SYNOPSYS®

How to Get the Most Lift From Your BSIMM Results

Table of contents

7 ways to take immediate action after a BSIMM assessment

An assessment of your software security initiative based on the Building Security In Maturity Model (BSIMM) reveals how your program compares to others. Your scorecard helps you highlight areas of strength and identify gaps. What happens after you see your results determines how you will lower your risk of a cyber attack.

1. Pick your destination.

After a BSIMM assessment, you can set new performance targets. For example, you may decide to take a position of leadership in your industry and increase your score across all domains of the BSIMM (Governance, Intelligence, SSDL Touchpoints, and Deployment) by your next assessment—or perhaps just one.

Get inspired: A regional bank had trouble with software security governance. The security team discovered that organizations with the highest BSIMM scores have software security groups that establish, communicate, and enforce security policies. The team reviewed governance models and decided to improve communication and strengthen satellite support within other departments in order to become a best-in-class organization.

2. Prioritize security.

A BSIMM assessment can open your eyes to new strategies used by companies you admire. You can use this information to help make investment decisions. For example, you can choose to shift budget, determine what skill sets you need to hire, and define requirements for partnerships.

Get inspired: A large financial services organization considered itself a security expert but didn't provide training for employees. After seeing how low the organization scored in training compared to other mature security initiatives, leaders shifted resources to fund security training classes to help their team stay current.

3. Create a flight plan.

The BSIMM ranks security activities based on three levels of maturity. Using the model as a guide, you can evolve your own security journey in stages, first building a strong foundation and undertaking more complex activities over time.

Get inspired: The security team of a consumer products company wanted to reduce security vulnerabilities found at the end of their development process. They decided to implement source code review. Their initial strategy was to perform ad hoc reviews, with a long-term goal of making source code review mandatory on all projects.

4. Aim high.

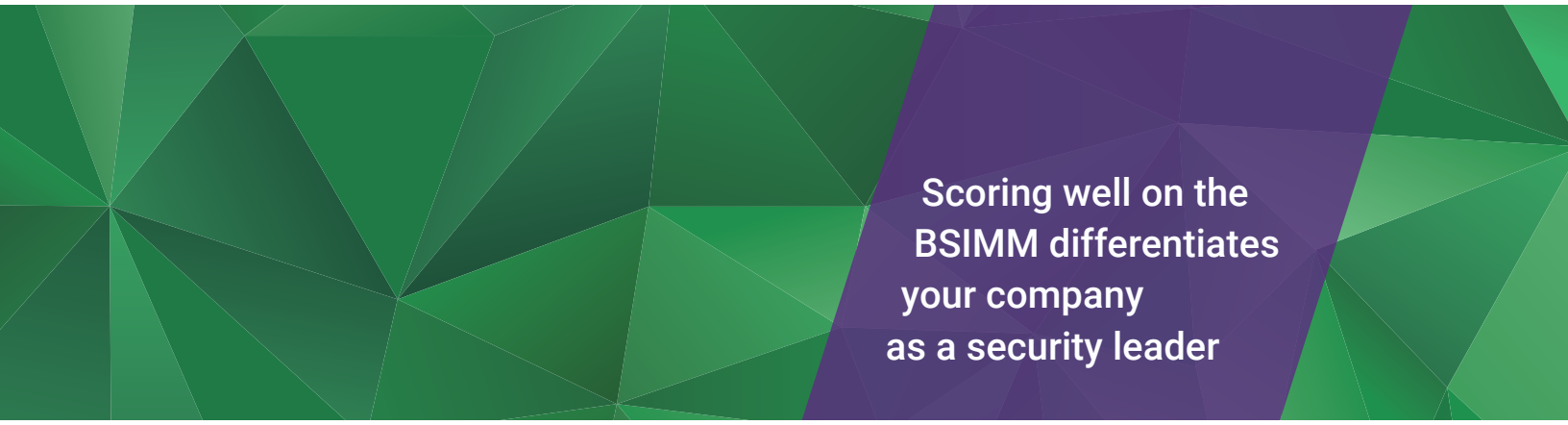
If you show your leadership irrefutable evidence that your company is not keeping up with similar organizations in the fight against cyber terror or that your peers are better at protecting their own and their customers' sensitive data, your leadership is more likely to approve security investments and resources.

Get inspired: A market leader had acquired several smaller companies and was struggling to cover all development projects with existing security resources. BSIMM results showed the ratio of the organization's security staff to developers was much lower than that of its peers. The organization used this information to make the case for additional headcount and third-party support.

