

GUIDE

Risk Management:

How Code Dx Can Help

Assessing risk requires multiple tools

Organizations should approach risk management by employing a variety of security testing tools that test code for security issues across all three layers of an application: the custom code developed by internal software engineers; third-party components, frequently used by engineering to accelerate development; and the network infrastructure where the application runs. Common tools for identifying risk include static analysis, dynamic analysis, and interactive analysis, as well as penetration testing for custom code, software composition analysis for open source components, and vulnerability assessment scanners for the deployment environment. To learn more about these types of tools, read our [previous white paper](#).

Multiple tools report vulnerabilities in disparate ways

These testing methodologies all provide valuable information about risk, but each does so in its own way. While static analysis identifies the file and line of code where a vulnerability exists, dynamic analysis and penetration tests report issues by providing the URL of the web application where the vulnerability was identified, along with an action/result. Software composition analysis reports when a third-party library or component includes a component for which vulnerabilities have been reported. In addition to reporting vulnerabilities differently, tools also describe and score vulnerabilities differently.


Complexity contributes to risk

Disparate results add complexity to triage and remediation efforts, and consequently increase the risk that issues will be misidentified, overlooked, or incorrectly prioritized. To address risk properly, security teams must take these individual reports and remove false positives, de (hplimie mg710.2u65 Tivi3cav)6.4 (5.7 (ir)8.8 (esm[These testing mer)-24. componnalualtyonentswher)9.5 (e t9t vulner)2yescrib7nent

Automated test execution

When a project is added to Code Dx, it performs a quick analysis to automatically identify the appropriate application

securityypee (ee a asqown in07 Tc 0 Tw0.0f-0.007 Tw 9 0 0tFigu97an0fe.804 .967v1.)8t 82.9 30ly



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.

690 E Middlefield Road
Mountain View, CA 94043 USA

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