

Cómo Iberia Cards utiliza Sara AI Pentesting para adelantarse a las amenazas modernas

Resumen ejecutivo

Para proteger su infraestructura de pagos y responder a las exigencias de un entorno financiero altamente regulado, Iberia Cards necesitaba un socio de seguridad ofensiva capaz de ofrecer una reducción real del riesgo junto con la trazabilidad regulatoria. Gracias a su colaboración con [Synack](#), el CISO José Manuel Rivera García dejó atrás los ejercicios de cumplimiento puntuales para adoptar un modelo de seguridad ofensiva y validación continuas basadas en inteligencia. Al combinar el [Synack Red Team](#) (SRT) con [Sara AI Pentesting](#), Iberia Cards creó un programa de pruebas que complementa la experiencia humana con una IA escalable que permite realizar validaciones frecuentes, mejorar la información destinada a la dirección y mantener una postura de seguridad adaptada al ritmo de las amenazas modernas.

El reto: infraestructura regulada y los límites de las pruebas puntuales

“Los problemas graves siempre están en la lógica de negocio”, afirma José Manuel Rivera García, CISO de Iberia Cards. “Siempre hay tiempo para mejorar el perímetro más adelante, pero si solo haces pruebas una vez al año, no estás encontrando lo que realmente importa.”

Para un Establecimiento Financiero de Crédito regulado por el Banco de España, la seguridad no puede limitarse a marcar una casilla de cumplimiento. Iberia Cards gestiona una infraestructura de pagos en la que los datos de los clientes son fundamentales para el negocio y la trazabilidad regulatoria es imprescindible. Las pruebas de penetración tradicionales, con proyectos de alcance fijo y entregables predeterminados, no estaban diseñadas para este tipo de entorno.



RETO

Como Establecimiento Financiero de Crédito regulado por el Banco de España, Iberia Cards opera bajo exigentes requisitos de cumplimiento mientras gestiona una infraestructura de pagos que no puede permitirse brechas en la cobertura de seguridad. Las pruebas de penetración tradicionales realizadas de forma puntual generaban una falsa sensación de seguridad, y un ejercicio anual dejaba largos periodos de exposición entre una evaluación y la siguiente. Además, los hallazgos genéricos de los escáneres automatizados no lograban detectar las vulnerabilidades de lógica de negocio que representan un riesgo real en un entorno financiero.

SOLUCIÓN

Iberia Cards se asoció con Synack para implementar un programa de seguridad ofensiva continua que combina el [Synack Red Team](#) para realizar evaluaciones profundas dirigidas por expertos humanos con [Sara AI Pentesting](#) para llevar a cabo validaciones frecuentes entre esos ciclos. Mediante un enfoque de caja gris con acceso autenticado, el programa va más allá del escaneo superficial para evaluar la lógica de negocio integrada en los servicios de pago orientados al cliente, las aplicaciones web asociadas y sus APIs, precisamente las áreas donde se encuentran las vulnerabilidades más graves.

Rivera García necesitaba un programa capaz de identificar riesgos reales, documentarlos de una forma que los reguladores pudieran seguir y repetir las pruebas con la frecuencia necesaria para mantenerse al ritmo de un panorama de amenazas que no espera a los ciclos de revisión anuales.

La creciente amenaza asociada a la IA hizo que esta necesidad fuera aún más urgente. Rivera García observó un cambio en el comportamiento de los atacantes: ataques de menor volumen, pero mucho mejor alineados con la lógica de negocio, a medida que los adversarios obtenían acceso a herramientas capaces de incorporar contexto específico de cada organización a las tareas de reconocimiento y explotación. Los escáneres de vulnerabilidades tradicionales estaban perdiendo relevancia frente a esta nueva clase de amenazas.

