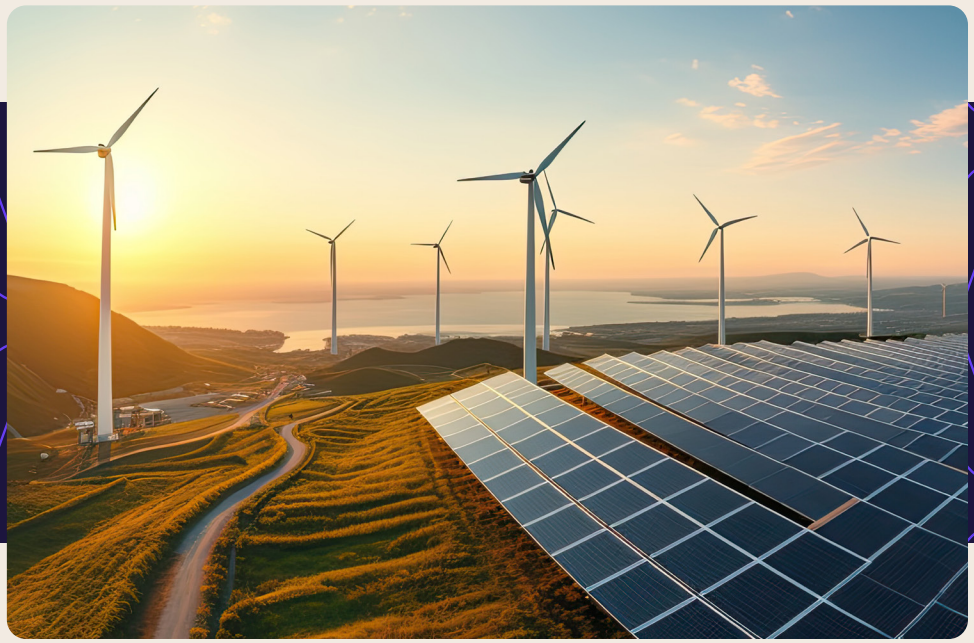
SecurityScorecard Solarig

CASE STUDY

IN PARTNERSHIP WITH 4BIZ» 4Business International

How Solarig consolidated continuous monitoring of its Digital Footprint and achieved a score of 100 with SecurityScorecard



USE CASE

Cyber Due Diligence

Third-Party Risk Management

Continuous Monitoring of the Digital Footprint

Executive Reporting and Standardization of Indicators

Solarig, a company in the energy sector focused on accelerating the energy transition, has integrated cybersecurity as a strategic pillar within its services and operations. To strengthen its own security posture and third-party risk management, the company adopted SecurityScorecard, transforming a manual and reactive process into a continuous monitoring model based on objective data.

THE RESULT: Greater agility in decision-making, standardization in supplier evaluation, and a score of 100 in its digital footprint in December 2025.

About Solarig

Solarig develops, finances, builds, and operates infrastructure for the energy transition. It currently manages more than 15 GW of photovoltaic assets and has a portfolio of energy projects exceeding 20 GW across 12 countries. The company drives global decarbonization in the regions where it operates through renewable energy and green gas solutions. Headquartered in Madrid, Spain, it has a strong presence in Europe, Central and South America, Japan, and Australia. Committed to innovation and sustainability, Solarig has a team of more than 1,500 professionals.

The Challenge

Solarig needed an objective and continuous assessment of its digital footprint and of its critical suppliers.

Before adopting SecurityScorecard, third-party risk management was mainly carried out through:

- Supplier questionnaires
- Document review (policies, certifications, and evidences)
- Spot checks

This approach presented clear limitations:

- Slow and poorly scalable processes
- Difficulty comparing suppliers in a consistent manner
- High reliance on self-reported information
- Lack of continuous monitoring after onboarding
- High manual effort for follow-up

The organization needed a more agile, comparable and evidence-based system.

The Solution

SecurityScorecard enabled Solarig to incorporate external, independent, and continuous monitoring of both its own digital footprint and of its suppliers.

Weekly Operational Use

The Cybersecurity team:

- Reviews Solarig's digital footprint score on a weekly basis
- Analyzes associated findings
- Follows up on corrective actions
- Monitors the portfolio of critical suppliers
- Receives automatic alerts when a supplier drops below a score of 80 or when a relevant change is detected

Before signing with a new supplier, Solarig analyzes it on the platform and, when necessary, generates a detailed report with findings and specific recommendations.

In addition, the company incorporated a contractual clause that requires maintaining a score above 85, establishing a minimum objective and measurable standard.

Results

Tangible Improvement in Security Posture

The most visible result was achieving a score of 100 in the digital footprint in December 2025, following an action plan initiated in April of the same year.

This achievement was made possible through coordinated collaboration between Cybersecurity, IT Systems, Networks, Development, and some external suppliers.

Continuous monitoring at scale

SecurityScorecard enabled Solarig to:

Visualize and compare multiple suppliers in a single dashboard

Detect score drops early

Prioritize actions based on risk level

Reduce manual effort in monitoring critical third parties

Faster and more informed decision-making

The platform made it possible to:

Accelerate go/no-go decisions with new suppliers

Prioritize remediation based on impact

Maintain data-driven discussions with suppliers

Standardize evaluation criteria

Greater operational efficiency

The use of alerts, structured reports, and historical tracking improved the efficiency of third-party evaluation and monitoring processes.

"We have managed to streamline decision-making, drive changes such as hosting migration, prioritize remediations, and gain efficiency. All of this has enabled us to achieve a score of 100 in a short period of time."

Paolo Vozzella
Chief Information Officer, Solarig

Standardization and operational change

SecurityScorecard has changed the way Solarig structures and shares cybersecurity information:

- Cybersecurity leads analysis and prioritization
- IT executes remediation actions
- Management receives a clear and traceable executive view
- Procurement integrates the score as a criterion in supplier selection

Internal communication is now based on comparable indicators: score, trends, and reports with historical tracking.

The approach has evolved toward a more proactive, data-driven model with smoother collaboration with suppliers.

FEATURES USED

Solarig primarily uses:

- **Reports:** for formal evaluation and internal communication
- **Alerts:** to react quickly to changes
- **History:** to measure progress and validate improvements
- **Portfolio:** to prioritize monitoring of critical suppliers

At this stage, the focus has been on strengthening both its own digital footprint and that of strategic suppliers.

Looking ahead

Solarig considers SecurityScorecard a key component for consolidating continuous monitoring of its digital footprint and strengthening its third-party risk management model. The company plans to expand the scope to more suppliers, maintain consistent evaluation criteria, and continue leveraging evidence-based reporting.