**Sebastian Tvein**
Head of Digitalization at Aquatim S.A.

**Ionel Draghici**
SCADA Expert at Aquatim S.A.

**Mihai Belcescu**
IT Expert at Aquatim S.A.

# Securing Water Infrastructure at the OT/IT Edge: How Aquatim is hardening SCADA under NIS2

Aquatim, the regional water and sewage utility serving Timișoara and Timiș County, is the first water utility in Romania to secure European Digital Europe Programme funding dedicated specifically to cybersecurity. The company is one of 13 partners across seven EU countries in CIPHER, a €8.67 million project fully financed through non-reimbursable EU grants and running from December 2025 to December 2028. As an essential entity under NIS2, Aquatim's pilot is built around one practical question: how do you converge SCADA and OT/IT security without slowing down — or endangering - the systems that keep water moving.

## The architecture behind the pilot

The platform is a passive-monitoring layer that never touches the fragile PLCs and RTUs it protects. Zeek and Suricata inspect network traffic while Wazuh EDR watches endpoints; a threat-intelligence feed (T2.1) pulls indicators from threat intel feeds. Everything publishes onto a central message broker, organised around topics for raw data, risk scores, attack paths, and feedback. A Risk Toolbox turns the raw feeds into composite scores, a visualisation layer renders dashboards, and Netdata joins the same broker for infrastructure health - so an operational fault and a security anomaly land on the same screen instead of two different tools.

ECCC
Funded by the European Union

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

## Real-time threat detection

Detection (T2.4) runs continuously off the Zeek/Suricata/Wazuh feed, and because monitoring is 100% passive, automation engineers get the one guarantee they actually need: nothing actively probes a decade-old PLC, so uptime stays untouched while the same telemetry doubles as a predictive-maintenance signal, flagging latency or configuration drift on a flaky cellular link before hardware fails. On the SOC side, this is what turns thousands of generic firewall alerts into a handful of high-fidelity ones — the platform understands industrial protocols like DNP3 and Modbus TCP well enough to catch a legitimate-looking but out-of-pattern command, such as an attempt to alter a chemical dosing register from an unusual asset at an odd hour, and hand the analyst a visual attack path with a one-click "Isolate WAN Link" response instead of a wall of noise.

## Automated vulnerability scanning

A separate vulnerability-assessment module (T2.3) scans configuration and firmware state across the fleet and publishes the results onto the same broker, replacing the periodic, manually scheduled audits that struggle to keep pace with an evolving threat landscape. For the CISO, this closes the blind spot that used to sit behind every compliance report: instead of guessing, they log into a single dashboard with a continuously updated inventory of every PLC, RTU, and local SCADA asset - direct evidence for NIS2 Article 21 risk-management obligations, and an instant answer, firmware version included, when an auditor asks for proof of supply-chain validation.

