DEBATES CiberseguridadTIC



Nunca hubo tanta información... ni tanta necesidad de decidir qué es prioritario

XM Cyber

IR A PÁGINA SIGUIENTE

XM Cyber

Nunca hubo tanta información... ni tanta necesidad de decidir qué es prioritario

La superficie de ataque no deja de crecer. Las organizaciones generan cada día miles de alertas, descubren nuevas vulnerabilidades y despliegan más herramientas de seguridad que nunca. Sin embargo, esa mayor capacidad de detección no siempre se traduce en una mejor protección. Al contrario, el exceso de información se ha convertido en uno de los principales desafíos para los equipos de ciberseguridad, obligados a distinguir qué riesgos pueden comprometer realmente el negocio y cuáles pueden esperar.

Rosalía Arroyo



Con ese punto de partida, Ciberseguridad TIC reunió en Barcelona a responsables de ciberseguridad de organizaciones públicas y privadas en el almuerzo ejecutivo “Nunca hemos tenido tantas alertas... ni tan claro qué es prioritario”, celebrado con el patrocinio de XM Cyber. La compañía, especializada en gestión continua de la exposición al riesgo (Continuous Exposure Management), plantea un enfoque que va más allá de la tradicional gestión de vulnerabilidades: identificar los caminos que podría recorrer un atacante para alcanzar los activos críticos y ayudar a priorizar aquellas acciones que realmente reducen el riesgo.



> “Ya no podemos gestionar la seguridad a partir de vulnerabilidades o alertas; tenemos que hacerlo desde las amenazas que realmente comprometen los servicios”

Alejo Riera,
CISO, **Agencia de Ciberseguretat de Catalunya**

Durante el encuentro, representantes de la Agencia de Ciberseguretat de Catalunya, Nestlé España, Lidl, Eurofragance y el Ayuntamiento de Barcelona debatieron sobre la evolución de los centros de operaciones de seguridad, el papel de la inteligencia artificial en la priorización de amenazas, la dificultad de medir el riesgo real y los retos culturales que acompañarán a la automatización de la ciberseguridad.

Del volumen de alertas a la gestión del riesgo: cuando ver ya no es suficiente

Durante años, los equipos de ciberseguridad han medido su eficacia por el número de alertas procesadas, las vulnerabilidades corregidas o los incidentes gestionados. Sin embargo, el crecimiento de la superficie de ataque, la complejidad de las infraestructuras y la falta de profesionales especializados están obligando a cambiar ese paradigma. Hoy el verdadero reto ya no consiste en detectar más amenazas, sino en comprender cuáles representan un riesgo real para el negocio y priorizar la respuesta. Ese cambio de mentalidad quedó patente desde el inicio del debate. Alejo Riera, CISO de la Agencia de Ciberseguretat de Catalunya, explicó que, en un entorno con cientos de miles de usuarios, una gran diversidad de sistemas y numerosos servicios esenciales para la ciudadanía, gestionar la seguridad únicamente a partir del volumen de alertas había dejado de ser sostenible. “Vimos claramente que ya no podíamos coordinarlo todo desde el punto de vista de vulnerabilidades o alertas”, recordó. A partir de ese momento, el foco pasó a situarse en las amenazas que realmente podían comprometer la prestación de los servicios y en priorizar la respuesta en función del riesgo.

En ese nuevo enfoque, el compromiso de credenciales ocupa un lugar destacado. Según explicó, buena parte de los incidentes que gestionan tienen su origen en el robo de identidades o en campañas de ingeniería social, por lo que la estrategia combina proyectos de modernización de la identidad digital, el despliegue progresivo de la autenticación multifactor y una creciente automatización de la respuesta. No obstante, insistió en que la tecnología, por sí sola, no basta. “Formación, formación, formación”, resumió, defendiendo que la concienciación continua y los simulacros de phishing siguen siendo imprescindibles en organizaciones con perfiles profesionales muy diversos y necesidades operativas muy distintas.

Ese cambio de enfoque también implica modificar la forma en que se mide la seguridad. David Esteban, CISO del Ayuntamiento de Barcelona,

lamentó que muchas organizaciones continúen evaluando el trabajo de los equipos de seguridad por el número de incidentes o de tickets gestionados porque miden más la actividad que la seguridad. En su opinión, la verdadera referencia debería ser el riesgo para el negocio y la probabilidad de que una amenaza llegue a materializarse, no el volumen de alertas que generan las herramientas.

