DEBATES ciberseguridadTIC

La ciberseguridad ya no falla por falta de alertas sino de contexto

XM Cyber

IR A PÁGINA SIGUIENTE

XM Cyber

La ciberseguridad ya no falla por falta de alertas sino de contexto

La ciberseguridad vive una paradoja incómoda. Nunca hemos tenido tantas alertas... ni tan poco contexto. Las organizaciones nunca han invertido tanto en herramientas, monitorización y capacidades de detección. Los SOC reciben millones de eventos al día, los cuadros de mando se llenan de indicadores y los parches críticos se multiplican. El problema ya no es ver más, es entender mejor. No se trata de contar vulnerabilidades, sino de identificar qué combinación de fallos abre una puerta real hacia lo crítico.

Rosalía Arroyo

Las grandes brechas recientes no se han producido por falta de herramientas, sino por rutas invisibles: credenciales olvidadas, permisos excesivos, integraciones heredadas, terceros insuficientemente controlados. El atacante no derriba el muro; encuentra el hueco.

Con este telón de fondo, responsables de seguridad de distintos sectores debatieron en un almuerzo ejecutivo impulsado por XM Cyber sobre

una cuestión central: cómo pasar del ruido a la priorización basada en riesgo real. Porque quizá la madurez ya no se mida por cuántas alertas gestionas, sino por cuántos caminos de ataque eres capaz de cerrar antes de que alguien los recorra.

Del volumen de alertas al contexto real: el reto de entender el riesgo

La conversación arrancó con una reflexión que, más que teórica, era fruto de experiencia acumulada. Durante años, la seguridad se ha medido por acumulación. Más herramientas, más controles, más alertas. La lógica parecía sólida: cuantos más sensores, más visibilidad. Sin embargo, esa ecuación empieza a mostrar sus límites cuando el volumen de información supera la capacidad real de interpretación.

Daniel Damas, Head of IT Assurance en Nationale-Nederlanden, lo describió como una evolución casi inevitable. En una primera fase, el objetivo era disponer de "todas las herramientas top", pero con el tiempo "empezamos a preguntarnos qué hacemos con toda esta información". El foco dejó de estar en sumar tecnología y se centró en hacerla gestionable para quien la analiza a diario.

> "El reto ya no es el volumen de eventos, sino convertirlos en análisis útil para quien está detrás del monitor"

Daniel Damas,
Head of IT Assurance de **Nationale-Nederlanden España**

En ese tránsito, la inteligencia artificial ha jugado un papel relevante, aunque —como matizó Damas— no es una novedad reciente. "La hemos estado usando desde el principio de los tiempos", recordaba, en referencia a los motores de correlación que ya permitían agrupar eventos y reducir falsos positivos. La diferencia, aseguraba, no es tanto la existencia de la IA como su capacidad para profundizar en patrones de comportamiento y ofrecer una lectura más contextualizada de lo que ocurre.

Desde Mapfre, Enrique Turrillo, subdirector de Protección del Dato e IA Responsable, introdujo un matiz distinto. El problema ya no es disponer de modelos predictivos sofisticados; el debate gira en torno a la confianza: hasta qué punto estamos dispuestos a aceptar que una máquina interprete mejor que nosotros determinados patrones de riesgo. "Siempre va a quedar la sospecha de si el resultado que me ha dado la máquina es mejor que lo que yo habría interpretado", aseguró durante el debate.

Jesús García, CISO de Banco Santander, añadió otra pieza imprescindible: la calidad del contexto de negocio. Para él, la información que demos modelo "debe ser suficientemente buena y estar suficientemente clara para que el resultado sea bueno". Sin esa base, cualquier sofisticación analítica corre el riesgo de quedarse en una aproximación técnica desconectada de la realidad operativa.

Su intervención abrió una reflexión más amplia sobre la medición de la seguridad. “Tenemos muchos datos, muchas mediciones, muchos scores, pero no es tan fácil trasladar eso a un consejo”, admitió. A diferencia de las métricas financieras, donde los ratios están consolidados y comparables, la ciberseguridad sigue buscando una forma homogénea de expresar el riesgo en términos comprensibles para la alta dirección.

