SYNOPSYS®

Maturity Action Plan (MAP)

Navigate your way toward building security into your software

Overview

As security and development teams collaborate to improve their software security posture throughout the organization and across their application portfolio, organizations are looking to prioritize achievable risk mitigation goals. They want to determine not only how to improve what they're doing but also what else they should be doing to meet their objectives. Developing a plan is essential to prioritize funding, streamline resources, and reduce the risk of software vulnerabilities. The Synopsys Maturity Action Plan (MAP) provides software security leaders and practitioners with actionable guidance for evolving an existing software security program (SSP) or chartering a new one. A MAP starts with an evaluation your security program's people, processes, and technology using a seven-factor analysis or Building Security In Maturity Model (BSIMM) framework. Synopsys will then partner with your SSP leaders to establish a multiyear strategy that is tailored to maximize ROI and reduce risk within your organization.

Actionable guidance from experts

Often conducted in tandem with a BSIMM assessment, the SSP MAP provides a compass for security leaders to navigate the dense field of possible investments across products, projects, and people. Our process is simple, and our expertise is unparalleled.

Build consensus for SSP objectives

Your software security initiative must be tailored to your organization. That starts with understanding the risk profiles facing the business, rationalizing stakeholder pressures, and building consensus for a program charter.

Determine the current state of your software security activities

In this phase, our consultants measure the current state of your enterprise software security activities, including your SSP and your secure software development life cycle (SDLC), using the industry standard for SSP measurement (BSIMM). For organizations with no formal SSP, we recommend a penetration test or secure code review in place of a BSIMM assessment, with an emphasis on discovering defects as early as possible in the SDLC to avoid expensive late-stage remediation efforts.

Once your MAP is developed, we can help you socialize it to get the buy-in, resources, and support you need to implement it.