SYNOPSYS®

GUIDE

Risk Management:

How Code Dx Can Help

Introduction

In a previous white paper on AppSec risk management, we detailed the precarious state of cyber security—specifically that most organizations are still combating the kind of cyber threats that were catastrophic a few decades ago, at the expense of adequate security in other layers. While the practices designed to mitigate threats such as viruses are still important, there are other more prevalent threats that cannot be addressed with firewalls and antivirus software. The software layer of cyber security is currently the layer most targeted by attackers, and it is therefore at the greatest risk of breach. It is crucial for organizations to ensure that they have properly secured the software they produce to mitigate that risk—because the consequences of a breach can be catastrophic. For more information on how to manage AppSec risk, read the white paper.

This white paper explores the ways AppSec platforms like Code Dx by Synopsys help organizations reduce their AppSec risk. Read more to learn how these platforms address the issues that organizations must solve to ensure their software is properly secured—without compromising their software development life cycle timelines. While some of the information in this white paper is specific to the Code Dx platform, readers are encouraged to seek out the right product to help them perform proper AppSec testing. The information provided here is intended to inform readers about currently available solutions so they can make the choice that is right for them.

The risk posed to organizations by vulnerable software is a board-level issue. Breaches across government agencies, financial services companies, technology firms, retailers, and others have resulted in exposed personal information, lost intellectual property, reputational damage, and loss of shareholder value.

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, determine which issues are duplicated by multiple testing methodologies, and normalize the vulnerability scores applied by the tools. Because of the time, effort, and expertise required to do all this, many organizations simply export all vulnerabilities to their bug-tracking systems.

A better way to manage risk

Code Dx is an AppSec solution that addresses the shortcomings of disparate tool reports by aggregating, normalizing, correlating, and prioritizing vulnerabilities across all three layers of an application. These capabilities allow security and development teams to focus their remediation efforts based on risk, which enables efficient application vulnerability management and less developer friction.

What Code Dx offers

Code Dx provides a variety of functions and features.

Automated test execution

When a project is added to Code Dx, it performs a quick analysis to automatically identify the appropriate application security tests needed, as shown in Figure 1. This includes tools bundled with Code Dx as well as separately licensed commercial tools. Users can remove or add other tests, change the rulesets used by the tools, or simply begin the analysis.

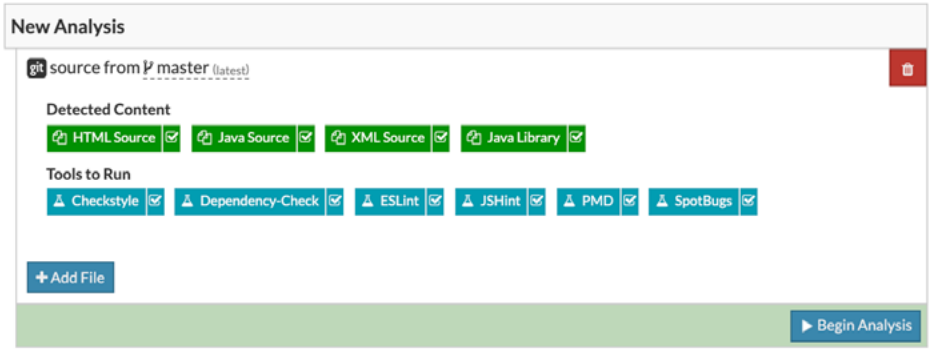

Figure 1: Code Dx automatically identifies the right tools to run

Normalized results

Results from all tools are aggregated and normalized to provide consistent scoring and descriptions for all issues, as shown in Figure 2.