Con ese objetivo, el Ayuntamiento está desarrollando un modelo en el que son las propias áreas de negocio las que identifican qué servicios consideran críticos y cuál sería el impacto de una interrupción. A partir de esa información, el equipo de ciberseguridad evalúa las amenazas y la probabilidad de que se produzcan. "Yo no defino qué es un servicio crítico; lo define el negocio", explicó Esteban, convencido de que la gestión del riesgo debe construirse desde el impacto real sobre la organización y no únicamente desde criterios técnicos.

Pese a ello, los responsables de seguridad reconocieron que los órganos de dirección siguen reclamando indicadores mucho más sencillos. "El volumen es interesante, pero no



"El cumplimiento normativo también puede ser una oportunidad para impulsar la cultura de ciberseguridad dentro de la organización"

Fermín Rodríguez,
Head of solutions&services, **Eurofragance**

te dice nada", decía Alejo Riera, recordando al mismo tiempo que un aumento del número de alertas suele ser consecuencia de una mayor capacidad de monitorización. "Quizá antes teníamos las mismas... y no lo veíamos", apuntó.

Esa dificultad para traducir el riesgo a indicadores comprensibles por el negocio también condiciona la forma en que se evalúa el trabajo de los equipos de seguridad. Josep Mulero, responsable de Ciberseguridad de Lidl, resumió esa paradoja con una frase que provocó el asentimiento del resto de participantes: "¿Cuál es mi trabajo? Que no pase nada". El problema, explicó, es que la prevención resulta difícil de medir cuando el principal indicador de éxito es precisamente la ausencia de incidentes.

Desde una perspectiva diferente, Fermín Rodríguez, Head of Solutions & Services de Eurofragance, explicó cómo el cumplimiento normativo se convirtió en un aliado para impulsar la cultura de la ciberseguridad dentro de la organización. La elaboración de un plan director permitió trasladar al comité de dirección no sólo los riesgos tecnológicos, sino también las implicaciones legales y de negocio asociadas a un incidente. "Al comité de dirección lo que le interesa es saber si su negocio está a salvo o no", afirmó, defendiendo la necesidad de traducir la información técnica a un lenguaje de riesgo y priorización, apoyándose en mapas de riesgo y en indicadores comprensibles para el negocio.

XM Cyber

Conocer los caminos del atacante: el reto ya no es proteger los activos, sino entender cómo se conectan

Si la primera conclusión del debate fue que la gestión de la seguridad debe centrarse en el riesgo y no en el volumen de alertas, la segunda apuntó a otro cambio de paradigma: identificar los activos críticos ya no es suficiente. El verdadero desafío consiste en comprender cómo podría llegar un atacante hasta ellos.

Karl Louis Alfaro, Cybersecurity SOC Architect de Nestlé España, reconoció que mantener un inventario completo de los activos sigue siendo una tarea compleja en grandes organizaciones. "Tener una CMDB en una gran organización es todo un reto", explicó. Aunque la compañía tiene identificadas las denominadas joyas de la corona, es decir, las aplicaciones y sistemas más importantes para el negocio, eso sólo representa una parte del problema, especialmente en entornos multicloud donde el crecimiento del *Shadow AI* añade nuevas capas de complejidad.

Una idea en la que coincidió Fermín Rodríguez. En su opinión, la protección ya no puede limitarse a blindar los activos más críticos, sino que debe tener en cuenta todas las interconexiones que existen entre ellos. "Los atacantes no van directos al activo crítico", recordó. En muchas ocasiones basta una identidad comprometida, una configuración incorrecta o un acceso insuficientemente protegido para iniciar un movimiento lateral que termine alcanzando sistemas mucho más sensibles. Por eso defendió la necesidad de disponer de la máxima visibilidad posible sobre esos "caminos críticos" y concentrar los esfuerzos allí donde realmente se puede interrumpir la progresión del atacante.

La irrupción de la inteligencia artificial añadió un nuevo elemento a esa ecuación. El crecimiento del denominado *Shadow AI* preocupa cada vez más a los responsables de seguridad, que ven cómo los usuarios incorporan herramientas de IA generativa a su trabajo diario al margen de los procesos corporativos.

En Nestlé, explicó Karl Louis Alfaro, la estrategia pasa por centralizar el uso de estas tecnologías a través de una "AI Platform centralizada y gobernada por un equipo". La organización ha definido políticas que impiden desplegar nuevos servicios de IA de forma autónoma y trabaja ahora en disponer de un inventario completo de todas las plataformas utilizadas por las distintas áreas de negocio.



