“Integrating static testing, dynamic testing and emulation, reverse engineering, attack mapping, and vulnerability analysis tools into the agile Continuous Integration and Continuous Deployment (CI/CD) pipeline is imperative.”

Product Security as a Service

AIT

Applied Integrated Technologies

Isiah Jones
Cyber Engineer (ICS OT IIoT IoT)

May 2023

Product Security as a Service

to Enhance Product Resilience through Continuous Improvements

With a resurgence on the secure design of components and devices, as well as enabling security features out of the box by default, it has become increasingly apparent to AIT that several product creators, installers, integrators, maintainers, and users do not know how to implement product security. To complicate matters, they also lack the tools and in-house personnel to enable these features. Regarding secure by design for industrial control systems (ICS), automation systems, operational technologies (OT), embedded systems, components and devices, firmware, software, applications, internet of things (IoT), safety systems, and industrial IoT (IIoT) there are the "*haves*" and the "*have nots*." Our Product Security as a Service will help you become one of the "haves"

Discover the benefits of integrating security into the product development lifecycle:

☑ **Enhanced product integrity** is achieved by checking the embedded components within a designed product, from the circuit board level chips to firmware, DevOps environments, to source code, APIs, applications, and software.

☑ **Seamless integration** of building, integrating, executing, and enforcing gate reviews, product test sampling, and regular scaling tests ensures rigorous product verification and validation throughout the development process.

☑ **Continuous improvements to product design** and independent third-party ongoing testing collaboration with the product teams.

☑ **Ability to scale product security maturity** with the help of independent third-party security engineers and hiring dedicated in-house product security staff.

☑ **Secure by design policies are codified and reinforced** particularly in cloud-based DevOps pipelines and code repositories with the adoption of testing, emulation, and modeling technologies.

☑ **Regular certification of the product development lifecycle** and individual products as significant features and version changes occur in an agile DevOps culture.

☑ **Product resilience is boosted** by routinely testing and verifying industry-discovered weaknesses in product design, components, and functionality.

☑ **Risks are swiftly identified and mitigated** thanks to regular in-house or trusted independent third-party discovery and mitigation of product design, component, or functionality weaknesses.

☑ **A thriving culture of *secure by design* and *secure by default* develops** and matures, promoting security-conscious functional testing as part of product innovation, due diligence, and due care.

☑ **Distinguishing your products from competitors** a time of increasing global awareness and concern over the safety and security of products, devices, firmware, software, and components.

We must continuously test, verify, validate to improve security of components, devices, hardware, firmware, applications, and software."

Several larger OT product vendors (e.g., Siemens, Emerson, Honeywell, Johnson Controls, Schneider Electric etcetera) have improved product security over the years due to formalizing and continuously improving their product development lifecycles. Many such vendors have even gotten their product development lifecycle practices certified under part 4-1 of ISA/IEC 62443, as all product creators should. However, when it comes to "secure by design," it is not enough to create and improve development lifecycle practices. Increasingly, there is a societal imperative to continuously test, verify, validate, and improve the components, devices, hardware, firmware, applications, and software.

Part 4-2 of ISA/IEC 62443 has yet to see security level 3 (SL3) product certifications. Most products on the market are only tested and certified to SL1 or SL2. Several effective technical component requirements appear at SL2, SL3, and SL4. But at SL3, you begin to get requirements such as concurrent session control, active monitoring and alerting of tampering attempts, and hardware security for symmetric key-based authentication, for example. Additionally, many of the certified products are only from the major OT vendors but lacking amongst the broader ecosystems of product vendors. For example, many of the packaged solutions vendors across several sectors (e.g., manufacturing, buildings and facilities, oil and gas, water, and wastewater) are not putting their products through secure design lifecycle practices or component product security testing and independent certifications to part 4-1, 4-2 and 3-3 of ISA/IEC 62443.

AIT sees a rise in the need for product creators, installers, integrators, modifiers, and users to have product security as a service provided by organizations that can help them build a mature product development lifecycle. More importantly, they need services to execute the testing, reverse engineering, vulnerability analysis, attack mapping, and continuous improvement feedback loops during the product development lifecycle. Having the ability to integrate static testing, dynamic testing and emulation, reverse engineering, attack mapping, and vulnerability analysis tools into the agile Continuous Integration and Continuous Deployment (CI/CD) pipeline is imperative. In addition, regularly executing security test cases, supporting supply chain testing of embedded components and devices, and helping target prioritized product improvements are essential to achieve component secure by design assurances.

Existing security practices, frameworks, guidelines, and standards require creating and continuously improving a secure product development lifecycle. Additionally, existing standards provide technical requirements for baseline product functionality and product design user story capability requirements. These technological capabilities, policies, practices, and procedures can then be validated, tested, verified, and enforced regularly in an agile CI/CD product design lifecycle. Some of those practices, frameworks, guidelines, and standards include:

- **NIST SP 800-218 Security Software Development Framework (SSDF)** – where preparing the organization, protecting software, producing well-secured software, and enabling the ability to respond to product vulnerabilities are practices further defined by minimum baseline tasks, requirements, and practices.

- **NIST SP 800-160 Systems Security Engineering** – defines how to integrate security into the Systems Engineering lifecycle by including systems engineering phases such as verification and technical validation processes.
- **ISA/IEC 62443 part 4-1 – Product Security Development Lifecycle Requirements** – where requirement practices such as security management, specification of security requirements, secure by design, secure implementation, security verification, and validation testing, management of security-related issues, security update management and security guidelines are baseline practices. These practices are further broken down into sub-requirements, tasks and product development lifecycle maturity levels of 1 (Initial), 2 (Managed), 3 (Defined and Practiced), and 4 (Continuously Improving).
- **ISA/IEC 62443 part 4-2 – Technical Security Requirements for Components –** where component types (host/platform, software/application, embedded devices/components, and communications components) are broken down into security levels and technical requirement enhancements. These break downs center around identification and authentication control, use control, system and component integrity, data confidentiality, restricted data flow, timely response to events and resource availability. **Note part 3-3 has the same family of security levels, requirements enhancements, and groupings of foundational requirements as part 4-2, but 3-3 focuses these requirements on the systems and systems of systems level rather than specific components and devices defined in part 4-2.**

AIT's engineering professionals have global experiences providing component and system design reviews, security assessments, QA/QC of code, attacking components and systems, validation and verification of component and system designs, and serving on security standards and practices committees, to drive continuous improvements throughout the global ecosystem. AIT's ICS OT security engineers are regular contributors and members of ISA/IEC 62443 and ISA84.00.09 standards committee working groups. AIT's staff also maintain current GICSP and CISSP certifications. Lastly, AIT regularly builds new relationships and partnerships with security tooling partners to enable customers to scale and integrate regular testing, validation, and verification into their product lifecycles and product design ecosystems. To seek out product security as a service support, email otcyber@ait-i.com.