CASE STUDY

How Iberia Cards Uses Sara AI Pentesting to Stay Ahead of Modern Threats

Executive Summary

To secure payment infrastructure and meet the demands of a highly regulated financial environment, Iberia Cards needed an offensive security partner that could deliver real risk reduction alongside regulatory traceability. By partnering with Synack, CISO José Manuel Rivera García moved beyond point-in-time compliance exercises toward a model of continuous, intelligence-driven offensive security and validation. By combining the Synack Red Team (SRT) with Sara AI Pentesting, Iberia Cards built a testing program that complements human expertise with scalable AI that enables frequent validation, stronger executive reporting, and a security posture built for the pace of modern threats.

The Challenge: Regulated Infrastructure and the Limits of Point-in-Time Testing

"The serious problems are always in the business logic," says José Manuel Rivera García, CISO of Iberia Cards. "There's always time to improve the perimeter later, but if you're only testing once a year, you're not finding what matters."

For a Credit Financial Institution operating under Bank of Spain regulation, security cannot be a check-the-box exercise. Iberia Cards manages payment infrastructure where customer data is core to the business and regulatory traceability is non-negotiable. Traditional penetration testing with fixed-scope engagements and predetermined deliverables was not built for that type of environment.

CHALLENGE

As a Credit Financial Institution regulated by the Bank of Spain, Iberia Cards operates under demanding compliance requirements while managing payment infrastructure that cannot afford gaps in security coverage. Traditional point-in-time penetration testing created a false sense of security and a once a year annual exercise left long windows of exposure between engagements. The generic findings from automated scanners also failed to surface the business-logic vulnerabilities that represent real risk in a financial environment.

SOLUTION

Iberia Cards partnered with Synack to implement a continuous offensive security program combining the Synack Red Team for deep, human-led engagements with Sara AI Pentesting for frequent validation between those cycles. Using a grey-box approach with authenticated access, the program goes beyond surface-level scanning to test the business logic embedded in customer-facing payment services, associated web applications and associated APIs, the areas where serious vulnerabilities actually live.

Rivera García needed a program that could surface real risk, document it in a way regulators could follow, and repeat often enough to keep pace with a threat landscape that does not wait for annual review cycles.

The emerging AI threat made urgency even clearer. Rivera García observed a shift in attacker behavior: lower-volume attacks becoming much better aligned with business logic, as adversaries gained access to tools that could add organization-specific context to reconnaissance and exploitation. Traditional vulnerability scanners were losing relevance against this new class of threat.

The Solution: Continuous Offensive Security

Rivera García's relationship with Synack predates Iberia Cards. Having first worked with the platform at RSI, the core banking system provider for the Caja Rural group, he was already convinced of the model before he arrived.

> "What keeps bringing me back to Synack is the convergence of three things you rarely find together: professionalism, breadth in vulnerability discovery, and real depth in findings."
>
> RIVERA GARCÍA, CISO, IBERIA CARDS

At Iberia Cards, Rivera García focused the program on customer-facing payment services and associated web applications, both public and authenticated, along with their associated APIs. He opted for a grey-box approach that provides user credentials so researchers could move beyond the exposed surface and test authenticated business logic directly.

RESULTS

- Surfaced high-impact, business-logic vulnerabilities that automated scanners missed
- Turned technical findings into documented, reproducible evidence for executive and board-level conversations
- Maintained full vulnerability tracking from discovery through remediation in the Synack Platform, meeting the Bank of Spain's regulatory compliance requirements
- Established Sara AI Pentesting as a recurring layer in the annual security program, covering cadence between deeper SRT engagements
- Built a continuous security validation testing model that solves risk reduction and compliance simultaneously

"In some cases the findings confirmed suspicions I already had," he explains. "But the most valuable outcome wasn't what they found, it was what it allowed me to do with it. For the first time I could go to senior management with a real case, not a hypothetical scenario."

The shift from technical intuition to documented, reproducible findings changed the executive conversation entirely.

