xylem
Let's Solve Water

Smarter Together

Building Cybersecurity in the Water and Wastewater Industry

GRIFFIN HARRISON
PRODUCT SECURITY LEADER

Why is cybersecurity important to water?

3 in 10 people worldwide lack access to safe drinking water

6 in 10 people worldwide lack access to safely managed sanitation services

$320
Billion USD

Estimated $320 Billion savings from 2016 to 2020 due to digital adoption

The key to solving the global water crisis lies with digital solutions

xylem

cybersecurity important to water?

$320
Billion USD

Estimated $320 Billion savings from 2016 to 2020 due to digital adoption

Water systems operators can benefit in terms of economics and sustainability

Re-investment in capital assets

Security is the foundation for a successful digital transformation

xylem

Why is cybersecurity important to water?

Over $1 Trillion USD / 950 Billion €
Lost globally due to cybercrime, more than a 50% increase since 2018. Average cost per incident is over $500k USD / 477 €.[1]

Number of Threat Actors Increasing
7 threat actors shown to specifically target water and wastewater infrastructure globally[2,3]

150 Vulnerable Products
Used in water and wastewater systems[4]

20,000 Utility Employees
Fear that cyber threats could have the biggest impact on operations[5]

3rd Most Targeted Sector
When compared to other critical infrastructure[6]

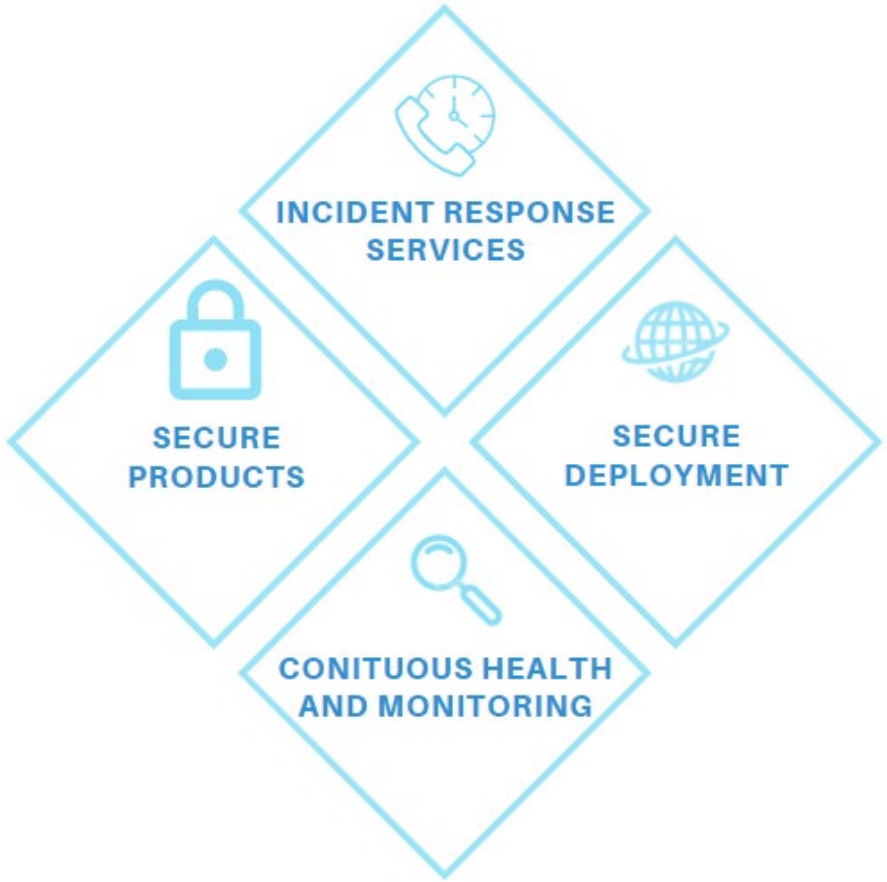
$18.2 Million USD / 17.5 Million €
Lost due to the 2019 ransomware attack against a single water utility[7]

See backup slides for sources

Attacks on water infrastructure are already happening today.

xylem

What is successful cybersecurity?



