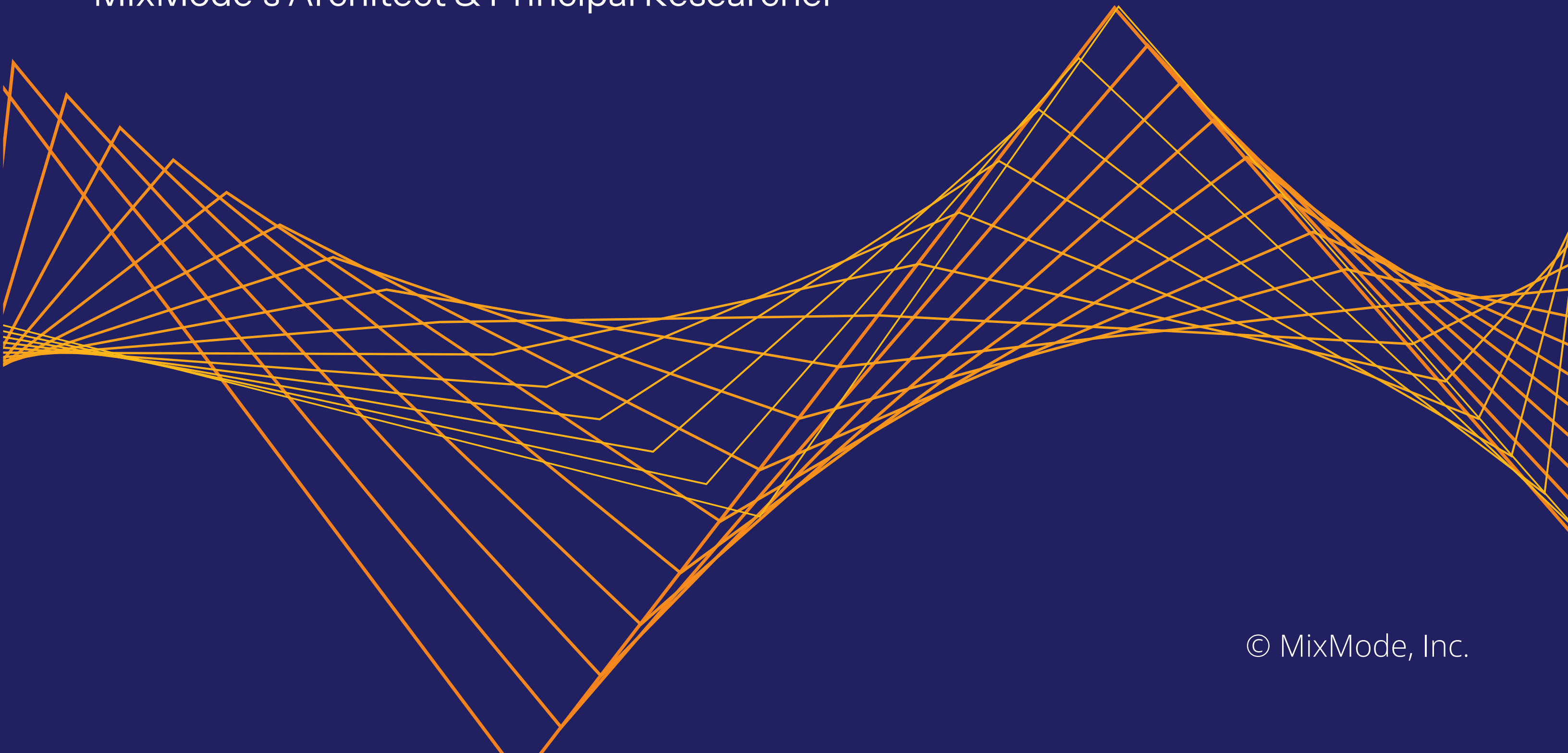
MixMode®

THREAT REPORT

Protecting Water Systems: Mitigating Cybersecurity Risks from Internet-Exposed HMIs with MixMode's Third-Wave AI

Michael Yelland
MixMode's Architect & Principal Researcher



The Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA) have issued a critical fact sheet highlighting the cybersecurity risks posed by internet-exposed Human Machine Interfaces (HMIs) in Water and Wastewater Systems.