Desde Aenor, Joaquín Oriente, su responsable de soluciones TIC reforzó esa idea desde la óptica de la gestión formal del riesgo. No basta con inventariar activos ni con desplegar monitorización avanzada; es necesario ser capaces de explicar qué riesgo existe y cómo las acciones adoptadas lo reducen de manera tangible. “Si no somos capaces de hacerlo de una manera consistente, difícilmente va a existir ese diálogo” con negocio. Y en muchos casos, añadió, se identifican activos críticos, pero no se analizan con la misma profundidad “esos caminos que realmente son importantes entre ellos”.

Fue en ese punto cuando XM Cyber introdujo su enfoque, no tanto como ruptura, sino como respuesta a una inquietud compartida en la mesa.

> “Tenemos muchos datos, muchas mediciones, muchos scores, pero no es tan fácil trasladar eso a un consejo de direccción”
>
> **Jesús García,**
> CISO de **Banco Santander**

Santiago Álvarez, Country Manager en España, recogió un problema que —según señaló— escuchan de forma recurrente en organizaciones de distintos sectores: exceso de alertas, múltiples fuentes de datos desconectadas y ausencia de una visión unificada que permita entender qué podría ocurrir si varios elementos fallan de forma combinada. “Hay múltiples fuentes de datos disjuntas y no hay una visión unificada de qué es lo que puede pasar con toda esta información”, aseguraba el directivo.

La propuesta pasa por generar un entorno replicado —un “gemelo digital”— que permita analizar de forma continua los posibles caminos de ataque hacia los activos definidos como críticos. Más allá de la tecnología concreta, el mensaje que puso sobre la mesa fue otro: la necesidad de pasar de miles de hallazgos dispersos a un conjunto reducido de acciones que realmente tengan impacto en la reducción del riesgo.

Raúl Pérez, Tech Director de XM Cyber, llevó esa idea al terreno del reporte ejecutivo. Lo relevante no es solo cuántas vulnerabilidades se corrigen, sino cuánto riesgo se reduce y cómo se puede explicar esa reducción al consejo. La pregunta que, según indicó, suele plantear la dirección es directa y difícil de esquivar: si un atacante consigue entrar, ¿cuál es el impacto real en la operación?

El bloque no cerró con una conclusión simplista, sino con una constatación compartida: la acumu-

lación de datos no equivale automáticamente a comprensión. Sin un filtro claro basado en riesgo real y en impacto de negocio, el ruido seguirá creciendo. Y en ese ruido, lo verdaderamente crítico puede quedar diluido.

Entre el ruido y la incertidumbre: priorizar en entornos cada vez más complejos

Si el primer bloque puso el foco en la acumulación de información y la dificultad de interpretarla, la conversación dio un paso más: ¿qué preocupa más hoy, no detectar un ataque o no saber priorizar lo realmente crítico?

La respuesta, en la práctica, dejó claro que ambos riesgos conviven y se retroalimentan.

Ventura Morcillo, IT Infrastructure, Support and Cybersecurity Manager en la Universidad Nebrija, expuso una dificultad compartida por muchas organizaciones: cuando se pregunta "¿cómo estamos en ciberseguridad?", no siempre es posible responder con un indicador claro. Como reconoció, resulta complicado traducir la situación real a una cifra concreta, y la conversación suele centrarse más en las medidas adoptadas que en una visión precisa de la exposición.

En el entorno universitario, explicó, la gestión de identidades es especialmente compleja por el elevado y cambiante volumen de cuentas. Parte de ellas se mantienen activas por inercia histórica, lo que incrementa la superficie de exposición y el número de alertas.

Más allá del volumen visible, lo que más inquieta es "ese pequeño porcentaje que ni siquiera te aparece en el gráfico": lo que puede quedar oculto bajo el ruido. Aunque la identidad concentra buena parte del riesgo, el endpoint y el perímetro siguen siendo vectores a vigilar. Y el phishing continúa siendo un desafío estructural. "¿Cómo puedes luchar contra eso?", se preguntaba, subrayando que no se trata solo de tecnología, sino también de comportamiento y contexto.