Secure products by finding and fixing weaknesses while engineering

Secure deployments with defense-in-depth that manages risks to the operations of systems and products

Continuous health and monitoring ensures continuous improvement against emerging vulnerabilities and threats

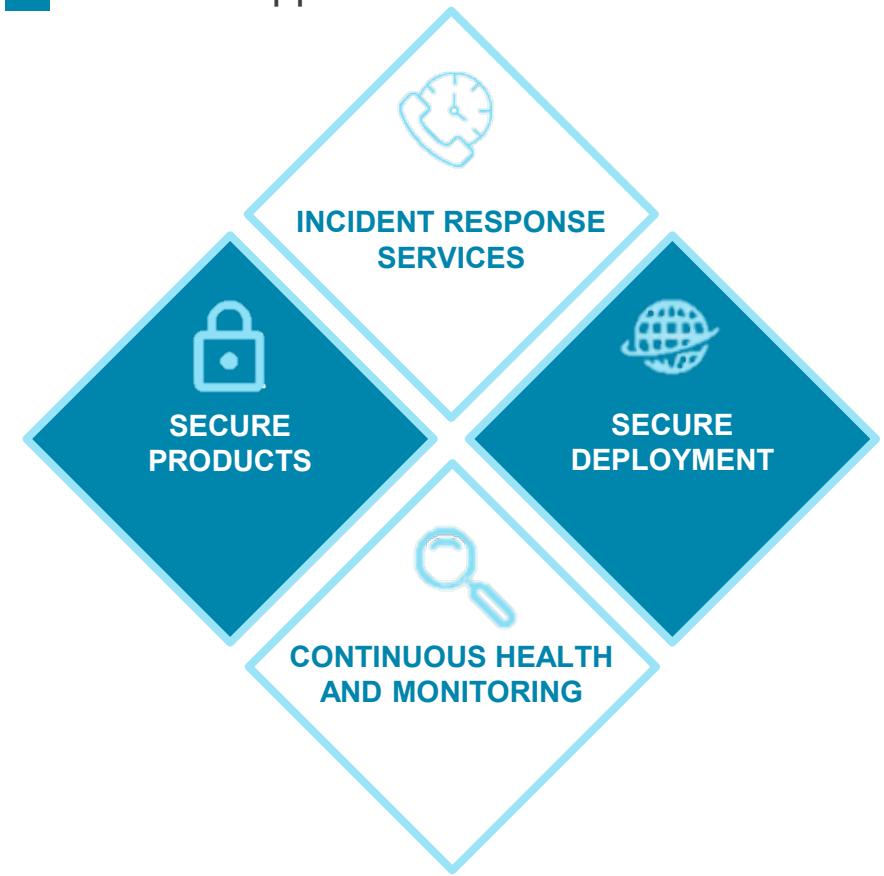
Incident response services assures optimal forensics and response for safe and continuous operations

