SYNOPSYS®

www.synopsys.com |

Security Control Design Analysis (SCDA)

How well do your security controls align with industry best practices?

We'll help you scale a standardized design review process across your entire portfolio to identify where software security related elements of your system design don't adhere to industry best practices.

Find flaws that typical tests miss

Our experts review up to eleven key security controls to find system defects related to security controls that are not identified through other activities such as pen testing, DAST, or SAST. These include:

- Authentication
- Authorization
- Cryptography
- Input Validation
- Output Encoding
- Auditing/Logging
- Availability
- Monitoring/Alerting
- Session Management
- Runtime Environment Verification
- Password Storage

3 benefits to implementing an SCDA

1. Identifies when security controls have been:
   - Reviewed and align with best practices
   - Reviewed and violate best practices
   - Reviewed and are missing
   - Haven't been reviewed
   - Aren't applicable
2. Highlights systematic software security problems within a:
   - Region
   - Business unit
   - Tech stack
   - Specific attack

Are your security controls as strong as they should be?

3. Provides useful insights

The insight an SCDA gives you into your software will help you improve your SDLC by highlighting what to test, where additional training might be recommended, and more.

We have the expertise, tools, and services you need

Synopsys offers the most comprehensive architecture and design solutions for building security and quality into your SDLC and supply chain. To complement an SCDA, check out:

- **Threat Modeling:** We unearth vulnerabilities in your applications by looking beyond the typical canned list of attacks to model all the ways different types of threat agents might interact with your attack surface.
- **Architecture Risk Analysis:** An ARA enables you to find and remediate security problems earlier in the SDLC, which is less expensive, invasive, and time consuming than waiting until code is written or QA tests are performed. However, even if you're system is already built or deployed, an ARA can be immensely valuable.

Whenever possible, guidance is provided on how to mitigate the identified risks and conform to industry best practices.

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