# DEBATES ciberseguridad TIC

# Pentesting en transformación: cómo escalar, cerrar vulnerabilidades y convivir con la IA sin frenar al negocio

Synack



IR A PÁGINA SIGUIENTE

# Pentesting en transformación: cómo escalar, cerrar vulnerabilidades y convivir con la IA sin frenar al negocio

**La superficie de ataque crece, los entornos se diversifican y la presión regulatoria aumenta. Los equipos de ciberseguridad deben demostrar que son capaces de reducir el riesgo real mientras lidian con sistemas heredados, ciclos de desarrollo acelerados y un volumen creciente de aplicaciones y servicios expuestos. En este contexto, el pentesting ya no es una prueba anual, sino una pieza crítica para mantener el control operativo, entender la verdadera exposición y anticiparse al atacante.**

Rosalía Arroyo

Con este escenario se celebró el almuerzo-debate organizado por Ciberseguridad TIC en colaboración con Synack, en el que responsables de seguridad de distintos sectores compartieron sus retos y experiencias alrededor del pentesting moderno. La conversación abordó

desde la dificultad de escalar las pruebas en organizaciones en constante crecimiento, hasta la gestión efectiva de vulnerabilidades, la confianza en equipos externos y el papel de la inteligencia artificial en el futuro inmediato de las pruebas de intrusión.

Participaron perfiles con realidades diversas, pero unidos por un denominador común: la necesidad de contar con evidencias explotables, rapidez, continuidad y servicios capaces de integrarse en el desarrollo y en la operación sin generar parones ni riesgos adicionales. El resultado fue una conversación sincera, técnica y muy práctica sobre lo que realmente funciona en el pentesting actual.

Entre los asistentes se encontraban Alejandro Velilla, CTO de Embou +ORANGE; Carlos Bereciartua, Manager Ciber de SABSEG Group; Israel Díaz, CISO de ASITUR; Álvaro Ontanón, CIO de Merlin Properties; Sergio Rubio, Account Manager Central & Southern Europe de Synack; y Thomas Hornung, Arquitecto de la solución de Synack; cuyas experiencias y aproximaciones configuraron una visión completa del estado del pentesting.

## Escalar la seguridad en entornos que crecen más rápido que los equipos

La primera pregunta del debate se centró en un problema recurrente: cómo escalar las pruebas de seguridad cuando la superficie de ataque crece más rápido que la capacidad del equipo para absorber cambios. Un reto especialmente evidente en organizaciones que trabajan mediante adquisiciones o que conviven con múltiples stacks tecnológicos.

Alejandro Velilla fue directo: “Es muy complicado, la verdad. Sobre todo porque ya no solo es que crezca la superficie de ataque, sino que cada nuevo entorno es diferente”. En entornos donde conviven sistemas heredados, plataformas dispares y procesos distintos, cada incorporación añade nuevas capas de complejidad. “Estás dimensionado para un cierto rango, y cuando amplías puede ser una ampliación muy relevante”, resumió.

Carlos Bereciartua compartió una realidad muy similar. SABSEG Group ha integrado más de 20 corredurías en poco tiempo. “El equipo inicial estaría dimensionado para una, dos, tres, cuatro... pero no crece tan rápido como la adquisición de 22 corredurías”. Aunque operan bajo un mismo modelo de negocio, cada empresa tiene niveles de madurez y profesionalización diferentes. “Parten de cero en algunas cosas”, admitió, lo que obliga a estandarizar controles mientras se gestiona la integración tecnológica. Ambos coincidieron en que el verdadero problema no son las herramientas, sino la capa-

> “Una vez que haces un pentesting, se empiezan a ver realmente los riesgos”
>
> **Carlos Bereciartua,**
> Manager Ciber de **SABSEG Group**

cidad de asimilación. La seguridad crece más lento que el negocio y ese desfase condiciona la eficacia de cualquier prueba.

## Cerrar vulnerabilidades: cuando la presión del tiempo manda

La segunda cuestión abordó otro desafío universal: cómo garantizar el seguimiento y cierre efectivo de vulnerabilidades, evitando que se conviertan en un ciclo interminable o en un requisito imposible de cumplir.

