Díaz Alegre, que advirtió de los riesgos de mezclar demasiados proveedores. Desde su experiencia, separar detección y respuesta puede introducir fricciones y retrasos: “es un error”, decía, porque en un incidente cada minuto cuenta y depender de varias escalas y llamadas puede hacer que el problema crezca. Sí veía útil incorporar capas como threat Hunting, pero solo en etapas más maduras. Su conclusión era clara: el MDR puede aportar valor, pero “hay que medir muy bien cómo se integra”.

El cierre lo puso Juan Luis García con una idea que, en el fondo, condensaba todo el debate. A la pregunta de qué le pediría a un MDR, respondió: “que a las 7 y media de la mañana todos los días estén levantados los sistemas”. Más allá de la tecnología, los casos de uso o la arquitectura, lo que se busca es continuidad operativa.

En esa misma línea, Álvaro Fernández resumía lo que muchos clientes esperan con una expresión muy sencilla: “dormir tranquilo”. O, como matizaba Juan Luis García, que todo ocurra “transparente para el usuario final”.

El debate se cerró así con una conclusión bastante clara: el MDR ya no se valora solo por su capacidad técnica, sino por su capacidad de absorber complejidad, actuar con criterio, integrarse bien con lo que ya existe y garantizar que el

> “El MDR es un servicio completo que integra detección y respuesta, y su valor está en cómo se adapta al nivel de madurez de cada organización”

Álvaro Fernández,
Sales Manager, **Sophos**

negocio siga funcionando. Pero también dejó al descubierto sus límites: la necesidad de contexto, la dificultad de automatizar ciertos entornos y el riesgo de añadir más complejidad si el servicio no está bien diseñado o bien integrado.

Sophos MDR: cuando la ciberseguridad pasa de monitorizar a intervenir

La propuesta de MDR (Managed Detection and Response) de Sophos se articula como un servicio integral que combina tecnología, inteligencia global y operación continua para ayudar a las organizaciones a detectar, investigar y responder a amenazas con mayor rapidez y contexto.

Tal y como explicaron durante el debate Jon Nieto y Álvaro Fernández, uno de los pilares clave es que el MDR no se plantea como una herramienta adicional, sino como un servicio completo que integra detección y respuesta. Esto implica ingestar telemetría de múltiples fuentes —no solo de soluciones propias, sino también de terceros—, normalizarla, correlacionarla y convertirla en casos de uso accionables. Sobre esa base, el servicio no se limita a alertar, sino que puede actuar directamente según los playbooks acordados con el cliente, incluyendo tareas como contención de amenazas, aislamiento de equipos o desactivación de cuentas comprometidas.

Otro elemento diferencial es la visión global. Sophos opera este servicio con equipos especializados que trabajan 24/7 y que analizan incidentes en miles de organizaciones en todo el mundo. Esa exposición permite trasladar a cada cliente una inteligencia colectiva basada en ataques reales, acelerando la detección de patrones y reduciendo el tiempo de respuesta ante amenazas emergentes.

La propuesta se apoya además en la plataforma Sophos XDR, que actúa como capa tecnológica para la recopilación y análisis de datos, y que permite integrar señales procedentes de endpoint, red, identidad o cloud. A partir de ahí, el equipo de analistas no solo investiga alertas, sino que prioriza riesgos y recomienda acciones, adaptando la respuesta al contexto específico de cada organización.

En línea con la evolución del mercado, Sophos ha reforzado su enfoque con la incorporación de capacidades adicionales, como el análisis continuo de vulnerabilidades o la monitorización de identidades comprometidas, dos de los vectores de ataque más habituales. Todo ello se complementa con servicios de incident response para escenarios críticos, donde se requiere una intervención más profunda.

En conjunto, la propuesta MDR de Sophos pone el foco en tres elementos: reducir la carga operativa del cliente, mejorar la velocidad de respuesta y aportar contexto real a la toma de decisiones, adaptándose tanto a organizaciones con alta madurez como a aquellas que necesitan externalizar gran parte de su operación de seguridad.