En ese punto, Joaquín Oriente introdujo una lectura más amplia. Estamos, en su opinión, en un escenario incómodo: una herencia tecnológica considerable, una digitalización acelerada y una cultura de seguridad que todavía no está plenamente interiorizada. Comparó la situación con la educación vial: hoy nadie discute el cinturón de seguridad o el semáforo en rojo,

"Muchas veces identificamos activos críticos, pero no analizamos suficientemente esos caminos que realmente son importantes entre ellos"

Joaquín Oriente,
Responsable de Soluciones TIC de **Aenor**

pero en el ámbito digital esa conciencia colectiva aún no se ha consolidado.

Raúl Pérez añadió un matiz relevante: a diferencia del tráfico, donde las reglas son relativamente

"El problema no es lo que ves en el gráfico; es ese pequeño porcentaje que ni siquiera aparece"

Ventura Morcillo , IT Infrastructure, Support and Cybersecurity Manager de **Universidad Nebrija**

estables, en el mundo digital "te intentan engañar todos los días". Los atacantes no solo buscan vulnerabilidades técnicas; buscan momentos de distracción, presión o cansancio. No es casualidad —apuntó— que muchas campañas se lancen en viernes por la tarde o en periodos de menor supervisión.

Daniel Damas lo expresó con franqueza desde la experiencia aseguradora: el negocio quiere vender, acelerar, salir a mercado. "Es bastante difícil balancear entre salgo rápido y salgo seguro". El apetito de riesgo nunca es cero, y la función de seguridad tiende a percibirlo más alto de lo que negocio considera asumible.

En ese contexto, la concienciación aparece como una herramienta necesaria, aunque no definitiva. Damas compartió una experiencia interna especialmente ilustrativa: una simulación de ransomware en un momento crítico del mes, bloqueando equipos y mostrando un mensaje de ataque durante unos minutos. El impacto fue inmediato. El ratio de clic en campañas de phishing descendió de forma significativa tras el ejercicio. Sin embargo, también dejó claro que el efecto no es permanente: "esto es una curva". Entra personal nuevo, se pierde tensión, baja la guardia y los indicadores vuelven a subir.

Desde Mapfre, Enrique Turrillo aportó otra palanca estructural: vincular la ciberseguridad a la responsabilidad individual. Introducir un "score de ciberseguridad" en la evaluación anual —positivo o negativo— busca trasladar la idea de

La tecnología ayuda, pero el comportamiento sigue marcando la diferencia

que la seguridad no es solo responsabilidad del área técnica. "No es solo mi responsabilidad, sino es la responsabilidad de todos". También subrayó la importancia de asumir el riesgo asociado a proveedores: contratar implica asumir consecuencias.

Enlazando con el bloque anterior, la conversación volvió a una idea de fondo: la gestión del riesgo ya no puede basarse únicamente en desplegar más controles o en acumular herramientas. Se trata de priorizar, podar, eliminar lo innecesario y reducir superficie de exposición.

La tecnología puede ayudar a filtrar y contextualizar, pero el factor humano —fatiga, exceso de confianza, presión comercial— seguirá siendo una variable estructural. Y en esa intersección entre señal técnica y comportamiento organizativo es donde se juega, en gran medida, la efectividad real de la defensa.

Activo crítico vs. camino real: cuando el riesgo está en lo que conecta, no en lo que proteges

Si el debate había dejado claro que el problema no es únicamente el volumen de alertas, sino la capacidad de interpretarlas y priorizarlas, el siguiente paso fue casi inevitable: muchas organizaciones tienen identificados sus "activos críticos", pero ¿están igual de claros los caminos que podrían llevar a un atacante hasta ellos?

Daniel Damas reconoció que, en su caso, el análisis de exposición no es un concepto nuevo. "El tema de exposición ya lo teníamos muy visto", explicó, en parte por la presión regulatoria y por prácticas ya consolidadas en el sector financiero. La entrada en vigor de DORA ha obligado a estructurar esa visión con mayor formalidad, especialmente en lo que respecta a terceros y proveedores críticos.

