Schneider Electric Strengthens Partnership with SECLAB to Elevate Cybersecurity for Critical Industrial Environments

- An industrial response to escalating cyber threats and the emergence of AI models capable of industrializing vulnerability discovery
- OT protection built on a hardware barrier and fine-grained application-level filtering of exchanges among Schneider Electric PLCs, DCS, and SIS
- An integrated offering, deployed and maintained end to end by Schneider Electric's OT cybersecurity teams in Europe, with a new DIN-rail generation planned for 2027

Rueil-Malmaison, France, September 24, 2026 – Schneider Electric, a global energy technology leader, and SECLAB, a French provider of OT cybersecurity solutions, today announced an expanded collaboration to give industrial infrastructure a level of protection that goes beyond software-only defenses.

A Cyber Threat on a New Scale

The threat to industrial environments has reached a new level. According to the IBM X-Force Threat Intelligence Index, manufacturing accounted for 27.7% of the incidents X-Force observed in 2025, making it the most targeted sector for the fifth consecutive year, primarily through the exploitation of exposed systems. At the same time, attackers are no longer focused only on stealing data: some now target PLCs and industrial processes directly, seeking to shut down production lines, damage equipment, or endanger operator safety.

Artificial intelligence is accelerating this shift even further. Automated code analysis can now uncover previously unknown vulnerabilities at unprecedented scale and speed, while published flaws are often exploited within days. In industrial environments, the challenge is response time: patching a PLC vulnerability usually means waiting for the next maintenance window, then retesting and requalifying the installation before bringing it back online. Months can pass while the vulnerability remains exposed. It is precisely this gap between the pace of vulnerability discovery and the pace of remediation that defense in depth must close.

Schneider Electric Media Relations – Andrée Clar, andree.clar@se.com – +33 (0)6 85 81 08 78
SECLAB Media Relations – Delphine Perez, dperez@seclab-security.com - +33 (0)6 63 53 53 47

Against this backdrop, Schneider Electric continues to raise the security level of its products, operations, and plants. This effort supports the requirements of the Cyber Resilience Act, which mandates security for products with digital elements throughout their lifecycle, and helps customers in critical sectors meet their NIS2 obligations by relying on compliant equipment and architectures.

Hardware-Based Protection Designed for OT Constraints

To strengthen defense in depth for industrial systems, Schneider Electric has chosen to deepen its collaboration with SECLAB. The two companies are combining their OT expertise to adapt SECLAB technology to Schneider Electric automation architectures, enabling fine-grained application-level filtering of the industrial protocols exchanged between programmable logic controllers (PLCs), distributed control systems (DCS), and safety instrumented systems (SIS).

This collaboration has produced a dedicated configuration for securing Schneider Electric OT protocols. Placed inline on critical communications, the appliance provides a hardware-based protocol break and allows only the communications strictly required by the process. Tests conducted on Schneider Electric platforms confirmed application-level filtering, proper operation in redundant configurations, and no perceptible latency for the process.

Schneider Electric's OT cybersecurity teams in Europe manage deployment end to end: architecture assessment, appliance supply, configuration, integration at the end-user site, functional testing, and periodic maintenance. This approach can complement existing automation service contracts between Schneider Electric and industrial customers, making cybersecurity part of the recurring maintenance of the industrial environment.

"As vulnerability discovery becomes industrialized, purely software-based security solutions are no longer enough: they remain exposed to the very flaws they are meant to block. With Schneider Electric, we combine strong hardware isolation, a deep understanding of OT flows, and controlled integration as close as possible to critical processes," said Michel Van Den Berghe, CEO of SECLAB.

"Our responsibility as an industrial company is to protect the continuity of our operations and those of our customers, while advancing the compliance and resilience of the industrial architectures we deploy. This partnership allows us to deliver complementary OT protection that has been proven with our automation systems, is integrated by our experts, and is maintained over time within existing service contracts," added Yann Bourjault, Vice President Digital Transformation & Cybersecurity Europe, Schneider Electric.

Schneider Electric Media Relations – Andrée Clar, andree.clar@se.com – +33 (0)6 85 81 08 78
SECLAB Media Relations – Delphine Perez, dperez@seclab-security.com - +33 (0)6 63 53 53 47

A Shared Industrial Roadmap

Several industrial companies whose operations depend on continuous OT service availability are already engaged in deployments supported by Schneider Electric. The two companies now intend to expand this approach and will collaborate on a new generation of OT-specific products in a DIN-rail form factor, with availability expected in 2027.

About Schneider Electric
Schneider Electric is a global energy technology leader, driving efficiency and sustainability by electrifying, automating, and digitalizing industries, businesses, and homes. Its technologies enable buildings, data centers, factories, infrastructure, and grids to operate as open, interconnected ecosystems, enhancing performance, resilience, and sustainability. The portfolio includes intelligent devices, software-defined architectures, AI-powered systems, digital services, and expert advisory. With 160,000 employees and 1 million partners in over 100 countries, Schneider Electric is consistently ranked among the world's most sustainable companies.
www.se.com
Follow us on:
Discover the newest perspectives shaping sustainability, Electricity 4.0, and next-generation automation on Schneider Electric Insights
Hashtags: #PressRelease #EnergyManagement #Foresight #DigitalEnergy

About SECLAB
SECLAB develops cybersecurity solutions for critical industrial and operational infrastructure.
Its Xcore platform combines asset and flow visibility, isolation of critical environments through patented Electronic AirGap technology, and continuous threat and anomaly detection.
www.seclab-security.com

Schneider Electric Media Relations – Andrée Clar, andree.clar@se.com – +33 (0)6 85 81 08 78
SECLAB Media Relations – Delphine Perez, dperez@seclab-security.com - +33 (0)6 63 53 53 47