DEBATES ciberseguridad TIC

“Detección y respuesta sin descanso: descubre el poder del MDR”

SOPHOS

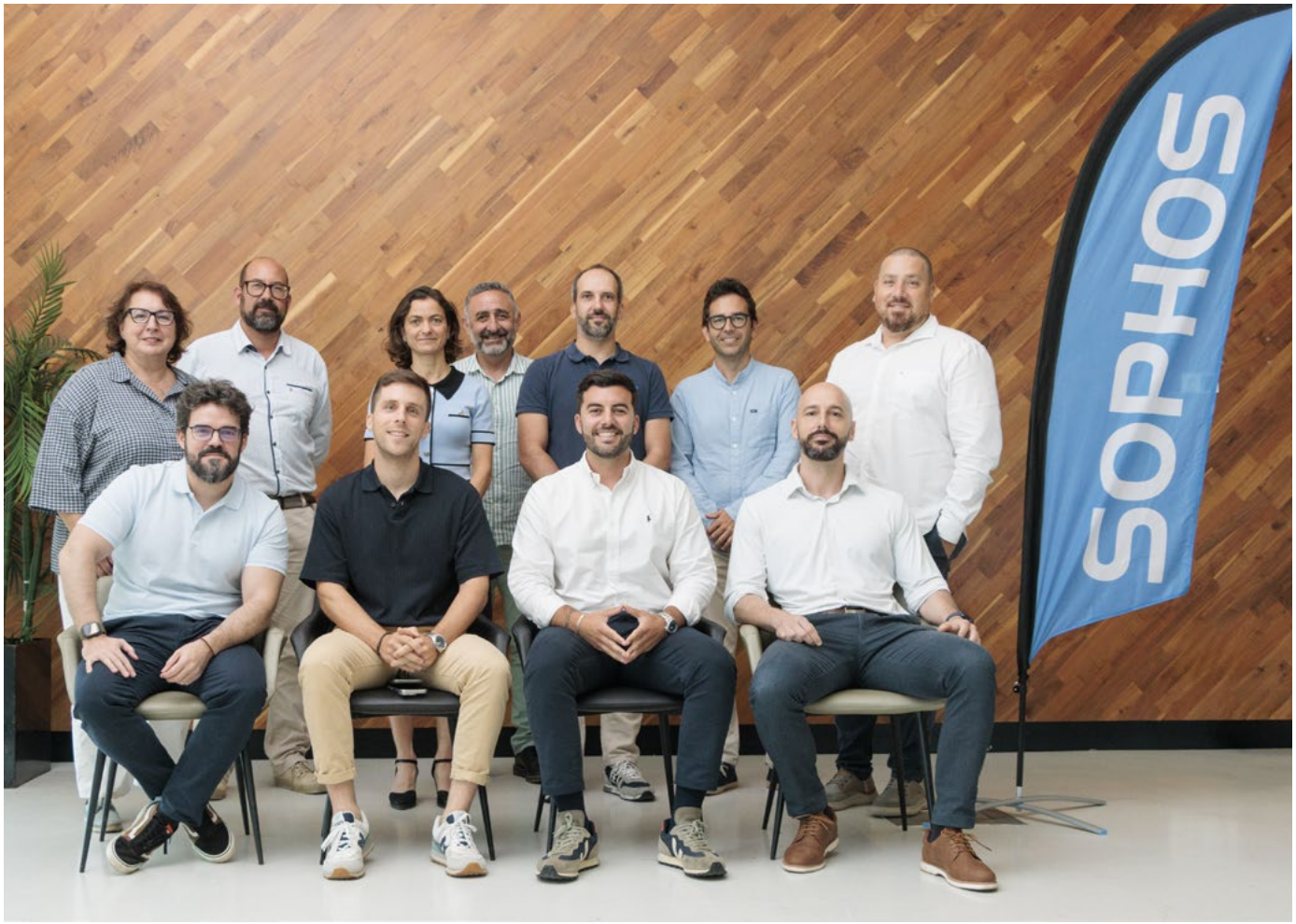
twt-ts
It for people

IR A PÁGINA SIGUIENTE

“Detección y respuesta sin descanso: descubre el poder del MDR”

Con entornos cada vez más complejos y equipos internos muy ajustados, muchas organizaciones buscan fórmulas para reforzar su protección sin multiplicar recursos. Los servicios de detección y respuesta gestionados (MDR) se consolidan como una opción efectiva.

