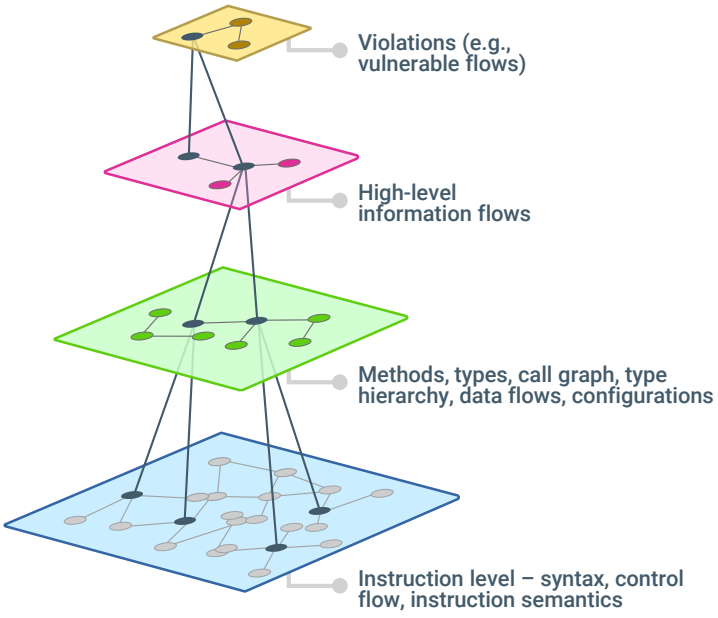
A CONTINUOUS PLATFORM FOR CODE ANALYSIS, RUNTIME PROTECTION, & VULNERABILITY RESEARCH

ShiftLeft is purpose-built security for the modern software development life cycle (SDLC). Whether agile SDLC, microservice architecture, cloud infrastructure, virtual machines, containers, serverless, or open source libraries and commercial SDKs, developing applications has undergone profound changes. ShiftLeft's product suite (Inspect, Protect, and Ocular) leverages the Code Property Graph (CPG) to enable organizations to embrace modern efficiencies without sacrificing security.

THE CODE PROPERTY GRAPH

ShiftLeft's core technology is the CPG, which is a fundamentally new and more precise way to rapidly analyze high volumes of source code for vulnerabilities. The CPG leverages semantic graphing to create a single multi-layered graph that summarizes code on various levels of abstraction, including abstract syntax trees, control flow graphs, call graphs, program dependency graphs, directory structures, etc. This enables ShiftLeft to understand the context of the application, allowing it to identify deviations accurately as vulnerabilities. This is especially critical for identifying complex vulnerabilities that are dependent on a series of conditions across various components that make up the application. Only by understanding how the components interact with each other can these complex vulnerabilities be identified.



Invented by Dr. Fabian Yamaguchi, the CPG extends the original open source project, Joern, to provide a feature-rich and enterprise-grade experience across multiple programming languages. As a measure of the effectiveness of the approach, Joern was used to identify 18 vulnerabilities in the Linux kernel that were accepted and fixed. If the CPG can find 18 real vulnerabilities in one of the most commonly used and hardened code bases, imagine what it can do for your source code!

INSPECT

ShiftLeft Inspect is a modern static application security testing (SAST) solution. It is purpose-built for the modern SDLC, in which speed and accuracy are paramount. Code analysis with Inspect takes just minutes, and it can be inserted into DevOps pipelines via code repository, continuous integration, and/or continuous delivery tools. Vulnerabilities can be confirmed and prioritized in UAT or QA environments with test traffic to weed out false positives.

Furthermore, Inspect evaluates your entire application, including custom code, frameworks, open source libraries, and commercial SDKs. Inspect can even identify multi-stage deserialization vulnerabilities that stem from how individual components interact with each other.

Key Benefits:

- **#1 SAST Benchmark Score**: Inspect scored 75% on the OWASP Benchmark, which is the highest score ever recorded and nearly three times the commercial average.
- **Speed**: Analyze 500,000 lines of code in less than 10 minutes. Release as fast as you can, securely!
- **Vulnerability Prioritization**: Don't waste precious time sifting through mountains of irrelevant alerts!
- **Built for DevOps**: Automate code analysis upon pull request, build, or release.
- **Single Pane of Glass for all Vulnerabilities**: Find and fix vulnerabilities in your code, open source libraries, and commercial SDKs.

PROTECT

ShiftLeft Protect, our flagship product, combines source code analysis in development with runtime protection in production. Protect creates a fully automated loop of continuous security from development to production and from production back to development.

In development, during the build process, Protect leverages ShiftLeft's proprietary CPG to extract the application's Security DNA. From the Security DNA, a custom Security Profile is created to safeguard the application in runtime via blocking and/or alerting during exploit attempts. Production data is used to confirm vulnerabilities definitively and prioritize fixes, as production cannot be replicated in QA or UAT environments.

Key Benefits:

- **Manual Policies RIP**: Safeguard the application in runtime, no manual policies required.
- **Comprehensive**: Identify and safeguard against vulnerabilities in your custom code, open source libraries, and commercial SDKs.
- **Compliance**: Map data flows, and identify and prevent data leakages.
- **Speed**: Secure every version of every release without slowing down.
- **Operational Simplicity**: Don't be overwhelmed by the mountain of false positives from your WAF.

OCULAR

ShiftLeft Ocular enables code auditors to leverage the power of the CPG with custom queries. Traditional code analysis tools run a generic set of tests against code. However, this leads to false positives and false negatives. With custom queries, the code auditor can use their knowledge of sources, transforms, and sinks to minimize false positives, such as alerting on unsanitized routes. Additionally, custom queries can identify vulnerabilities in indirect data flows that generic tests miss. Lastly, queries can be saved as policies and automatically inserted to evaluate every release in DevOps pipeline.

Key Benefits:

- **Accuracy:** Write custom queries that understand your unique environment.
- **Cross-language Policies:** Save queries as policy and run them against all your applications, regardless of programming language.
- **Automate Policy Checks**: Automatically run policies upon pull request, build, or release.