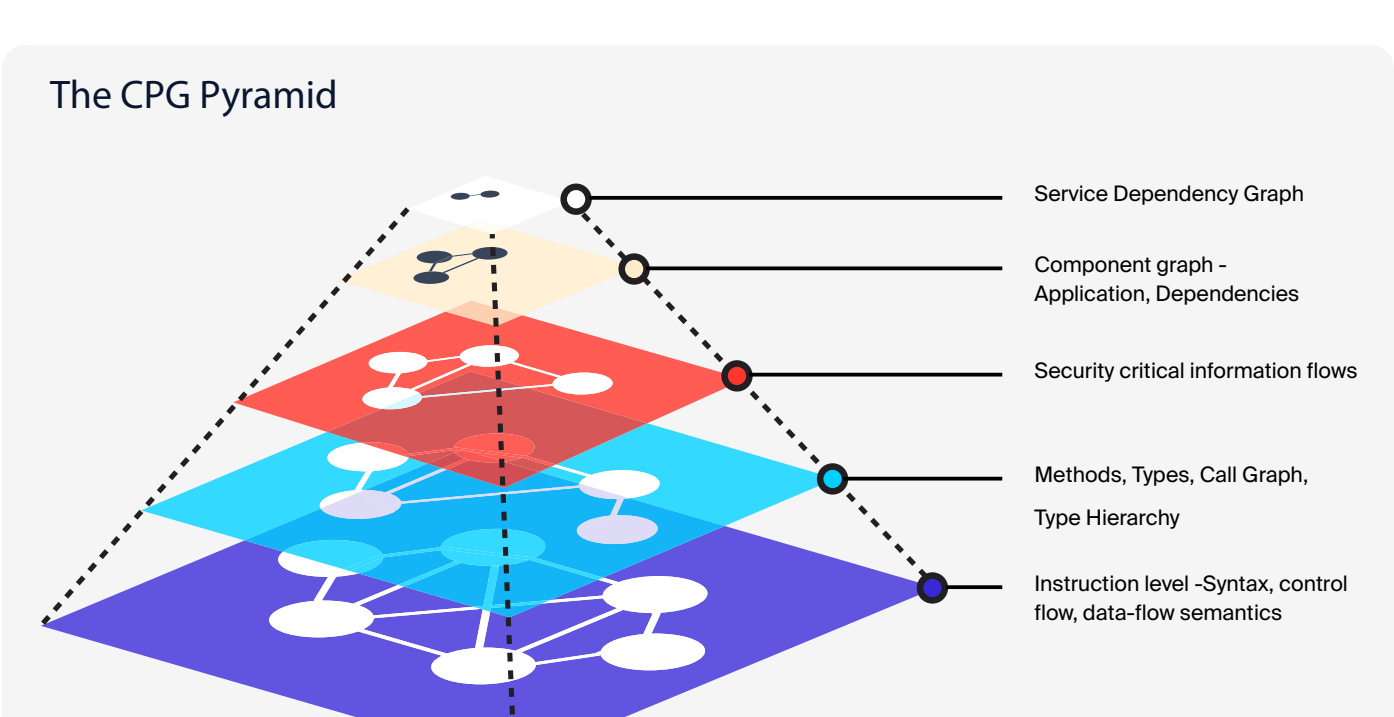
ShiftLeft

Secure Code Scanning with the CPG

Safely scan your repo without code ever leaving your server

Code Property Graph

What is the Code Property Graph?



The Code Property Graph (CPG) powers the ShiftLeft CORE SaaS platform. It creates an intermediate representation of your code and sends that, not your source code, to ShiftLeft servers for analysis.

The CPG constitutes the code represented in the form of a layered graph that can be queried to obtain security relevant information about the code. The complete intermediate representation is packaged into a binary that is stored in encrypted cloud storage and cannot be accessed or decrypted. The workhorse of the CPG is a state-of-the-art data flow tracker that operates on the intermediate representation: it is interprocedural, flow-sensitive, context-sensitive, and field-sensitive.

For more information on the CPG, see the **Code Property Graph whitepaper.**

How and Where Can the CPG be Created and What are the Security Controls Established in the SaaS Infrastructure?

The CPG can be created in the customer's CI sandbox using ShiftLeft's **sl** command

```
sl analyze --app <name> --java [<path-to-JAR/WAR>]
```

This command can be executed as a CI action in the CI sandbox (Jenkins/Travis/Circle/GitHub Action/Azure pipelines, etc) leading to the CPG being created (and obfuscated) on the sandbox. Thereafter the graph is compressed, signed and securely transmitted to the tenant account in our SaaS cloud.

The on-disk representation of the CPG is encrypted using server-side encryption with customer master keys (CMKs) stored in a Key Management Service.

The encrypted format on SaaS storage units are only accessible by our internal APIs. Even upon access, they can only be parsed by ShiftLeft's proprietary tools and hence, on-disk the graphs are extremely secure. All access points are restricted based on Admin RBAC controls governed by SOC-2 type 2 standards.

Can the CPG be Reverse Engineered or Reconstituted to the Target Source Representation?

No, it cannot be reversed for the following reasons

1. The representation (based on CPG specification) contains only certain properties (metadata representing syntax trees, variable declarations, blocks, scope, type information, etc.) and NOT the full code representation

2. The representation (as CPG) is in a binary/obfuscated form that cannot be queried upon or loaded without ShiftLeft's proprietary toolchain (for analysis)

3. All CPGs stored in ShifLeft's SaaS infrastructure are governed and restricted by automated controls defined by SOC-2