Rosalía Arroyo



Así se puso de manifiesto en el almuerzo-debate organizado por Ciberseguridad TIC con el patrocinio de Sophos y TWT, que reunió en Valencia a responsables de tecnología de diversos sectores. Una idea clave se repitió a lo largo de la jornada: la dificultad para mantener una vigilancia permanente con recursos propios. La falta de visibilidad en todos los entornos y la imposibilidad de responder rápidamente ante un incidente fuera del horario la-

> “El proveedor de MDR debe conocer bien la infraestructura desde el principio para actuar con precisión”

Christian Salcedo, Responsable de Ciberseguridad y Comunicaciones, **Aquaservice**

boral son preocupaciones comunes entre los participantes.

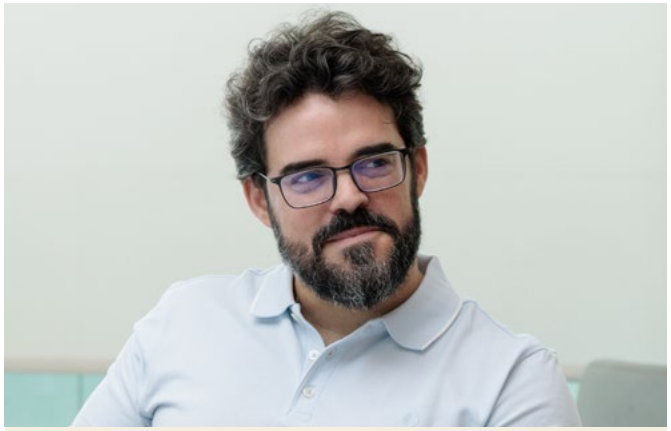
David Carrasco, responsable de infraestructura y CISO de San Lúcar Fruit, explicó que su equipo está bien preparado, pero no puede estar disponible todo el tiempo. “Desgraciadamente, nuestro cuerpo no está preparado para un 24/7. Tenemos que dormir y confiar en herramientas o en unos ojos de algún partner que pueda ayudarte a intervenir”, señaló.

Una opinión compartida por Pilar Raro, CIO y CISO de Victoria Ceramics, quien fue rotunda: “No, imposible. Para eso están las empresas que nos apoyan. Nuestro negocio no es la ciberseguridad, nuestro negocio es producir azulejos de calidad”.

También David Pérez, director técnico general de DAM, describió un escenario de alta dispersión, con instalaciones en lugares remotos, baja conectividad y rotación frecuente de empleados, a la hora de hablar de los grandes retos a los que se tienen que enfrentar las empresas.

Qué se espera de un servicio MDR

Los asistentes coincidieron en que un buen servicio MDR debe aportar agilidad, conocimiento del entorno y confianza. Pilar Raro resumió su visión con claridad: “Yo lo que espero es dormir tranquila. Que alguien esté ahí, como el gran hermano de nuestra infraestructura, que me asesore y me ayude a mejorar”.



> “Queremos plataformas unificadas: gestionar múltiples consolas es cada vez más inviable”

David Sánchez,
Responsable IT, **Broseta Abogados**

Ángel Zuriaga, director TIC de SITVAL, remarcó que “la rapidez fuera de horario es lo básico. Pero también importa cómo se acota el problema: no vale parar todo por contener una amenaza”.

Por su parte, Christian Salcedo, responsable de ciberseguridad en Aquaservice, subrayó la importancia de que el proveedor conozca bien

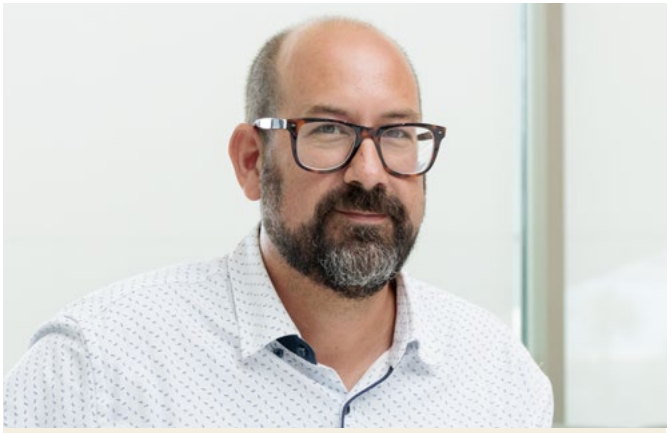
"Unificar herramientas bajo un único proveedor nos ha dado visibilidad y agilidad de gestión"