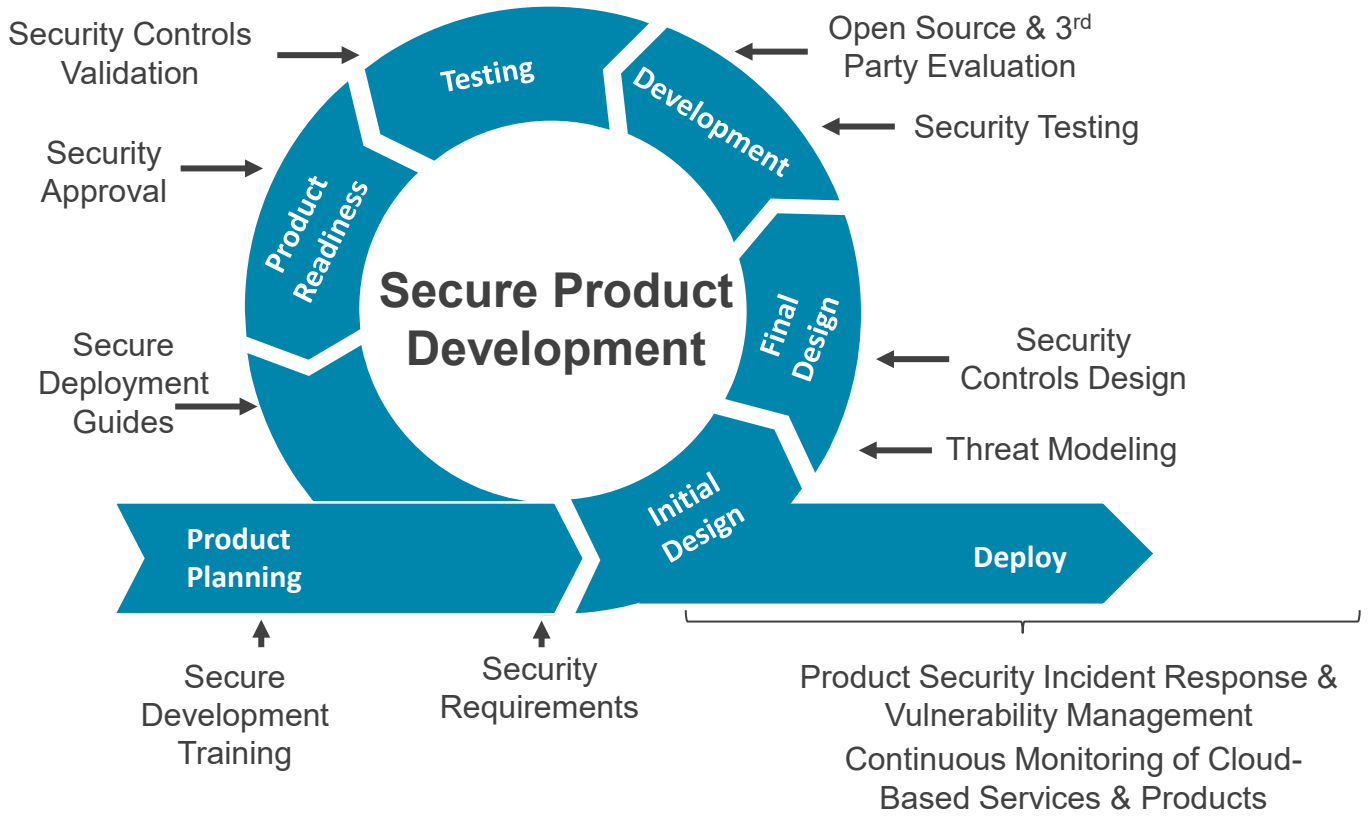
The operator of the utility is the end owner of security risk, but responsibility for security protection falls on the product vendor, integrator, and operator.

Product Supplier Responsibilities

- Secure – By Design: *From Initial Concept to End of Life*
- Global Visibility – From emerging regulation, to localized threats
- Defended – With transparency