Carlos Bereciartua explicó cómo la relación con las aseguradoras influye en la gestión de vulnerabilidades. Comentó que, en muchos procesos de suscripción, se realizan análisis externos y que determinados hallazgos pueden condicionar la contratación o las condiciones de la póliza. En algunos casos, las aseguradoras conceden plazos para corregirlas y, si pasado ese tiempo persisten y se produce un incidente, pueden aplicarse limitaciones o restricciones en la cobertura. “Al final, hay vulnerabilidades que las aseguradoras consideran críticas, y si no se resuelven, pueden afectar a la póliza”, apuntó.

> “Para mí es esencial que una vulnerabilidad pueda demostrarse; si no es explotable, difícilmente puedo priorizarla”
>
> **Israel Díaz,** CISO de **ASITUR**

Alejandro Velilla explicó que la gestión de vulnerabilidades requiere equilibrio y realismo, especialmente cuando llegan en volúmenes elevados. Subrayó que las vulnerabilidades realmente críticas deben abordarse con rapidez, mientras que las de menor impacto se analizan caso por caso para determinar si su explotación es viable o si representan un riesgo real. Puso como ejemplo algunas detecciones que, pese a aparecer en herramientas automáticas, “en la práctica no tienen recorrido ni aplican a nuestro contexto”, lo que obliga a priorizar con criterio para no desviar recursos hacia hallazgos irrelevantes.

Para Israel Díaz toda vulnerabilidad debe venir acompañada de evidencia explotable. “Para mí es esencial que una vulnerabilidad pueda demostrarse; si no es explotable, difícilmente puedo priorizarla”, explicó. La falta de pruebas no solo complica la gestión técnica, sino también la documentación necesaria para justificar decisiones. “Si no hay evidencias suficientes, resulta muy difícil sostener cualquier análisis o recomendación”, señaló.

Álvaro Ontanón amplió el debate subrayando la necesidad de priorizar en función del impacto real. “Esto es el cuento de nunca acabar. A mí que me diga las vulnerabilidades que tiene este sistema me parece fenomenal, pero... ¿es explotable? ¿Dónde está? ¿Con qué conecta?”.

La conversación dejó claro que la gestión de vulnerabilidades no puede basarse únicamente

en volúmenes o listados: requiere foco, priorización y evidencia.

## ¿Un pentesting al año es suficiente en 2025?

La tercera pregunta abrió un debate que, pese a ser habitual, sigue generando visiones muy distintas según el sector, el nivel de madurez y la presión regulatoria de cada organización: ¿cuántas veces debe someterse una empresa a un pentesting para tener garantías reales de seguridad? La práctica tradicional —una prueba anual, generalmente ligada a auditorías o renovaciones de certificaciones— convive hoy con entornos mucho más dinámicos, donde los cambios continuos, la exposición creciente y la proliferación de servicios conectados cuestionan si esa frecuencia es realmente suficiente.

Recordando que, por cumplimiento, "tenemos que hacer bastantes más de uno al año", aseguró Alejandro Velilla que su organización realiza pruebas trimestrales en servicios expuestos y pruebas adicionales dependiendo de los proyectos. Para clientes más pequeños, sin embargo, lo habitual es "uno al año o cada semestre".

> "Las vulnerabilidades críticas tienen que cerrarse rápido; ahí no hay vuelta de hoja"
>
> **Alejandro Velilla,**
> CTO de **Embou +ORANGE**

En opinión de Carlos Bereciartua los pentesting recurrentes son un ejercicio de madurez: "Hay empresas pequeñas muy tecnológicas y maduras... y otras que no han hecho nunca un pentesting". En estos casos, empezar por uno es ya un avance: "Una vez que haces uno, empiezan a ver".

Israel Díaz aportó una visión más rígida por exigencias regulatorias. En su organización, el pentesting es anual, con pruebas adicionales por proyecto. Pero subrayó que el verdadero problema está en la remediación y en la tecnología obsoleta: "Te encuentras con Windows 2012... o incluso más antiguos". Esto obliga a aplicar workarounds complejos y, en su experiencia, puede generar tensiones con las aseguradoras: "A las aseguradoras no les suele encajar que se mantengan versiones tan antiguas".