HMIs are essential for managing Supervisory Control and Data Acquisition (SCADA) systems connected to programmable logic controllers (PLCs), enabling operators to monitor and control water treatment processes.

However, when these systems are accessible online without robust cybersecurity controls, they become prime targets for malicious actors, threatening the safety and reliability of critical infrastructure.

The Threat Landscape for Water Systems

The EPA and CISA emphasize that internet-exposed HMIs are easily discoverable through publicly available web-based search platforms, making them vulnerable to exploitation. Unauthorized users can exploit these systems to:

- View sensitive HMI data, including graphical user interfaces, distribution system maps, event logs, and security settings.
- Make unauthorized changes, such as altering set points or disabling alarms, potentially disrupting water or wastewater treatment processes.

Real-world incidents underscore the severity of this threat. In 2024, pro-Russia hacktivists targeted HMIs at multiple U.S. water utilities, manipulating water pumps and blower equipment to exceed normal operating parameters. These cyber attackers maxed out set points, turned off alarm mechanisms, and changed administrative passwords to lock out operators.

The result was nearly catastrophic.

Operational disruptions followed that forced facilities to revert to manual operations. The joint fact sheet Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity provides further details on these incidents, emphasizing the need for immediate action.

Cyber risks are compounded by the fact that many water utilities lack the resources or expertise to secure their operational technology (OT) environments. Advanced threat actors exploit these weaknesses with ease, using techniques to locate and compromise exposed HMIs.

The EPA and CISA stress that without proactive measures, water systems remain at high risk of cyberattacks that could jeopardize public health and safety.

EPA and CISA's Recommended Mitigations

To address these vulnerabilities, the EPA and CISA provide a comprehensive set of mitigations to harden remote access to HMIs and reduce the attack surface. These include:

- Inventory and Isolation: Conduct a thorough inventory of all internet-exposed devices and disconnect HMIs from the public-facing internet whenever possible. For systems that must remain online, secure them with strong, unique passwords, replacing factory defaults immediately.

- Access Controls: Implement multifactor authentication (MFA) for all HMI and OT network access to prevent unauthorized logins. Log remote login attempts, monitor for failed attempts, and flag unusual activity, such as logins at odd hours.

- Network Segmentation: Deploy a demilitarized zone (DMZ) or bastion host at the OT network boundary to limit unauthorized access and prevent reconnaissance by malicious actors. Geo-fencing can further restrict access based on specific locations.

- System Hygiene: Keep all systems and software up to date with the latest patches and security updates. Establish an allowlist to permit only authorized IP addresses to access HMIs.

- Vendor and Agency Support: Follow vendor recommendations for securing specific products and leverage CISA's free cybersecurity vulnerability scanning service (available by emailing vulnerability@cisa.dhs.gov) to identify and remediate software vulnerabilities.

The fact sheet also points to additional resources, such as the Top Cyber Actions for Securing Water Systems joint fact sheet, EPA's Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems, and CISA's Stuff Off Search tool for identifying exposed assets. Water utilities can further benefit from contacting regional CISA Cybersecurity Advisors or the EPA for tailored assistance. For OT-specific guidance, the NIST TN 2283 (Initial Public Draft) offers insights into secure remote access architectures.

Why These Measures Matter

Implementing these mitigations *is not just a technical necessity but a public safety imperative.*

Water and wastewater systems serve as critical infrastructure for U.S. citizens. Disruptions can have cascading effects on communities, from contaminated water supplies to environmental damage.

The 2024 hacktivist attacks demonstrate that even small-scale utilities are not immune, as cyber threat actors increasingly target less secure critical infrastructure defenses with unsecured HMIs.

By adopting these recommendations, water utilities can significantly reduce their risk profile and enhance resilience against rapidly evolving advanced cyber threats.