La conversación se desplazó entonces hacia un terreno especialmente sensible: terceros y cadena de suministro. En un contexto de adquisiciones, integraciones y externalización de servicios, la pregunta dejó de ser teórica. ¿Cómo evaluar realmente la exposición cuando se incorpora una nueva compañía o se conecta un proveedor estratégico?

> "El respaldo en materia de seguridad se convierte en un criterio determinante en la elección de un proveedor"
>
> **Juan Miguel Gil,**
> IT Manager Spain Holding **ArcelorMittal**

Desde XM Cyber, Raúl Pérez defendió la necesidad de ir más allá del "checklist" declarativo. El clásico "tiene EDR, check... tiene firewall, check...", puede generar una sensación de cumplimiento formal, pero no necesariamente refleja la realidad operativa. En muchos casos, lo que se observa desde fuera —incluso con herramientas de rating externas— es solo la "punta del iceberg". El riesgo real puede estar en configuraciones internas, permisos heredados o credenciales mal gestionadas que no aparecen en un informe superficial.

Joaquín Oriente recogió esa incertidumbre como parte estructural del riesgo de terceros. La exposición es, muchas veces, "variable" y "oscura". Los estándares y regulaciones establecen una base mínima de higiene, pero el salto cualitativo llega cuando el proveedor es crítico. Ahí cobra sentido el "right to audit". Aunque sea una "foto estática", es preferible a no tener ninguna visibilidad.

Daniel Damas lo conectó directamente con DORA: si un proveedor es considerado crítico, el contrato debe contemplar que se le pueda auditar "al menos una vez al año", incluso a través de un tercero. Esa palanca regulatoria no existe en todos los sectores. Fuera del marco financiero, muchas organizaciones dependen más de la palanca comercial —el peso del cliente en el negocio del proveedor— para

exigir evidencias o elevar el nivel de control.

En paralelo, el debate añadió otra tensión de fondo: la minimización de datos frente a las necesidades reales de negocio. Enrique Turrillo reconoció que el principio de minimizar información compartida con terceros es deseable, pero choca con modelos donde el valor añadido depende precisamente del acceso a datos.

La conclusión fue pragmática: el riesgo no desaparece por decreto. Se gestiona, se reduce, se comparte.

Del SOC al consejo: alertas infinitas, cloud dinámico y la necesidad de decidir

La entrada de nuevos participantes permitió retomar la conversación desde otro ángulo, más pegado a la operación diaria y al impacto real en la toma de decisiones. La pregunta que sobrevoló el almuerzo volvió a formularse, esta vez con mayor concreción: ¿en qué momento dejamos de medir la seguridad por volumen y empezamos a medirla por comprensión real del riesgo?

Juan Miguel Gil, IT Manager Holdings Spain de ArcelorMittal, describió esa evolución como un proceso casi inevitable. En las primeras etapas de madurez, “parece que solo con saber qué es lo que detectaban unas alertas ya se sabía qué estaba pasando”. Tener visibilidad era, en sí mismo, una victoria. Sin embargo, la experiencia —propia o cercana— cambia la perspectiva. Cuando se vive un incidente o se observa uno en el entorno, la pregunta deja de ser cuántas alertas se generan y pasa a ser otra: cuál es la dimensión real del problema, cómo reaccionar y, sobre todo, cómo priorizar.

Esa madurez tiene además una consecuencia que trasciende lo técnico. La seguridad no es un elemento accesorio sino que forma parte estructural de la toma de decisiones. “No puedes dedicarte solo a analizar funcionalmente o económicamente un proveedor”, apuntó. El respaldo en materia de seguridad se convierte en un criterio determinante, y en determinados contextos puede llegar a ser “lo más importante”.

Carlos García, Cybersecurity Operations Manager del sector banca, añadió otra variable clave: el cambio en la naturaleza de las señales. En entornos cloud cada acción genera telemetría —accesos, modificaciones, interacciones— y el volumen es mucho más granular que en el modelo tradicional on-premise. Asegurando que el reto no es solo la cantidad, sino el criterio, dejó claro que decidir qué investigar, qué escalar y qué cerrar como falso positivo se complica en arquitecturas elásticas y cambiantes.