Todos coincidieron en que la frecuencia depende del tamaño, madurez, criticidad del negocio y exposición real.

## Confiar en equipos externos: cómo se construye esa relación

El debate avanzó hacia una cuestión más psicológica que técnica: el grado de confianza que una organización está dispuesta a conceder cuando permite que un equipo externo acceda a sus sistemas para realizar pruebas de intrusión. Carlos Bereciartua lo resumió con naturalidad: "Vas poco a poco generando confianza. Pero lo primero es tirar de lo conocido". Admitió que

> “Cuando el riesgo se multiplique de forma exponencial, será imposible controlarlo sin tecnología”
>
> **Álvaro Ontanón,**
> CIO de **Merlin Properties**

escuchar que un proveedor trabaja con cientos o miles de especialistas puede impresionar: “Asusta… porque este tipo de perfiles están en otro lado, están en dos sitios”. Ese recelo no solo tiene que ver con la intrusión en sí, sino con la seguridad de que lo reportado es legítimo: “¿Quién te dice que te cuentan un agujero y no es así?”.

> El ataque real nunca es estático, por eso el test debe ser continuo

Para Alejandro Velilla la preocupación principal tiene que ver con el comportamiento y la integridad de quien accede a los sistemas: “Es más relevante incluso que el nivel de habilidad”. Cuando se abre acceso a datos, perímetros o configuraciones, la confianza se vuelve esencial: “Hay cosas que están cerradas y las tienes que abrir para que lo revisen”.

A continuación, los portavoces de Synack ofrecieron una visión complementaria desde el lado del proveedor, explicando —de forma general— por qué este tipo de servicios requiere mecanismos sólidos de seguridad y supervisión. Sergio Rubio recordó que la confianza se construye “mediante procesos rigurosos de validación y control”, y subrayó que los testers trabajan siempre dentro de un marco de reglas de juego, metodologías auditables y restricciones configuradas por el propio cliente. Thomas Hornung, por su parte reforzó esta idea recordando que la actividad se realiza en entornos monitorizados y con trazabilidad completa, de modo que cualquier acción queda registrada.

En conjunto, el bloque dejó claro que la confianza en un equipo externo no es un punto de partida, sino un proceso que se construye con transparencia, visibilidad, reglas claras y garantías de control por ambas partes.

## IA y pentesting: lo que ya está pasando y lo que viene

Una de las reflexiones más amplias del debate surgió al preguntarse: ¿cómo evolucionará el pentesting con la llegada de la IA, la automatización y los modelos colaborativos?

Explicó Israel Díaz que ya usan IA en varios procesos, especialmente en triaje: “Con la IA algo que tarda cuatro o cinco días te lleva un par de horas”. También la emplea en el SOC para automatizar tareas repetitivas, activar acciones o asistir en análisis complejos. Pero subrayó que

la IA debe estar entrenada, ser propietaria y utilizarse con criterio.

La conversación abordó también la necesidad de aprender a atacarla: “Estamos preparando una metodología para ver cómo hacemos pruebas de inyecciones de prompts”, señaló el CISO de ASITUR, admitiendo que este tipo de pruebas son un territorio nuevo.

Álvaro Ontanón ofreció una perspectiva más macro. Recordó que la IA ya está transformando infraestructuras enteras y que apenas hemos visto “1/10 de lo que tenemos en el pipeline” en España. Su impacto llegará a OT, IoT y cualquier dispositivo conectado: “Vamos a abrir un campo enorme en ciberseguridad y pentesting”.

Por su parte, Alejandro Velilla destacó que la IA permitirá optimizar recursos y agilizar procesos, sobre todo en áreas muy operativas. Explicó que ya se utiliza en tareas como la gestión de backups, el análisis en sistemas SIEM o la detección perimetral, automatizando funciones que antes requerían un esfuerzo manual considerable. Según señaló, estas capacidades permiten redistribuir mejor el trabajo y dedicar más tiempo a tareas de mayor valor para la organización.

