CASO PRÁCTICO

Cómo Iberia Cards utiliza el pentesting de Sara AI para adelantarse a las amenazas actuales

Resumen ejecutivo

Para proteger su infraestructura de pagos y cumplir con las exigencias de un entorno financiero muy regulado, Iberia Cards necesitaba un socio de seguridad ofensiva que pudiera ofrecer una reducción real del riesgo junto con la trazabilidad regulatoria. Al asociarse con Synack, el CISO José Manuel Rivera García pasó de los ejercicios de cumplimiento puntuales a un modelo inteligente de seguridad ofensiva y validación continuas. Al combinar el Synack Red Team (SRT) con las pruebas de penetración de Sara AI, Iberia Cards creó un programa de pruebas que complementa la experiencia humana con una IA escalable que permite una validación frecuente, informes ejecutivos más sólidos y una postura de seguridad adaptada al ritmo de las amenazas actuales.

El reto: la 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 detectando lo que realmente importa».

Para una entidad de crédito que opera bajo la regulación del Banco de España, la seguridad no puede ser un mero trámite. 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 innegociable. Las pruebas de penetración tradicionales, con alcances fijos y resultados predeterminados, no estaban pensadas para ese tipo de entorno.

IBERIA CARDS

RETO

Como entidad financiera de crédito regulada por el Banco de España, Iberia Cards opera bajo exigentes requisitos de cumplimiento normativo al tiempo que gestiona una infraestructura de pagos que no puede permitirse brechas en la cobertura de seguridad. Las pruebas de penetración tradicionales, realizadas en un momento concreto, creaban una falsa sensación de seguridad, y al ser un ejercicio anual dejaban largos periodos de exposición entre una prueba y otra. Los resultados genéricos de los escáneres automatizados tampoco lograban detectar las vulnerabilidades de la lógica de negocio que suponen 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 evaluaciones exhaustivas dirigidas por personas— con Sara AI Pentesting —para validaciones frecuentes entre esos ciclos—. Mediante un enfoque de «caja gris» con acceso autenticado, el programa va más allá de los análisis superficiales para poner a prueba la lógica de negocio integrada en los servicios de pago orientados al cliente, las aplicaciones web asociadas y las API correspondientes, que son precisamente las áreas donde se esconden las vulnerabilidades graves.

Rivera García necesitaba un programa capaz de detectar riesgos reales, documentarlos de forma que los reguladores pudieran entenderlos y repetirlo con la frecuencia suficiente para seguir el ritmo de un panorama de amenazas que no espera a los ciclos de revisión anuales.

La amenaza emergente de la IA dejó aún más clara la urgencia. Rivera García observó un cambio en el comportamiento de los atacantes: los ataques de menor volumen se adaptaban cada vez mejor a la lógica empresarial, a medida que los adversarios conseguían acceso a herramientas capaces de añadir contexto específico de la organización al reconocimiento y la explotación. Los escáneres de vulnerabilidades tradicionales estaban perdiendo relevancia frente a esta nueva clase de amenaza.

La solución: seguridad ofensiva continua

La relación de Rivera García con Synack es anterior a Iberia Cards. Tras trabajar por primera vez con la plataforma mientras estaba en RSI, el proveedor del sistema bancario central del grupo Caja Rural, ya estaba convencido del modelo antes de llegar a Iberia Cards.

> "Lo que me hace volver una y otra vez a Synack es la convergencia de tres cosas que rara vez se encuentran juntas: profesionalidad, amplitud en la detección de vulnerabilidades y verdadera profundidad en los resultados."

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 API correspondientes. 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 probar directamente la lógica de negocio autenticada.

RESULTADOS

- Se detectaron vulnerabilidades de gran impacto en la lógica de negocio que los escáneres automatizados pasaban por alto
- Se convirtieron los hallazgos técnicos en pruebas documentadas y reproducibles para las conversaciones con la dirección y el consejo de administración
- Se mantuvo un seguimiento completo de las vulnerabilidades desde su detección hasta su corrección en la plataforma Synack, cumpliendo con los requisitos de cumplimiento normativo del Banco de España
- Se estableció «Sara AI Pentesting» como una capa recurrente en el programa de seguridad anual, cubriendo el intervalo entre los proyectos más exhaustivos de SRT
- Se creó un modelo de pruebas de validación de seguridad continuas que resuelve simultáneamente la reducción de riesgos y el cumplimiento normativo

«En algunos casos, los resultados confirmaron las sospechas que ya tenía», explica. «Pero lo más valioso no fue lo que encontraron, sino lo que pude 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 unos resultados documentados y reproducibles cambió por completo el tono de la conversación con los directivos.

