ShiftLeft

ShiftLeft CORE
A Code Security Platform

ShiftLeft CORE is a code security platform designed to help organizations deliver secure code without compromising software delivery timelines. It establishes collaboration between AppSec and Developers allowing each to focus on their key goals - for AppSec to identify and reduce risk associated with their applications and for developers to fix vulnerabilities while minimizing impact to their productivity.

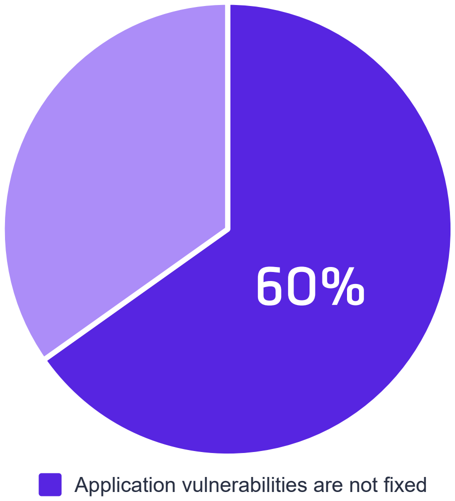
Fast, Accurate and Very Easy to Use

ShiftLeft CORE is designed to fit seamlessly into the developer's pull request-based workflow that decreases MTTR (Mean-time-to-repair). With a single insertion, ShiftLeft CORE conducts multiple analyses. This has enabled ShiftLeft customers to go from analyzing once in months to analyzing multiple times per week.

ShiftLeft CORE is loved by developers because its analysis is completed within the DevOps time window, while the pull request is still fresh in the developer's mind allowing him to fix the vulnerability much more quickly. ShiftLeft CORE analyzes 1M lines-of-code (LOC) in less than 10 minutes; 100K LOC in less than 1min.

ShiftLeft CORE is the most accurate code analysis solution (OWASP Benchmark score of 75%) because of the Code Property Graph which is the most comprehensive representation of code including dependencies and APIs and includes various compiler representations that are critical to performing accurate code analysis.

Industry benchmark data shows that 60% of application vulnerabilities are not fixed*



*https://www.darkreading.com/most-enterprises-do-not-fix-60-percent-of-security-vulnerabilities-they-discover/d/d-id/1321064

Multi-Featured Platform: Static analysis, Intelligent SCA, Secrets, Insights, Developer Education

Static Code Analysis

Shiftleft supports multiple languages: Java, C-Sharp, Python, JavaScript/TypeScript, Scala, Python, Go, Terraform and many other languages that are upcoming. It covers OWASP Top 10, CWE Top 25 along with a range of language specific vulnerability categories.

Intelligent Software Composition Analysis

ShiftLeft Intelligent SCA uses the concept of "Attacker Reachability" to prioritize only a subset of OSS vulnerabilities for mitigation. It can trace code paths that can potentially lead attackers from insecure inputs directly to open source vulnerabilities, using the power of Code Property Graph. Based on a ShiftLeft study, Customers were able to reduce the number of open source vulnerability tickets by more than 90%.

Secret Detection

ShiftLeft detects Secrets, or hard-coded values (e.g., client Secrets, username/password combinations) and sensitive information (e.g., phone numbers and addresses). Unlike "grepping" for these patterns that lead to false positives, the use of Code Property Graph identifies when secrets are being leaked without proper transformation or obfuscation.

Security Insights

Security Insights are potential security issues in the code that may not be vulnerabilities today but are bad practices based on industry best-practice. These are conditions that can lead to OWASP Top 10 or CWE Top 25 vulnerabilities.

ShiftLeft Educate

ShiftLeft Educate provides developers with in-context education to help them mitigate security vulnerabilities. E.g. for an XSS vulnerability reported in a Java application, targeted training is provided on how to fix XSS vulnerabilities in Java. What's more, the developer can learn, fix the vulnerability, analyse it again, and get immediate feedback on whether the fix worked!