Carlos García,
IT Manager, **Consorcio Hospitalario Provincial de Castellón**

el entorno del cliente: "Es clave que el servicio MDR entienda desde el inicio la infraestructura de la organización para saber con precisión dónde actuar y cómo hacerlo".

David Sánchez, responsable IT de Broseta Abogados, añadió otro matiz: "Un falso positivo en nuestro entorno puede bloquear a un usuario durante horas. Hay que equilibrar seguridad y usabilidad, sobre todo con perfiles no técnicos". En este punto, Iván Mateos, Sales Engineer de Sophos Iberia, ofreció una reflexión desde la experiencia con numerosos clientes: "A nadie de los presentes le preocupa cuán malos son los atacantes. Lo que de verdad inquieta es tener visibilidad completa, que el negocio no se detenga y que alguien se encargue de vigilar lo que no se puede cubrir internamente". Según explicó, los servicios MDR están precisamente diseñados para aliviar esa presión: "No se trata de poner una consola bonita, sino de asumir por ti la vigilancia continua, la respuesta y el asesoramiento, con criterio y contexto".

MDR libera al equipo interno y mejora la respuesta sin necesidad de ampliar plantilla

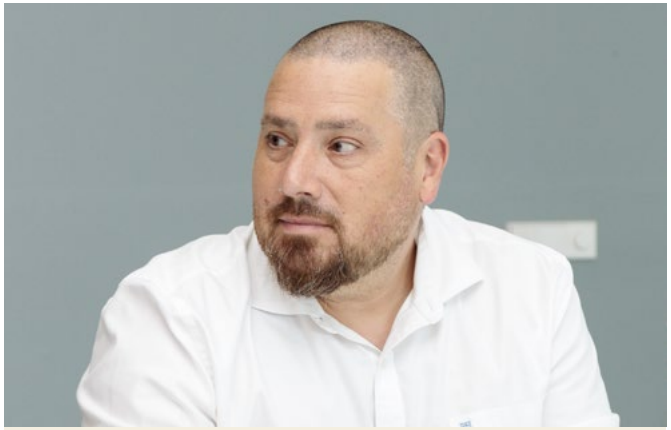


"Los entornos colaborativos con múltiples actores y normativas hacen muy compleja la gestión segura"

David Pérez,
director técnico General, **Depuración de Aguas del Mediterráneo (DAM)**

La cadena de suministro, otro frente clave

Al hablar de la cadena de suministro, varios participantes coincidieron en la necesidad de empezar por medidas fundamentales, como la segmentación de red y el refuerzo de la segu-



> “No podemos estar operativos 24/7; necesitamos partners y herramientas que nos respalden sin parar el negocio”

David Carrasco,
IT Infrastructure & CISO, **San Lúcar Fruit**

ridad en instalaciones críticas, tal como apuntó Christian Salcedo.

David Sánchez incidió en la utilidad de dividir entornos y funciones clave para facilitar el control y reducir riesgos, asegurando que “así podemos tener un ojito más o mejor puesto en cada cosa”.

David Carrasco aportó una visión práctica sobre las dificultades de concienciación digital entre ciertos colaboradores externos: “Hacemos lo posible por evangelizar, pero no siempre es fácil explicar por qué hay que seguir ciertas prácticas básicas. Tienes que ceder a veces”.

