These challenges result in low-efficiency AppSec, which means you risk releasing poor-quality code to production. Faulty code in production leaves your organization open to attacks, including data mining and ransomware. Breaches in your software are not only expensive but lead to reputational damage—while customers understand that software risk is ubiquitous, they want to know that they can trust your organization. Customers want to know that they can trust vendors to be proactive about preventing exploits and to adhere to industry standards, including quality checks and security requirements for software going into production.

The siloed nature of security testing, and the abundance of data that is produced, means that most organizations struggle to determine their most impactful security activities. Because of this, they have difficulty enforcing standards for compliance and risk assessment across their applications, which makes it difficult to standardize secure software development practices.

These structural issues have historically contributed to the security gap between development and security teams that hinders collaboration of data, tools, and process. When you do not know the top vulnerabilities in your organization and lack a central system of record, it is nearly impossible to gain a global perspective of your business risk when it comes to software.

Elevate your AppSec program with Code Dx

The solution to this problem is to adopt an application vulnerability correlation (AVC) solution like Code Dx® to elevate your AppSec program in a scalable, efficient fashion. AVC tools work by aggregating results, normalizing them, and correlating the security findings returned by multiple tools. Code Dx aggregates application security testing (AST) results across your organization, including diverse testing types such as static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and software composition analysis (SCA)—even container security scan results and manual processes such as threat modeling and code reviews—into a single repository. It then normalizes these results and presents them in a consistent, standardized format that can be recorded and viewed in this repository. Code Dx also correlates instances in which the same issue is found by multiple tools and presents them as a single finding. This reduces the number of duplicate tickets, eliminating inefficiencies and unnecessary friction for developers. In addition, Code Dx can deduplicate data to highlight unique issues, providing a clearer understanding of risks and the associated burden of remediating them.

Scaling existing processes in line with a next-gen AppSec approach starts with implementing a robust AVC solution. Here are some questions to ask when evaluating your AppSec needs and determining how an AVC can help.

AVC tools work by aggregating results, normalizing them, and correlating the security findings returned by multiple tools.