Persona: Thomas – Industrial IoT Systems Manager

Age: 45
Location: Katowice, Poland
Occupation: Industrial IoT / Automation Manager
Tech Level: Advanced

Context

Works at a manufacturing plant using 120+ IoT devices: sensors, robots, PLCs, gateways. Security incidents may cause downtime and safety risks. Responsible for OT network security and reliability.

Goals

- Ensure continuous, stable production.
- Comply with security standards (e.g. NIS2, ISO 27001).
- Standardize secure onboarding for all devices.
- Prevent unauthorized access to OT systems.

Pains

- Legacy devices with weak authentication.
- Multi-vendor ecosystem with inconsistent security.
- Difficult to verify device identity.
- Risky updates due to production constraints.
- Contractors sometimes add devices without proper checks.

Needs

- Central platform for authentication and access control.
- Unique cryptographic identity for each device.
- Real-time detection of anomalous traffic.
- Local-only secure communication, no cloud dependency.

How Our Protocol Helps

- Per-device keys prevent spoofing and rogue devices.
- Central secure gateway blocks unauthorized connections.
- Unified onboarding workflow usable across vendors.
- Detailed logs for audits and compliance reports.
- Ability to isolate a single device without stopping the line.