MixMode's Third-Wave AI: A Self-Contained Cybersecurity Solution

While the EPA and CISA provide a strong foundation for securing water systems, traditional cybersecurity tools often struggle to keep pace with sophisticated, dynamic threats. MixMode's Third-Wave AI offers a transformative advanced cyber threat solution.

Unlike conventional security tools that rely on external threat intelligence feeds, predefined rules, or frequent AI model updates, MixMode's AI is out-of-band, environment-agnostic, and self-contained. Here's how MixMode's technology operates and secures water systems against advanced cyber threats:

Independent and Adaptive

MixMode's Third-Wave AI learns the unique behavioral patterns of your OT network without depending on external threat feeds or intelligence. This makes it effective against zero-day attacks and novel threats, such as those perpetrated by hacktivists targeting HMIs.

No Tuning Required

The platform autonomously adapts to your environment, eliminating the need for manual tuning or constant updates. This reduces the burden on resource-constrained water utilities, ensuring continuous protection without ongoing maintenance.

Real-Time Anomaly Detection

MixMode detects deviations from normal HMI and network behavior in real time, flagging unauthorized access, configuration changes, or abnormal equipment operations before they cause harm.

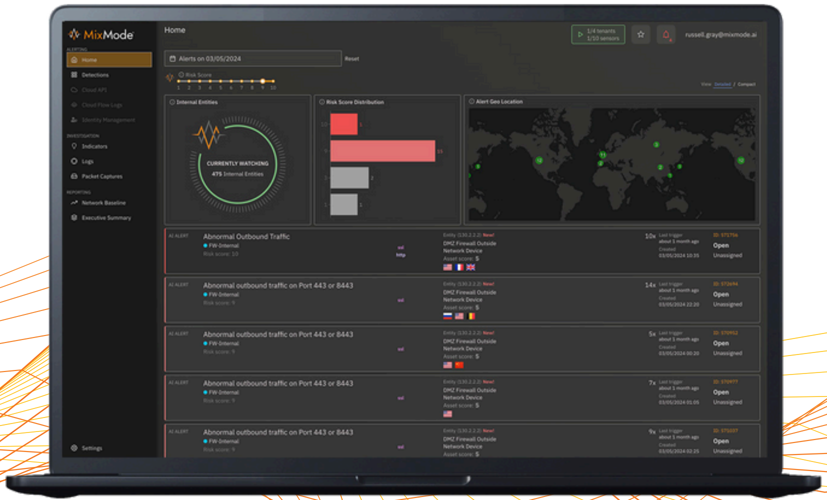
Native Scalability

Designed for distributed OT environments, MixMode integrates seamlessly with water utilities' infrastructure, providing comprehensive visibility and protection across all assets.

By deploying MixMode, water utilities can proactively address the EPA and CISA's recommendations, securing HMIs and OT networks against both known and emerging threats. MixMode's self-learning technology reduces human errors and allows utilities with limited cybersecurity resources to achieve US Department of Defense-grade protection.

Don't let your water system become the next target. Visit MixMode.ai to discover how MixMode's Third-Wave AI can safeguard your critical infrastructure with unmatched efficiency and effectiveness. Secure your HMIs, protect your operations, and stay ahead of cyber threats with a solution that works smarter, not harder.

For more information on EPA and CISA's guidance, access the fact sheet at cisa.gov or request free vulnerability scanning by emailing vulnerability@cisa.dhs.gov.



AI ALERT Abnormal Outbound Traffic
FW-Internal
Risk score: 10
DMZ Firewall Outside Network Device
Asset score: 5
10x Last trigger about 1 month ago
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
DMZ Firewall Outside Network Device
Asset score: 5
14x Last trigger about 1 month ago
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
DMZ Firewall Outside Network Device
Asset score: 5
5x Last trigger about 1 month ago
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
DMZ Firewall Outside Network Device
Asset score: 5
7x Last trigger about 1 month ago
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
DMZ Firewall Outside Network Device
Asset score: 5
9x Last trigger about 1 month ago
Open
Unassigned

MixMode®

mixmode.ai