> “El problema no es el volumen de alertas, sino saber cuáles merecen realmente nuestra atención”

Carlos García,
Cybersecurity Operations Manager **sector banca**

A esa presión técnica se suma la alta rotación en los puestos de análisis que dificulta acumular el contexto necesario para interpretar bien el riesgo. En ese escenario, la inteligencia artificial aparece como apoyo, pero no como solución cerrada. La definió como “arma de doble filo”: útil para el triaje inicial, pero todavía con interrogantes.

A partir de ahí, la conversación volvió a la cuestión estructural: la diferencia entre gestionar señales aisladas y tener una visión contextualizada. XM Cyber defendió que el verdadero filtro no debería basarse únicamente en el volumen de alertas ni en el patrón individual, sino en el riesgo real de compromiso a través de caminos de ataque concretos.

La discusión se volvió especialmente interesante cuando Carlos García planteó una objeción técnica lógica: ¿qué precisión puede tener una “foto” de la infraestructura en entornos cloud que cambian constantemente? Por la mañana hay un número de instancias; por la tarde puede haber cien más. ¿Cómo se mantiene actualizada esa visión?

La respuesta apuntó a dos elementos. Por un lado, la actualización frecuente del modelo mediante APIs y procesos automatizados. Por otro

> “El reto no es tener el modelo, sino confiar en que el resultado es mejor que mi propia interpretación”
>
> **Enrique Turrillo,**
> Subdirector Protección del Dato e IA Responsable **Mapfre**

—y quizá más relevante—, una observación sobre incidentes híbridos: en muchos casos, el problema no reside tanto en la configuración formal del entorno cloud, que suele estar correctamente securizado, sino en la gestión de credenciales o en integraciones con entornos on-premise.

La metáfora volvió a aparecer, esta vez con mayor fuerza: puedes tener “un castillo estupendo”, pero si las llaves están expuestas en otro sitio, el riesgo no está en el muro, sino en el acceso. Un usuario con privilegios excesivos, una clave que no caduca, una credencial reutilizada, pueden convertirse en el puente entre un equipo comprometido y una base de datos crítica en la nube.

El debate avanzó entonces hacia la priorización práctica. ¿Cómo decidir entre miles de vulnerabilidades publicadas cada mes? Desde XM Cyber se defendió que el enfoque pasa por correlacionar vulnerabilidades, configuraciones y permisos con rutas reales hacia activos críticos. No se trata de parchear todo de inmediato —algo operativamente inviable— sino de identificar ese pequeño porcentaje que, combinado con otros elementos, puede abrir una puerta real.

En ese sentido, el concepto que más resonó fue el de ponerse “en el lado del atacante”. Joaquín Oriente lo verbalizó de forma directa: la cuestión es hasta qué punto ese mapa de exposición intersecta con el comportamiento habitual o esperado de un adversario. Ver vulnerabilidades es una cosa; entender cómo se combinan para al-

> “No se trata de cuántas vulnerabilidades tienes, sino de qué caminos reales existen hacia lo crítico”

Santiago Álvarez de Cienfuegos,
Country Manager Spain de **XM Cyber**

canzar un objetivo concreto es otra muy distinta.

Raúl Pérez lo explicó desde otra perspectiva: los muros tecnológicos —EDR, XDR y sucesivas capas de control— no han eliminado el problema. Lo han desplazado. Los atacantes no siempre intentan derribar el muro frontalmente; lo examinan, lo miran “al trasluz” y buscan los pequeños agujeros que dejan configuraciones imperfectas, credenciales olvidadas o permisos excesivos.

Frente a un red team tradicional, limitado en tiempo y alcance, la propuesta es automatizar esa búsqueda de rutas posibles de forma continua. No sustituir necesariamente los ejercicios puntuales, sino complementar la visión con un análisis constante de cómo se podrían encadenar fallos aparentemente menores.

