DEBATES ciberseguridad TIC

MDR, confianza y colaboración: los nuevos pilares de la defensa digital

SOPHOS

TEKPYME

IR A PÁGINA SIGUIENTE

MDR, confianza y colaboración: los nuevos pilares de la defensa digital

Cuando una alerta salta a medianoche y el equipo de seguridad no está frente a la pantalla, lo que marca la diferencia no es la suerte, sino la preparación. Esa fue una de las conclusiones que compartieron los responsables de IT y ciberseguridad reunidos en Sevilla: la defensa digital ya no entiende de horarios ni de turnos, y exige anticipación, coordinación y confianza.

Rosalía Arroyo

Con ese espíritu se celebró el almuerzo-debate “Detección y respuesta sin descanso. Descubre el poder de MDR”, organizado por Ciberseguridad TIC con el patrocinio de Sophos y Tekpyme. En el encuentro, representantes de compañías como EMASESA, Grupo Alvic, Aceites Abasa, Ametel, Ghenova Ingeniería, Corporación Jiménez Maña y Grupo Sevilla Control compartieron sus experiencias y preocupaciones en torno a la detección y respuesta ante incidentes. Una conversación que reflejó la realidad de muchas organizaciones: recursos limitados, marcos normativos cada vez más exigentes y una amenaza constante que no se detiene.

> “Cuando tengo un problema, quiero levantar el teléfono y que haya alguien al otro lado”

Alfonso López Escobar,
jefe seguridad de la información **EMASESA**

El valor de la visibilidad

Un asunto repetido durante la sesión fue la dificultad de mantener una visibilidad completa del entorno tecnológico. “Me preocupa lo que no veo”, reconocía Alfonso López Escobar, jefe de Seguridad de la Información de EMASESA, aludiendo al riesgo que suponen los puntos ciegos en la infraestructura digital. Su reflexión resumía un temor compartido: los ataques más peligrosos son los que pasan inadvertidos. López Escobar añadía que esa falta de visibilidad también puede derivarse de la distancia entre los equipos internos y los SOC externos, cuando no comparten suficiente contexto sobre el negocio.

Desde el ámbito industrial, Jesús Morgan, responsable de IT en Ametel, coincidía en esa preocupación. Admitía que la rapidez con la que evolucionan los vectores de ataque hace imposible sentirse completamente preparado. “Siempre piensas que estás protegido, pero también tienes esa intranquilidad de si lo estarás lo suficiente”, reconocía. Recordó además la dificultad de extender la cultura de ciberseguridad al conjunto de la organización, más allá del departamento técnico: “No sólo se trata de proteger sistemas, sino de concienciar a quienes los usan; y eso, en empresas grandes, es un desafío continuo”.

En el caso de Aceites Abasa, el foco está en armonizar los marcos regulatorios y de seguridad en todos los países donde opera la compañía. “Estamos construyendo nuestro marco de

> “Preferimos hacer las cosas despacio y bien configuradas, contrastadas por el fabricante y el partner”

Eneko Ferrero,
CIO, **Aceites Abasa**

ciberseguridad sobre las bases de NIS y NIST, buscando un framework común para todas las sedes”, explicaba su CIO, Eneko Ferrero, convencido de que la simplicidad y la coherencia normativa son esenciales para no perder control en entornos multinube.

"La ciberseguridad no es cosa de una persona; hay que apoyarse en partners especializados"

Migue Ángel García,
jefe de proyectos de ciberseguridad, **Gehova ingeniería**

Desde Ametel, Fernando García ampliaba la visión recordando que el ransomware es sólo una parte del problema: "Hay muchos más riesgos; las fugas de información o los nuevos vectores de ataque nos preocupan igual o más". En la misma línea, Fernando Lianes, CEO de Tekpyme, destacaba que escuchar esa reflexión de boca

La protección de la identidad se ha consolidado como uno de los ejes centrales de la ciberseguridad

de los clientes es un signo de madurez: "Durante años hemos intentado explicar que la ciberseguridad no se limita al ransomware, y es alentador ver que las empresas empiezan a percibirlo así".