> "Tenemos tal volumen de vulnerabilidades que el problema ya no es encontrarlas, sino decidir cuáles corregir primero"

Josep Mulero,
Responsible Cybersecurity, **Lidl**

La realidad de la Administración pública es diferente. Alejo Riera reconoció que resulta prácticamente imposible impedir el acceso a todas las herramientas de inteligencia artificial disponibles

en Internet. Por ello, la Agencia de Ciberseguretat de Catalunya ha optado por ofrecer una alternativa corporativa y limitar el riesgo asociado al uso de servicios externos.

La automatización acelera la respuesta, pero el criterio sigue siendo humano

La inteligencia artificial está llamada a transformar la forma en que operan los centros de operaciones de seguridad (SOC), pero los participantes coincidieron en que su principal aportación no será sustituir a los analistas, sino ayudarles a tomar mejores decisiones en un entorno donde el volumen y la velocidad de los ataques no dejan de crecer. El desafío ya no consiste únicamente en responder antes, sino en identificar con rapidez qué merece realmente una respuesta.

"No se ataca más rápido, se ataca más", resumió David Esteban, recordando que la capacidad humana ha llegado a un límite y la única forma de mantener el ritmo pasa por incorporar automatización e inteligencia artificial a las operaciones de seguridad. "Tenemos que decidir mejor y más rápido", afirmó, recordando que el tiempo que transcurre entre la publicación de una vulnerabilidad y la aparición de un exploit funcional se ha reducido drásticamente; "antes hablábamos de días o semanas; ahora hablamos de minutos". En ese contexto, defendió que la IA debe servir para eliminar ruido, descartar aquello que no requiere atención inmediata y ayudar a los analistas a concentrarse en los incidentes que realmente



"No sólo se ataca más rápido; se ataca más. Por eso necesitamos decidir mejor y mucho más deprisa"

David Esteban,
CISO, **Ayuntamiento de Barcelona**

comprometen al negocio. Alejo Riera compartió esa visión asegurando que, a su juicio, la IA todavía no está preparada para sustituir el criterio de un profesional experimentado: "responder mejor que una persona... todavía no; más rápido, sí", resumió. Donde realmente aportará valor, explicó, será en la capacidad de integrar grandes volúmenes de información procedente de múltiples fuentes y acelerar la respuesta operativa.

La conversación derivó entonces hacia una consecuencia menos evidente de esta automatización: el impacto sobre el desarrollo del talento. Riera mostró su preocupación por la desaparición progresiva de las tareas más básicas que tradicionalmente realizaban los analistas de primer nivel y que servían para adquirir experiencia antes de asumir mayores responsabilidades. Karl Louis Alfaro apuntó que ese problema no afectará únicamente a la ciberseguridad sino que "va a ser un problema de industria".

Santiago Álvarez recordó que las organizaciones se han estado apoyando en una amplia base de perfiles junior que, con el paso de los años, alimentaban los puestos de liderazgo. La automatización está estrechando esa base y amenaza

con romper el relevo generacional. “No tenemos un problema de inteligencia; tenemos un problema de tasa de reemplazo en el liderazgo”, afirmó. La pregunta, añadió, ya no es si la IA hará determinadas tareas mejor que las personas, sino “quién va a dirigir esto dentro de diez años”.

El mayor desafío no será la tecnología, sino el cambio cultural

La inteligencia artificial promete transformar la forma en que las organizaciones identifican riesgos, priorizan vulnerabilidades o responden a los incidentes. Sin embargo, cuando el debate se proyectó hacia el medio plazo, la mayoría de los participantes coincidió en que el principal reto no será tecnológico. La tecnología seguirá evolucionando y acabará convirtiéndose en un elemento común para todas las organizaciones; el verdadero desafío será aprender a convivir con ella y generar la confianza suficiente para incorporarla a la toma de decisiones.

Santiago Álvarez fue uno de los más claros al respecto. A su juicio, existe una cierta tendencia a atribuir a la inteligencia artificial capacidades que no siempre son necesarias. “Hay cosas que son deterministas, no hace falta IA”, afirmó, recordando que muchas tareas pueden resolverse mediante analítica tradicional. En su opinión, el acceso a la inteligencia artificial terminará por democratizarse, dejará de ser un elemento diferenciador, y lo realmente decisivo será la forma en que las personas aprendan a relacionarse con esas herramientas y, al mismo tiempo, mantengan su capacidad para trabajar y comunicarse entre ellas; “El reto, para mí, es cultural”, aseguró.