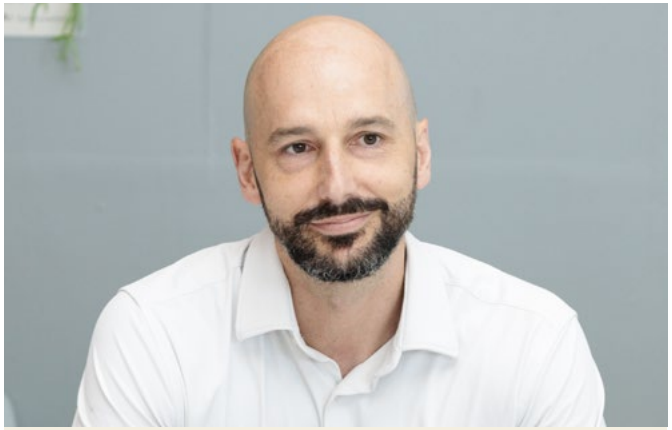
Por su parte, David Pérez remarcó la complejidad que suponen los entornos colaborativos y descentralizados, donde intervienen distintas organizaciones, normativas y flujos de trabajo: “Todo está muy acotado, pero con muchos accesos cruzados que requieren atención constante”.

Una experiencia real con MDR

Carlos García, IT manager del Consorcio Hospitalario Provincial de Castellón, explicó cómo su organización adoptó un servicio MDR de Sophos en un momento crítico: “No teníamos recursos humanos y buscábamos algo fácil de desplegar y que nos protegiera desde el minuto uno”.

Aseguró que el resultado fue positivo, hasta el punto de que “nunca nos ha cortado un servicio. Y eso que al principio no les dimos toda la información técnica. El sistema funciona y si hay un problema, te lo recuerda de forma insistente hasta que lo resuelves”.

Además, decidieron unificar herramientas bajo un único proveedor porque “nos aporta más



> “Lo básico que pido a un MDR es rapidez y capacidad de acotar sin interrumpir el servicio”

Ángel Zuriaga,
director TIC, **SITVAL**

“Lo que espero de un servicio MDR es poder dormir tranquila: que me asesoren, actúen y me ayuden a mejorar”

Pilar Raro,
CIO & CISO, **Victoria Ceramics**

que la diversificación. Simplifica la gestión y mejora la visibilidad”.

Iván Mateos añadió que este enfoque integrado facilita no solo la gestión diaria, sino también la eficacia del propio servicio MDR: “Cuando las distintas capas de seguridad comparten información, la detección es más precisa y la respuesta más ágil. No se trata de eliminar fabricantes, sino de evitar puntos ciegos”.

La falta de visibilidad y la dispersión complican la respuesta ante incidentes

Formación, cultura y usuarios: parte del ecosistema

Más allá de las herramientas, los participantes insistieron en el papel de la cultura interna.

Ángel Zuriaga explicó que una formación de cinco horas en su organización fue “la acción que más ha mejorado la seguridad”, al lograr que muchos empleados tomaran conciencia real de los riesgos. Pilar Raro, por su parte, compartió el éxito de una iniciativa competitiva y formativa: una “liga de ciberseguridad” en la que diferentes equipos compiten mensualmente a través de píldoras formativas y pruebas de conocimiento. “Se genera un ambiente de participación muy positivo, con implicación real por parte de los empleados, ya que, además, hay premios”, afirmó.

No obstante, también se subrayó que estas iniciativas deben ir acompañadas de una buena comunicación. Como apuntó David Pérez, si las medidas de seguridad se imponen sin contexto, “se perciben como una excusa para controlarte o despedirte”, lo que genera rechazo en lugar de colaboración.

Carlos García coincidió en la necesidad de adoptar un enfoque realista: “El usuario siempre se equivoca. No se trata de confiar ciegamente, sino de asumir que los errores van a pasar y limitar su impacto”.

Seguridad con impacto real: el argumento que convence

La relación entre ciberseguridad y negocio centró buena parte del debate, especialmente en lo relativo a cómo trasladar su valor a los comités

de dirección. Los participantes coincidieron en que hablar en términos técnicos rara vez resulta efectivo, y que es necesario traducir los riesgos en impacto económico y operacional.

Pilar Raro explicó cómo logra justificar inversiones clave ante dirección general: “Planteo cuánto costaría parar la producción un día en tres fábricas con ocho hornos a pleno rendimiento”. Y entonces son conscientes de que hay que invertir en ciberseguridad y solemos tener aprobada una partida de presupuesto anual indispensable”. En su experiencia, poner cifras al riesgo y vincularlo directamente con el negocio es lo que realmente activa la toma de decisiones.