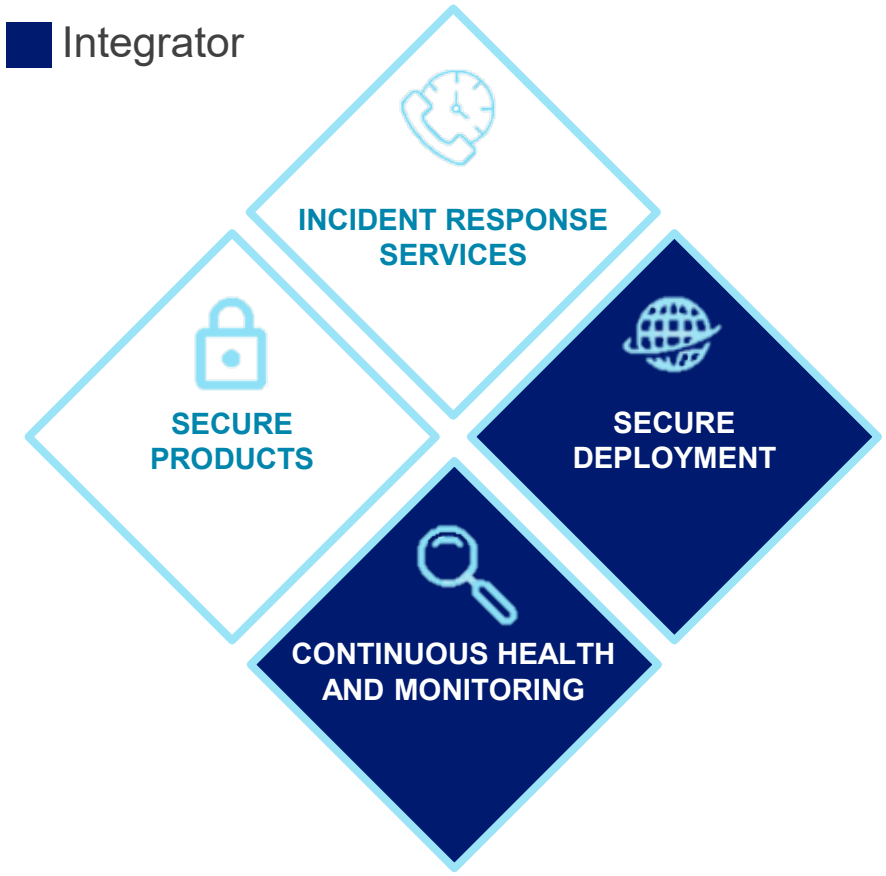
Product Supplier

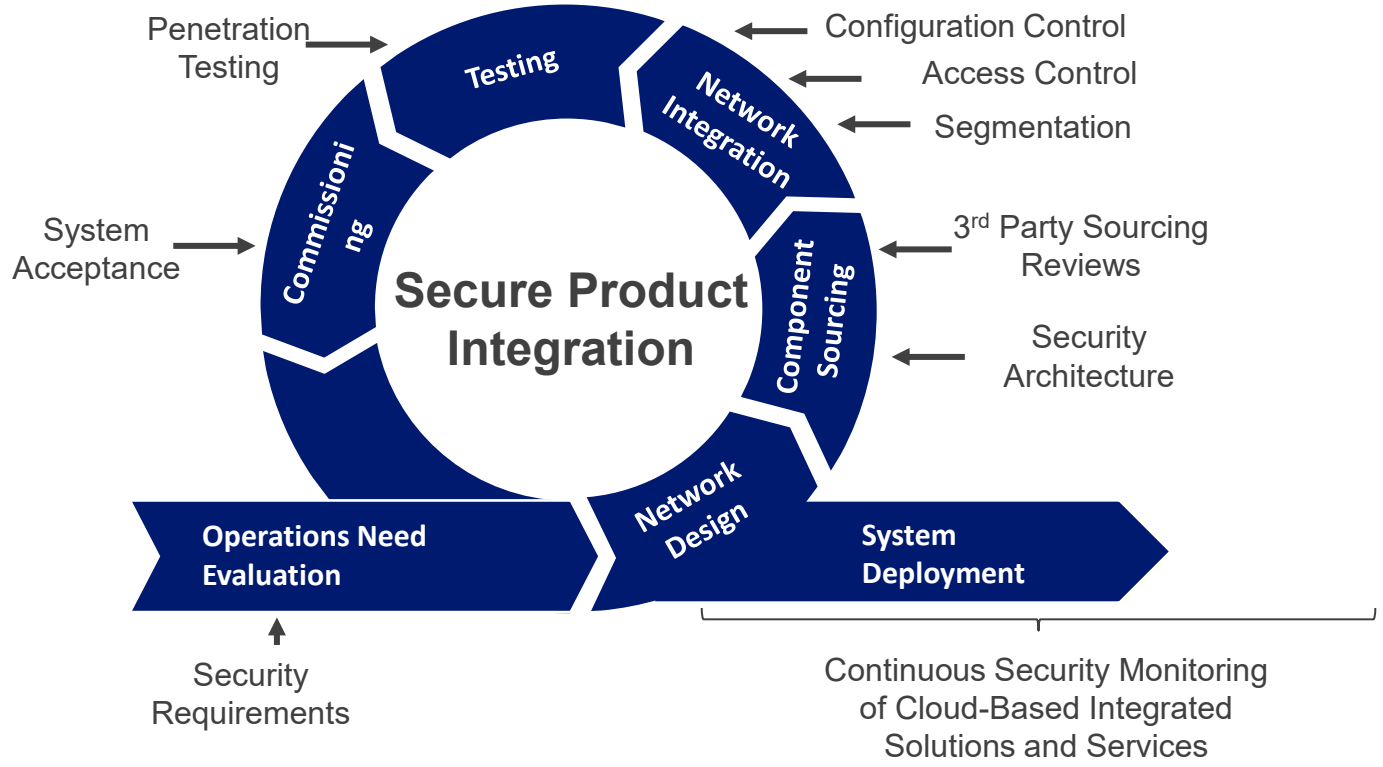




Integrators Responsibilities

- Secure Deployment
- Establish continuous health and monitoring: *Patch Management, Collection Management Framework, Access/Identity Evaluation, Anti-malware, Firewalls, Secure DMZ*

