

Culper-I

Cybersecurity and resiliency Early Warning System (EWS) for water and wastewater systems

Culper-I watches your SCADA, PLCs and remote sites around the clock, learns what normal looks like, and warns your operators the moment something changes, whether it is an intrusion or a failing connection, before it becomes an outage or malicious access affects water pressure and quality.

/01 Why control systems need their own watch

A water system is not one control system. It is ten, built by different vendors in different decades, and most of them now talk to each other and to the internet. An attacker only needs one.

Office security tools were not built for PLCs, and an active scan can upset fragile equipment. Culper-I was. It learns how your control network behaves and flags the change that matters: a new device, an unexpected spike, an off-hours login, or a PLC suddenly reachable from the internet.

/02 How early warning works

01 Listen

A Culper-I appliance in your control room sees every conversation between HMIs, PLCs, historians and remote sites.

02 Learn

Culper-I builds a baseline of normal: which devices talk, which commands they send, and when.

03 Warn

A new device, an unexpected spike, an off-hours login, an unstable network or a lost connection raises an alert to our operations center within seconds.

04 Respond

An analyst confirms it, calls your operator, and helps your team isolate the problem and run safely in manual.

/03 The question operators ask first

Will Culper-I interfere with our PLCs or SCADA?

No. Monitoring is passive. It listens to a copy of network traffic and never sends commands to control equipment. Vulnerability assessments are non-intrusive, follow NIST SP 800-82, and run only with your approval.

AT A GLANCE

HOW IT CONNECTS

A Culper-I appliance in your control room. Monitoring is passive and never sends commands to your equipment

WHAT IT WATCHES

SCADA, HMIs, PLCs, historians, field devices and remote sites, for attacks and for failures

WHO RESPONDS

Our US-based SOC, 24/7, by phone within the hour for high-severity alerts

BUILT FOR

Water and wastewater utilities and MUAs, departments of public works, and schools and colleges

COMPLIANCE RESULT

Water and wastewater compliance: SDWA Section 1433, NJ WQAA, NYSDOH Appendix 5-E, the MEL Deductible Reduction Groups and NIST SP 800-82

LEARN MORE

[digitalteamsix.com
/platform/culper-i](https://digitalteamsix.com/platform/culper-i)

/ 04

One framework. Four disciplines.

01	02	03	04
Asset management An inventory of your IT and OT assets, with non-intrusive vulnerability assessments on demand.	Access management Operator and administrator access managed in the control room, with a kiosk mode for SCADA.	Network management Segmentation built around your ICS, OT and SCADA assets, with secure remote access across control rooms.	Incident management An on-premises SIEM appliance for your control rooms, integrated with a dedicated, US-based SOC built around your control system.
Culper-I comes in three tiers, Subscription, System and Solution, each including the one before. Details at digitalteamsix.com/platform/culper-i .			

/ 05

Discovery to live monitoring, per control room

01	02	03
Discovery A non-intrusive assessment to NIST SP 800-82: 1 day on site, then 2 days to report.	Staging 2 weeks in our lab: trust zones mapped, rules configured and tested.	Deployment 2 days on site, tested with your operators and SCADA integrator.

/ 06

When Culper-I raises an alert

SEVERITY RESILIENCY		CYBERSECURITY
High	Phone and ticket, 1-hour SLA. Outages and loss of operator access.	Phone and ticket, 1-hour SLA. Signs of compromise in an asset, the network or user activity.
Medium	Ticket, 6-hour SLA or residual risk accepted. Degraded performance and unstable connections.	Ticket, 8-hour SLA or residual risk accepted. Vulnerabilities with no evidence of compromise.
Low	Ticket, 1-week SLA or residual risk accepted. Legacy operating infrastructure.	Ticket, 8-hour SLA or residual risk accepted. Minor version patches less than 60 days overdue, with no security vulnerabilities.

/ 07

The result: water and wastewater compliance

REQUIREMENT	WHAT IT ASKS	WHAT CULPER-I PROVIDES
SDWA Section 1433	Assess, plan, and recertify to EPA every five years.	An inventory, findings and incident records for both.
NJ WQAA	A program aligned to NIST CSF, CIS Controls or ISO 27000, with reporting to NJCCIC.	Controls mapped to your framework, and incident details ready for NJCCIC.
NYSDOH and NY DEC	A program or controls, with 24-hour incident reports.	An inventory, findings and the controls they ask for.
NJ MEL Deductible Reduction Groups	Three levels of controls for Joint Insurance Fund members.	Support for all three levels, with the evidence your JIF asks for.

See Culper-I on a control network like yours.

One working session with an OT engineer, built around your plant rather than a slide deck.

Request an assessment

digitalteamsix.com/platform/culper-i

973-339-0090

sales@digitalteamsix.com