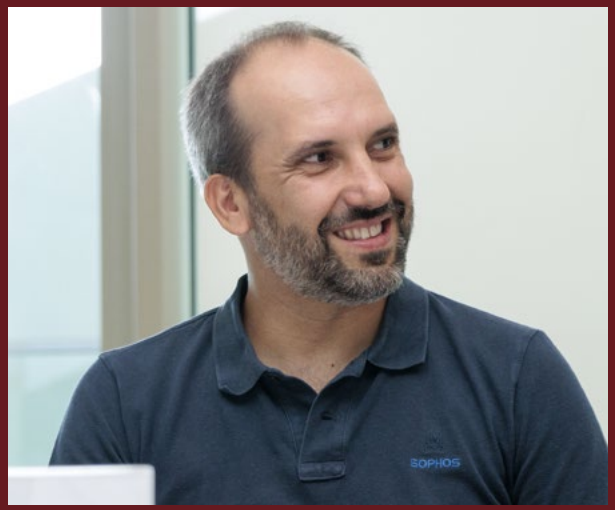
Otros participantes, como David Carrasco y David Pérez, recomendaron recurrir a escenarios tangibles y comparativas claras entre lo que cuesta protegerse y lo que puede suponer una parada forzada o una filtración de datos. “Después de sufrir un incidente, los argumentos se entienden mejor. Ya no se discute si hay que actuar, sino cómo”, comentó uno de ellos durante la sesión.

Iván Mateos, de Sophos, reforzó esta línea argumental desde la perspectiva del mercado ase-

SOPHOS

twt-ts It for people

Visión del fabricante: Iván Mateos, Sophos Iberia



Durante el encuentro, Iván Mateos, Sales Engineer de Sophos Iberia, compartió una visión directa y realista sobre el papel del MDR en las organizaciones actuales. Estas fueron algunas de sus reflexiones más destacadas:

- **“A nadie le preocupa ya cuán malos son los atacantes. Lo que de verdad inquieta es tener visibilidad completa, que el negocio no se detenga y que alguien vigile lo que no se puede cubrir internamente”.**
- **“El MDR no es solo una consola bonita. Es un equipo que asume por ti la vigilancia continua, la respuesta y el asesoramiento, con criterio y contexto”.**
- **“Cuando las distintas capas de seguridad comparten información, la detección es más precisa y la respuesta más ágil. No se trata de eliminar fabricantes, sino de evitar puntos ciegos”.**
- **“Cada vez más ciberseguros exigen un servicio MDR para ofrecer cobertura. Ese tipo de argumentos ayudan a que se entienda el valor estratégico de la ciberseguridad”.**
- **“No es solo proteger. También necesitamos pentesting, análisis continuos, cumplimiento... Es hora de ampliar el catálogo de servicios pensando en las empresas medianas, no solo en las grandes”.**

gurador: “Cada vez más ciberseguros exigen un servicio MDR para ofrecer cobertura. Ese tipo de argumentos ayudan a que se entienda el valor estratégico”. Además, añadió que disponer de este tipo de servicios puede ser clave para reducir la prima del seguro o incluso acceder a pólizas que de otro modo no estarían disponibles.

¿Qué piden las organizaciones al mercado?

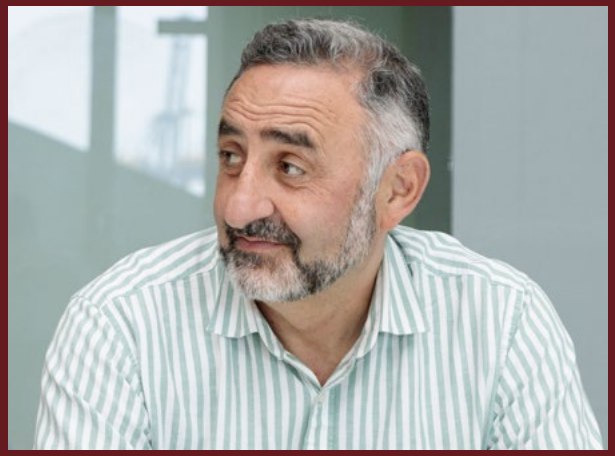
En la parte final del debate, se propuso una “carta a los Reyes Magos” para el sector de la ciberseguridad.

Christian Salcedo y David Sánchez coincidieron en pedir plataformas unificadas, con todo en un solo lugar: “Queremos una consola para verlo todo, porque es imposible gestionar tantas piezas separadas”.