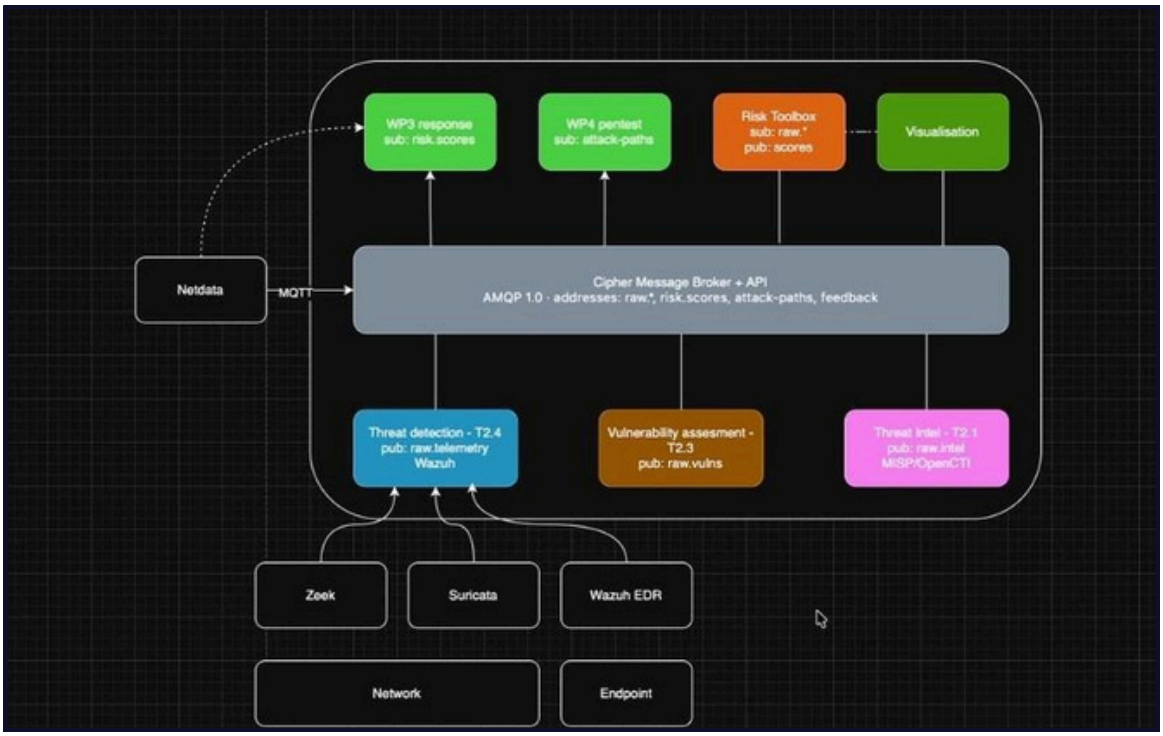
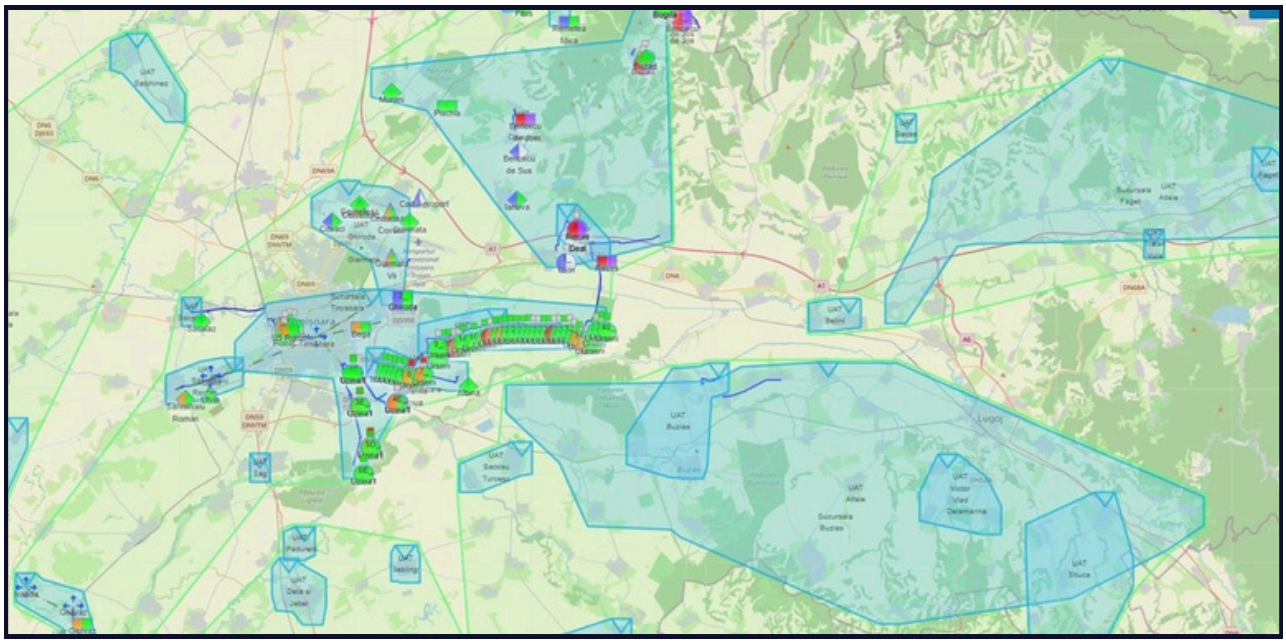



*Figure 1 - CIPHER OT security architecture — Zeek, Suricata and Wazuh EDR feed Threat Detection (T2.4), Vulnerability Assessment (T2.3) and Threat Intel (T2.1) into the Cipher Message Broker over AMQP 1.0; the broker feeds WP3 response, WP4 pentest, the Risk Toolbox and the Visualisation layer, with Netdata connected via MQTT.*

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

# Incident response in regional distribution networks

The message broker feeds WP3's incident-response workflow directly off the risk-score topic, so containment doesn't wait for someone to piece events together manually. When an incident occurs - say, a contractor's infected laptop touching a SCADA switch at a regional treatment plant — the system generates an incident summary detailing what happened, when, and which assets were affected, which is what lets a CCO or legal team meet NIS2's 24-hour early-warning deadline without scrambling for facts, and what keeps the utility clear of fines that can reach €10 million or 2% of global turnover. The same discipline extends to remediation: field technicians and third-party vendors no longer need a slow corporate VPN or a truck roll to fix a broken pump or update PLC logic.



*Photos: AQUATIM Regional SCADA Center.*

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.

## Why this matters under NIS2

Aquatim has been designated an essential entity under Annex 1 of OUG nr. 155/2024, with personal liability exposure for the executive board if controls aren't demonstrably in place. The CIPHER pilot is built to make that risk manageable in practice: continuous detection and scanning generate the ongoing risk-monitoring evidence Article 21 expects, and the automated incident-summary workflow addresses the notification obligations that follow a confirmed breach. For OT security engineers and CISOs elsewhere in the water sector, the goal is a reference architecture rather than a theoretical compliance checklist.

## Project background

The proposal was authored and submitted by Sebastian Tvein under the DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER call, which supports EU member states in building resilience against cyber threats for large-scale industrial infrastructure. It was evaluated at 14.5 out of 15 points and confirmed as a winning proposal in late 2025. On Aquatim's side, the project is managed by Sebastian Tvein (project manager), with Ionel Draghici as SCADA expert, Mihai Belcescu as IT expert. The diagram below maps the topology described above -sensors, message broker, and the work packages consuming its feeds - the same layout Aquatim's team is validating against its own regional distribution network as the pilot moves from design into testing.

**Follow Aquatim S.A.**

**To follow the three areas named in the brief directly: real-time threat detection, automated vulnerability scanning, and incident response in regional water distribution networks/SCADA*

FOLLOW US!

Funded by the European Union's Digital Europe Programme under Grant Agreement No 101249732. The views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority (European Cybersecurity Industrial, Technology and Research Competence Centre). Neither the European Union nor the granting authority can be held responsible for them.