GitHub 2020

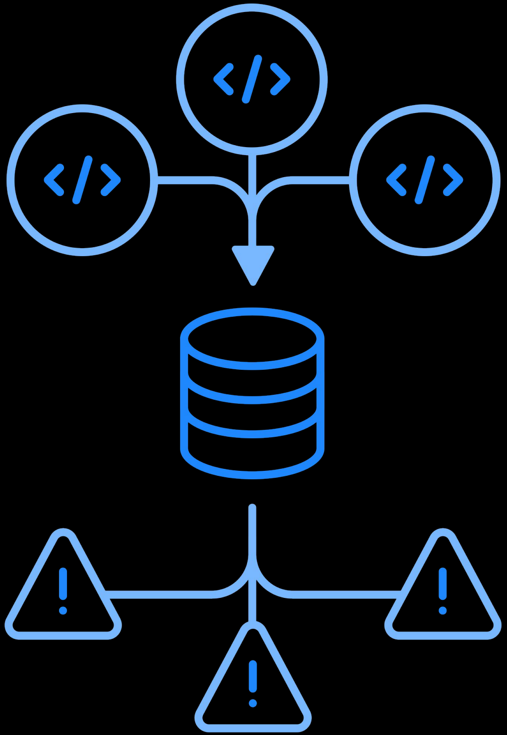
Introduction to CodeQL

CodeQL

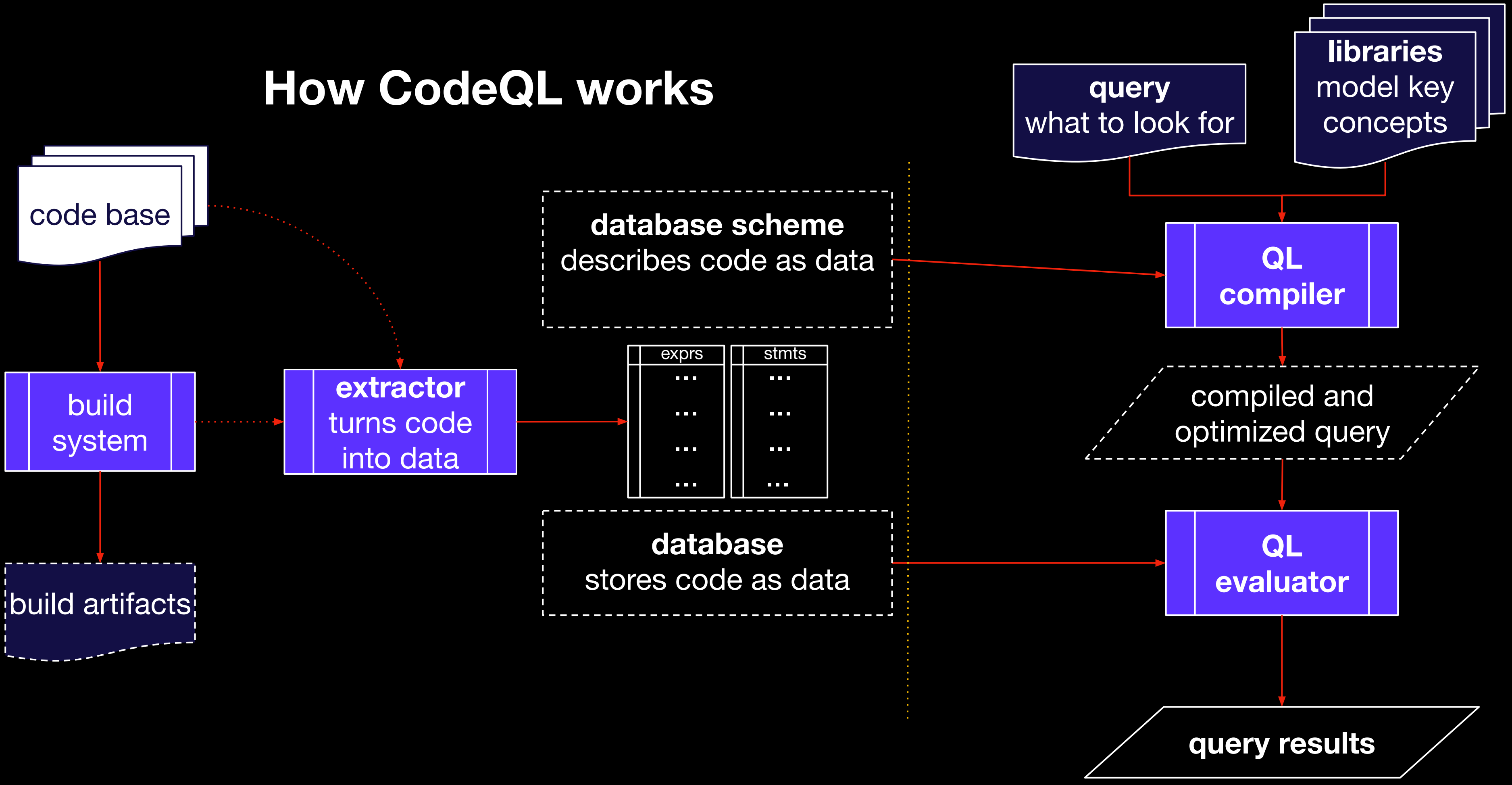
Analyze code as data using expressive queries to say what you want to find, not how to find it

Quickly refine analyses to increase precision within your codebase

Share security knowledge within your teams using codified, readable and executable queries



How CodeQL works



The QL query language

- a **logic language** based on first-order logic
- a **declarative language** without side effects
- an **object-oriented language**
- a **query language** working on a read-only snapshot database

+

- rich **standard libraries** for program analysis
- **tools to create databases** from source code
- CLI and IDE extensions