Pruebas a la velocidad de la IA

Cuando Sara AI Pentesting salió al mercado, Rivera García lo abordó con un escepticismo deliberado. «Mi punto de partida con cualquier herramienta de automatización es el escepticismo. He visto demasiadas soluciones que se quedan en lo superficial». 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 se habían tomado en cuanto a su inteligencia y contexto, y cómo el triaje separa los hallazgos triviales de los que representan un riesgo real.

Probaron Sara AI Pentesting en los mismos activos que habían probado antes investigadores humanos, creando a propósito un punto de comparación directo. Incluso en una configuración sin autenticación —que limita la profundidad por diseño—, los resultados aportaron valor. Su siguiente paso es ejecutar Sara AI Pentesting con credenciales, dándole el mismo punto de partida que el SRT, para evaluar todo lo que puede detectar.

Su valoración de Sara AI Pentesting es precisa: «Lo que realmente lo diferencia no es que sustituya al modelo de investigador, sino que lo complementa. Permite realizar pruebas más frecuentes a un coste y con un esfuerzo razonables».

Para Iberia Cards, Sara AI Pentesting cubre una carencia práctica en su programa anual, al tiempo que mantiene una cadencia de pruebas funcional entre los proyectos más exhaustivos del SRT sin añadir costes significativos ni sobrecarga operativa.

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 medible en el negocio. La plataforma de Synack se encarga de la infraestructura de informes, lo que mantiene el seguimiento de las vulnerabilidades transparente y auditable desde el primer hallazgo hasta la corrección final.

«Con Synack resuelvo dos problemas a la vez», dice. «Una reducción efectiva del riesgo: cada vulnerabilidad notificada tiene un impacto real. Y el cumplimiento normativo. La plataforma me permite mantener la trazabilidad que exige el regulador».

La combinación de la plataforma de Synack y las pruebas de penetración con Sara AI ofrece una validación continua de la seguridad sin sacrificar las pruebas de cumplimiento normativo. Es el modelo al que apunta Rivera García cuando aconseja a otros responsables de seguridad que se plantean adoptar el modelo PTaaS.

La ventaja de Synack

MÁS ALLÁ DEL CUMPLIMIENTO PUNTUAL

Con Synack, Iberia Cards pasó de auditorías anuales de alcance fijo a un modelo de pruebas continuas que se centra en las vulnerabilidades de la lógica de negocio. El tipo de hallazgos que más importan en una infraestructura financiera regulada.

DETECTA LAS VULNERABILIDADES QUE REALMENTE IMPORTAN

La investigación dirigida por personas de Synack saca a la luz hallazgos de gran impacto que los escáneres automatizados pasan por alto, lo que proporciona a los equipos de seguridad las pruebas documentadas necesarias para impulsar medidas correctivas reales y conseguir el apoyo de la dirección.

ESCALA CON LAS PRUEBAS DE PENETRACIÓN DE SARA AI

Las pruebas de penetración de Sara AI amplían el alcance del programa al permitir una validación frecuente entre las intervenciones exhaustivas del SRT y ofrecer una mayor cobertura a un coste y con una cadencia que se ajustan a las limitaciones operativas reales.

Acerca de Iberia Cards

Iberia Cards es una entidad de crédito regulada por el Banco de España, con más de 20 años de experiencia. Como parte del Grupo IAG, la empresa cuenta con el respaldo del Banco Santander como accionista, y BBVA también actúa como distribuidor de sus tarjetas de crédito. Actualmente, con más de 200 000 clientes, Iberia Cards 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, paga después» diseñada específicamente para 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, cuyo objetivo es mejorar la experiencia de viaje y aportar valor a través del uso diario de la tarjeta.

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

Acerca de Synack

Synack ofrece validación de seguridad continua a través de su plataforma «Human + AI» para pruebas de penetración continuas. Sara AI Pentesting, impulsada por el Synack Autonomous Red Agent, combina la IA autónoma con el Synack Red Team —la comunidad de investigadores de seguridad más rigurosamente seleccionada del mundo— para ayudar a las organizaciones a reducir el riesgo de forma proactiva, cumplir con la normativa y adelantarse a las amenazas cibernéticas en constante evolución. Sara se encarga del reconocimiento, la cartografía de la superficie de ataque y la validación inicial de vulnerabilidades a gran escala, 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 agentes de la NSA, Synack ha facilitado casi 10 millones de horas de pruebas de seguridad para proteger activos críticos, desde sistemas financieros globales hasta las redes del Departamento de Defensa de EE. UU. Synack fue reconocida por el «2025 PTaaS Radar» de GigaOm como «Líder» y «Fast Mover», y recibió los premios Global InfoSec Awards en las categorías de «Líder de mercado en ciberseguridad impulsada por IA» y «Pionera en PTaaS».

Más información en www.synack.com

Synack