SYNOPSYS®

www.synopsys.com |

Software Security Metrics Development

You can't manage what you don't measure

If you're like most organizations, you have limited visibility into the impact your security choices have on your business goals. You might not even be collecting data at all. We can help you choose well-defined, achievable metrics tailored to your company's risk profile and business processes.

Visibility, accountability, and support

Metrics can ensure visibility, accountability, and management of your Software Security Initiative (SSI). Without metrics, you can't communicate the value of your SSI to your company's leadership team. That can compromise your ability to get funding for the program, leading to greater vulnerabilities in your software and a lower-quality product. Stakeholders who understand the context of raw numbers are more likely to accurately interpret them and make smart, strategic decisions to improve their security posture.

There are four key areas metrics can help you track:

- **Defect discovery**: How effectively are you finding defects and risks?
- **Policy compliance**: How effectively are you complying with industry standards and requirements?
- **Risk reduction**: How effectively are you fixing vulnerabilities?
- **Risk prevention**: How effectively are you preventing future risk and building security in?

3 phases of security metrics

To select metrics that can demonstrate if your SSI is making reasonable progress, we...

1. Define your plan

We'll help you identify what measurements provide the most visibility, define your software security objectives, take inventory of your current activity, define key metrics, and provide objective insight into your SSI.

2. Turn measurements into knowledge

We help you identify process flows and data sources, and automate your data collection. This enables you to use metrics to drive actionable intelligence and improve performance.

Support your SSI with actual data

3. Communicate your findings

We'll work with you to define the context for your metrics in the form of business goals so you can better interpret your data and communicate it to the right people at the right time with the right visuals.

We'll guide you to success

Our goal is to show you how you can use metrics to determine what's working, what isn't, and what you need to change to improve your performance.

"We found 10 critical vulnerabilities this week."

Is that good or not? Without context, raw data can result in inaccurate perceptions of security and poor decisions.

Metrics can help you answer:

- How well protected your assets are
- How well you're detecting malware
- How well you're meeting your compliance goals
- What your high profile areas of risk are
- What's broken and needs fixing
- Whether processes are being performed consistently
- Whether service-level agreements are being breached

Metrics can help you track:

- Percentage of applications with penetration testing
- Percentage of defects eradicated
- Cost to fix per software security bug
- Cost of application security resources
- Number of applications tested
- Number of applications that meet or exceed compliance requirements
- Number of code errors that reach production
- Number of critical applications that require in-depth testing
- Time to create a secure application
- Time to run test per application

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