Alejo Riera llevó esa reflexión al terreno de la Administración pública. Más allá de la capacidad tecnológica, planteó cómo reaccionarán los ciudadanos cuando determinadas gestiones sean atendidas directamente por agentes de inteligencia artificial. “Imagínate que la administración pública ya no te contesta un funcionario, sino una IA”, planteó. Habrá quien valore la rapidez y la disponibilidad permanente del servicio, mientras que otros seguirán prefiriendo la atención personal. A su juicio, la aceptación de estos modelos dependerá tanto de factores culturales como tecnológicos.

Karl Louis Alfaro introdujo un criterio más pragmático. Desde su punto de vista, el éxito de un agente de IA debería medirse por el resultado obtenido y no por quién presta finalmente el servicio. “Si realmente ha resuelto tu consulta, tu problema, es un caso de éxito”, resumió.



> “Identificar las joyas de la corona ya no basta; el verdadero reto es conocer los caminos que llevan hasta ellas”
>
> **Karl Louis Alfaro,**
> Cybersecurity SOC Architect, **Nestle España**

Esa idea fue matizada por Fermín Rodríguez, quien recordó que las expectativas de los usuarios no



> “El objetivo no es corregir todas las vulnerabilidades, sino impedir que un atacante alcance los activos críticos”
>
> **Santiago Álvarez,** director general de **XM Cyber**

siempre son las mismas. Mientras algunas personas solo buscan completar un trámite en el menor tiempo posible, otras siguen valorando el componente humano que ofrece la atención presencial. “Hay muchas variedades”, señaló, apuntando que la transformación digital deberá adaptarse también a esa diversidad de perfiles y necesidades.

“La cultura cambia más despacio”, comentó el CISO de la Agencia de Ciberseguretat de Catalunya, asegurando que el verdadero desafío de los próximos años no será tecnológico, sino cultural. Igual que ocurrió con otros procesos de transformación digital, será necesario un periodo de adaptación en el que convivirán distintas formas de relacionarse con la inteligencia artificial, añadió, asegurando que “habrá un impasse que será nuestro, no de la IA. Será cultural puramente, no tecnológico”. En su opinión, la tecnología evolucionará mucho más rápido que la capacidad de las organizaciones y de los propios usuarios para incorporarla con total naturalidad a su día a día.

La visibilidad como punto de partida para reducir la exposición

Como cierre del debate, la conversación volvió a una idea que había estado presente desde el principio: cuando una organización gestiona miles de vulnerabilidades, configuraciones y activos, el problema ya no es encontrar riesgos, sino saber cuáles conviene corregir primero. En ese contexto, los participantes coincidieron en que las nuevas plataformas de gestión de la exposición están ayudando a cambiar la forma de priorizar.

La última parte del debate permitió conocer la experiencia práctica de dos de las organizaciones presentes que ya utilizan XM Cyber. Josep Mulero, responsable de Ciberseguridad de Lidl, explicó que la necesidad surgió al comprobar que gestionar miles de vulnerabilidades ya no era el principal problema; “tienes tal volumen de vulnerabilidades… que tienes que decidir cómo priorizarla”, aseguró. En su opinión, el valor de la plataforma reside en que va más allá de los tradicionales escáneres de vulnerabilidades y ayuda a comprender cómo podría avanzar un atacante dentro del entorno corporativo. “No sólo tiene los CVE, sino que te muestra otras cosas que utilizaría un atacante: unas credenciales almacenadas, una mala configuración o cómo hacer movimientos laterales”. Esa visión contextualizada del riesgo, concluyó, permite concentrar los esfuerzos donde realmente tienen un mayor impacto.

Como ejemplo, recordó uno de los primeros hallazgos tras el despliegue de la plataforma. La herramienta detectó una comunicación entre dos sistemas que, según las políticas de segmentación definidas por la organización, no debería existir. “Fuimos al equipo de redes y les dijimos:



'XM Cyber dice que desde aquí se puede llegar aquí'. Lo revisaron y había una regla mal puesta". Se trataba de un problema sencillo de corregir, pero difícil de detectar mediante un escáner convencional, ya que no se trataba de una vulnerabilidad, sino de una combinación de configuraciones que abría un posible camino de ataque.