Pilar Raro propuso que las campañas de concienciación formen parte de las soluciones: “Si el propio fabricante te permite lanzar píldoras y simulacros, te ahorras tiempo y dinero”.

David Pérez pidió formación básica para empleados no técnicos: “Si no explicas el porqué,

Visión del integrador: José Ignacio Guijarro, TWT



Desde la perspectiva del integrador, José Ignacio Guijarro, director general de TWT, subrayó la necesidad de colaboración, especialización y realismo en la forma en que las empresas abordan la ciberseguridad. Estas fueron algunas de sus ideas clave:

- **“La seguridad es cosa de todos. No se puede pensar solo en las grandes. El 99% de las empresas necesitan soluciones pensadas para ellas”.**
- **“Nuestro papel como partner es garantizar que la infraestructura esté preparada, pero la inteligencia y la respuesta ante amenazas requieren de un equipo especializado”.**
- **“No tiene sentido que cada empresa monte su propio SOC. Ni siquiera para muchos integradores es rentable hacerlo. Lo eficiente es apoyarse en un servicio experto como el MDR”.**
- **“La clave está en crear un ecosistema bien conectado, donde cada pieza —inventario, segmentación, visibilidad— funcione correctamente para que el servicio MDR pueda hacer su trabajo”.**
- **“La seguridad exige trabajo continuo. El MDR ayuda a dormir más tranquilo, sí, pero no significa que podamos desentendernos. Requiere compromiso, revisión y mejora constante”.**

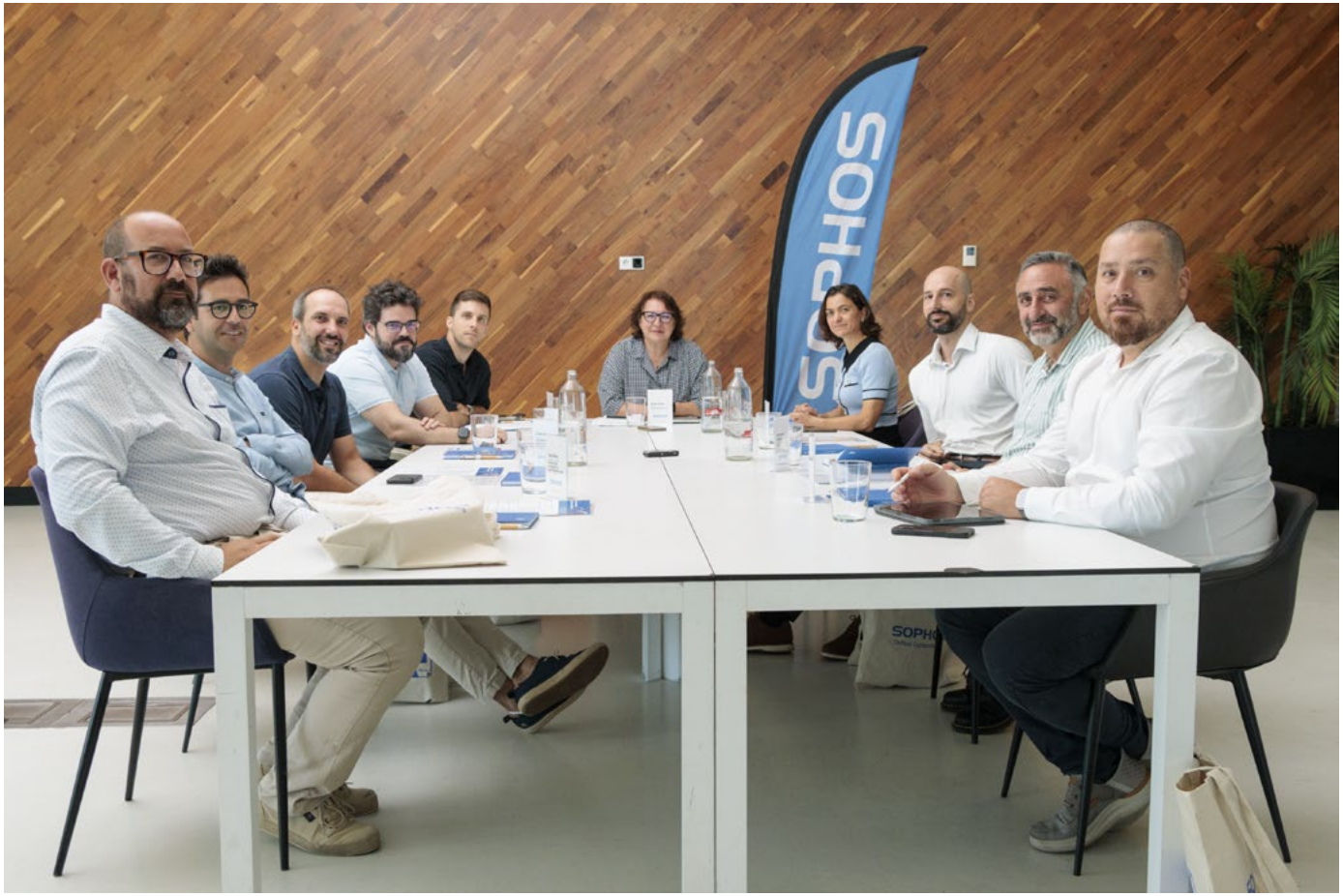
las medidas se ven como una imposición".