> “Nunca explotamos más de lo necesario: el objetivo es demostrar la vulnerabilidad, no romper nada”
>
> **Sergio Rubio,**
> Account Manager Central & Southern Europe de **Synack**

Israel Díaz introdujo también un efecto colateral: el péndulo laboral. La IA elimina perfiles junior, cambia roles y obliga a recolocar talento: “Pensar que la IA viene a sustituir a la gente es un error: viene a complementar”.

Añadió Carlos Bereciartua el impacto que está teniendo la inteligencia artificial en el fraude: “Ya hacen el doble engaño con la IA para romper el doble check”, explicó, refiriéndose al vishing avanzado contra empleados.

Quedó claro que la IA acelerará el pentesting, ampliará su alcance y obligará a repensar la monitorización, los controles y la propia lógica defensiva.

## Integrar el pentesting en DevSecOps: ¿beneficio o fricción?

El debate se acercó al terreno del desarrollo preguntando por el valor de integrar el pentesting dentro del ciclo de DevSecOps, así como por la “carta a los Reyes Magos” de un pentesting ideal.

Alejandro Velilla fue muy claro: hoy por hoy, para ellos es más un problema que una ventaja. Explicó que muchos entornos de desarrollo están externalizados y se levantan aplicaciones temporales para pruebas. El resultado es que “el 90% de las vulnerabilidades bajas son falsos positivos o entornos que ni siquiera están abiertos al mundo”. Esto genera esfuerzos innecesarios y obliga a “deshacer lo hecho para volver a montarlo”.

## Con Synack cada vulnerabilidad pasa por tres verificaciones antes de llegar al cliente

En su lista ideal, incluyó tres prioridades: “Cero falsos positivos, rapidez y cero impacto en producción”.

Carlos Bereciartua coincidió en que el entorno de producción es donde realmente se validan los modelos. Aunque no desarrollan internamente, están comenzando a entrenar modelos de IA y consideran imprescindible integrar esas capacidades en los entornos reales: “Hasta que no lo veamos en producción, no podremos evaluar su impacto de manera completa”.

A partir de su experiencia, también apuntó qué necesitaría de un pentesting ideal: claridad en los informes, evidencias que realmente ayuden a priorizar, y un encaje más ágil con los requisitos de auditoría y de terceros. Para él, una de las grandes dificultades no está solo en encontrar vulnerabilidades, sino en contar con documentación que permita justificar decisiones ante revisiones internas, externas o regulatorias sin que suponga una carga adicional para el equipo. En su visión, un servicio de pentesting óptimo debería ofrecer información precisa, contextualizada y fácilmente trasladable a procesos de cumplimiento.

Destacó Israel Díaz la necesidad de pentesters muy formados, con certificaciones y con la capacidad de pensar de forma no lineal, algo que considera esencial para reproducir el enfoque real de un atacante. Subrayó también la importancia del reporte final: “Si el reporte es una castaña, luego no vale para ningún lado”, señaló, insistiendo en que la calidad de la documentación es clave para poder tomar decisiones y defenderlas ante auditorías o equipos internos.

En su experiencia, una parte relevante del riesgo no está únicamente en el código desarrollado internamente, sino en el uso de librerías y componentes de terceros que se integran de forma casi automática en los proyectos: “Los desarrolladores meten cosas que ni saben de dónde vienen”. Para él, este es uno de los puntos más críticos y menos atendidos en muchos procesos de seguridad.

A partir de esa experiencia, Israel Díaz expuso también lo que, en su opinión, debería ofrecer un pentesting ideal: evidencias claras y explota-

“El análisis de causa raíz permite ver qué vulnerabilidades se repiten y por qué”

**Thomas Hornung,**
Arquitecto de la solución de **Synack**

bles, agilidad para ejecutar pruebas sin generar interrupciones innecesarias, y la capacidad de identificar no solo fallos aislados, sino patrones y debilidades estructurales que puedan estar repitiéndose. Considera igualmente imprescindible que el servicio sea capaz de detectar problemas derivados de bibliotecas externas, porque “en muchos casos, ahí es donde se esconden los verdaderos puntos ciegos”.

