SYNOPSYS®

www.synopsys.com |

Architecture Risk Analysis
(ARA)

Identify flaws within a system's design to improve your security posture

Years of experience have taught us that half of the software defects that create security problems are flaws in your system's design. Simply scanning software for security bugs within lines of code or penetration testing your applications ignores half of the problems that leave your organization vulnerable to attack.

Remediate problems early in your SDLC

By addressing security early in your design, you can avoid costly rework to address security defects found later in the SDLC. Most importantly, finding and remediating security problems earlier in the Software Development Lifecycle (SDLC) is less expensive, invasive, and time consuming than waiting until code is written or QA tests are performed.

Get a clear picture of your risks

Our experts will produce a list of technical risks and recommendations on the methods, tools, and strategies for mitigating the identified technical risks. We'll also help you understand the related business risks and provide proper mitigation advice to reduce risk to an acceptable level.

Uncover weaknesses in your design

An ARA reviews your application design in depth to look for weaknesses that might allow attacks to succeed. These design deficiencies are found by analyzing the system's major software components, trust zones, assets, security controls, asset flows, and threat agents. An ARA can point out if any of your security controls can be bypassed, are weak, or are the wrong controls for what you're trying to achieve.

Find and remediate weaknesses in your design

BEFORE THEY ARE EXPLOITED.

How an ARA works

Our architecture risk analysis consists of four essential steps:

1. Analyze business context

We conduct interviews with business owners of the system to gather and analyze the information to better understand the security risks that impact the business goals of the system.

2. Create a threat model

We identify major components, assets, threat agents, and security controls that exist in the system then create a diagram to capture these entities and the relationships between them.

You'll walk away with a comprehensive list of system options for removing risk completely or mitigating risk to an acceptable level for your business.

3. Conduct a risk analysis

We identify software-based risks and prioritize them according to business impact (e.g., unauthorized access to data or service availability). Activities that comprise our analysis include:

- **Known Attack Analysis.** We draw from a set of known attack patterns to model subsystem and application behavior for the components in the system being reviewed.
- **System-Specific Attack Analysis**. We evaluate the foundations of system architecture as it relates to well-established security principles. We also look for unspecified software behaviors with little independent impact that may combine to create critical vulnerabilities.
- **Dependency Analysis**. We focus on peeling back the layers of the software in the platform to understand the security risks introduced or mitigated by each layer.

4. Provide mitigation advice

At the end of each assessment we conduct a read-out call with the appropriate development team to review each vulnerability identified during the assessment, answer any questions that the team might have around each vulnerability, and discuss mitigation/remediation strategies.

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

© Copyright 2017 Synopsys, Inc. All Rights Reserved Worldwide. | www.synopsys.com |