Carlos García fue tajante: "No puedes confiar en los usuarios. Lo mejor es asumir que se van a equivocar y estar preparados".

Desde Sophos, Iván Mateos recogió las peticiones y pidió ampliar el catálogo de servicios más allá de la detección de amenazas. "No es sólo proteger. También necesitamos pentesting, análisis continuos, cumplimiento...", afirmó. Y recordó la importancia del diseño seguro desde el origen: "No hace falta sacar la funcionalidad el primero, sino que cuando salga, sea segura".

José Ignacio Guijarro, director general de TWT, cerró con una llamada de atención: "La seguridad es cosa de todos. No se puede pensar solo en las grandes. El 99 % de las empresas necesitan soluciones pensadas para ellas".

Desde su experiencia como partner tecnológico, Guijarro también subrayó la importancia de rodearse de especialistas: "Nuestro papel es garantizar que la infraestructura esté preparada, pero la inteligencia y la respuesta ante amenazas requieren de un equipo especializado. Por eso apostamos por el MDR de Sophos, porque sabemos que detrás hay músculo, visibilidad global y una operativa profesional que nosotros solos no podríamos replicar".

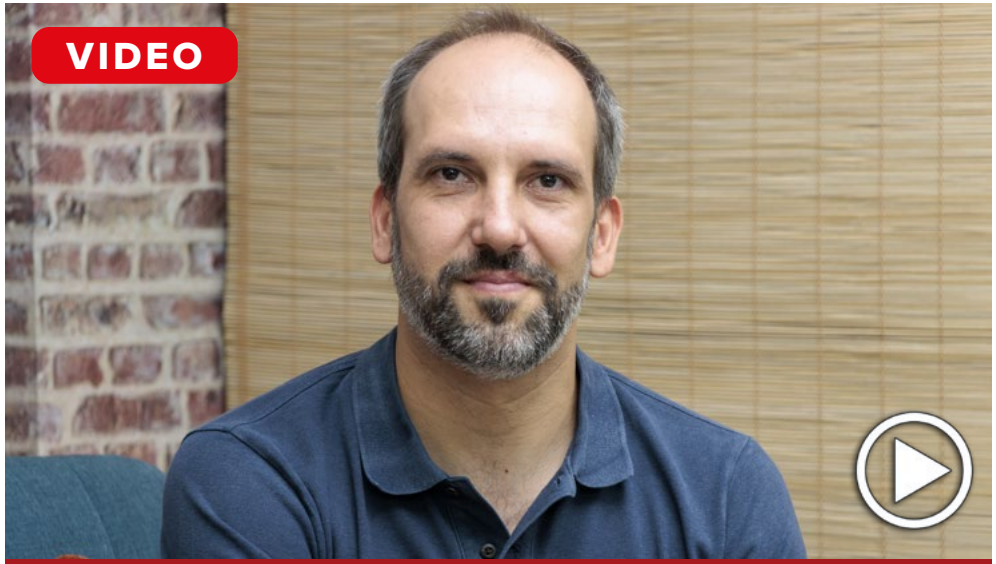


El debate puso de relieve que los servicios MDR son hoy una herramienta fundamental para muchas organizaciones. No sólo permiten detectar y responder ante amenazas complejas, sino que también ayudan a liberar a los equipos internos, mejorar la visibilidad y reforzar la estrategia de seguridad.

