



Nozomi Hour

The latest OT/IoT
cybersecurity industry
updates and insights

Q3 2026

Anton Shipulin, CISSP, CSSA, NNCE

Industrial Cybersecurity Strategist, Nozomi Networks

Anton.Shipulin@nozominetworks.com

Agenda

Q3 2026

1. OT/IoT **threat landscape** updates: incidents, vulnerabilities, and attack techniques
2. OT/IoT security **regulation, standards**, and frameworks news
3. OT/IoT security **technology trends, research, tools**, and best practices
4. A dedicated **discussion** for company-specific interests and concerns

1. Threat landscape updates

2. Regulation/Standards news

3. Technology trends

4. Q&A



PLC Threat Warnings

Exposed controllers remain active targets across multiple sectors

CISA: Iran-affiliated PLC activity

- The updated CISA advisory describes overwritten project files and disabled alarms, including changes to Rockwell AOIs that may be easy to miss.
- **Watch:** Internet-accessible PLCs, contractor connections, and unauthorized changes to projects, AOIs or alarm states.
- **Why it matters:** The activity shows that attackers can modify controller projects, not merely reach the devices.

CISA: AI-assisted Siemens S7 tooling

- U.S. agencies warn of active targeting of exposed or poorly segmented S7 PLCs. The reported tooling uses Snap7 and S7comm to read and write PLC data and configuration.
- **Watch:** Internet exposure on TCP port 102, unusual S7comm activity, and unauthorized configuration changes.
- **Why it matters:** Attackers are developing PLC access capabilities faster. The advisory reports no confirmed physical-process disruption.

Cyberattacks on Water Systems in North America

From Regional Campaign to Process Manipulation

US EPA reported more than 100 drinking-water and wastewater systems targeted across 12 states in 2026, many with internet-exposed PLCs often connected through cellular modems. Reported impacts include modified PLC projects, pressure loss and flooding.

Minnesota — Partial shutdown and manual control

More than 30 community water systems were targeted on July 26–27. Braham shut down parts of its system for about two hours. Plymouth lost communications with two water towers and several wastewater lift stations, then operated manually.

Colorado — Operating settings changed

At two small utilities, intruders changed equipment settings and pumping cycles, disabled alarms and cut off remote access. Operators regained control after brief disruptions. Officials reported no impact on water quality or service.

New Jersey — Remote control lost

Two municipal utilities temporarily lost remote monitoring and management of exposed control systems. Operators switched to manual procedures and maintained safe drinking-water service.

Saint-Noël, Canada — Pumps stopped

An operator detected an intrusion at the drinking-water plant. Subsequent reporting describes disabled water-level alarms and a changed chlorine-dosing setting; the plant entered a protective state and pumping stopped. Operators restored normal operation quickly, with no reported water-quality impact.

Significant Cyber-Physical Incidents in Q3

Cyber incidents that affected physical operations or exposed cyber-physical risk



USA

Food & Beverage

Fairlife (Coca-Cola) was hit by ransomware on production-related systems. **Production halted at all four U.S. plants**; most operations were restored within about two weeks. No PLC or SCADA compromise confirmed.



United Kingdom

Energy

A **small-scale UK power generator** was hit by a reported Iran-linked attack. **The facility was offline for four days**; the wider electricity system was unaffected. No direct manipulation of plant controls established.



Australia

Food & Agriculture

Mackay Sugar confirmed unauthorized access to its IT environment. **Two mills stopped** and harvesting and cane-rail logistics were disrupted; limited manual crushing continued. Full operations returned over 2+ weeks.



USA

Maritime & Ports

North Carolina Ports suffered an IT compromise across Wilmington, Morehead City and Charlotte Inland Port. **Gate transactions moved to manual processing**, delaying customers; vessel operations stayed on schedule.



USA

Maritime Energy

A U.S. Coast Guard and FBI investigation confirmed malicious cyber activity aboard **VL Prosperity**, a Liberia-flagged crude tanker. Access vector unknown; **no navigation, safety or physical-process disruption** confirmed.



Malaysia

Maritime & Ports

Port of Tanjung Pelepas detected a cyber incident in its terminal systems. **Container operations were suspended**, then restored in phases while some gate processes ran manually. Ransomware attribution unconfirmed.

Stuxnet Reconstructed

A New Defensive Research Artifact

What is it?