La clave, tal y como se fue asentando en la mesa, no está en eliminar el ruido —porque el ruido seguirá creciendo— sino en introducir un criterio de priorización basado en impacto real. Solo así puede pasarse de la fatiga operativa a una gestión más estratégica del riesgo, capaz de traducirse en decisiones comprensibles para negocio.

Eficiencia, fricciones internas y definición de lo crítico

El tramo final del almuerzo abordó una cuestión inevitable cada vez que se introduce una nueva tecnología en seguridad: ¿estamos ante una capa adicional que se suma a la complejidad existente o ante un enfoque que permite simplificar?

La pregunta fue directa. Si se adopta una solución como la planteada, ¿sustituye al red team? ¿Permite retirar herramientas? ¿O simplemente se añade a un stack ya de por sí saturado?

Santiago Álvarez respondió sin rodeos: el objetivo no es añadir ruido, sino optimizar. En su planteamiento, sí es posible reducir parte del esfuerzo dedicado a escaneos masivos de vulnerabilidades o a determinados ejercicios puntuales de red team, y redirigir presupuesto y recursos hacia acciones más concretas y priorizadas. No se trata de prescindir de equipos, sino de “liberar ancho de banda”. Si un equipo tiene 50.000 tareas abiertas, pero solo cinco de ellas son realmente críticas, la diferencia en términos de eficiencia puede ser sustancial.

Más interesante aún fue la reflexión sobre lo que ocurre cuando se presentan los resultados. Según explicó Raúl Pérez, en los primeros clientes hubo incluso tensiones internas. Cuando los informes mostraban credenciales con privilegios elevados en máquinas concretas o configuraciones que incumplían políticas internas, aparecían nombres propios. En algún caso, tras un incidente grave, el responsable llegó a preguntar literalmente quién había dejado esas credenciales ex-

puestas. La herramienta, más que una auditoría externa, actuaba como un espejo interno.

Esa dimensión organizativa no es menor. No se trata solo de identificar un riesgo técnico, sino de gestionar el impacto que esa identificación tiene en dinámicas internas, responsabilidades y cultura de cumplimiento.

Carlos García introdujo entonces una cuestión clave desde el lado del cliente: el modelo parte de que la organización defina cuáles son sus "joyas de la corona". Pero ¿hasta qué punto esa identificación es siempre clara? En infraestructuras grandes y complejas puede haber resistencia —por motivos políticos o de responsabilidad— o simplemente desconocimiento de la interdependencia real entre sistemas.

La respuesta fue pragmática. En sectores regulados como el financiero, ese ejercicio ya está avanzado por exigencias como DORA. La identificación de funciones críticas y servicios esenciales forma parte del marco normativo. En otros contextos, sin embargo, el patrón suele repetirse: datos de clientes, sistemas transaccionales, nómina, logística, propiedad intelectual. "El 80% de activos críticos son muy parecidos", se apuntó en la mesa. A partir de ahí, cada organización puede afinar según su modelo de negocio.

> "El análisis de causa raíz permite ver qué vulnerabilidades se repiten y por qué"
>
> **Raúl Pérez,**
> Tech Director **XM Cyber**

Ese debate derivó en un uso especialmente ilustrativo: la simulación de escenarios concretos. ¿Qué ocurriría si un atacante comprometiera el equipo del presidente, el financiero o un perfil con privilegios elevados? ¿Hasta dónde podría llegar desde ahí? Este tipo de ejercicio no se limita a enumerar vulnerabilidades, sino que construye una narrativa de impacto que resulta más comprensible para la alta dirección.