Álvaro Ontanón añadió que desarrollo y ciberseguridad son, por naturaleza, disciplinas llamadas a friccionar. “Lo primero que te dicen es: quítame el antivirus, quítame el firewall… y ya funciona”, bromeó, señalando que esta tensión forma parte inherente del ciclo de vida del software. En su visión, la IA puede ayudar a que los desarrolladores integren criterios de seguridad de manera más orgánica, desde fases tempranas del proceso. También apuntó sus propios deseos para un pentesting ideal: informes realmente accionables, capaces de priorizar en función del impacto dentro del negocio, y pruebas que puedan ejecutarse sin interrumpir servicios críticos pero que, al mismo tiempo, revelen con claridad si una vulnerabilidad es relevante o no en su contexto. Para él, uno de los grandes retos sigue siendo disponer de resultados que traduzcan lo encontrado en decisiones prácticas y asumibles por equipos con recursos limitados

## Los cinco pilares de la propuesta de Synack

- **Selección extrema del talento ofensivo**
- **Trazabilidad total y control absoluto**
- **Modelo “stop and report” para evitar impactos**
- **Validación estricta y retests ilimitados**
- **Plataforma como motor de inteligencia: análisis de causa raíz**

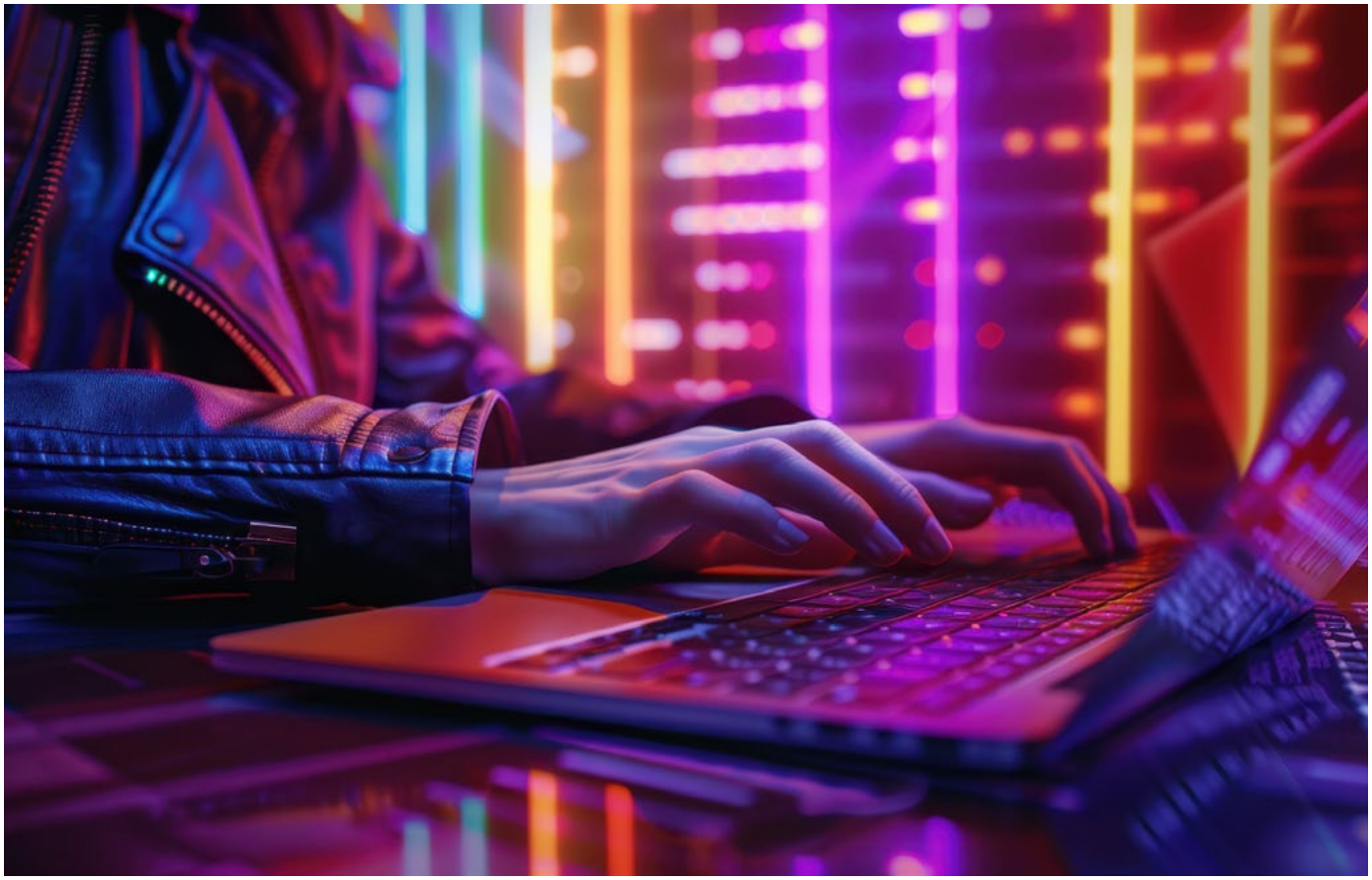