La solución: seguridad ofensiva continua

La relación de Rivera García con Synack comenzó antes de su llegada a Iberia Cards. Había trabajado por primera vez con la plataforma en RSI, el proveedor del sistema bancario central del Grupo Caja Rural, por lo que ya estaba convencido del modelo antes de incorporarse a Iberia Cards.

// Lo que hace que siga volviendo a Synack es la convergencia de tres aspectos que rara vez se encuentran juntos: profesionalidad, amplitud en la detección de vulnerabilidades y una verdadera profundidad en los hallazgos. //

RIVERA GARCÍA, CISO, IBERIA CARDS

En Iberia Cards, Rivera García centró el programa en los servicios de pago orientados al cliente y las aplicaciones web asociadas, tanto públicas como autenticadas, junto con sus APIs. Optó por un enfoque de caja gris que proporciona credenciales de usuario para que los investigadores pudieran ir más allá de la superficie expuesta y evaluar directamente la lógica de negocio autenticada.

RESULTADOS

- Identificación de vulnerabilidades de lógica de negocio de alto impacto que los escáneres automatizados no habían detectado.
- Conversión de hallazgos técnicos en evidencias documentadas y reproducibles para conversaciones con la dirección ejecutiva y el consejo de administración.
- Trazabilidad completa de las vulnerabilidades desde su descubrimiento hasta su corrección dentro de la [Synack Platform](#), cumpliendo los requisitos regulatorios del Banco de España.
- Incorporación de [Sara AI Pentesting](#) como una capa recurrente dentro del programa anual de seguridad, proporcionando una cadencia de pruebas entre las evaluaciones más profundas realizadas por el SRT.
- Creación de un modelo de validación continua de la seguridad que permite abordar simultáneamente la reducción del riesgo y el cumplimiento normativo.

“En algunos casos, los hallazgos confirmaron sospechas que ya tenía”, explica. “Pero el resultado más valioso no fue lo que encontraron, sino lo que aquello me permitió hacer con esa información. Por primera vez pude acudir a la alta dirección con un caso real, no con un escenario hipotético.”

El paso de la intuición técnica a hallazgos documentados y reproducibles cambió por completo la conversación con la dirección.

Pruebas a la velocidad de la IA

Cuando [Sara AI Pentesting](#) estuvo disponible, Rivera García se acercó a la solución con un escepticismo deliberado. “Mi punto de partida con cualquier herramienta de automatización es el escepticismo. He visto demasiadas soluciones que se quedan en la superficie.” Lo que le hizo cambiar de opinión no fue una demostración del producto, sino una conversación técnica con los equipos de producto e ingeniería de Synack sobre cómo se había desarrollado Sara, qué decisiones sustentaban su inteligencia y contexto, y cómo el proceso de triaje separa los hallazgos triviales de aquellos que representan un riesgo real.

Ejecutó Sara AI Pentesting sobre los mismos activos que anteriormente habían sido evaluados por investigadores humanos, creando deliberadamente un punto de comparación directo. Incluso en una configuración no autenticada, que por diseño limita la profundidad de las pruebas, los resultados aportaron valor. Su siguiente paso es ejecutar Sara AI Pentesting con credenciales, ofreciéndole el mismo punto de partida que al SRT, para evaluar todo el alcance de lo que puede llegar a identificar.

Su valoración de Sara AI Pentesting es precisa: “El verdadero factor diferenciador no es que sustituya al modelo basado en investigadores, sino que lo complementa. Permite realizar pruebas con mayor frecuencia, con un coste y un esfuerzo razonables.”

Para Iberia Cards, Sara AI Pentesting cubre una necesidad práctica dentro de su programa anual, manteniendo una cadencia funcional de pruebas entre las evaluaciones más profundas del SRT sin añadir costes ni carga operativa significativos.

Comunicar el riesgo a la dirección

Rivera García no habla con la alta dirección sobre el número de vulnerabilidades. Habla de riesgos documentados con un impacto empresarial medible. La [Synack Platform](#) proporciona la infraestructura de reporting y mantiene el seguimiento de las vulnerabilidades de forma transparente y auditable, desde el primer hallazgo hasta su corrección definitiva.