- Source-level reconstruction based on decompiled Stuxnet binaries and public research
- Covers Windows components, Step 7 interception, and reconstructed PLC payload logic
- Not original source code and not a new Stuxnet variant

Why it matters for OT/IoT cybersecurity

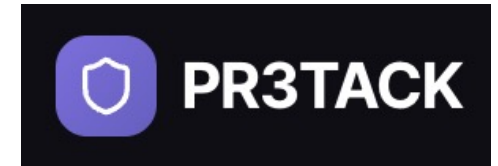
- Makes the full IT-to-PLC attack chain easier to study
- Useful for malware analysis, detection engineering, and OT lab exercises
- Reinforces a key lesson: engineering workstations and trusted PLC programming paths are critical attack surfaces

Source: <https://github.com/Sadpainy/Stuxnet>



PR3TACK: The Preemptive Tactics & Countermeasures Knowledgebase

Community-driven framework presented at FIRSTCON26



What is it?

- Community-driven framework presented at **FIRSTCON26**
- Open framework for cataloguing **technically plausible but not yet publicly observed adversary TTPs**
- Complements MITRE ATT&CK's evidence-based view with a **“what could attackers do next?”** perspective
- Covers 17 tactical areas, including **pre-positioning, resilience erosion, AI/ML subversion, cognitive manipulation and operational-tempo manipulation**
- Techniques are tagged by feasibility based on proof-of-concept evidence, technical reasoning or early research
- Not an OT-specific matrix, but useful for **forward-looking threat modeling**
- Helps develop scenarios for **tabletops, red/purple-team exercises and resilience testing**

Source: <https://pr3tack.org/>

The background of the slide features a blue-toned globe with binary code (0s and 1s) overlaid. A series of white-outlined diamond shapes are arranged in a grid-like pattern across the right side of the image. Orange and yellow light trails or orbits curve around the globe.

1. Threat landscape updates

2. Regulation/Standards news

3. Technology trends

4. Q&A

NIST Draft SP 800-82 Rev. 4

Updated Guide to Operational Technology Security

One of the **foundational OT cybersecurity references**, widely used to build a common understanding of how cybersecurity applies in OT environments.

What's New

- Broader OT scope: BMS, water, food and agriculture, freight rail, maritime, IIoT and cloud
- **Aligned with NIST CSF 2.0:** restructures guidance around the updated framework, including the new Govern function
- **Stronger enterprise-risk integration:** connects OT cybersecurity more directly with enterprise risk management
- **Adds OT guidance for the NIST Risk Management Framework (RMF)**
- **More implementation detail** for asset management, network monitoring and detection
- **Updated architecture guidance** covering management-plane protection and zero-trust concepts adapted to OT reliability and safety constraints



Source: <https://csrc.nist.gov/pubs/sp/800/82/r4/ipd>

EU CRA Reporting Goes Live on Sep 11, 2026

Mandatory vulnerability and incident reporting starts as ENISA launches the Single Reporting Platform

- CRA reporting obligations for manufacturers are now in force for **actively exploited vulnerabilities** and **severe security incidents**
- ENISA's **Single Reporting Platform** became the official submission channel
- The requirement applies to relevant products already placed on the EU market, not only new products
- Broader CRA product-security obligations generally apply from **December 11, 2027**

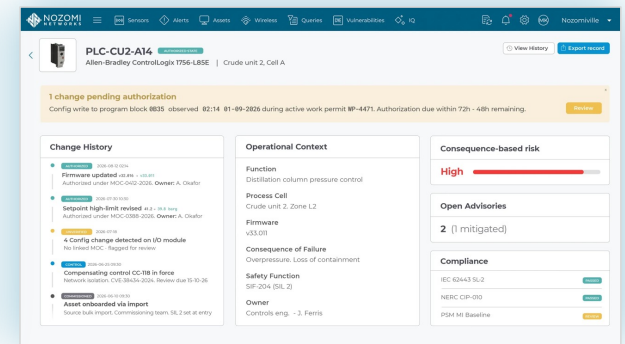
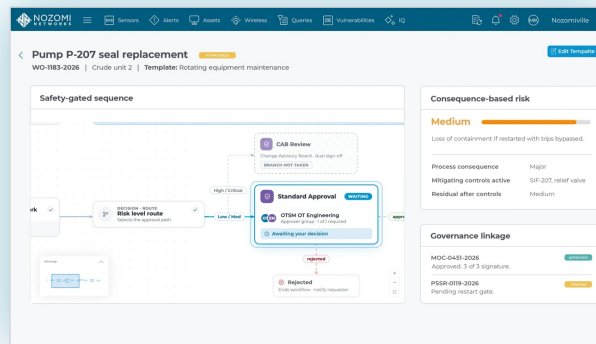
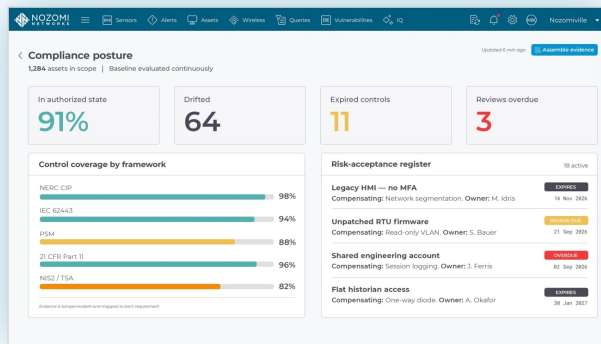


1. Threat landscape updates
2. Regulation/Standards news
- 3. Technology trends**
4. Q&A



Nozomi Networks Introduces Nozomi Compass

OT-native Asset Governance, Compliance and Service Management



Built on a source of truth

Every workflow, risk score and audit runs on the broadest, most current OT asset record, always a complete and real-time picture.

