


10 Things You Ought to Know Before You Benchmark Your Software Security Program





Benchmarking your security initiative is essential

Evaluating the progress of your software security journey is essential, but it can be a considerable challenge. Tracking operational metrics doesn't tell you whether you are doing the right things. Analyst reports are often too general to provide tactical direction. And companies hold their security plans so close to the vest, it makes competitive research nearly impossible.

Benchmarking can help you get a new software security initiative off the ground or navigate an existing one. It is different from other measurement techniques because it focuses on excellence, includes detailed comparisons, and pools confidential information among numerous organizations.

Benchmarking your software security initiative can tell you if you are keeping pace with your peers, or if you should accelerate your efforts to rise above the competition. The results of a benchmarking assessment can help you identify new security strategies and prioritize scarce resources to be most effective.

10 things you ought to know

Consider these 10 tips to get the most out of your benchmarking assessment.

1. Select the right instruments.

When you choose a methodology to assess your program, make sure you select a transparent model that is commonly used by security experts and reflects the latest practices in the industry. The terminology will be more commonly understood, the assessment will be more comprehensive, and the results will gain more respect.

2. Evaluate real-world conditions.

An assessment that is based on current data from real-world companies will be more accurate than a theoretical checklist. Look beyond the high-level findings and ask: What companies are included in the benchmarks? Do I consider them examples of companies I want to follow?

3. Learn from experienced pilots.

If you operate in an industry that has not historically invested in security, you may have an outdated idea of what is necessary to mitigate risk. Look to industries that are considered leaders to get inspired with ideas you can adapt to your own software security initiative.

4. Verify your launch point.

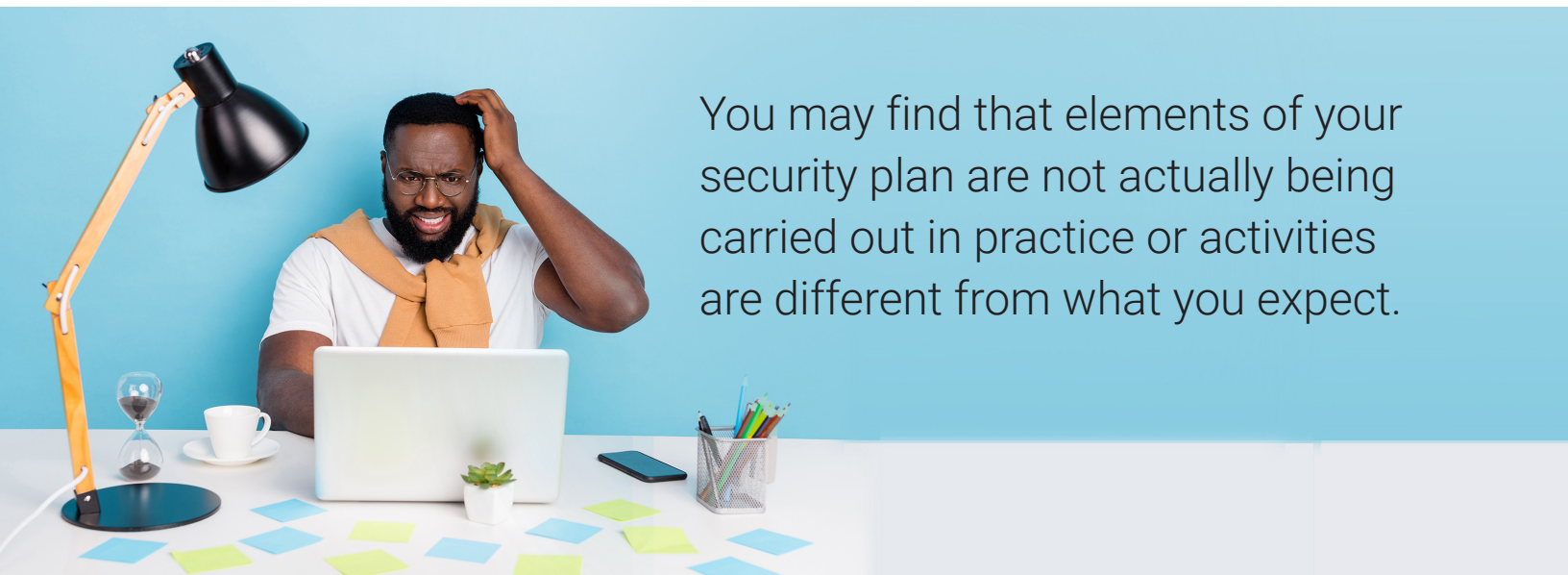
Quick surveys such as online assessments are a great way to launch your benchmarking strategy. They can give you an initial read on where you stand. Unfortunately, they may give you a false sense of security. To capture your current security posture in detail, a follow-up assessment should include interviews with multiple parties and documented activities to verify specifics. You may find that elements of your security plan are not actually being carried out in practice or activities are different from what you expect.

5. Beware of overinflation.

Internal-only assessments can unintentionally inflate results based on assumptions and take you off course. A third party that has no stake in the outcome can evaluate your security processes with an unbiased perspective.

6. Weigh everything in your basket.

You'll want an aggregate assessment of your security posture, but you should also look at the details. For example, an "average" result may hide the fact that a single business unit has particular strengths while another has certain weaknesses. Deconstruct your results or consider separate assessments.



You may find that elements of your security plan are not actually being carried out in practice or activities are different from what you expect.

7. Take a 360° view.

Consider your results in context. Not every element of the framework you choose may apply to your business. For example, if you don't rely on third parties to develop software, you don't need to develop vendor service-level agreements.

8. Reflect on your journey.

Don't spend all your time collecting and measuring data. Your results are simply numbers on a page until you devote time to analysis. Make sure you leave some room in your budget and your timeline to apply results and prepare your maneuvers.

9. Share your experience.

Anytime you invest in an external audit of your business operations, executives will want to know what the results mean. Have a plan to communicate your results with business context to increase your leadership's understanding of software security and build support for the resources you need to evolve your program.

10. Test the wind at different altitudes.

Most companies find it makes sense to do an in-depth assessment about every two years to track their progress. During that time, you'll be able to see improvements in more resource-intensive, time-consuming activities.

Where are you on your software security journey?

Benchmarking your security strategies against the activities of real-world organizations provides meaningful context to help you make decisions.

The Building Security In Maturity Model (BSIMM) is an assessment framework based on data gathered from 130 software security initiatives that are currently active. It categorizes 125 software security activities into three maturity levels based on their rate of observation and complexity.

A BSIMM assessment gives you insight into how other organizations value security activities and an unbiased perspective on the strengths and weaknesses of your own program.

Get an inside glimpse at the top software security initiatives.

Download BSIMM



The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.

690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:

U.S. Sales: 800.873.8193

International Sales: +1 415.321.5237

Email: sig-info@synopsys.com