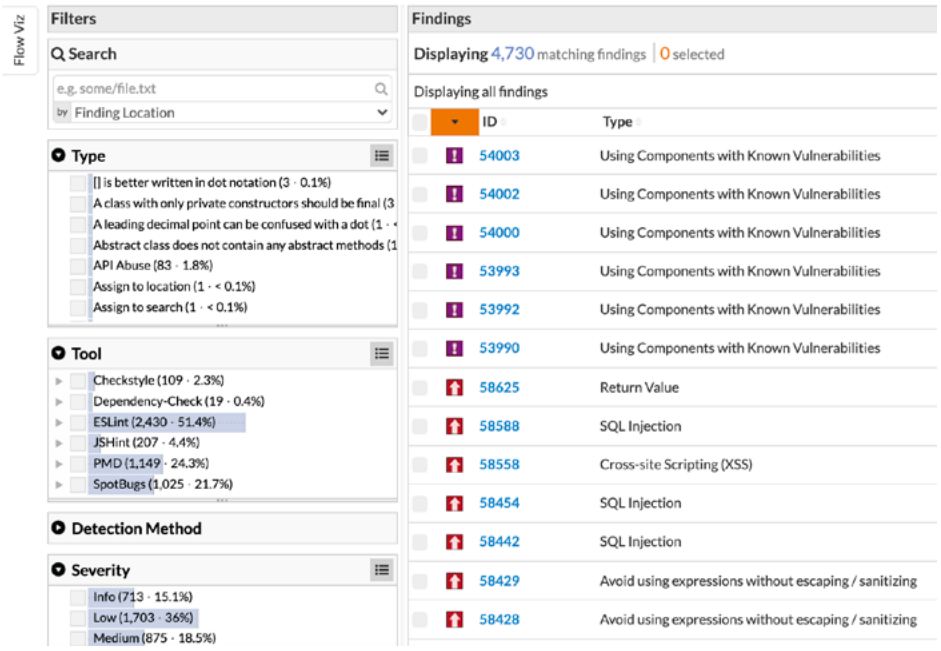

Figure 2: Terminology from different tools is normalized

Correlated and deduplicated issues

Using multiple tools or running multiple scans can result in a single vulnerability being found by multiple tools and reported as multiple issues. Code Dx examines the results from similar tools to eliminate duplicate vulnerabilities found by more than one tool. Code Dx correlation and deduplication eliminated over 1,000 issues, reducing the triage workload by 20%, as shown in Figure 4.

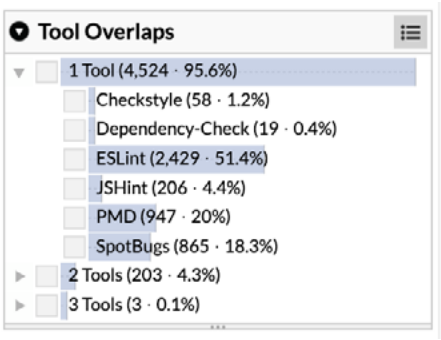

Figure 3: Vulnerability overlaps across tools

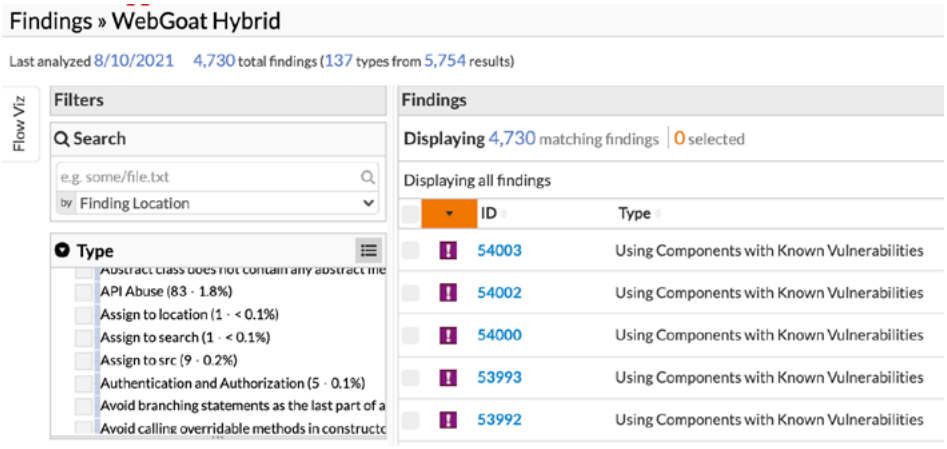

Figure 4: Duplicate vulnerabilities automatically removed

Faster triage and prioritization

Most scanning solutions allow users to sort by issue severity. Code Dx's Hybrid Correlation engine correlates results from both dynamic analysis and static analysis tools. Using DAST tools to examine SAST results, hybrid analysis identifies which vulnerabilities in the code can be exploited from the outside. This provides teams with a short list of vulnerabilities that are exploitable—the ones you should fix first.

Regulatory risk and compliance mapping

Many organizations are subject to regulatory standards like PCI DSS, HIPAA, DISA-STIG, and others. Many of these require organizations to test for specific types of vulnerabilities such as those identified in the OWASP Top 10 or CWE Top 25. Others require that organizations comply with coding standards like CERT C, CLASP, and others. Code Dx can filter results by standards and type of vulnerability to quickly identify issues that violate policies, as shown in Figure 5. This can save organizations money (potentially millions) as noncompliance can result in fines.

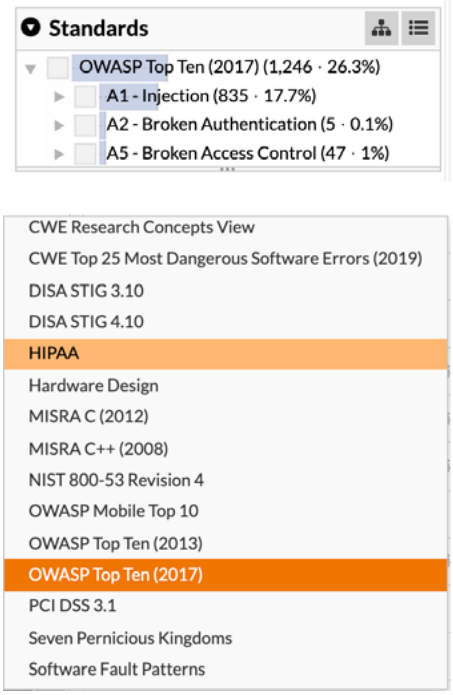

Figure 5: Vulnerabilities mapped against compliance standards

Consistent and continuous risk reports

Code Dx provides real-time risk reports, as shown in Figure 6, for individual applications, business units, and across application portfolios.