Prepararse para el ataque

Más allá de las herramientas, el debate giró en torno a la capacidad real de respuesta cuando ocurre un incidente. En Ghenova Ingeniería, esa capacidad se apoya en una estructura distribuida. "Replicamos el mismo tipo de ciberseguridad en Europa y Latinoamérica, con el SOC centralizado en Sevilla", explicaba Miguel Ángel García, convencido de que la continuidad operativa requiere procedimientos homogéneos y bien documentados.

"Hay muchos más problemas que el ransomware; las fugas de información nos inquietan igual o más"

Fernando García,
Consejero Ejecutivo, **AMETEL**

Otros participantes hablaron desde la experiencia acumulada en la gestión de incidentes. Miguel del Valle, director de Tecnología de Corporación Jiménez Maña, reflexionó sobre el impacto emocional y operativo que puede generar una situación crítica de seguridad:

IR A PÁGINA ANTERIOR

IR A PÁGINA SIGUIENTE

"Es esencial poder auditar las decisiones que un servicio toma por ti"

Miguel del Valle Gracia,
Director de Tecnología y Sistemas,
Corporación Jiménez Maña

"Cuando te enfrentas a un incidente, aprendes mucho... pero es un mal día para aprender", aseguró, subrayando la importancia de mantener la perspectiva: "A veces el miedo a repetir una situación pasada puede llevarte a sobre reaccionar, centrando todos los esfuerzos en prevenir lo mismo y descuidando otros frentes".

Iván Mateos, Senior Sales Engineer de Sophos, coincidía en que la preparación se forja con la experiencia, pero advertía del riesgo de improvisar: "Esto se aprende a base de golpes. Si cada minuto cuenta, necesitas ayuda para responder rápido; si no, te quedas atrás". Su intervención sirvió para abrir un consenso: la rapidez es tan importante como la precisión, y ambas dependen de combinar automatización con criterio humano.

OT y normativa: una combinación delicada

La conversación se desplazó después hacia los entornos industriales, donde la convergencia entre IT y OT plantea nuevos desafíos. "Nuestro principal campo de batalla está en el entorno OT", comentaba Javier Morales, CIO del Grupo Alvic, una empresa que opera fábricas y centros de producción en varios continentes. Tras implementar un servicio MDR de Sophos, explicaba, han logrado "no sólo más seguridad, sino también la tranquilidad de saber que hay expertos vigilando cuando nosotros no estamos".

En organizaciones con servicios esenciales,

"Pediría más formación y capacidad de auditar lo que hace el servicio MDR"

Javier Morales,
CIO, **Grupo ALVIC**

como EMASESA, la dimensión normativa añade una presión adicional. López Escobar señalaba que, "cuando hablamos de OT y normativa, hablamos de operadores esenciales y de directivas como NIS2. La regulación se convierte en un motor para mejorar la seguridad".

Desde Tekpyme, Alberto Blanco aportó una visión práctica basada en su experiencia con

> “El principal valor de un partner es la cercanía; si tengo que hacer su trabajo, algo falla”

Antonio Megolla,
CIO, **Grupo Sevilla Control**

clientes industriales: “Si la integración entre IT y OT no se planifica desde el principio, se vuelve ingobernable”. Un mensaje que Eduardo Corrales, de Sophos, completó con un toque de realismo: “En OT cualquier cambio tiene impacto operativo; la seguridad tiene que aplicarse con tacto y con consenso interno”.

El arte de priorizar

La saturación de alertas y la fatiga de los equipos fueron otro punto clave del debate. “Si una herramienta me bombardea con alertas, la quito del medio”, afirmaba López Escobar, explicando que la confianza en la herramienta depende tanto de su precisión como de la experiencia del equipo que la gestiona.