## Conclusión

El debate dejó claro que el pentesting vive un momento de transición. La superficie crece, los equipos no escalan al mismo ritmo, la presión de las auditorías y aseguradoras se intensifica y la IA acelera tanto el ataque como la defensa. En este contexto, los modelos tradicionales —puntuales, PDF en mano, sin continuidad— se quedan cortos frente a la necesidad de evidencia real, rapidez, priorización y visibilidad.

Los CISOs presentes coincidieron en que el pentesting del futuro deberá ser continuo, integrado, basado en evidencia explotable y capaz de convivir con el desarrollo sin paralizarlo. La IA jugará un papel decisivo, tanto para automatizar tareas como para abrir nuevas superficies de riesgo.

El almuerzo evidenció que estamos ante un escenario en el que la seguridad ya no puede ser un ejercicio anual, sino un proceso vivo, adaptativo y profundamente conectado con el negocio.

# Synack: “Si entregáramos ruido, estaríamos fuera al día siguiente”



**A lo largo del debate, los portavoces de Synack —Sergio Rubio y Thomas Hornung— fueron detallando cómo su modelo intenta dar respuesta a muchos de los desafíos que los CISOs habían mencionado: la necesidad de evidencias explotables, la trazabilidad completa, la reducción de falsos positivos o la continuidad sin impacto en producción. Este apartado reúne esas explicaciones dispersas del debate, estructurándolas para ofrecer una visión clara y coherente del enfoque de la compañía.**

