

Cybersecurity for water and wastewater utilities

Early warning for the plant, one team for IT and OT

Protect treatment, pumping and distribution without taking the plant offline. We secure the control systems behind every stage, from intake to tap and from collection to outfall, and watch them around the clock with Culper-I.

/01 The risk is on the record

97

drinking water systems serving about 26.6 million people had critical or high-risk cybersecurity vulnerabilities.

EPA OFFICE OF INSPECTOR GENERAL, NOV 2024

70%+

of community water systems EPA inspected since September 2023 violated basic Section 1433 requirements.

EPA ENFORCEMENT ALERT, MAY 2024

7 states

reported attacks on internet-facing PLCs from July 27, 2026, with loss of pressure and flooding.

FBI AND EPA, ALERT I-073026-PSA, JUL 30, 2026

/02 Ten systems. One attack surface.

A water system is not one control system. It is ten, built by different vendors in different decades and spread from the intake to the last smart meter in town. Each connection is a way in, and each needs a different kind of protection.

- Process control (ICS/SCADA)
- Chemical feed
- Safety instrumented systems
- Smart water and IoT
- Building management
- Instrumentation and field devices
- Pumping and distribution
- Telemetry and communications
- Power and electrical
- HVAC and environmental

/03 Why utilities choose DT6

- Monitoring is passive and never sends commands to your controllers
- Works alongside your SCADA integrator, not around them
- One SOC covers the plant and the office network
- A New Jersey team, close enough to be at the plant

AT A GLANCE

BUILT FOR

Drinking water and wastewater systems, municipal utility authorities, small and rural systems

LEAD PRODUCT

Culper-I, an Early Warning System (EWS) for water and wastewater systems

COMPLIANCE

SDWA Section 1433, the NJ Water Quality Accountability Act, NYSDOH Appendix 5-E and NY DEC wastewater rules

NEXT DEADLINE

Dec 31, 2026: Emergency Response Plans for systems serving 3,301 to 49,999 people

LEARN MORE

digitalteamsix.com/solutions/water-wastewater

/04

Three phases. In the right order.



Crawl

REVIEW

Know what you have.

We map every connected device, find what is exposed to the internet, and give you a prioritized plan your board can fund.



Walk

HARDEN

Close the open doors.

We separate the plant network from office IT, put vendor remote access behind logged sessions, and retire default and shared passwords.



Run

PROTECT

Watch it around the clock.

Culper-I monitors your OT network. If something looks wrong, our SOC calls your operator and helps you run safely in manual.

/05

Compliance, built in

REQUIREMENT	WHAT IT ASKS	WHAT YOU GET
SDWA Section 1433	A Risk and Resilience Assessment covering automated systems, an Emergency Response Plan, and EPA certification every five years.	The cyber section of your RRA, the cyber incident procedures in your ERP, a tabletop exercise, and evidence mapped to EPA's checklist.
NJ Water Quality Accountability Act	A program aligned to NIST CSF, CIS Controls or ISO 27000, prompt incident reporting to NJCCIC, and cyber insurance.	Controls mapped to your framework, incident details ready for NJCCIC, and documentation for your annual certification.
NYSDOH Appendix 5-E and NY DEC wastewater rules	A cybersecurity program or written controls, with incident reports within 24 hours.	A program and reporting process for New York. Much of the same work covers your New Jersey obligations.

/06

Recent incidents, and what would have stopped them

INCIDENT	WHAT HAPPENED	WHAT WOULD HAVE STOPPED IT
Aliquippa, PA, November 2023	An internet-facing booster station PLC with a default password was taken over. Operators ran the station by hand.	No direct internet exposure, and no default passwords.
Muleshoe, TX, January 2024	Attackers broke into a remote login system for industrial software and overflowed a water tank for 30 to 45 minutes.	Remote access through a gateway with MFA, and alerts on abnormal tank commands.
Seven states, July 2026	Attackers changed IP addresses and passwords on internet-facing MicroLogix PLCs. Utilities lost monitoring and control, and some saw pressure loss and flooding.	An inventory of every internet-facing PLC and cellular modem, and practiced manual operation.

Sources: CISA alert, Nov 28, 2023; AP and CNN reporting, Apr 2024; FBI and EPA alert I-073026-PSA, Jul 30, 2026. Full briefings at digitalteamsix.com/resources.

Find out what an attacker can see.

Request an OT risk assessment. An engineer will walk you through how it works and where we would start at your plant.

Request an assessment

digitalteamsix.com/solutions/water-wastewater

973-339-0090

sales@digitalteamsix.com