Iván Mateos, directivo de Sophos, puso cifras al problema: “Cuando un servicio envía 300 alertas al día, el cliente acaba sin mirar ninguna. La clave es priorizar, correlacionar y notificar sólo lo que realmente importa”. Su intervención puso sobre la mesa un reto recurrente: la fatiga de alertas puede convertir la defensa en un ejercicio de resistencia. Los asistentes coincidieron en que la solución pasa por combinar IA y análisis contextual, evitando tanto el exceso de automatización como la dependencia absoluta de los procesos manuales.

La confianza como cimiento de la ciberseguridad

A medida que avanzaba la conversación, quedó claro que la tecnología, por sí sola, no basta.

> “La confianza es crítica: no pones tu core de negocio en manos de cualquiera”

Fernando Lianes,
CEO, **Tekpyme**

En ciberseguridad, la confianza entre cliente y partner es el cimiento sobre el que se construye cualquier estrategia eficaz.

“La ciberseguridad no depende de un sólo perfil; hay que apoyarse en partners de confianza para las áreas más especializadas”, señalaba Miguel Ángel García, de Ghenova Ingeniería, destacando que la colaboración entre equipos

> “En OT cualquier cambio tiene impacto operativo; la seguridad hay que aplicarla con tacto”

Eduardo Corrales Guerrero
Ejecutivo de Cuentas Senior del Territorio Sur, **Sophos**

internos y externos permite reforzar tanto la detección como la respuesta.

Desde EMASESA, Alfonso López Escobar subrayaba la importancia de la cercanía y la disponibilidad humana frente a los canales impersonales: “Cuando tengo un problema, quiero levantar el teléfono y que haya alguien al otro lado”, aseguraba.

> La rapidez es tan importante como la precisión, y ambas dependen de combinar automatización con criterio humano

En esa misma línea, Antonio Megolla, CIO del Grupo Sevilla Control, defendía que la relación con un proveedor debe ser sencilla y resolutiva: “El principal valor de un partner es la facilidad; si tengo que hacer tu trabajo, algo falla”.

Por último, Fernando Lianes, CEO de Tekpyme, resumía el sentir general con una reflexión que fue más allá de la técnica: “La confianza no se compra, se construye. Al final estás poniendo tu negocio en manos de alguien más”.

¿Qué pides a un MDR?

El tramo final del debate miró hacia el futuro y dejó claro que los servicios de detección y respuesta gestionada (MDR) ya no se valoran solo por su capacidad técnica, sino por el acompañamiento que ofrecen. Las organizaciones buscan transparencia, formación, contexto y colaboración real con sus proveedores.

> “Hay que diseñar con cabeza desde el inicio; si no, los entornos OT se vuelven ingobernables”

Alberto Blanco,
Sales Director, **Tekpyme**

“Nos gustaría tener más formación y capacidad de auditar lo que hace el servicio”, planteaba Javier Morales, de Grupo Alvic, subrayando la necesidad de que las empresas entiendan me-

> “Si cada minuto cuenta, necesitas ayuda para responder rápido”
>
> **Iván Mateos,**
> Senior Sales Engineer, **Sophos**

jor cómo opera la defensa que han puesto en manos de terceros.

Para Antonio Megolla, de Grupo Sevilla Control, la evolución pasa por facilitar la interacción: “Necesitamos una IA tipo ChatGPT con la que podamos conversar y entender de forma natural qué está pasando”. Una petición que enlazó con la de otros participantes, interesados en contar con herramientas más intuitivas y visuales que traduzcan la complejidad técnica a un lenguaje operativo.

Jesús Morgan, responsable IT de Ametel, puso el acento en otro aspecto clave: la gestión de falsos positivos. “Las herramientas son cada vez más potentes, pero generan mucha información. Entre esos avisos puede esconderse un ataque real, y hay que tener tiempo y conocimiento para distinguirlo”, advirtió, insistiendo en que la automatización debe ir acompañada de supervisión humana.