Rosalía Arroyo

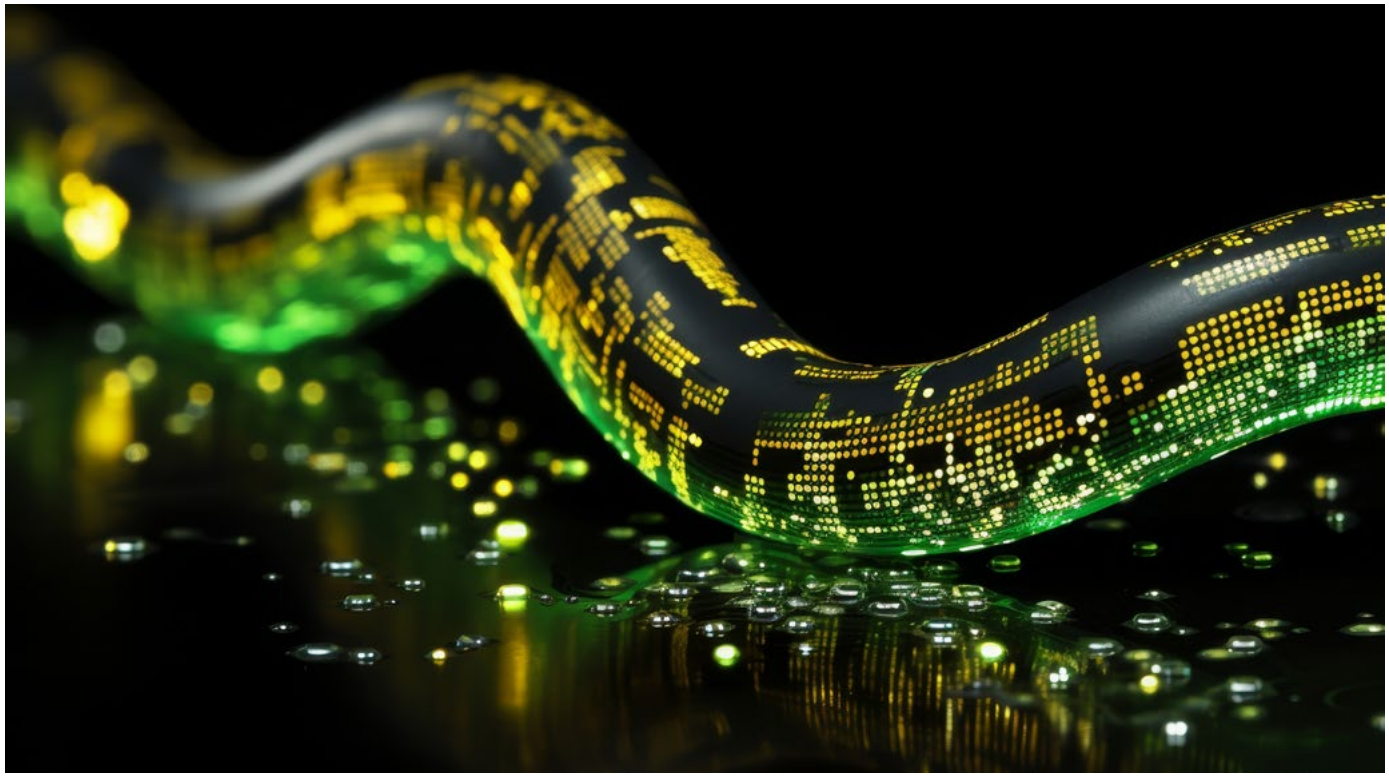
Synack explicó que su servicio combina un equipo global de hackers éticos cuidadosamente seleccionados —“solo alrededor del 8 % supera el proceso de entrada”, recordó Sergio— con una plataforma que centraliza toda la operación. Desde ella se controla cada acceso, cada acción y cada reporte, lo que permite una trazabilidad total: “Todo lo que hacen pasa por la plataforma; no pueden testear fuera de ella”, subrayó. Esto aporta al cliente visibilidad completa de logs, horas conectadas, retests realizados y cumplimiento de las reglas de juego.

Synack

Uno de los elementos diferenciales señalados durante el debate fue su enfoque de “stop and report”: toda vulnerabilidad se reporta en cuanto se confirma su explotación, pero sin ir más allá de lo necesario para evidenciarla. Sergio lo resumió así: “Nunca explotamos más de lo necesario; el objetivo es demostrarla, no romper nada”. Esta filosofía, añadieron, reduce riesgos en producción y permite priorizar sobre hechos, no sobre supuestos.

Antes de llegar al cliente, cada hallazgo pasa por un triaje interno realizado por el equipo de operaciones. “Es fundamental asegurar que lo que recibe el cliente es real, explotable y no ruido”, explicó Sergio. Solo entonces se publica en tiempo real en la plataforma, permitiendo actuar sin esperar al informe final. Desde ese momento, los equipos pueden parchear y solicitar retests tantas veces como necesiten: “El re-test es ilimitado mientras el contrato esté activo”.

Otro aspecto destacado fue la capacidad de la plataforma para integrarse con herramientas como ServiceNow u otros sistemas de ticketing. Esta integración evita a los equipos tener que



gestionar una plataforma adicional cuando ya disponen de flujos de trabajo consolidados.

Thomas añadió una capa más estratégica al destacar la importancia del análisis de causa raíz: “La plataforma permite ver patrones: qué equipos repiten las mismas vulnerabilidades o qué aplicaciones concentran más problemas”. Esto ayuda a las organizaciones a tomar decisiones estructurales —cambiar un framework, reforzar controles o revisar componentes— en lugar de limitarse a corregir hallazgos aislados.

Por último, los portavoces recordaron el historial de la compañía como garantía de solidez. Thomas fue directo: “Desde 2013 trabajamos para organizaciones muy sensibles. Si entregáramos ruido, no seguiríamos aquí”. Y mencionó ejemplos como grandes bancos españoles o incluso el Pentágono: “Si nos equivocamos, estamos fuera al día siguiente”, dijo, subrayando la importancia que dan al rigor metodológico.