xylem
Let's Solve Water

ASK YOUR POTENTIAL VENDORS – "ARE YOU HELPING ME ON MY CYBERSECURITY JOURNEY?"

How do you choose the right digital vendor provider and partner? How can you be sure that your vendors are trustworthy and reliable? By asking about how a provider delivers, not just what they deliver, you'll gain better insights.

Xylem is a partner with MITRE and others in the development of a System of Trust Framework, which provides a taxonomy of ways to build trust in suppliers, their supplies, and their services. The following questions represent examples from the System of Trust that align with what Xylem asks its suppliers.

Sample questions to ask your potential vendor(s):

1. What are your **general cybersecurity practices**? For example, how will your company protect my information?

Be on the lookout for or ask specifically about how they will protect your billing information, process requirements, and specifications.

The potential vendor could mention alignment to standards such as ISO 27001 (information security management objectives) or ISA/IEC 62443-2-4 (cybersecurity expectations of automation vendors and system integrators).

2. What is your **secure development process?** For example, how does your team manage security processes involved in requirements collection, product design, development testing, and vulnerability disclosure?

This answer will help you determine if the potential vendor's product was designed with security in mind, and on an ongoing basis. You want to be kept current on any uncovered product vulnerabilities that are discovered over time.

Standards and best practices for secure development, which will help ensure you are buying secure products, include:

a. ISA/IEC 62443-4-1 - ISA-developed standard for an engineering office to have the processes and procedures to design, develop, and test secure industrial automation and control components.

b. NIST SP800-218 – The NIST Secure Software Development Framework (SSDF) is a framework to create a standard language for asking what secure design, development, and testing practices product vendors implement.

c. OWASP SAMM – The Software Assurance Maturity Model is a way for offices that develop software or digital products to describe the state of their secure development processes.

d. Synopsis BSIMM – The Building Security In Maturity Model is a reference framework that Synopsis uses to benchmark security development processes of organizations that develop digital products.

e. SAE JA7496 – This standard provides descriptions of technical processes that result in a security assurance case for a cyber-physical system or component.

3. What kind of **secure deployment guidance** will you provide to my team related to your systems, products, and components? Will you provide security context for each of your components, products, or systems we purchase, which may include: describing security requirements, defense-in-depth controls, etc.?

This will help you determine if the potential vendor is a partner who will help you securely install and maintain your software.

Standards or references that may help confirm the potential vendor will provide you with respected industry standard secure deployment guidance include:

a. ISA/IEC 62443-4-2 provides a list of specific security controls that you would expect in an industrial automation/control component.

b. ISA/IEC 62443-3-3 provides a list of specific security controls for a packaged industrial automation/control system.

c. NEMA HN 1-2019 while not a water sector standard, this provides criterion for how the medical device industry expects disclosure of security controls.

4. Can you provide a software bill of materials (SBOM)?

This will help give your team an understanding of the potential vendor's product components and composition. While there is no standard for water, NTIA has published The Minimum Elements for a Software Bill of Materials (SBOM).

5. Where do you responsibly disclose vulnerabilities? What service level agreements (SLAs) do you promise for sustaining products (e.g., frequency of updates)? What processes do you have for coordinating with customers' incident response, when the incident involves your products?

These answers will help you understand potential vendor's **incident response and vulnerability management practices.**

FIRST.org provides guidance on what to expect from a Vendor's Product Security Incident Response Team (PSIRT) Services Framework. Most companies provide this information publicly to the National Vulnerability Database (NVD) and on their own website e.g., company.com/security. Xylem publicly discloses security vulnerabilities here.

6. (For **Cloud Connected Products**) Ask potential vendors, "What continuous monitoring services are included with your cloud-based products?"

This will help you determine if the potential vendor's cloud-based software / service is safe to engage with, eg: is it kept under constant surveillance, where is your data stored, if you stop working with them, can you take your data with you, is your private information kept secure and/or are identifying data points stripped so that your business is not identifiable in case of a hack, etc.

While there is no standard for water, Cloud Security Alliance (CSA)'s C-STAR has common criteria for cloud service organizations.

7. Does your business provide security services beyond your products, systems, and components? For example, do you have a security service to check my systems for security or integration readiness?

If your business needs this, it is nice to have a vendor partner who is equipped to offer these services to your team.

Additional Tip: Instead of questionnaires, it may be better to establish a minimum expectation and have vendors sign up to agree to those minimum expectations in the product or services contract. If you follow this course of action, then you might consider requesting audit rights at a reasonable frequency (e.g., annually) on your master services agreement / contract (MSA).

Learn more about Xylem's Utility Cyber Security practices.

xylem
Let's Solve Water

www.xylem.com/security