5. Show where you soar the highest.

Scoring well on the BSIMM differentiates your company as a security leader. When you communicate your security posture to customers, partners, and regulators, you'll know you have the data to back it up.

Get inspired: After confirming the company's position as a security leader using the BSIMM, an established security organization required all third-party development shops to integrate software security best practices into their development process before the company would take them on as new vendors.



6. Make sure you're all headed the same way.

You can use the BSIMM as a common framework to structure conversations about software security. You can share the terminology and methodology with security teams, developers, software architects, business owners, and executives in your communications and progress reports.

Get inspired: A large healthcare company had difficulty integrating security into their development process. The developers didn't believe it could be done. The security team used BSIMM data to show that many other companies successfully integrate security earlier in the development cycle.

7. Ask for directions.

Conducting a BSIMM assessment gives you automatic access to the private BSIMM community. You can attend annual conferences and participate in an online group to ask questions and get direct, confidential feedback on your software security challenges from your peers.

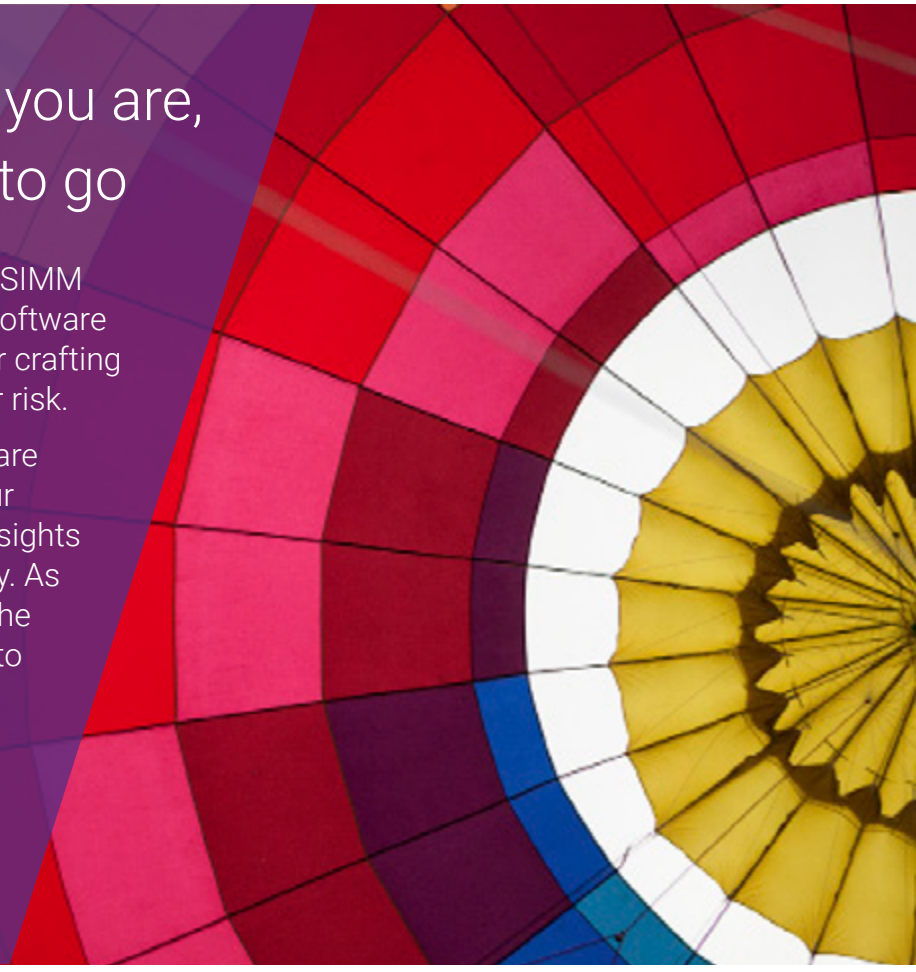
Get inspired: A multinational bank had not conducted a BSIMM assessment in some time. When security managers attended the annual BSIMM conference, they learned that several activities that they didn't include in their own software security initiative had been added to the methodology. They spoke to several security leaders at the event to learn how these new activities could help them reduce risk.

Once you know where you are, you can decide where to go

Benchmarking your organization with a BSIMM assessment is an essential step in your software security journey. It sets the foundation for crafting an effective strategy to reduce your cyber risk.

Not only will you find out how your software security initiative compares to that of your peers, but you will also gain actionable insights you can apply to your business right away. As your program evolves, you can return to the BSIMM framework as often as you need to make decisions and chart your progress.

GET STARTED



SYNOPSYS®

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

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