optimyze® Cybersecurity Reference Guide

Xylem values system security and resilience. Defending against cybersecurity threats is a shared responsibility. Xylem builds products that are secure by design. Our customers have a responsibility to understand the risks inherent in their processes and take steps to operate and maintain their solutions securely. This section reviews security features and provides guidance to help securely operate this product. For details and updates on Xylem product cybersecurity visit https://www.xylem.com/en-us/about-xylem/cybersecurity/.

Please note:

- Cloud connections, data flows, and cloud infrastructure are continuously monitored by the **Product Security Operations Center (PSOC)**
- Product security is **governed through a three lines of defense model** that includes: product developers, product security engineers, and audit staff

Security Recommendations for End-User

optimyze Gateway has been tailored for very specific condition monitoring applications, as such most security hardening is already in place. The following guidance provides recommendation for customers for hardening the operating environment, secure operations, account management, and disposal. In the table below: Safeguards describe the security guidance, Security Context & Rationale provide overview of security features and value of the security safeguard, and References provide additional resources for further investigation for implementing the recommended safeguards.

Safeguard	Security Context & Rationale	References
"Restrict physical access • Ensure physical access to assets is limited. Include physical isolation to protect the environment and equip ment therein. • Ensure strict control over physical access in and out of the facility."	Each of the communication ports have been hardened to restrict access and ensure integrity of device operations. For example, data transit to the cloud is encrypted and the device is provisioned before shipping. BLE pairing requires proximity and the magnetic key on the optimyze sensor. Command line con- nection requires authentication. This safeguard supports the ability to further limit exposure associated with physical threats to the device itself.	"ATT&CK for ICS: M0801 NIST SP 800-53 Rev5: AC-3, PE-3 ISA/IEC 62443-3-3: SR 2.1"
Each account should be tied to an individual. Organizations should control individual accounts through policy.	Mobile application requires registration and authentication and security events are logged. This safeguard ensures all activities are traceable and non- repudi- able.	"ATT&CK for ICS: M0801 NIST SP 800-53 Rev5: AC-3(7) ISA/IEC 62443-3-3: SR 1.1"

Safeguard	Security Context & Rationale	References
Ensure Magnet Key is removed after putting the optimyze sensor in Configuration Mode so that the device does not re-enter Configuration Mode unexpectedly and enable alternative access to your data.	Protections, such as the magnet key, are put in place to make pairing deliberate and to require physical proximity to the device. This safeguard provides additional checks and ensures no fingerprinting of BLE devices takes place.	"NIST SP 800-53 Rev5: AC-18 ISA/IEC 62443-4-2: CR 4.1, NDR 1.6"
Ensure Bluetooth signal cannot be received outside the organization-controlled boundaries by employing emission security and purposefully positioning the device.	Multiple BLE pairing mechanisms are available to ensure availability of data. This safeguard reduces the likelihood of capturing or intercepting signals.	"ATT&CK for ICS: M0806 NIST SP 800-53 Rev5: AC-18, SC-40 ISA/IEC 62443-3-3: SR 5.2"
"Implement specific inventory, logging and monitoring of hardware and report security- related incidents associated with optimyze devices to Xylem. These might include unexpected operations, confirmed tampering, or theft of the device."	Devices are hardened and Xylem provides PSIRT to help customers investigate potential security incidents. This safeguard supports the ability to track assets and recognize potential security events.	"ATT&CK for ICS: M0947 NIST SP 800-53 Rev5: SM-8 ISA/IEC 62443-3-3: SR 1.11, SR 2.8, SR 3.4"
Maintain updated firmware and software on all devices and apps.	Device firmware integrity is maintained by cryptographically signing at the source and then verifying the authenticity and integrity at runtime. It builds on modern tools provided by our partners. Sometime vulnerabilities are discovered, and we work with our partners to deploy updates to security and resilience. This safeguard mitigates exploitation risks and ensures security patching.	"ATT&CK for ICS ID: M0951 NIST SP 800-53 Rev5: MA-3(6) ISA/IEC 62443-3-3: SR 3.1.3, SR 7.1"
Ensure cybersecurity policies, awareness, and training to the operators, administrators and other personnel.	While the system has been hardened in many ways, this safeguard prevents Social Engineering attacks and promotes awareness related to cybersecurity.	NIST SP 800-53 Rev5: AT-2 ISA/IEC 62443-2-4: SP.01
Before device disposal clear all paired connections and disable accounts.	No data is persistent on the Gateway device, but BLE bonding is enabled for continuous gathering of sensor data. This safeguard ensures that no one can connect to your sensors using already-paired devices.	ATT&CK for ICS ID: M0942 NIST SP 800-53 Rev5: SR-12 ISA/IEC 62443-3-3: SR 4.2

For additional information see references:

- ATT&CK for ICS available online: https://collaborate.mitre.org/attackics/index.php/ Mitigations
- NIST SP 800-53 Rev 5 available online: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-53r5.pdf
- ISA/IEC 62443 standards available for purchase from ISA, IEC, or ANSI.

xylem
Let's Solve Water

Xylem Inc.
8200 N. Austin Avenue
Morton Grove, Illinois 60053
Phone: (847) 966-3700
Fax: (847) 965-8379
www.xylem.com

Xylem is a registered trademark of Xylem Inc. or one of its subsidiaries. All other trademarks or registered trademarks are property of their respective owners.
© 2023 Xylem Inc. XYL-CYGD-14008 August 2023