

Loyalty card for security: CherryChain's digital resilience

March 3, 2026

FBK's Center for Cybersecurity supported the company through a process of technical analysis and risk governance as part of InnovAction.

In December 2025, FBK's [Center for Cybersecurity](#) completed a major technical and strategic assessment to strengthen the service platform developed by [CherryChain](#) for industrial partners to manage end-customer data-sharing flows. By identifying and evaluating the business assets to be protected—such as services, customer data databases, and dedicated software—the company turned key focus areas into opportunities for improvement, ensuring strong protection of user data.

The project is part of EDIH SoE [InnovAction](#), an initiative within the European Digital Innovation Hubs network for technological innovation funded by the European Union (Next Generation EU). It also provided an opportunity for the Center for Cybersecurity and the Center for Digital Industry at **Fondazione Bruno Kessler** (FBK) to continue supporting Italian SMEs in their “Twin Transition.”

The work, carried out between July and December 2025, was conducted by researchers **Matteo Brosolo**, Umberto Morelli, and **Matteo Rizzi**, and included both technical verification of the application (Service 1) and the definition of a risk governance strategy (Service 2).

Thinking like an attacker: technical analysis

To test the effectiveness of the defenses, the researchers adopted the perspective of a potential external adversary (black-box approach). The analysis included:

- **Static Analysis:** Review of the Android mobile app code using tools such as JADX and MobSF.
- **Dynamic Analysis:** Verification of client- and server-side defenses under real-world usage scenarios.
- **API Stress Testing:** Assessment of the robustness of communication protocols and data exchange mechanisms.

After presenting the results, the team conducted a more in-depth code review with the development team (white-box approach) to define recommendations and improve the security posture in line with the Zero Trust paradigm, based on the principle of “never trust, always verify” for every user, device, or application attempting to access enterprise resources.

From vulnerabilities to mitigations

CherryChain responded promptly to the technical feedback, implementing an immediate remediation plan that significantly enhanced its security profile. Key actions included additional static and dynamic analysis of the application and verification of the web services it connects to.

Overall resilience has improved, and close attention remains on all assets identified as critical. For these, the working group recommended concrete measures that could be implemented in the future to further strengthen the long-term security of the solutions. As a result, a roadmap based on a multi-layered (defense-in-depth) strategy was defined, including adoption of the Zero Trust architecture and continuous monitoring through SIEM/UEBA platforms.

The importance of analyzing SMEs’ security posture

Initiatives such as InnovAction are vital to the national and local economic landscape. Micro, small, and medium-sized enterprises (SMEs) represent the backbone of Italy’s production system, yet they are often the most vulnerable due to a significant gap in internal cybersecurity expertise.

At the national level, protecting these organizations has become a collective security priority: the entry into force of the NIS2 Directive (implemented in Italy through Legislative Decree 138/2024) introduces strict risk governance requirements. At the local level, FBK’s Center for Cybersecurity acts as the central node of an innovation network aimed at making digital security accessible and sustainable for the region.

The “Test Before Invest” model, available in the catalogue [below](#) and offered by InnovAction, allows SMEs to test advanced technologies in a protected environment before full implementation, reducing investment-related risks. Analyzing security posture means not only “patching” identified issues, but aligning business management with leading international standards (such as ISO/IEC 27001), transforming cybersecurity from a cost center into a competitive advantage.

PERMALINK

<https://magazine.fbk.eu/en/news/loyalty-card-for-security-cherrychains-digital-resilience/>

TAGS

- #cherrychain
- #cybersecurity
- #digitalindustry
- #edih
- #EDIHSoE
- #innovaction
- #innovation
- #PMI

- #twin transition

AUTHORS

- Martina Cicaloni