SYNOPSYS®

www.synopsys.com |

Policies and Standards Development

Give your software security initiative a clear direction

We work with you to create policies and standards that define the scope of software security program within your organization, establish roles and responsibilities, and provide a common definition of terms that facilitate communication.

Do I really need policies and standards?

Definitely. You can reduce or eliminate many security vulnerabilities simply by documenting application development security standards and policies. These standards provide developers pragmatic and clear guidance on what your company will accept and what it will not. They also help to:

- Measure the effectiveness of your security program
- Ensure consistent development and application testing
- Establish acceptable security minimums for building and deploying applications

3 areas of policies and standards

We'll help you create policies and standards that define the scope of software security program in your organization, establish roles and responsibilities, and develop common term definitions. This includes:

1. Governance and strategy

Define authority and responsibility to address software security across your organization. Establish driving principles and requirements for software development and acquisition projects. Define clear intersection-points (gates) when projects must inject security and verify achievement.

2. Portfolio risk assessment

Identify the asset catalog exposing your organization to software-induced risks. Leverage an optimal question set to focus resources on assets posing highest risk.

3. Standards development

Reduce threat realization through language-independent and architecturally neutral standards which deliver actionable technology and language-specific instructions for developers.

Final goal: Risks identified and addressed!

Everything you need to succeed

Policy and standards development starts by gaining appreciation for your unique business circumstances. We highlight key decisions required, outline options, and customize appropriately. A typical Policy, Standards, and Guidelines framework comprises the following elements:

> Know your mission, communicate to stakeholders, identify risks, and secure the enterprise.

- **Software Security Initiative Charter.** Specifies authority and organizational scope for the program.
- **Secure Software Development Life Cycle (SSDLC) and Product Development Life Cycle (PDLC).** Outlines a secure overlay for your agile, spiral, or traditional SDLC and acquisition process.
- **Software Security Policy**. Describes overarching principles of operation. For example, the directive regarding SSDLC contains a brief instruction for the two formal interactions between security and development.
- **Secure Coding Guidelines**. Provide extensive range of technology/language-specific help for development teams.
- **Software Risk Ranking Policy and Calculator**. Defines a methodology and attributes to assign a risk ranking to software assets.
- **Project (Impact) Risk Ranking Policy, Calculator, and Activity Selection Matrix**. Defines a methodology and attributes to assign a risk ranking to projects modifying software assets.
- **Data Classification Policy.** Defines classification levels including example data elements for each category.

A roadmap to guide you forward

We'll provide you with an 8-Quarter Roadmap outlining a path from current state to a maturing SSI. You can use this roadmap to circulate the total scope of an effective SSI with executive and development stakeholders as a first step to seeing policy positively accepted and implemented.

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

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: software-integrity-sales@synopsys.com