Testing at AI Speed

When Sara AI Pentesting became available, Rivera García approached it with deliberate skepticism. "My starting point with any automation tool is skepticism. I've seen too many solutions that stay on the surface." What changed his mind was not a product demo, but a technical conversation with Synack's product and engineering teams about how Sara was built, what decisions went into its intelligence and context, and how triage separates trivial findings from those representing real risk.

He ran Sara AI Pentesting on the same assets previously tested by human researchers, deliberately creating a direct point of comparison. Even in an unauthenticated configuration which limits depth by design, the results delivered value. His next step is running Sara AI Pentesting with credentials, giving it the same starting point as the SRT, to evaluate the full scope of what it can surface.

His assessment of Sara AI Pentesting is precise: "The real differentiator is not that it replaces the researcher model, but that it complements it. It enables more frequent testing at a reasonable cost and effort."

For Iberia Cards, Sara AI Pentesting fills a practical gap in their annual program while maintaining a functional testing cadence between deeper SRT engagements without adding significant cost or operational overhead.

Communicating Risk to Leadership

Rivera García does not talk to senior management about vulnerability counts. He talks about documented risk with measurable business impact. Synack's platform handles the reporting infrastructure, keeping vulnerability tracking transparent and auditable from first finding to final fix.

"With Synack I solve two problems simultaneously," he says. "Effective risk reduction, every vulnerability reported has real impact. And regulatory compliance. The platform allows me to maintain the traceability the regulator requires."

The combination of the Synack Platform and Sara AI Pentesting delivers continuous security validation without sacrificing compliance evidence. It is the model Rivera García points to when advising other security leaders considering PTaaS.

The Synack Advantage

MOVING BEYOND POINT-IN-TIME COMPLIANCE

With Synack, Iberia Cards moved from annual fixed-scope engagements to a continuous testing model that targets business logic vulnerabilities. The class of findings that matter most in regulated financial infrastructure.

FIND VULNERABILITIES THAT MATTER

Synack's human-led research surfaces high-impact findings that automated scanners miss, giving security teams the documented evidence needed to drive real remediation and executive leadership alignment.

SCALE WITH SARA AI PENTESTING

Sara AI Pentesting extends the program's reach by enabling frequent validation between deep SRT engagements and delivering more coverage at a cost and cadence that works within real operational constraints.

About Iberia Cards

Iberia Cards is a financial credit institution regulated by the Bank of Spain, with over 20 years of experience. A member of the IAG Group, the company is backed by Banco Santander as a shareholder, with BBVA also acting as a distributor of its credit cards. Currently serving more than 200,000 customers, Iberia Cards issues co-branded cards for both individuals and corporations, linked to the Iberia Club and On Business loyalty programs. Since 2023, it has offered a "buy now, pay later" solution tailored for businesses within the travel sector.

Its product portfolio combines flexible payment solutions with a loyalty ecosystem powered by Avios accumulation and redemption, aimed at enhancing the travel experience and delivering value through everyday card usage.

Visit us at www.iberia.com/es/en/iberiacards/.

About Synack

Synack delivers continuous security validation through its Human + AI platform for continuous pentesting. Sara AI Pentesting, powered by the Synack Autonomous Red Agent, combines agentic AI with the Synack Red Team—the world's most rigorously vetted community of security researchers—to help organizations proactively reduce risk, stay compliant, and stay ahead of evolving cyber threats. Sara handles reconnaissance, attack surface mapping, and initial exploit validation at scale, while human experts validate real-world exploitability and provide the creativity and judgement automation cannot replicate. Founded by former NSA operatives, Synack has enabled nearly 10 million hours of security testing to protect critical assets, from global financial systems to U.S. Defense Department networks. Synack was recognized by GigaOm's 2025 PTaaS Radar as both a Leader and Fast Mover, and received Global InfoSec Awards for Market Leader in AI-Powered Cybersecurity and Trailblazer in PTaaS.

Learn more at www.synack.com.