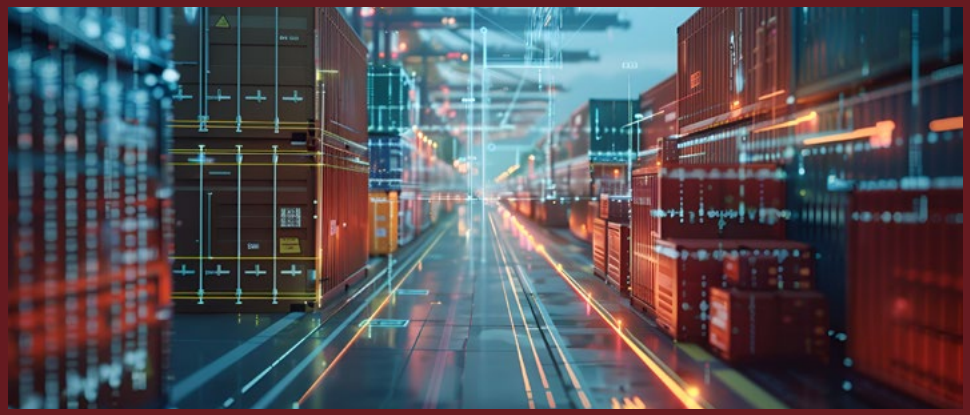
Enrique Turrillo añadió un matiz relevante en términos de priorización: la sensibilidad de la información. No todas las cuentas cloud tienen el mismo impacto. ¿Es posible ponderar el riesgo en función del volumen o criticidad del dataset asociado? La respuesta fue que el modelo puede configurarse para dar mayor peso a determinados grupos o cuentas con información especialmente sensible. La priorización no es solo técnica; también es contextual.

Más allá del detalle concreto, lo que quedó sobre la mesa fue una tensión constante entre automatización y criterio humano.

La diferencia entre gestionar miles de hallazgos y gestionar riesgo real no está en la cantidad de datos disponibles, sino en la capacidad de identificar qué caminos deben cerrarse antes de que alguien los recorra. Y esa capacidad no depende únicamente de la tecnología, sino de cómo la organización integra esa visión en su gobierno, su cultura y su diálogo con negocio.

XM Cyber

XM Cyber: del listado de vulnerabilidades al mapa real del atacante



XM Cyber plantea un cambio de enfoque en la gestión del riesgo de ciberseguridad. Parte de una idea sencilla: las organizaciones ya conocen sus vulnerabilidades, pero no siempre entienden cómo pueden combinarse para crear un camino real hacia sus activos críticos.

En lugar de centrarse en el inventario aislado de CVE o en el volumen de alertas, su modelo analiza cómo distintas debilidades —configuraciones incorrectas, credenciales expuestas, permisos excesivos o integraciones heredadas— pueden encadenarse y permitir a un atacante avanzar dentro del entorno. El objetivo no es parchear todo, sino identificar qué combinaciones de fallos generan un riesgo efectivo de compromiso.

Para ello, la compañía construye un "gemelo digital" de la infraestructura, tanto en entornos on-premise como en cloud e híbridos. A partir de la telemetría disponible, genera una réplica lógica sobre la que simula de forma continua posibles rutas de ataque. No analiza el código de las aplicaciones, sino el entorno que las sostiene: sistemas operativos, relaciones de identidad, privilegios, configuraciones y credenciales.

Uno de los elementos diferenciales es su capacidad para ofrecer una visión holística e híbrida. El modelo tiene en cuenta las interdependencias entre entornos locales y cloud, identificando cómo una brecha en un equipo interno o una credencial mal gestionada puede convertirse en un puente hacia recursos críticos en la nube. El foco no está únicamente en la protección del activo final, sino en los caminos que conducen hasta él.

Este enfoque permite reducir miles de hallazgos técnicos a un conjunto limitado de puntos de intervención prioritarios. En lugar de abordar indiscriminadamente todo el backlog de vulnerabilidades, la plataforma identifica aquellas que forman parte de rutas viables de compromiso y prioriza su remediación en función del impacto real.

Desde el punto de vista operativo, la solución no solo detecta riesgos, sino que propone acciones concretas para mitigarlos, ofreciendo distintas alternativas de remediación adaptadas al contexto del cliente. Esto facilita la toma de decisiones y optimiza el uso de recursos técnicos.

En el plano ejecutivo, el valor se traduce en una métrica más comprensible: no cuántas vulnerabilidades existen, sino hasta dónde podría llegar un atacante y cómo se reduce ese recorrido tras aplicar medidas correctivas.