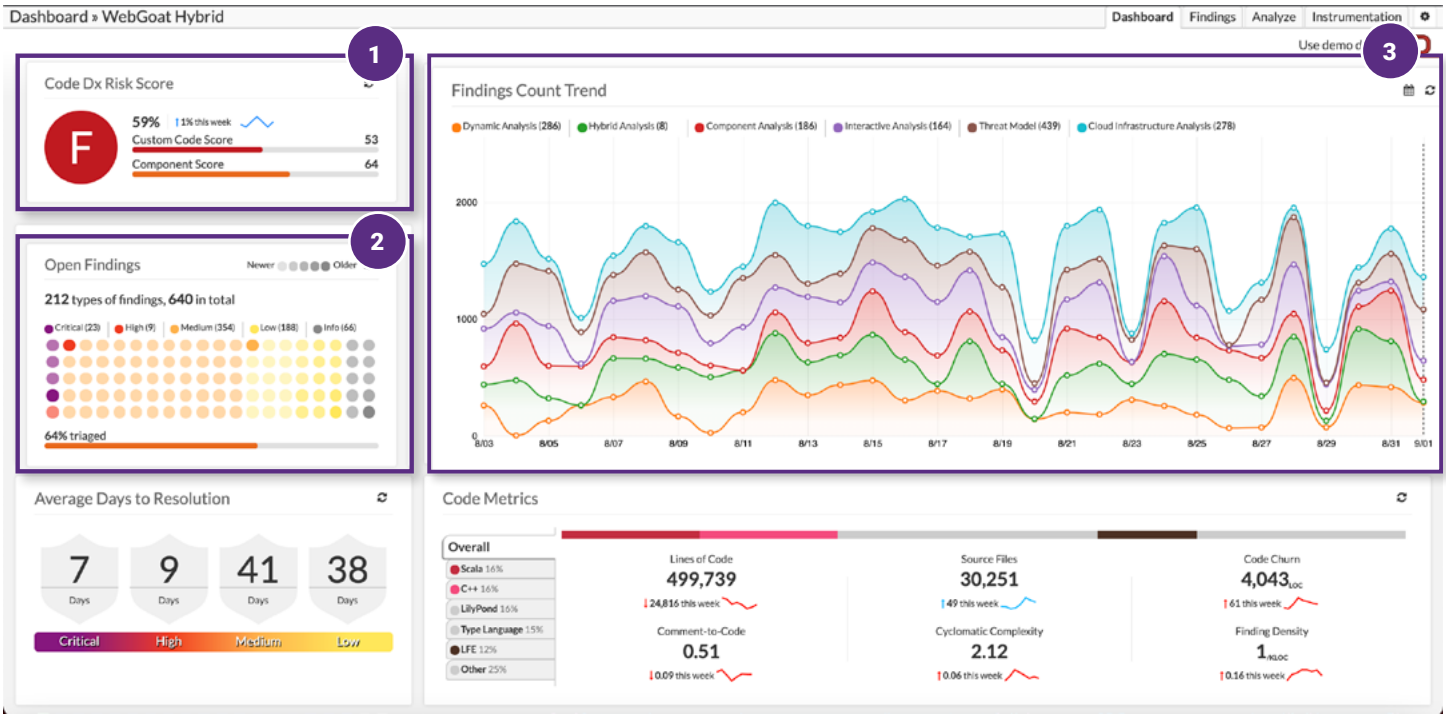

Figure 6: Real-time reports on your AppSec risk

Risk scores

The Code Dx risk score is a letter grade that represents the overall quality of the project, as shown in Box 1. The letter grade is based on a percentage score, which is the average of the scores for each layer of the application—custom code, third-party components, and the application's network infrastructure.

Open findings

The Open Finding chart, shown in Box 2, provides a severity and age breakdown of the untriaged findings in a project, with each circle representing 1% of the issues. Lighter circles indicate findings that are relatively new, while darker circles represent finding that are relatively old.

Issue-tracking by testing methodology over time

Code Dx tracks issues by tool type over time for each project, as shown in Box 3. This allows security to quickly evaluate and communicate progress. The average number of days to resolve issues by issue severity helps managers spot out-of-compliance vulnerabilities and issues that require escalation.

Learn more

To find out more about Code Dx by Synopsys, download our datasheet or visit our website and request a demo today.

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.
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