OT-ready and OT-safe

Out of the box, OT-specific workflows with process-aware context, safety modeling and Purdue-level asset relationships allow for faster change management and easier governance.

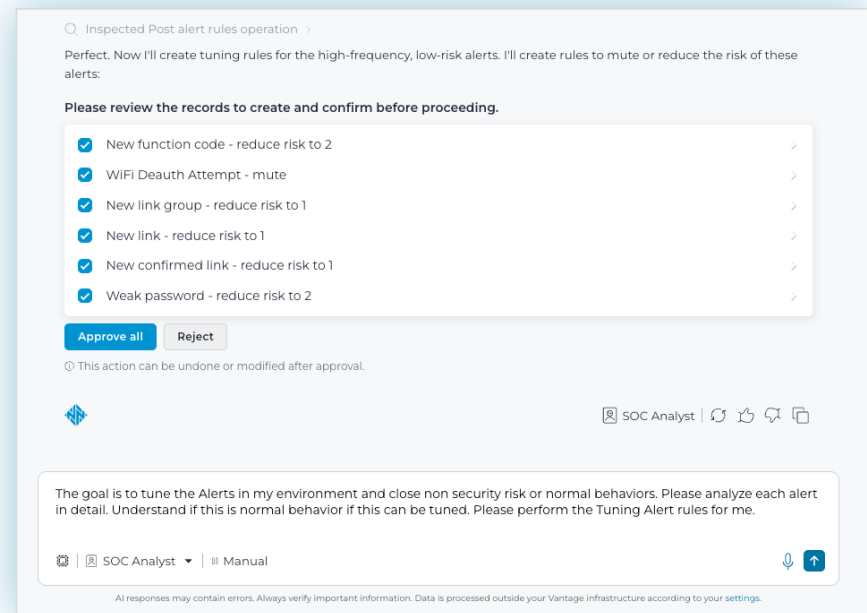
Auto-generated reports

Custom reports provide continuous audit-ready evidence mapped to local and global regulatory frameworks.

Nozomi Vantage IQ Active Actions

From AI insight to approved action: faster remediation, with the user still in control

- Vantage IQ can prepare a change directly in Vantage
- The proposed action is shown to the user for review
- Nothing changes until the user selects **Apply**
- Supported actions can be **Reverted**
- Uses existing Vantage APIs and creates a foundation for more action types over time



New Practical Resources from CISA & Partners

Practical guidance for Critical-Infrastructure Defenders

Detecting and Mitigating Active Directory Compromises

Guidance on 17 common Active Directory compromise techniques and recommended mitigations, including updated coverage of DCSync and Shadow Credentials.

Updated Insider Threat Mitigation Guide

Updated guidance for building or improving an insider threat program, including hybrid work, AI-related considerations, access control and workforce risk.

Using Cyber Decoys for Detection and Response

Practical guidance on tripwires, breadcrumbs and honeytokens to detect lateral movement, stolen credentials and post-compromise activity.

Working With Third-Party ICS Integrators

CISA/FBI recommendations for controlling integrator access, applying least privilege, logging remote activity and preserving operational resilience.

CI Fortify – Advice for isolating vital systems

Guidance for identifying vital OT and enabling systems, mapping dependencies and preparing isolation plans to sustain essential operations during a major cyber incident.



Source: <https://www.cisa.gov/resources-tools/resources>

Conpot 1.0.0 released

One of the better-known open-source ICS honeypots

- A large part of the protocol stack has been refreshed, including S7, Modbus, IEC 104, ENIP/CIP, BACnet, HTTP, SNMP, FTP, IPMI and TFTP, with a strong focus on correctness, stability and hardening.
- Logging has also been reworked into a much more structured form across JSON, SQLite, syslog, HPFriends and TAXII, making Conpot more practical as a source for SOC workflows and threat research pipelines.

Useful update for anyone running or experimenting with ICS honeypots.



Source: <https://github.com/mushorg/conpot>

1. Threat landscape updates
2. Regulation/Standards news
3. Technology trends

4. Q&A





Anton Shipulin, CISSP, CSSA, NNCE
Anton.Shipulin@nozominetworks.com

Thank You!

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com