SYNOPSYS®

Building Security Into Your Medical Device Development Process

Achieve practical, cost-effective security risk management by building security directly into your medical devices and systems

Overview

As medical devices and systems become more connected, they deliver better patient care, but their exposure to malicious attacks increases. Safety risk management is not enough to ensure your medical products are secure. You also need to identify security risk, balance that risk with usability and availability, and achieve regulatory approval. Practical, cost-effective security risk management requires building security directly into your products, and Synopsys can help you get there with tools and services to find, fix, and even prevent security vulnerabilities.

Medical device security expertise

Whether you need to test one device quickly, identify the risks in a complex system of devices and applications, or establish a secure development process, Synopsys experts can help. Our assessment experience includes a broad range of both medical embedded systems, including implanted devices, drug delivery systems, and surgical imaging systems, and nonmedical systems, such as ATMs, gaming consoles, and smart meters.

Beyond regulatory compliance

Move beyond the minimum compliance requirements for security risk management, and focus on building security into your program. We can help you proactively respond to, mitigate, and even prevent potential data breaches and software security attacks through flexible secure-design services.

Leadership for medical device security

We are actively involved in medical and healthcare industry efforts to help customers build more secure care-delivery systems. Our team collaboratively creates secure-design guidance documents through the Association for the Advancement of Medical Instrumentation (AAMI) working groups, including IEEE's Avoiding the Top 10 Software Security Design Flaws and Building Code for Medical Device Software Security.

Raising security programs to maturity

Whether your organization is traditionally reactive or compliance-driven, our industry-leading experts can help you elevate your secure development program through a proactive and disciplined approach, leading to security maturity. Our unique approach and flexible, scalable services allow you to integrate security throughout the entire development life cycle.

Service	Description
Penetration Testing	Pen testing embedded and software-only systems helps you identify risks so you can resolve them and prevent them from reoccurring. We perform high-quality, multidepth system pen testing for embedded devices, mobile apps, and applications at any stage of the development life cycle. For any system, no matter the environmental complexity, we have a solution to meet your needs.
Threat Modeling	Our expert teams can help you build a threat model that describes your system's attack surface by identifying major software components, assets, threat agents, security controls, and corresponding relationships between objects. The threat model produces a traceability matrix that you can incorporate into both design inputs and regulatory submissions.
Architecture Risk Analysis	A deeper examination than a threat model, architecture risk analysis highlights design flaws that automated tools can't find. It also provides specific mitigation and remediation advice for individual defects. Draft guidance from the FDA requires that organizations consider cyber security risks as part of the development process. Consider an ARA a step beyond what's required for cyber security risk management.
Secure Code Review	Are you looking to have source code reviewed for a single application or outsource your entire program? Are you incorporating open source software and want to know what you are using? Synopsys conducts hundreds of source code reviews every year, using automated and manual code review techniques.
Software Development Life Cycle (SDLC)	Synopsys can help you build an SDLC that includes each of the security touchpoints necessary to create secure products. Each SDLC phase requires different tools and techniques for creating more secure products, from requirements and use cases to medical device post-market monitoring.
Instructor-Led Training (ILT)	Available as an annual subscription, our suite of software security training classes helps customers attain compliant internal secure coding standards. If you want a more focused, hands-on approach, our instructors will come to you and deliver a full day of training on topics such as threat modeling, architecture analysis, software security fundamentals, security requirements, defensive programming, secure code review, and more.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™