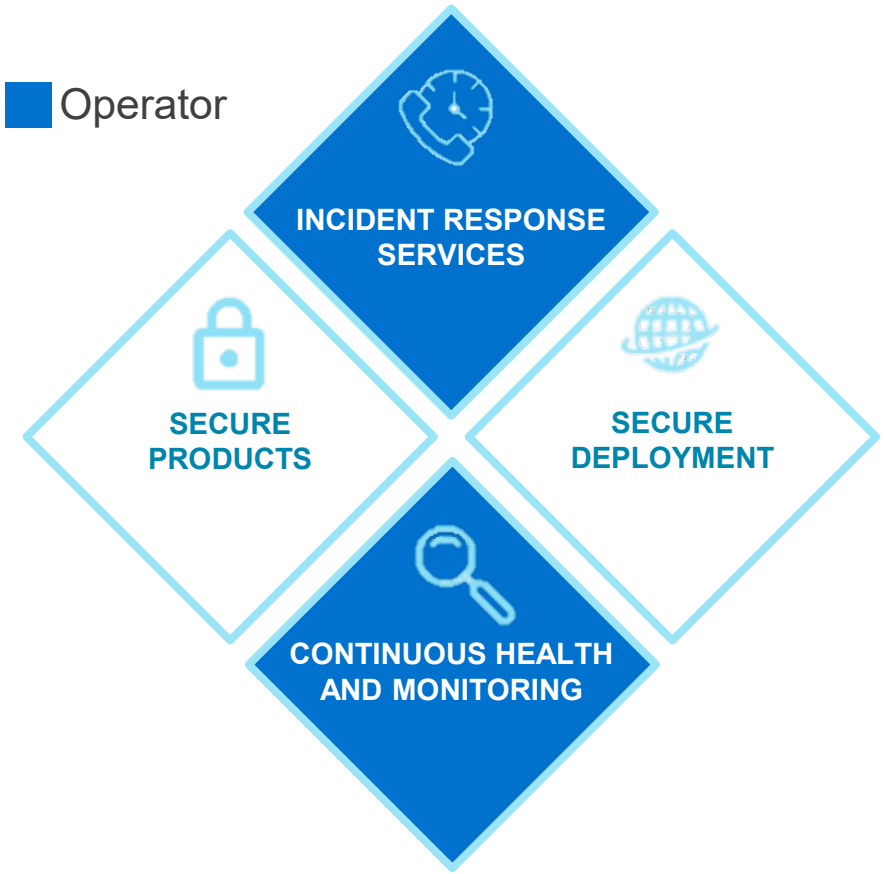


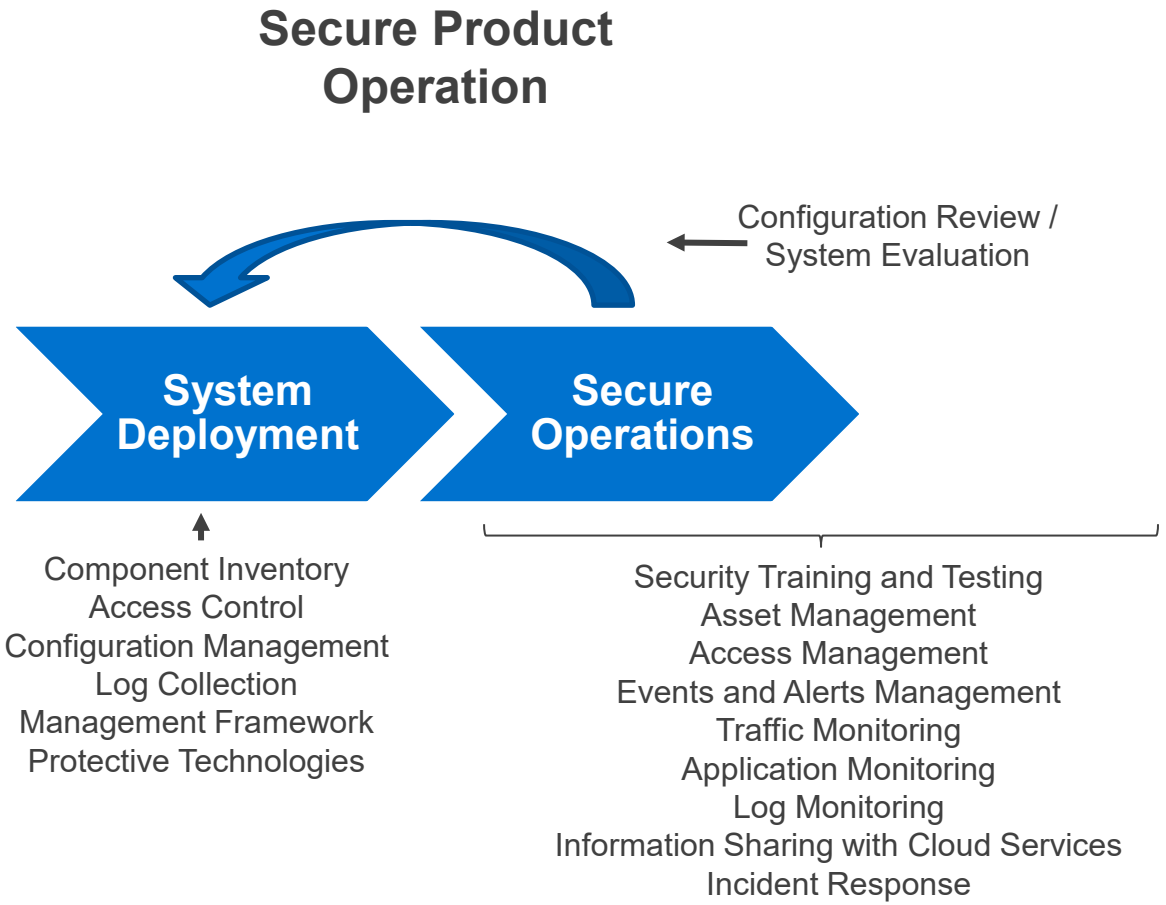


xylem

Operator Responsibilities

- Continuous health and monitoring strategies: *Log Monitoring, Event Monitoring, Backups, Patch Management, Anti-malware, Firewalls, Produce Reviews, Secure DMZ, External Reviews, Threat hunting*
- Incident response: *Log Management, Cyber Intel, Incident Reporting, Escalation Management, Security Exercises, Response and Recovery, Digital Forensics*