Alfonso López Escobar, de EMASESA, insistió en que la eficacia depende de la personalización: “Si el proveedor no entiende bien tu organización, los falsos positivos no desaparecerán nunca”. Por su parte, Miguel del Valle, de Corporación Jiménez Maña, añadió que la confianza se consolida con transparencia: “Poder auditar las decisiones que se toman por ti es esencial para confiar en el servicio”.

Desde Sophos, Iván Mateos confirmó que el fabricante ya está avanzando en esa dirección, y explicó cómo la compañía está integrando la inteligencia artificial para que la relación entre las

> “No se trata únicamente de proteger sistemas, sino de concienciar a quienes los usan; y eso, en empresas grandes, es un desafío continuo”
>
> **Jesús Morgan,**
> responsable de IT, **Ametel**

herramientas y los equipos humanos sea más ágil y productiva. “La consola de Sophos incorpora asistentes con IA para threat hunting y una interacción más visual y natural”, señaló.

> La integración entre la seguridad IT y OT sigue siendo uno de los grandes retos en sectores críticos

El experto subrayó que el objetivo no es sustituir al analista, sino aumentar su capacidad de decisión: “Cuando la IA te ayuda a formular preguntas, interpretar patrones y proponer respuestas, el tiempo de reacción se reduce y la confianza en el diagnóstico aumenta”. Además, añadió que la evolución del MDR pasa por combinar la automatización con el conocimiento humano, asegurando que la tecnología aprenda de cada incidente para reforzar la protección futura.

El cierre lo puso Alberto Blanco, de Tekpyme, quien resumió la conclusión compartida de la jornada: “No basta con tener buena seguridad; hay que alinear la estrategia con las exigencias regulatorias y hacerlo sin ahogar a los equipos técnicos”.

El debate dejó una sensación compartida: la ciberseguridad moderna es un trabajo de fondo. No se trata únicamente de detener ataques, sino de mantener la visibilidad, reducir la fatiga operativa y fortalecer la confianza entre fabricantes, partners y clientes. Los servicios MDR se consolidan como el eslabón que une tecnología, conocimiento y acompañamiento continuo, en un momento en el que las empresas necesitan certezas más que herramientas.

Como apuntó uno de los participantes, “en este sector, lo difícil no es detectar, sino reaccionar a tiempo”. Una frase que resume el verdadero desafío de la ciberseguridad actual.

“El MDR ha pasado de ser una opción a una necesidad”

Iván Mateos, Sales Engineer de Sophos Iberia, explica en este vídeo cómo el modelo Managed Detection and Response (MDR) se ha consolidado como respuesta natural a la complejidad de las ciberamenazas. Señala que “las empresas ya no buscan solo productos, sino servicios que les respalden las 24 horas” y describe el trabajo del equipo de Sophos como “un día a día muy de película”, con ataques y respuestas continuas.

También destaca el directivo la flexibilidad del servicio, capaz de adaptarse al entorno de cada cliente, y advirtió que, aunque la inteligencia artificial aporta agilidad, “no puede sustituir la supervisión humana”. El MDR, concluye, combina tecnología avanzada y experiencia experta para reforzar la defensa empresarial.

Iván Mateos, Senior Sales Engineer, **Sophos**

Tekpyme: “El futuro de la ciberseguridad se construye sobre relaciones a largo plazo”

Tekpyme acompaña a las empresas en la adopción de servicios MDR, combinando tecnología avanzada y cercanía operativa. Su director comercial, Alberto Blanco, destaca tres grandes retos para las organizaciones: “la visibilidad, la velocidad y el talento”.

Frente a un escenario donde los ataques se ejecutan en minutos, Tekpyme apuesta por un modelo colaborativo con los equipos internos del cliente, adaptando procesos y decisiones para garantizar una respuesta ágil y transparente.

Alberto Blanco, director comercial, **Tekpyme**

El directivo insiste en que el MDR no es exclusivo de grandes compañías y puede escalarse según las necesidades. Para él, la clave está en la colaboración: “El futuro de la ciberseguridad se construye sobre relaciones a largo plazo, donde fabricantes y partners trabajen sincronizados”.