Eso sí: para que sean realmente eficaces, deben adaptarse al contexto de cada empresa, convivir con los recursos existentes y estar al servicio de quienes deben mantener en marcha el negocio todos los días, sin descanso.

Sophos: “Dormir tranquilo no es evitar ataques, es tener un equipo que responde por ti”

Tras el debate sobre MDR organizado por Ciberseguridad TIC, Iván Mateos, Sales Engineer de Sophos Iberia, profundiza en cómo estos servicios ayudan a liberar a los equipos internos y garantizar una vigilancia real 24/7. “Dormir tranquilo no es evitar ataques, es tener un equipo que responde por ti”, resume. Además del componente humano, destaca la importancia del diseño seguro de los productos y la visibilidad total del entorno: “La seguridad no está solo en el endpoint, también en el cloud, el backup o el firewall”.

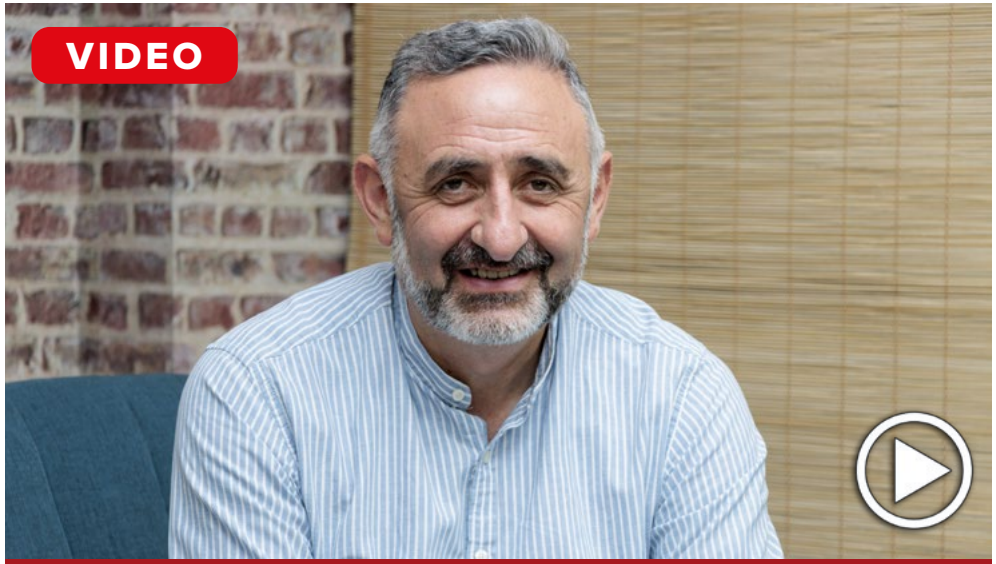


Iván Mateos, Sales Engineer de **Sophos Iberia**

Tras la adquisición de SecureWorks, Sophos apuesta por ampliar su catálogo de servicios con capacidades como virtual CISO o cumplimiento normativo. “Nuestros partners aportan el contexto; nosotros, el músculo del MDR”, concluye.

TWT: “La clave está en proteger sin añadir complejidad al cliente”

José Ignacio Guijarro, director general de TWT, destaca que muchas organizaciones buscan reforzar su seguridad sin añadir complejidad, especialmente en el segmento medio del mercado. “Nuestro conocimiento es nuestro mayor valor”, afirma, y explica que su enfoque combina soporte proactivo, revisiones periódicas y una atención personalizada. Subraya la importancia de que el entorno tecnológico esté bien configurado para que el MDR funcione correctamente.



José Ignacio Guijarro, director general de **TWT**

Respecto a la colaboración con Sophos, valora su capacidad de especialización y su enfoque en empresas de todos los tamaños: “Necesitamos fabricantes que inviertan y estén al día, y Sophos lo hace”. También resalta el equilibrio de TWT: “Somos lo bastante grandes para estar actualizados, y lo bastante cercanos para tratar a cada cliente de forma personalizada”.