Enhancing Security for American Water Utilities

case study

American water utilities and water districts are critical infrastructure sectors that require robust security measures to protect against cyber threats. One significant risk is the use of compromised passwords by employees, which can lead to unauthorized access and potential sabotage of water supply systems.

Enzoic provides a solution to this problem by continuously screening employee accounts for compromised passwords and enhancing overall cybersecurity posture.

Objectives

To implement a continuous monitoring system that screens employee accounts for compromised passwords, thereby preventing unauthorized access and ensuring the security and integrity of water utility operations.

CHALLENGES

Critical Infrastructure Protection

Water utilities are considered critical infrastructure and are prime targets for cyber-attacks according to CISA.

Regulatory Compliance

Ensuring compliance with industry standards and government regulations like NIST Password Guidelines and CISA Directives regarding cybersecurity.

Credential-Based Attacks

Employees may inadvertently use compromised passwords, exposing the utility to breaches.

Operational Continuity

Maintaining uninterrupted water supply services while implementing enhanced security measures.

ENZOIC

case study

Solution: Compromised Password Screening

Implementation Steps

Integration with Existing Systems: Integrate Enzoic's compromised password monitoring solution with the water utility's existing IT infrastructure, including Active Directory and other user authentication systems.

Continuous Monitoring: Deploy continuous monitoring to scan employee passwords against Enzoic's extensive database of compromised credentials.

Automated Alerts and Actions: Set up automated alerts to notify IT security teams whenever a compromised password is detected. Implement automated actions such as forced password resets and user account lockdowns to mitigate the risk immediately.

User Education and Training: Conduct regular training sessions for employees to educate them about the importance of strong, unique passwords and the risks associated with password reuse.

Compliance Reporting: Generate regular reports on password security status to demonstrate compliance with regulatory requirements and industry standards.

BENEFITS

Enhanced Security

By continuously monitoring and screening passwords, water utilities can significantly reduce the risk of unauthorized access and cyber-attacks.

Regulatory Compliance

Ensuring passwords are not compromised helps utilities comply with cybersecurity regulations and standards such as NIST, CIS Controls, and others relevant to critical infrastructure.

Operational Continuity

Proactively addressing compromised passwords minimizes the risk of disruptions in water supply operations due to cyber incidents.

Increased Employee Awareness

Regular training and alerts raise awareness among employees about cybersecurity best practices, leading to a more security-conscious workforce.

Conclusion

Implementing Enzoic's compromised password screening solution provides American water utilities and water districts with a robust defense against credential-based cyber threats. By continuously monitoring employee accounts and automatically responding to detected threats, these utilities can enhance their overall security posture, ensure regulatory compliance, and maintain the uninterrupted operation of critical water supply systems. Enzoic works with water districts across the US. Our solution is easy to implement and can be set up by an IT Administrator in just 20 minutes, providing a quick way to secure the #1 threat vector for breaches.