“Con Synack resuelvo dos problemas simultáneamente”, afirma. “Una reducción efectiva del riesgo, porque cada vulnerabilidad reportada tiene un impacto real. Y el cumplimiento regulatorio. La plataforma me permite mantener la trazabilidad que exige el regulador.”

La combinación de la Synack Platform y Sara AI Pentesting ofrece validación continua de la seguridad sin sacrificar las evidencias necesarias para demostrar el cumplimiento normativo. Este es el modelo que Rivera García recomienda a otros responsables de seguridad que están considerando PTaaS.

La ventaja de Synack

SUPERAR EL CUMPLIMIENTO BASADO EN PRUEBAS PUNTUALES

Con Synack, Iberia Cards pasó de evaluaciones anuales con un alcance fijo a un modelo de pruebas continuas centrado en las vulnerabilidades de lógica de negocio, la clase de hallazgos que más importan en una infraestructura financiera regulada.

ENCONTRAR LAS VULNERABILIDADES QUE REALMENTE IMPORTAN

La investigación dirigida por expertos humanos de Synack identifica hallazgos de alto impacto que los escáneres automatizados no detectan, proporcionando a los equipos de seguridad las evidencias documentadas necesarias para impulsar una corrección efectiva y alinear a la dirección ejecutiva.

ESCALAR CON SARA AI PENTESTING

Sara AI Pentesting amplía el alcance del programa al permitir validaciones frecuentes entre las evaluaciones profundas del SRT y ofrecer una mayor cobertura con un coste y una cadencia compatibles con las restricciones operativas reales.

Acerca de Iberia Cards

Iberia Cards es un Establecimiento Financiero de Crédito regulado por el Banco de España, con más de 20 años de experiencia. Como miembro del Grupo IAG, la compañía cuenta con Banco Santander como accionista, mientras que BBVA también actúa como distribuidor de sus tarjetas de crédito. Actualmente presta servicio a más de 200.000 clientes y emite tarjetas de marca compartida tanto para particulares como para empresas, vinculadas a los programas de fidelización Iberia Club y On Business. Desde 2023, ofrece una solución de “compra ahora y paga después” adaptada a empresas del sector de los viajes.

Su cartera de productos combina soluciones de pago flexibles con un ecosistema de fidelización basado en la acumulación y el canje de Avios, con el objetivo de mejorar la experiencia de viaje y generar valor a través del uso cotidiano de las tarjetas.

Visítanos en: www.iberia.com/es/en/iberiacards/.

Acerca de Synack

Synack ofrece validación continua de la seguridad a través de su plataforma Human + AI para pentesting continuo. Sara AI Pentesting, impulsada por Synack Autonomous Red Agent, combina IA agéntica con el Synack Red Team, la comunidad de investigadores de seguridad sometida al proceso de selección más riguroso del mundo, para ayudar a las organizaciones a reducir el riesgo de forma proactiva, mantener el cumplimiento normativo y adelantarse a las amenazas cibernéticas en constante evolución. Sara realiza a escala tareas de reconocimiento, mapeo de la superficie de ataque y validación inicial de exploits, mientras que los expertos humanos validan la explotabilidad en el mundo real y aportan la creatividad y el criterio que la automatización no puede replicar. Fundada por antiguos profesionales de la NSA, Synack ha hecho posibles cerca de 10 millones de horas de pruebas de seguridad para proteger activos críticos, desde sistemas financieros globales hasta redes del Departamento de Defensa de Estados Unidos. Synack fue reconocida por el GigaOm 2025 PTaaS Radar como Leader y Fast Mover, y recibió los Global InfoSec Awards como Market Leader in AI-Powered Cybersecurity y Trailblazer in PTaaS.

Más información en: www.synack.com.