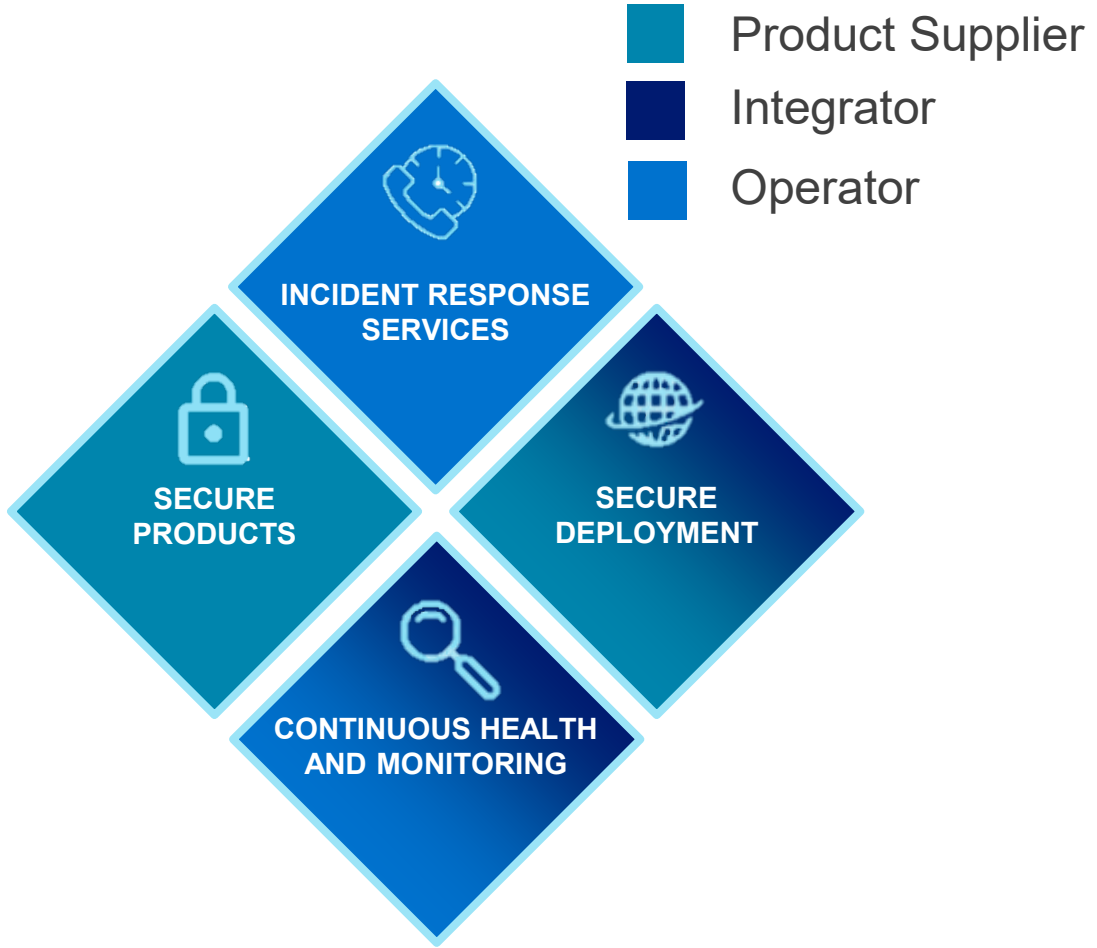


Closing: Strong Security Requires Partnership

1. **Digital transformation is necessary** to enable environmental and financial benefits in the water industry

2. Strong security will be built out through a **multi-barrier approach** involving **collaboration and engagement** across multiple parties

3. Industry focus should be on building **strong access control,** organizing **collection management and response,** and creating **strong IIOT-based reference architecture for evaluation**



Strong cyber security requires clearly defined roles for security management and partnerships across certain responsibilities.

Closing: Strong Security Requires Partnership

We offer these 5 Cybersecurity Assessment Services:

1. **Architecture Review** – *related to data flows*
2. **Vulnerability Review** – *checks customer's assets against cybersecurity databases (NVD, etc.) and recommends what needs to be fixed*
3. **Maturity Assessment** – *reviews customer's remediation skills and processes*
4. **Health Check** – *reviews deployed Xylem products to ensure their ongoing cybersecurity*
5. **Incident Response** - *based on prepaid retainer hours with specific response time service level agreement (SLA) commitments.*

Questions?

For more information, visit or contact us at:

- Xylem.com/security
- security.services@xylem.com

Slide 4 Sources, Cited

- 1. Malekos-Smith, Z., & Lostri, E. (2020, December). The Hidden Costs of Cybercrime. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
- 2. YouTube. (2021, May 21). Building Cyber Security in the Water and Wastewater Industry [Video]. https://youtu.be/RhKRu5egoZo
- 3. Baseline Information on Malevolent Acts for Community Water Systems. (2022, June). EPA. https://www.epa.gov/waterriskassessment/baseline-information-malevolent-acts-community-water-systems
- 4. Sreedhar, B., & Bhatnagar, S. (2020, August). Industrial Control System Security Market - Global Forecast to 2025 (TC 3075). Markets and Markets.
- 5. Germano, J. H. (2019). Cybersecurity Risk & Responsibility in the Water Sector". American Waterworks Association. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013
- 6. Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeldf, A., & Banks, M. K. (2020). A Review of Cybersecurity Incidents in the Water Sector. Journal of Environmental Engineering, 146, 1.
- 7. Duncan, I. (2019, May 29). Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts". The Baltimore Sun. https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html

xylem