Más allá de ese caso concreto, Josep Mulero destacó la utilidad de disponer en una misma plataforma de información relacionada con configuraciones de Active Directory, cuentas obsoletas, políticas de contraseñas o credenciales sin uso. El valor, insistió, no está en generar más información, sino en ayudar a establecer prioridades. Al final, añadió, el objetivo no es evitar cualquier incidente —algo prácticamente imposible—, sino dificultar al máximo el trabajo del atacante; "si alguien entra, que lo tenga difícil para hacerte daño". De ahí que definiera este tipo de soluciones como una "herramienta de higiene": mantener el entorno limpio reduce las posibilidades de que un incidente termine propagándose.

Otro aspecto que destacó fue la facilidad de implantación. Frente a otros proyectos de seguridad con un impacto importante sobre la operación, explicó que el despliegue resultó prácticamente transparente para los usuarios. "Fue sorprendentemente silencioso; ningún impacto", señaló, un aspecto especialmente relevante en un entorno donde determinadas aplicaciones críticas requieren mantener un rendimiento constante.

> La inteligencia artificial acelerará la respuesta, pero el criterio para decidir qué es realmente importante seguirá siendo humano

Santiago Álvarez coincidió en que la principal dificultad rara vez es tecnológica. "El elefante en la habitación es que hay que desplegar el sensor", reconoció. Sin embargo, precisó que el verdadero obstáculo suele ser organizativo. Mientras algunas compañías son capaces de desplegar miles de agentes en pocos días, en otras los procesos internos, las aprobaciones o la propia burocracia ralentizan considerablemente el proyecto. "No es un problema tecnológico, es un problema de proceso", insistió

Una vez superada esa fase, explicó, la principal ventaja es disponer de una visibilidad mucho más amplia sobre el entorno. La plataforma permite detectar desde configuraciones incorrectas hasta equipos donde determinadas herramientas de protección han dejado de funcionar. "Cuando está desplegado, lo ves todo", afirmó, comparándolo con un estadio completamente a oscuras en el que alguien enciende un mechero y, de repente, resulta posible localizar cualquier anomalía. Esa visión global, añadió, permite medir de forma consistente la evolución del riesgo y comprobar si las acciones emprendidas realmente mejoran la postura de seguridad de la organización.

En definitiva, la conversación terminó reforzando una de las principales conclusiones del encuentro: en un escenario donde las amenazas siguen creciendo y los recursos continúan siendo limitados, la diferencia ya no la marca quién detecta más vulnerabilidades, sino quién es capaz de comprender mejor su impacto sobre el negocio y actuar primero sobre aquello que realmente reduce la exposición al riesgo.

XM Cyber

Del inventario de vulnerabilidades al mapa real del riesgo



Antes de iniciar el debate, Santiago Álvarez, director general de XM Cyber, explicó el enfoque de la compañía, basado en un planteamiento diferente al de las herramientas tradicionales de gestión de vulnerabilidades. En lugar de generar nuevas listas de incidencias, el objetivo es identificar qué riesgos son realmente explotables y qué acciones tendrán un mayor impacto para impedir que un atacante alcance los activos más críticos de la organización.

Para ello, la plataforma XM Cyber construye un gemelo digital del entorno desde el punto de vista de la ciberseguridad y simula los posibles caminos que podría seguir un atacante desde un punto de entrada hasta los sistemas más sensibles. “Es el mapa del atacante; saber lo que puede pasar antes de que pase”, resumió Álvarez. A diferencia de un análisis basado únicamente en vulnerabilidades individuales, este enfoque permite comprender cómo pueden combinarse configuraciones, permisos, credenciales o fallos de seguridad para facilitar un movimiento lateral dentro de la infraestructura.

Ese análisis pone de manifiesto que muchos de esos caminos terminan convergiendo en un número reducido de elementos. La plataforma identifica esos “puntos de estrangulamiento”, como los denomina la compañía, donde una única acción correctiva puede bloquear múltiples rutas de ataque. “Si quiero parar al atacante, sólo toco esos puntos y el atacante no progresa”, explicó.

Según Álvarez, esa visión permite reducir significativamente el esfuerzo dedicado a la corrección de vulnerabilidades. “Con el 2 % de las vulnerabilidades eres capaz de matar el riesgo”, aseguró, en referencia a la capacidad de priorizar aquellas acciones que realmente reducen la exposición de la organización, frente a un modelo basado en corregir el mayor número posible de incidencias.